NCIA/ACQ/2026/06694

NCIA Request for Information (RFI)

PROVISION OF COMMERCIAL IP TRANSPORT
42603961

NATO Communications and Information Agency

NCIA/ACQ/2026/06694
Wednesday, 18 March 2026

NCIA Request for Information (RFI)

1. The NATO Communications and Information Agency (NCIA) is conducting market research to identify qualified vendors and gather input on potential solutions to support the upcoming provision of a commercial IP Transport Service between NATO and Partner Nations. To that end, we are issuing this Request for Information (RFI) 42603961 to solicit feedback from capable and interested industry partners.

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

3. We hereby invite interested industry to provide a price estimate along with a review and comments on our draft requirements (Annexes A and B), including recommendations for improving performance outcomes, competition, efficiency and identifying any risks or concerns that should be considered during planning.

4. Submission instructions and additional details can be found in the Annexes to the RFI Instructions.

5. 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).

6. Should you have any questions or need clarifications, please contact Stefania Iacob at **42603961_AirC2RFI@ncia.nato.int.**

7. 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:

Elena Iftimie-Paraschiv

Digitally signed by Elena Iftimie-Paraschiv
Date: 2026.03.18 13:36:52 +01'00'

Elena Iftimie-Paraschiv,
Senior Contracting Assistant
(On behalf of Stefania Iacob)

Enclosures:
1. Distribution List
2. Request for Information Instructions, with Annexes A, B, and C
3. Security Requirements for NATO R*stricted (NR) Information

NCIA/ACQ/2026/06694

Enclosure 1: Distribution List

NATO Delegation (Attn: Infrastructure Adviser)

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

All NATEXs

Enclosure 2: Request for Information Instructions

A. Submission Instructions

1. Interested parties are invited to respond in accordance with the instructions below:

   a. Submit responses via the email address in section D below **no later than 12:00 hours Central European Time (CET) on 16 May 2026**.

   b. Responses for Annex A and comments on Annex B in PDF or Word format excluding:
      - Cover page;
      - Company brochures or product literature.

   c. Use the following subject line for submission: "Response to RFI [RFI Number] - [Company Name]".

B. Disclaimer

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. The 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. The 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.

2. NCIA reserves the right, at any time, to cancel this 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.

C. Use of Information Provided through Responses

1. Confidentiality of Responses

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.

D. NCIA RFI Point of Contact (POC)

Stefania Iacob at: 42603961_AirC2RFI@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

   c. Feedback and Recommendations
      i. Responses to the following RFI Questions:
         1) What types of VPN/IP transport technologies do you recommend (e.g., IPsec, MPLS…)?
         2) How do you ensure secure, encrypted communication across national boundaries?
         3) What redundancy and/or failover mechanisms are available in your solution?
         4) How do you guarantee QoS for traffic?
         5) What monitoring and reporting tools are provided to NCIA/Partner Nations?
         6) How do you measure and report SLA compliance?
         7) How do you handle service degradation during crises or high-traffic events?
         8) What cybersecurity standards does your solution comply with?
         9) What encryption protocols and key management practices are supported?
         10) How do you manage access control and protect against insider threats?
         11) What certifications (ISO, SOC, etc.) does your company hold?
         12) What pricing models do you offer (fixed, usage-based, hybrid)?
         13) What optional services (e.g., managed security, advanced monitoring) are available?
         14) What assumptions underpin your Rough Order of Magnitude (ROM) cost estimate?
         15) What transition assistance do you provide upon contract termination or migration?

16) What risks or barriers do you foresee in implementing commercial IP transport between NATO and the Partner Nations in Annex C?

17) What risks do you identify on the draft requirements in this RFI and what mitigation strategies do you recommend?

18) What innovative approaches or alternative architectures could improve resilience, cost-effectiveness, or security in relation to the diagram included in this RFI.

19) Can you share lessons learned from similar government/defence projects?

20) If a Partner Nation would like to use its own authorized Telecom provider (please see the diagram included below), would it be possible?

21) What are the Sub-Contractors you would expect to work with for this prospective project?

ii. Comments on the draft available in Annex B.

iii. Rough Order of Magnitude (ROM), including any assumptions upon which they are based.

