RFI-ACT-SACT-22-03
Headquarters Supreme Allied Commander Transformation
Norfolk Virginia

REQUEST FOR INFORMATION
RFI-ACT-SACT-22-03

This document contains a Request for Information (RFI) Call for NATO Nation and Industry input to HQ SACT's Exploratory Activity into End-to-End Encrypted and Quantum-Resistant Communication Solutions

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

This RFI is open to NATO Nations and industry located in NATO Nations

RFI-ACT-SACT-22-03

HQ Supreme Allied Commander Transformation RFI 22-03 General Information	
Request For Information No.	22-03
Project Title	Request for NATO Nation or industry input to HQ SACT investigation into end-to-end encrypted and quantum-resistant communication solutions
Due date for submission of requested information	01 March 2022
Contracting Office Address	NATO, HQ Supreme Allied Commander Transformation (SACT) Purchasing & Contracting Suite 100 7857 Blandy Rd, Norfolk, VA, 23511-2490
Contracting Points of Contact	1. Ms Tonya Bonilla e-mail : tonya.bonilla@act.nato.int Tel : +1 757 747 3575 2. Ms Catherine Giglio e-mail : catherine.giglio@act.nato.int Tel :+1 757 747 3856
Technical Points of Contact	1. Krzysztof Skurzak, e-mail : krzysztof.skurzak@act.nato.int Tel : +1 757 747 3206

1 - INTRODUCTION

1.1 **Summary**. Headquarters Supreme Allied Commander Transformation (HQ SACT) is issuing this Request for Information (RFI) in order to engage with NATO Nations, industry and academia. The intention is to conduct an exploratory examination of state-of-the-art and art-of-the-possible technologies, products, and services in the area of end-to-end encrypted communication protocols and post-quantum encryption. The information received through this RFI will support HQ SACT in defining and refining requirements for future capabilities of NATO.

1.2 The purpose of this request is to involve NATO Nations or industry through collaboration, in an examination of capabilities related to end-to-end encrypted communications for military or government use, with additional focus on post-quantum encryption.

1.3 This RFI DOES NOT constitute a current Request for Proposal (RFP) nor a commitment to issue a future RFP. HQ SACT is not seeking proposals at this time. Therefore, HQ SACT will not accept unsolicited proposals in respect of this RFI. Responders note that HQ SACT will not pay for any information or administrative costs incurred in responding to this RFI. All costs for responding to this RFI shall be borne solely by the responding vendor. Not responding to this RFI does not preclude participation in any future RFP if issued.

2 – GENERAL BACKGROUND: Framework for Collaborative Interaction (FFCI)

2.1 ACT has implemented a Framework for Collaborative Interaction (FFCI) to increase opportunities for industry and academia to contribute to ACT capability development efforts through collaborative work. Such collaboration enables HQ SACT, and NATO as a whole, to benefit from 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 industry / academia with an improved understanding of NATO's capability requirements and the associated issues and development challenges to be addressed by HQ SACT. Potential collaborative projects are on specific topics that are of mutual interest to both parties but shall be restricted to collaborations in non-procurement areas. Several mechanisms have been already developed to support the initiation of collaborative projects between industry/academia and ACT 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 ACT FFCI initiative can be found on the ACT web site being developed to support FFCI projects at http://www.act.nato.int/ffci.

2.4 No FFCI agreement is required to respond to this RFI. However, the principles underlying the FFCI initiative apply to this RFI.

3 - DESCRIPTION OF THE PROGRAMME

3.1 **Programme Vision**

3.1.1 HQ SACT is investigating enterprise, commercial, open-source or self-developed solutions for secure messaging that would address contemporary data security concerns related to existing messaging services available for privately owned mobile devices. Third party ownership of user data and associated metadata poses a security concern to military and government organizations, particularly in light of informal communications among military or government personnel. Furthermore, modern cryptographic solutions are not quantum resistant and are thus vulnerable to decryption with advancements in quantum computing technology. This poses a security risk to long-term data that is susceptible to "harvest now, decrypt later" tactics.

3.1.2 HQ SACT is exploring state-of-the-art and art-of-the-possible technologies, products, and services in the area of end-to-end encrypted communication protocols and post-quantum encryption. This exploratory activity is focused on possible solutions that would provide end-to-end encrypted, quantum-resistant messaging services for the personal, non-NATO issued mobile phones of NATO Staff.

3.1.2 HQ SACT requests NATO Nations, industry and academia for ideas and descriptions of existing or future planned solutions for end-to-end encrypted communications applications for personal mobile devices.

The proposed solutions shall meet to the maximum possible extent the following basic set of requirements:

- Active: the creators of the protocol and/or encryption mechanism continue to develop and support the solution. For open-source projects, this means the project has had a commit in the last twelve months.
- Secure: defined as providing end-to-end encryption through classical cryptography, quantum-resistant cryptography, quantum random number generation or any combination thereof
- Zero-data footprint: minimal user data and associated metadata retention
- Bring Your Own Device (BYOD) compatible: available on personal, non-government or non-military issued, mobile devices
- Interoperable: cryptographic system can interoperate with existing communications protocols, networks, and operating systems or/else is open with potential for standardization
- Infrastructure ownership: the server and associated solution infrastructure must be deployable within owned and operated by the government or military body
- Ease of adoption: minimal implementation/start-up procedures for users when using solution for the first time
- High learnability: users can intuitively learn to use the solution without training or users manuals
- Anonymous: Users' activity on the application should be anonymized to the maximum possible extent. This includes also the fact of establishing connections among users.

