## Headquarters Supreme Allied Commander Transformation
## Norfolk, Virginia

# REQUEST FOR INFORMATION
# RFI-ACT-SACT-26-25

This document contains a Request for Information (RFI) Call for Nations, Industry and Academia input to provide elements of NATO's

**Next Generation Deployable Communications and Information Systems (NG DCIS) Scalable Capability**

Parties wishing to respond to this RFI should read this document carefully and follow the guidance for responding.

| HQ Supreme Allied Commander Transformation RFI 26-25<br><br>**General Information** | |
|---|---|
| Request For Information No. | 26-25 |
| Project Title | Request for Nations, Industry and Academia input to provide elements of NATO's Next Generation Deployable Communications and Information Systems Scalable Capability |
| Due date for questions concerning related information | 9:00 am EST 03 March 2026 |
| Due date for submission of requested information | 9:00 am EST 24 March 2026 |
| Contracting Office Address | NATO, HQ Supreme Allied Commander Transformation (SACT)<br>Purchasing & Contracting<br>Suite 100, 7857 Blandy Rd, Norfolk, VA, 23511-2490 |
| Contracting Points of Contact | 1. Mr. Robert Friend<br>e-mail: robert.friend@nato.int<br>Tel: +1 757 747 4433<br>2. Ms. Catherine Giglio<br>e-mail: catherine.giglio@nato.int<br>Tel: +1 757 747 3856 |
| Technical Points of Contact | 1. LTC Sebastian Schweers (DEU-A)<br>e-mail: sebastian.schweers@nato.int<br>Tel: +1 757 747 4218<br>2. Dr. Kamil Akel<br>e-mail: kamil.akel@nato.int<br>Tel: +1 757 747 3796 |

## 1 - INTRODUCTION

1.1 **Summary** Headquarters Supreme Allied Commander Transformation (HQ SACT) is issuing this Request For Information (RFI) in order to engage with Nations, Industry and Academia. The intention is to discover the art-of-the-possible and state-of-the-art products or services, with respect to technologies in the area of NATO's DCIS, that are immediately available to support NATO Governance decision-making on Common-Funded Capability Development.

1.2. This RFI does not constitute a commitment to issue a future Request For Proposal (RFP). The purpose of this RFI is to involve Nations, Industry and Academia through collaboration, in an examination of future capabilities related to DCIS assets, with a focus on technologies, products or services. HQ SACT has not

made a commitment to procure any of the items described herein, and release of this RFI shall not be construed as such a commitment, nor as authorization to incur cost for which reimbursement will be required or sought. Further, respondents are advised that HQ SACT will not pay for any information or administrative costs incurred in responding to this RFI. The costs for responding to this RFI shall be borne solely by the responding party. Not responding to this RFI does not preclude participation in any subsequent RFP, if issued in the future.

## 2 - GENERAL BACKGROUND: HQ SACT Framework For Collaborative Interaction (FFCI)

2.1 HQ SACT has implemented an FFCI to increase opportunities for Nations, Industry and Academia to contribute to HQ SACT capability development efforts through collaborative work. Such collaboration enables HQ SACT, and NATO as a whole, to benefit from Nations/Industry/Academia models, advice, capabilities and experience in the course of this work. In addition to the benefits HQ SACT gains from such projects, this collaborative effort will provide Nations/Industry/Academia with an improved understanding of NATO's capability requirements and the associated issues and development challenges that need to be addressed by HQ SACT. Potential collaborative projects are on specific topics that are of mutual interest to all parties but shall be restricted to collaborations in non-procurement areas. Several mechanisms have been developed to support the initiation of collaborative projects between Nations/Industry/Academia and HQ SACT ranging from informal information exchanges, workshops, studies or more extensive collaboration on research and experimentation.

2.2 Depending on the level and type of interaction needed for a collaborative project, a specific agreement may be needed between parties. The FFCI agreement for any specific project, if required by either party for the project to proceed, will range from "Non-disclosure Agreements" (NDA) for projects involving exchange of specific information, to more extensive "Declaration Of Mutual Collaboration" (DOMC) to address intellectual property and other issues.