Annex B – Draft Requirements

1. Background

The NCIA requires enhanced IP transport capabilities to facilitate the exchange of NATO Unclassified (NU) data, including Air Situation Data Exchange (ASDE). NCIA is exploring commercial IP transport options to improve interoperability, resilience, and cost efficiency while maintaining compliance with NATO security standards.

2. Scope

At this stage, NCIA has not yet finalized the technical design or detailed requirements for commercial IP transport between NATO and Partner Nations.

Input from industry is requested to:

a. Provide insights and recommendations to help fine-tune the design of the proposed solution.
b. Suggest best practices, standards, and architectures that could be adopted.
c. Identify potential risks, constraints, and dependencies NCIA should consider.
d. Highlight innovative approaches or emerging technologies that may improve resilience, scalability or cost-effectiveness.

3. General requirements

a. Site-to-Site VPN connectivity between NATO and Partner Nations (in Annex C):
- Type of VPN offered (e.g., IPsec, MPLS, SSL etc.).
- Detail encryption standards and security features.
- Provide hardware, installation support, and maintenance post-warranty.
- Describe monitoring, incident response and support services.
- Define SLA guarantees including uptime, latency.

b. VoIP services suitable for business communication:
- Call quality and reliability.
- Define SLA and support options.

c. Bandwidth:
- Guarantee minimum 10 Mbps symmetric bandwidth as baseline.
- Offer scalability options - ability to scale up to higher capacities (e.g., 50 Mbps, 100 Mbps) upon demand.

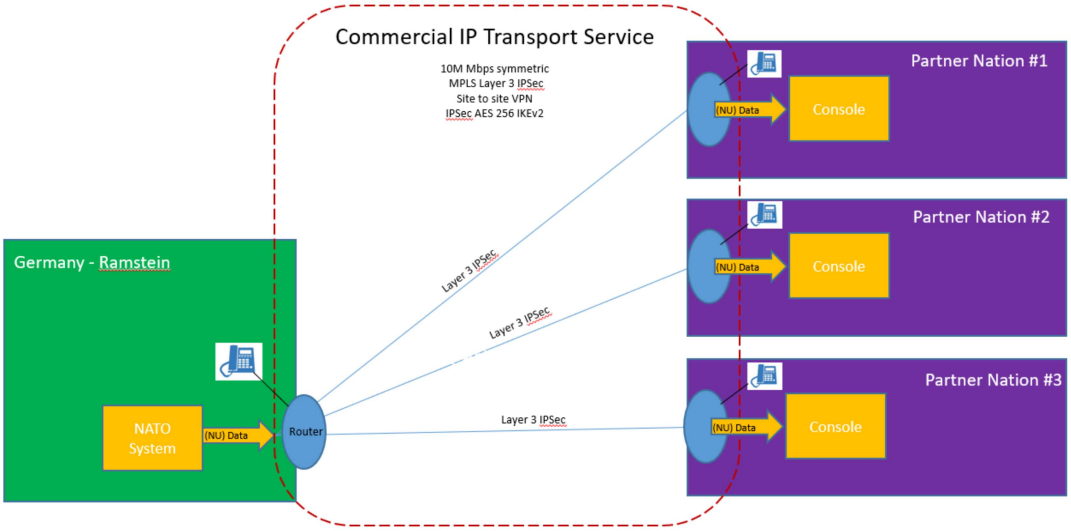
d. Pricing:
- Provide one-time setup costs.
- Detail monthly recurring charges.
- List optional services and associated costs.

e. Transition assistance:
- Upon termination or expiration, the Vendor shall provide reasonable

cooperation and technical support to ensure seamless migration of services to another provider.

- Documentation, configuration data, and technical support must be made available to facilitate transition.

High level diagram



4. Performance Requirements

a. Availability & Uptime:

- Minimum 99.9% service availability guaranteed under SLA.
- Redundant paths and failover mechanisms to ensure continuity of service.

b. Latency & Jitter:

- End to end latency not exceeding 150 ms between NATO and Partner Nation endpoints.
- Jitter maintained below 30 ms to support real time applications VoIP.

c. Quality of Service (QoS):

- Prioritization of traffic, data, VoIP.
- Mechanisms to prevent congestion and packet loss.

d. Security and Integrity:

- End-to-end encryption (IPsec or equivalent).
- Continuous monitoring for intrusion detection and anomaly reporting.

e. Resilience and Recovery:

- Automatic rerouting in case of link failure.

