

NCIA/ACQ/2025/07378
Wednesday, 22 October 2025

NCIA Request for Information (RFI)

To: Industry Partners

Subject: **SECURE MOBILE COMMUNICATION CAPABILITY
RFI-07378-SMCC**

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 acquisition for secure mobile communication function up to and including \$ECRET level operating on commercial GSM networks covering the globe. To that end, we are issuing the attached Request for Information (RFI) RFI-07378-SMCC 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 value your insight and invite you to:
 - a. Share relevant corporate capabilities and experience;
 - b. Review and comment on our draft requirements (Annexes A and B) with a view in providing recommendations for improving performance outcomes, competition, and efficiency; and identifying any risks or concerns that should be considered during planning.
4. Submission instructions and additional details can be found in the enclosure to this RFI.
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 clarification, please contact Mihaela Zoicas at Mihaela.Zoicas@ncia.nato.int.

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:

Mihaela Zoicas
Contracting Officer

Enclosure:

- Request for Information with Annexes A and B
- 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

Table of Contents

REQUEST FOR INFORMATION 4

A. Introduction 4

B. Purpose 4

C. Background 4

D. Submission Instructions 4

E. Industry Engagement (Optional) 5

F. Disclaimer 5

G. Use of Information Provided through Responses 5

H. RFI Point of Contact 5

Annex A – Requested Information 6

Annex B – Draft Requirements / Statement of Work (SOW/PWS) 7

REQUEST FOR INFORMATION

A. Introduction

1. The NATO Communications and Information Agency (NCIA) is conducting market research to identify potential sources and gather information regarding industry capabilities to support secure mobile voice communication function up to and including \$ECRET level operating on commercial GSM networks covering the globe with a potential gateway functionality to the fixed secure SIP phone network . This Request for Information (RFI) is issued solely for informational purposes and does not constitute a Request for Proposal (RFP), Request for Quotation (RFQ), or invitation for bid.

B. Purpose

1. The purpose of this RFI is to obtain input from industry to help inform the NCIA's acquisition planning. Responses to this RFI will assist in refining requirements, identifying capabilities, and shaping the strategy for any future solicitation.

C. Background

1. NCI Agency is the primary communications enabler for NATO Enterprise on different security classification levels.
2. One of the communications service being utilized by the NATO users worldwide is secure mobile voice communication function.
3. Secure Mobile Voice Communications Function aims to utilize the existing commercial GSM networks available worldwide, enabling a point to point or a point to multi-point encrypted (resistant to quantum processing) communication path, up to and including \$ECRET level, approved by a NATO nation's security accreditation authority.

D. Submission Instructions

1. Interested parties are invited to respond in accordance with the instructions below:
 - a. Submit responses via the email address in section H no later than **12:00 hours Central European Time (CET) on 05 November 2025.**
 - b. Responses should be submitted in PDF or Word format and must not exceed **15 pages**, including:
 - i. 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
 - c. Use the following subject line for submission
 - i. "Response to RFI-07378-SMCC – [Company Name]"
 - d. All responses should address the items listed in [Annex A](#) – Requested Information.

- e. Respondents are also encouraged to review and comment on the draft requirements in [Annex B](#) – Draft Statement of Work (SOW)/Performance Work Statement (PWS).

E. Industry Engagement (Optional)

1. Not Applicable

F. 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 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.

G. 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.

H. RFI Point of Contact

1. Mihaela Zoicas
2. Mihaela.Zoicas@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. Comments on the draft Statement of Work (SOW)/ Performance Work Statement (PWS)
- ii. Responses to the following RFI Questions
 1. Do you have a secure mobile voice communication solution that operates over conventional commercial GSM networks?
 2. Does your solution support all GSM frequencies on the planet without requiring an extra device or an extra add-on?
 3. Is your secure mobile voice communication solution accredited and certified to be used up to classified level by a NATO member country?
 4. Is your secure mobile voice communication presented to user consumption with a device? If so what are the physical properties of this device?
 5. Does your secure mobile communication capability require a backend? If so what are the properties of that backend and what requirements does it have?
 6. Does your backend have integration capabilities with fixed telephony or other radio solutions?
 7. Does your backend have redundancy and resiliency? If so, how is it achieved?
 8. Does your secure mobile voice communication solution also acts as a data bearer?
 9. What sort of tempering capabilities does your secure mobile voice communication solution have?
 10. Rough Order Magnitude (ROM), including any assumptions upon which they are based
- iii. Innovations or alternatives
- iv. This RFI is based on the existence of 180 GSM Secure Mobile Voice endpoints to be used by the clients and a backend to be installed at two different locations for redundancy.

d. Questions or Concerns

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

Annex B – Draft Requirements / Statement of Work (SOW/PWS)

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

1. Background

The NATO Communications and Information Agency (NCIA) requires a GSM based secure mobile voice communication capability. This capability support the NCIA's mission to communicate among the NATO and National stakeholders in a mobile, secure and uninterrupted way.