2.3 More extensive information on the HQ SACT FFCI initiative can be found on the ACT website http://www.act.nato.int/ffci.

2.4 Note that recipients of this RFI are not required to initiate an FFCI agreement to respond to this RFI.

## 3 - DESCRIPTION OF THE PROGRAMME

### 3.1 Programme Vision

3.1.1 The Programme's vision can be described as:

NATO requires Allied Joint Force and Land Commanders to be provided with flexible, interoperable and scalable DCIS Capability, capable of utilizing three (3) Network Domains[1] in order to plan, execute, and maintain Command and Control (C2) of military operations at Tactical, Operational and Strategic levels.

[1] NATO SECR3T, MISSION SECR3T and NATO UNCLASSIFIED

3.1.2 NATO's DCIS capability will be mainly employed in support of NATO Command and Force Structures. The effect and benefits are identified as:

- Providing NATO Forces with a fully integrated, federated, scalable, and measurable suite of deployable communications components that allow real-time/near real-time communications within three (3) Network Domains;
- Providing a standardized hardware to all commands and force structure supporting all the NATO tools connected (communication ability) to each others in terms of:
  - Supporting Allied Joint Force and Land Commanders in the decision-making process;
  - Delivering effective C2 of NATO Land Forces, including planning support, targeting and interoperability capabilities;
  - Enabling operational information exchange requirements (IERs) across the whole of the NATO Domain and especially to the Joint Force (Air, Maritime, Special Operations Forces, etc.);
  - Providing the Recognized Air and Maritime picture; and
  - Supporting Battlespace Management and related situational awareness for NATO forces within the Joint Operations Area, in order to minimize the risk of collateral damage and fratricide.
- Using state of the art technologies for better performance in:
  - communication and treatment speed;
  - deployability speed and modularity;
  - better obsolescence management;
  - safe and secure communications and embedded information; and
  - ensuring seamless communications between NATO command and force structures
- Providing the best solutions for use in Contested-Congested/Degraded-Disconnected (C2D2) conditions.

## 3.2 **Short Background**

3.2.1 Former DCIS Capability Package 149 series was initiated in 2002 to address NATO's Level of Ambition (LoA) and a NATO Response Force (NRF) Posture. Recent changes to NATO's LoA supporting an Allied Response Force (ARF), in addition to elaboration of NATO's Digital Backbone (NDBB), prompted the approach to capability development of more agile and scalable DCIS.

3.2.2 Having made these operational assessments, NATO planners were able to develop the required Command and Force structures and establish the Information Exchange and Communications requirements to match their broad operational conditions.

3.2.3 HQ SACT seeks data from Nations, Industry and Academia that will inform capability development to take existing NATO DCIS to the next generation by improving upon legacy DCIS in terms of time, cost and technology, with requirements covering a specific spectrum of capability.

3.2.4 This RFI is focused on the upcoming Capability Programme Plan (CPP) for NG DCIS which intends to deliver capability requirements for DCIS Scalable. Further detail on DCIS Scalable requirements can be found in Annex A.

3.3 **Current Status**

3.3.1 The NG DCIS Capability Requirements Brief (CRB) was approved in early 2026. The CRB informs the NG DCIS Capability Programme Plan (CPP) which will be developed in late 2026. This phase of the NATO Common-Funded Capability Delivery Governance Model (CFCDGM) examines and confirms the means and methods that are best-suited to deliver the Capability within scope, cost and schedule. For NG DCIS, the NATO CFCDGM includes decision points on the:

- Viability of a capability-based programme to satisfy the requirements (via the CRB); and
- Establishment of a programme to deliver capabilities and to drive the transformational change (via the CPP).