- Recovery time objective (RTO) of less than 4 hours for major outage.

f. Support and Monitoring:
- 24/7 monitoring and incident response.
- Clear escalation procedures and reporting mechanisms.

5. Further planned deliverables for this prospective project

The table below is not final and non-exhaustive.

Further Deliverables	Description
Technical Documentation	Network design proposals, architecture diagrams and configuration details.
Service Implementation Report	Details of installation, commissioning and integration of VPN/VoIP/IP transport services
Performance Reports	SLA compliance (uptime, latency, jitter, bandwidth usage), incident logs, QoS metrics
Monitoring & Incident Logs	Real-time monitoring data, incident reports, escalation records
Training & Knowledge Transfer Materials	User guides, operational manuals, training sessions for NATO/Partner Nation staff
Transition Assistance Plan	Documentation and technical support for migration to another provider

6. Period of Performance

Sites are not expected to be activated at the same time. Activation will occur sequentially according to the agreed implementation schedule.

7. Place of Performance

Place of performance is available in **Annex C – Place of performance (NR).**

Annex C – Place of performance (NR)

Interested firms can request the contents of this Annex C by writing an email to *42603961_AirC2RFI@ncia.nato.int* and completing the required security documentation which will be provided by the NCIA RFI POC.

More details related to the security requirements and obligations can be found below in Enclosure 3: Security Requirements for NATO R*stricted (NR) Information.

Enclosure 3: Security Requirements for NATO R*stricted (NR) Information

1. These requirements are to be followed in addition to all other requirements in this RFI.
2. NATO R*stricted (NR) level is the highest access to NATO classified information expected to be given for this RFI. For this reason, the Vendor shall have the appropriate Facility Security Clearance (FSC), for NR Level, if necessary, by the respective National Security Authority (NSA) or Designated Security Authority/Agency (DSA), under National laws and regulations.
3. Vendors handling and/or storing NR information shall appoint an individual of suitable seniority who shall act as the Security Officer (SO) of the facility with responsibility for ensuring the protection of NR information in compliance with the provision of the security requirements and any other additional requirements advised by NCIA.
4. The Vendor shall be responsible for the safeguarding of information that is indicated as “NATO classified" (“NATO classified information") such as NU, NR, NC, NS and CTS, under the "need to know" principle, as well as NATO classified and "In Confidence" documentation and/or material entrusted to them or generated by them in connection with this RFI.
5. For Vendor access to NATO R*stricted (NR) information the Vendor shall also require a Certificate of Security of Obligation (CSO). The NCIA will provide this form to the Vendor, upon request. Upon completion of the form, the Vendor shall submit it to the NCIA’s Security Office through the NCIA’s RFI POC for approval, at least 21 calendar days before the RFI closing date or as soon as the information is available.
6. For:
    i. Vendor personnel from Denmark, Luxemburg, Republic of Türkiye requiring access to NATO R*stricted Information; or
    ii. Vendor access to NATO Unclassified (NU) and NR information with physical unescorted access to sites, if any may be required for this RFI; or
    iii. Vendor access to NATO Classified (NC) and above information or physical unescorted access to sites, if any may be required for this RFI;

    the NCIA may require a Request for Visit (RFV).

    iv. The RFV form shall be submitted to the Agency’s Security Office at least 21 calendar days before the RFI closing date or as soon as the information is available. The NCIA will provide this form to the Vendor upon request. The Vendor shall submit the RFV(s) through their National Security Authority. More details can be found in the NCIA Guidance for RFVs and CSOs, and can be requested from the RFI POC.