2. Scope

The Contractor shall provide secure mobile voice communication capability including, but not limited to:

- a) Capability aims to utilize the existing commercial GSM networks available worldwide (all 5 continents where there is a GSM network), enabling a point to point or a point to multi-point encrypted (resistant to quantum processing) communication path,
- b) Capability should support mobile voice communications up to and including SECRET level,
- c) Capability should be approved by a NATO nation's security accreditation authority.
- d) This capability is presented to the user with devices with the same shape and size of an ordinary mobile phone. The user device will be mentioned as "end point" from now and on.
- e) The endpoint is expected to have certain functions that make it hardware and software temper proof.
- f) The endpoint can be connected to a computer/laptop and be used as a secure transmission medium if needed and should have the capability to be used as a data encryption device with enough bandwidth to carry an audio and video conference session.
- g) The endpoint generally connects to a system at a secure facility where the provisioning, troubleshooting, remote management and inventorial process is done. This system will be identified as "backend"
- h) Backend can also facilitate core functions if needed, like key distribution, registering to the secure communications ring (group).
- i) Backend should have necessary physical and software functions that make is temper proof.
- j) Both backend and frontend support redundant configurations for service uptime and resiliency.
- k) The backend and frontend is generally expected to be compliant with SCIP (Secure Communications Interoperability Protocol).
- l) The backend also can integrate with the existing static classified telephony and video network that operates using the well known standard SIP.
- m) All the secure mobile voice communication happens in real-time with no support for store and forward.
- n) The backend should have capabilities to be monitored by a 24/7 service desk with standard tools used to probe the system as well as its functionalities.
- o) The backend should be scalable so that when the system grows to the whole NATO footprint, service quality, availability should not be effected by the number

of endpoints.

- p) NATO has a security accreditation process which the product approved by a nation to be used up to Secret level should still go through.

3. Objectives

- a. Improve communication capability and efficiency across the enterprise
- b. Bring industry expertise and excellence in delivering an end to end secure mobile communication capability
- c. Ensure synergy among the existing capabilities and to be delivered capability to increase efficiency and effectiveness of communications among NATO Enterprise and other stakeholders
- d. Implement a long term solution compliant with NATO strategy (SCIP - Secure Communications Interoperability Protocol)

4. Performance Requirements

- a. The solution that is going to be selected will have to comply to a 24/7/365 operating model where company will be responding to issues escalated by a centralized service desk or an on duty support staff from NCIA services
- b. The methods for responding to an incident/issue is negotiable.
- c. The time to respond to any incident/issue can not be longer than 30 minutes.
- d. Resolution guarantee can not be expected however a potential resolution time estimate must be supplied in 2 hours after the incident/issue is raised to the company.
- e. The support staff and any staff in direct relation/access with the product has to have the necessary security clearances.
- f. Any information shared with the company for incidents/issues/performance evaluation/contracts has to stay inside the borders of a NATO country and has to be treated by staff that are citizens of a NATO nation.
- g. There are currently 200 endpoints in operation and a backend at two separate locations in Belgium, any response should be including buyback/replacing both the backend and endpoints.
- h. The response should take into account the extra time and human resource required for accreditation process.
- i. The ownership of the backend and frontend will be with the company and contract will operate based on a rent/lease model where the technological obsolescence of the endpoints and the backend will be under the responsibility of the company.
- j. If the solution requires warm bodies, the company is expected to staff compliant with NATO regulations at the performance locations.

5. Deliverables

Deliverable	Description	Frequency	Format

6. Period of Performance

- a. The period for this contract will be 5+2 years (2 times one year), with a caveat of termination in case the product line changes do not comply with NATO strategic IT Technologies direction.

7. Place of Performance

- a. Belgium – Brussels (active)
- b. Belgium – Mons (active)
- c. Italy – Lago Patria (possible)
- d. Netherlands – The Hague (possible)