3.3.2 The CRB supports the Analysis of Alternatives (AoA) which intends to determine the viability of a range of potential alternatives to address the capability requirements, including consideration of the possibility of “Adopt”-ing (an existing solution already in-service by Nations), “Buy”-ing (acquiring a solution from industry), or “Create”-ing (developing a solution bespoke to NATO). In the case of Buy or Create, solutions could either be delivered through a NATO agency or a Nation being the Host Nation. Alternatives allow meeting the requirement through any of the NATO-recognised lines of development including: doctrine, organisation, training, materiel (including services), leadership, personnel, facilities and interoperability (DOTMLPFI). The viability of the alternatives comprises an assessment of the effectiveness, affordability, and risks (including schedule and technical maturity).

3.3.3 To apply due diligence in discovering alternatives, an RFI is necessary to ‘examine the market’ and determine relevant technologies and products or services that may exist or could be created within Nations and commercial market (as part of the consideration of Adopt, Buy or Create). This request intends to identify prospective (sub-) systems or products/services for which the capability development team may need to conduct additional in-depth discussions. This is not a formal request for submissions as part of a procurement; it is intended to determine whether any possible systems or products exist.

3.4 **Intent/Objectives** To support the transformational change of how NATO NG DCIS will be facilitated in the future, this RFI is intended to provide Nations, Industry and Academia an opportunity to provide data that would allow NATO to determine potential benefits realised from a product or service.

3.5 **Expected benefits to respondents** Nations and industry participants will have the chance to reveal state-of-the-art technologies and products to NATO.

3.6 **Expected Benefits to NATO** Exposure to, and understanding of, emerging technology and technological drivers.

3.7 **Expected input from Nations/Industry/Academia** Expected input to this RFI is Nations/Industry/Academia perspective on relevant current, emerging, and future technologies and products.

## 4 - REQUESTED INFORMATION

4.1 **Answers to the RFI** The response(s) to this RFI may be submitted by e-mail to the Points of Contact listed above.

4.2 **Classified Information** NATO information that is CLASSIFIED is not included herein but can be passed to authorized industry recipients with appropriate clearances and control measures.

4.3 **Eligibility to Respond** Only NATO member Nations, Industry, and Academia that originate or are chartered/incorporated within NATO member Nations are eligible to respond to this RFI.

4.4 **Format** Please DO NOT change the format of the questionnaire; send your inputs/answers in the spreadsheet provided.

4.5 **Follow-on**

4.5.1 The data collected in response to this RFI will be used to develop a report to inform the NATO NG DCIS Capability Programme. The report will provide an assessment to support a decision as to whether NATO should pursue an Adopt, Buy or Create approach to meet NG DCIS requirements.

4.5.2 In the event that there is a future competitive bidding process as part of NATO Common-Funded Capability Development, the provision of, or lack of, data will not prejudice any respondent.

4.6 **Handling of proprietary information** Proprietary information, if any, should be clearly marked as such. HQ SACT will treat proprietary information with the same due care as the Command treats its own proprietary information, and will exercise due caution to prevent its unauthorized disclosure outside of NATO. Please be advised that all submissions become HQ SACT property and will not be returned.

4.7 **Questions** Inquiries of a technical nature about this RFI shall be submitted by e-mail solely to the aforementioned POCs by 03 March 2026, 9:00 am EST to allow for appropriate response time prior to RFI submission due date. Accordingly, questions in an e-mail shall not contain proprietary and/or classified information. Answers will be posted as soon as possible on the HQ SACT P&C website at: https://www.act.nato.int/opportunities/contracting/.

4.8 **RFI Response Date** 24 March 2026, 9:00 am EST

## 5 - ADDITIONAL INFORMATION

5.1 **Non-disclosure Principles and/or Non-disclosure Agreement (NDA) with Third Party Company.** Please be informed that HQ SACT may contract a company to conduct the Analysis of Alternatives (AoA) investigation in support of this project.