7. Vendor's personnel acting as Privileged Users shall also be required to comply with the regulations described under the Supplier Code of Conduct and directives for NATO CIS Privileged Users.
8. A Personnel Security Clearance (PSC) is not required for access to information classified NR. Individuals who require access to NR information shall be briefed on security procedures and their responsibilities by the nominated SO, have a need-to-know and acknowledge in writing that they fully understand their security responsibilities and the consequences if information passes into unauthorized hands either by intent or through negligence. A record of the acknowledgement of responsibilities by Vendor's employees shall be retained by the facility SO.
9. Physical Security:
    i. NR information shall be stored in a locked container that deters unauthorised access; such as a locked desk or cabinet, or in a room or area to which access is controlled (hereinafter referred to as Administrative Zone).
    ii. NR information shall be handled in Administrative Zones or held under personal custody.
    iii. Access to NR information shall be granted only to personnel involved in this RFI who fulfil the conditions according to Paragraph 9 above, second sentence.
    iv. Documents, extracts, and translations of information classified NR may be reproduced by individuals authorized for access to the information and on equipment with controlled access.
    v. NR information shall be physically destroyed in such a manner that ensures it cannot be reconstructed in full or in part.
    vi. Destruction of reproduction equipment utilizing electronic storage media shall be in accordance with the applicable requirements in this Enclosure.
    vii. Information classified NR shall, as a minimum, be transmitted in a single opaque envelope or wrapping. The markings on the package shall not reveal that it contains information classified NR.
    viii. NR information carried within the perimeter of the site or establishment shall be covered in order to prevent observation of its contents.
    ix. The carriage of NR material shall as a minimum be in a single opaque envelope or packing (no marking shall be visible on the outer envelope) and may be:
        a) moved by postal or commercial services;
        b) carried by Vendor's personnel; or

c) transported as freight by commercial services.

x. Any Incident, which has or may lead to NR information being lost or compromised shall immediately be reported by the SO to the NCIA RFI POC.

10. Basic Safeguarding of Vendor Communication and Information Systems (CIS):

i. Definitions, as used in this section:

"*NATO Information*" means all information, classified and unclassified, circulated within NATO, whether such information originates in NATO Civil or Military bodies or is received from member nations or from non-NATO sources to include but not limited to:

NATO Information that is provided by or generated for the NCIA under a contract or RFI to develop or deliver a product or service to NATO, but not including information provided by the NCIA to the public (such as on public websites) or simple transactional information, such as necessary to process payments. Examples of NATO Information are:

NATO technical information that is subject to controls on its access, use, reproduction, modification, performance, display, release, disclosure, or dissemination that is technical data or computer software in nature; such as, research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, executable code and source code, design details, or formulae and related material that would enable the software to be reproduced, recreated, or recompiled.

NATO infrastructure information such as Emergency Management, Infrastructure Security Information, Information Systems Vulnerability Information, Physical Security.

NATO security information such as Internal Data or Operations Security, Security Agreement Information, Security Enforcement Information, Transportation Arrangements, Personnel Security Information, Privacy Information, or Sensitive Personally Identifiable Information.

"Information" means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

"Safeguarding" means measures or controls that are prescribed to protect information systems.

ii. The Vendor shall provide adequate security on all Vendor CIS. To provide adequate security, the Vendor shall implement, at a minimum:

a) For Vendor CIS storing, processing, or transmitting NATO R*STRICTED Information the security requirements as mandated in NATO's Security Committee reference document number, AC/35-D/2003-REV5, dated 13 May 2015, entitled, "Directive on Classified Project and Industrial Security" shall apply.

b) Other requirements. This Enclosure does not relieve the Vendor of other applicable NATO or national regulatory requirements.

c) A breach of these obligations may subject the Vendor to actions in law.

11. Cyber Incident Reporting:

i. The Vendor shall report to NCIA without delay and take remedial action upon discovery or awareness of cyber incidents.

ii. Cyber incident means actions taken directly or indirectly through the use of computer networks that result in a compromise or a potential compromise, or an actual or potentially adverse effect, on an information system and/or the information residing therein.

iii. Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media or external networks may have occurred.

iv. Cyber incidents are considered cyber security issues. The Vendor shall establish and maintain a process for identifying, tracking, reviewing, reporting, and resolving cybersecurity issues. The Vendor shall provide all relevant information on cybersecurity issues from this process to NCIA without delay. Without delay for the purposes of this Enclosure means one working day or as soon as possible under the circumstances.

v. This Enclosure is in addition to any other requirements placed upon the Vendor, and does not replace or modify any other requirement.

12. The Vendor shall not share the NR information further, without the written approval of the NCIA RFI POC.

13. Although the security measures as mentioned in this Enclosure are deemed sufficiently clear, the Vendors should request more detailed information in case of doubt.