3.2 **Intent/Objectives.**
Request for Information is intended to provide NATO Nations or industry an opportunity to provide data that would allow NATO to determine potential benefits they might receive from a product or service.

3.3 **Expected benefits to respondents**
Industry participants will have the chance to expose NATO participants to state-of the-art-technologies and products.

3.4 **Expected input from industry/academia**.
Expected input to this RFI is NATO Nation and industry perspective on relevant current and future processes, techniques, technologies, products and services.

4 - REQUESTED INFORMATION

With this RFI HQ SACT requests NATO Nations, industry and academia to share their secure communication solutions that have potential, have been, or are in the progress of being, deployed to military or government personnel. Particularly, the following points shall be addressed for:

NATO Nations:

- Technology Solution
  - Description of technology solution
  - The choice between commercial, open-source, or self-developed communications protocols and/or post-quantum encryption algorithms and the reasons behind the decision, including but not limited to considerations of cost, level of customization, policy contexts, and compliance to government or regulatory organizations.
  - Details of the implementation process, timelines, and dedicated resource planning (internal, contractors, managed service etc.)
  - Outcomes of any feature prioritization exercises conducted
  - Description of data security policies, including but not limited to protection of intellectual property, protection of user data and metadata
  - Description of functional and non-functional solution requirements
  - Outcomes of solution usability testing
- Quality Assurance (QA)
  - Description of the QA process including, but not limited to, which tools are used, or being considered for use, for the quality assurance of the solution
  - How is performance of the solution managed, including but not limited to stress, load, volume, and security testing
- Costs
  - Description of project costing by phase
  - Description of operation and maintenance costs including what is necessary for licensing and accreditation
- Success factors
  - Description of the ability of the solution to scale to target number of users
  - Description of solution user adoption, new user registrations, and retention rates since implementation
  - Lessons learned analysis

Industry, Academia:

- Technology Solution
  - Description of the technology solution with detailed mapping to the requirements stated in 3.1.2. above
- Quality Assurance (QA)
  - What is the performance of the solution including but not limited to stress, load, volume, and security testing
- Costs
  - Description of projected CAPEX
  - Description of projected OPEX
- Success factors
  - Ability of the solution to scale to high volume of users (>10 000)

4.6 **Answers to the RFI**.

The answer to this RFI may be submitted by e-mail to the Points of Contact listed above.

4.7 **Follow-on**.

4.7.1 The data collected in response to this RFI will be used to provide an assessment of state-of-the-art and art-of-the-possible technology solutions for end-to-end encrypted communication protocols and post-quantum encryption. The information received through this RFI will support HQ SACT in defining and refining operational requirements for future capabilities developed for the NATO Enterprise.

4.7.2 Provision of data, or lack of, will not prejudice any respondent in the event that there is a competitive bidding process later as part of NATO Common-Funded Capability Development.

4.8 **Handling of Proprietary information.** Proprietary information, if 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, and will exercise due caution to prevent its unauthorized disclosure. Please be advised that all submissions become HQ SACT property and will not be returned**.**

4.9 **Questions.** Questions of a technical nature about this RFI announcement shall be submitted by e-mail solely to the above-mentioned POCs. Accordingly, questions in an e-mail shall not contain proprietary and/or classified information. Answers will be posted on the HQ SACT P&C website at: www.act.nato.int/contracting.

4.10 **Response Date**. 01 March 2022

5. Non-disclosure principles and/or nondisclosure agreement (NDA) with third party company

5.1 HQ SACT will follow non-disclosure principles and possibly conclude an NDA with any companies to protect submitted information from further disclosure. As the third party beneficiary of this nondisclosure, this RFI serves to inform you of how HQ SACT plans to proceed and of HQ SACT's intent to protect information from unauthorized disclosure, requiring 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. This includes the following responsibilities and obligations:

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 concluded;
- 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 interviews.

Exceptions to Obligations. The third party company receiving the information may disclose, publish, disseminate, and use Proprietary Information:

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

5.2 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. Organizational Conflicts of Interest. Companies responding to this RFI are hereby placed on notice responding to this RFI could conceivably create an organizational conflict of interest (OCI) on a future procurement, if a future procurement were to occur within the capability development process. Companies are cautioned to consider OCI when responding to this RFI, and to consider internal mitigation measures that would prevent OCI's from adversely affecting a company's future procurement prospects. OCI's can often be mitigated or prevented with simple, early acquisition analysis and planning and the use of barriers, teaming arrangements, internal corporate nondisclosure policies and firewalls, and similar prophylactic measures. HQ SACT is not in a position to advise responding companies on the existence of OCI or remedial measures, and encourages responding companies to consult internal or external procurement and legal consultants and in-house counsel.

7. Summary. THIS IS A REQUEST FOR INFORMATION (RFI) ONLY with the purpose of involving Nations, industry in an examination of existing or future capabilities related to end-to-end encrypted messaging services with a focus on post-quantum encryption**.** The information provided in this RFI is subject to change and is not binding on HQ SACT. 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. To reiterate, this is a RFI and not a RFP of any kind.

Tonya Bonilla

RFI-ACT-SACT-22-03

ACT Contracting Officer - Allied Command Transformation (ACT) NATO/HQ SACT
Tel: (757) 747-3575, **E-mail: tonya.bonilla@act.nato.int**