5.1.1 HQ SACT will follow nondisclosure principles and possibly execute an NDA with that company to protect submitted information from further disclosure. As the third-party beneficiary of this nondisclosure, this RFI serves to inform you how HQ SACT plans to proceed and HQ SACT's intent to protect information from unauthorized disclosure. This requires the third-party company to protect the disclosed information using the highest degree of care that the company utilizes to protect its own proprietary information of a similar nature, and no less than reasonable care.

5.1.2 The third-party company receiving the information shall not, without explicit, written consent of HQ SACT:

- Discuss, disclose, publish or disseminate any proprietary information received or accessed under nondisclosure principles and subject to an NDA, if an NDA is executed;
- Use disclosed proprietary information in any way except for the purpose for which it was disclosed in furtherance of the goals of the instant project, collaboration, activity or contract; or
- Mention the other Party or disclose the relationship including, without limitation, in marketing materials, presentations, press releases or interview.

5.2 **Organizational Conflicts of Interest.** As Procurement/Contracting involves the expenditure of funds allocated by the member nations, we must always strive to maintain trust in, and preserve the integrity of, the procurement procedures. It is essential that our procedures facilitate transparent and robust competition from industry.

5.2.1 Contractor and subcontractor personnel performing work under an HQ SACT contract may receive, have access to, or participate in the development of sensitive information relating to source selection methodology, cost or pricing information, budget information, and future specifications, requirements or Statements of Work, or perform evaluation services that may create a current or subsequent Organizational Conflict of Interest (OCI). Similarly, companies responding to an HQ SACT RFI may create a subsequent OCI determination when pursuing future NATO contracts generated from that RFI.

5.2.2 Each individual contracting situation will be examined on the basis of its particular facts and the nature of any proposed contract. The exercise of common sense, good judgment, and sound discretion is required in both the decision on whether a significant potential conflict exists and, if it does, the development of an appropriate means for resolving it.

5.2.3 In anticipation of a future OCI determination, any company either awarded an HQ SACT contract or responding to an HQ SACT RFI while also anticipating bidding on future NATO contracts relating to this work, should consider having a mitigation plan in place to address or mitigate any OCI concerns now, or in the future.

5.3 **Handling of Proprietary Information.** Proprietary information, if there is any, should be minimized and clearly marked as such. HQ SACT will treat proprietary information with the same due care as the command treats its own proprietary information. HQ SACT will exercise due care to prevent unauthorized disclosure. Please be advised that all submissions become HQ SACT property and will not be returned.

5.4 **Exceptions to Obligations.** The third-party company receiving the information may disclose, publish, disseminate, and use proprietary information:

5.4.1 To its employees, officers, directors, contractors, and affiliates of the recipient who have a need to know and who have an organizational code of conduct or written agreement with the recipient requiring them to treat the disclosed proprietary information in accordance with nondisclosure principles and

the NDA (if executed);

5.4.2 To the extent required by law, however, the company receiving the information will give HQ SACT prompt notice to allow HQ SACT a reasonable opportunity to obtain a protective order, or otherwise protect the disclosed information through legal process that is:

- demonstrated in written record to have been developed independently;
- already in the possession of the company receiving the information without obligation of confidentiality, prior to the date of receipt from HQ SACT;
- disclosed or used with prior written approval from HQ SACT; or
- obtained from a source other than HQ SACT without obligation of confidentiality; or publicly available when received.

5.5 **Any response to this RFI is considered to establish consent to this process. A copy of the NDA, if or when concluded, can be provided on request.**

## 6 - SUMMARY

This is an RFI only. **The purpose of this RFI is to involve Nations, Industry, and Academia through collaboration**, in an examination of future capabilities related to NATO NG DCIS with a focus on related technologies and commercial products. HQ SACT has not made a commitment to procure any items described herein, and release of this RFI shall not be construed as such a commitment, nor as authorization to incur cost for which reimbursement will be required or sought. **It is emphasised that this is an RFI, and not an RFP of any kind.**

| RFI Statement Number | RFI Capability Requirement Statement |
|---|---|
| 1 | The DCIS Scalable capability shall include deployable HQs which can seamlessly scale from of 11-500 users |
| 2 | The DCIS Scalable capability shall be identified as Small, Medium, and Large (based on the number of users in the range) |
| 3 | Each DCIS scalable system shall be comprised of CIS, non-CIS and Transmission elements per system size |
| 4 | The DCIS Scalable capability shall be road, air, rail, and maritime transportable per system size using industry-standard loading |
| 5 | The DCIS Scalable capability shall have a fast set-up time per system size |
| 6 | The DCIS Scalable capability shall have a fast tear-down time per system size |
| 7 | The DCIS Scalable capability shall have the smallest possible footprint when fully deployed |
| 8 | The DCIS Scalable capability shall be able to fully deploy with the least amount of vehicles per system size |
| 9 | The DCIS Scalable capability shall be able to fully deploy with amount of personnel for set-up, sustain, and tear-down per system size |
| 10 | The DCIS scalable capability shall be able to scale from Small to Larger with amount of time |
| 11 | The DCIS scalable capability shall be able to scale from Large to Smaller with amount of time |
| 12 | The DCIS scalable capability shall seamlessly interconnect to other Scalable and legacy systems |
| 13 | The DCIS scalable capability shall describe the appropriate non-CIS to fulfill operational deployments per system size |
| 14 | The DCIS Scalable capability shall enable access to C3 Services, in accordance with operational needs and system size |
| 15 | The DCIS Scalable capability shall provide Anchoring capability |
| 16 | The DCIS Scalable capability shall provide access to multiple network domains (NS, MS, NR/NU) |
| 17 | The DCIS Scalable capability shall be technology-ready to provide access to any future cloud-based evolutions of security domains |
| 18 | The DCIS Scalable capability shall be digitally secure in compliance with NATO digital security standards |
| 19 | The DCIS Scalable capability shall be accredited for use within the NATO enterprise |
| 20 | The DCIS Scalable capability shall be accredited for use within Unclassified domains |
| 21 | The DCIS Scalable capability shall be accredited for use within the NR domain |

| | |
|---|---|
| 22 | The DCIS Scalable capability shall be accredited for use within the NS domain |
| 23 | The DCIS Scalable capability shall be accredited for use within MS domains |
| 24 | The DCIS Scalable capability shall connect through wired (NATO/National) communications bearers. |
| 25 | The DCIS Scalable capability shall connect through military satellite communications bearers. |
| 26 | The DCIS Scalable capability shall connect through commercial satellite communications bearers. |
| 27 | The DCIS Scalable capability shall connect through Line of Sight (LOS) communications bearers. |
| 28 | The DCIS Scalable capability shall connect through Beyond Line of Sight (BLOS) communications bearers. |
| 29 | The DCIS Scalable capability shall connect to the internet through local mobile telecom bearers. |
| 30 | The DCIS Scalable capability shall connect to the internet through Wi-Fi communications bearers of opportunity. |
| 31 | The DCIS Scalable capability shall connect to the internet through wired communications bearers of opportunity. |
| 32 | The DCIS Scalable capability shall connect to the internet through commercial satellite communications |
| 33 | The DCIS Scalable capability shall connect through HF Radio communications bearers. |
| 34 | The DCIS Scalable capability shall provide information exchange |
| 35 | The DCIS Scalable capability shall be able to be alternatively anchored to in-theatre DCIS nodes, in accordance with mission requirements. |
| 36 | The DCIS Scalable capability training shall be optimized for the least amount of training required for full user qualification |
| 37 | The DCIS Scalable capability shall locally optimize and prioritize information exchanges in accordance with mission information exchange priorities. |
| 38 | The DCIS Scalable capability shall ensure automatic failover between connectivity means. |
| 39 | The DCIS Scalable capability shall be able to be locally configured. |
| 40 | The DCIS Scalable capability shall be protected against GNSS signal disruption or corruption. |
| 41 | The DCIS Scalable shall be able to operate offline for up to 72 hours. |