RFI-ACT-SACT-22-22

Headquarters Supreme Allied Commander Transformation

Norfolk Virginia

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

This document contains a Request for Information (RFI) call to industry and academia in support of NATO cyberspace operations concepts and enabling capabilities.

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

RFI-ACT-SACT-22-22

HQ Supreme Allied Commander Transformation RFI 22-22 General Information	
Request For Information No.	22-22
Project Title	Request for Information (RFI) call to industry and academia in support of NATO cyberspace operations concepts and enabling capabilities.
Due date for submission of requested information	04 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. Mr. Michael Council, E-mail : michael.council@act.nato.int Tel : +1 757 747 3420 2. Mr. Antoine Landry, E-mail : antoine.landry@act.nato.int Tel : +1 757 747 3965

1 - INTRODUCTION

1.1 **Summary**. Headquarters Supreme Allied Commander Transformation (HQ SACT) is issuing this Request for Information (RFI) in order to engage with industry and academia. The objective is to identify existing and under-development industrial/commercial/academic concepts, products, or capabilities which NATO could consider towards the development of capabilities in support of operations in and through cyberspace. This will include potential for tailoring and further development, evaluation, testing, and experimentation.

1.2. This RFI does not constitute a commitment to issue a future Request for Proposal (RFP). The purpose of this request is to involve industry and academia through collaboration, in an examination of existing and under-development concepts, products or capabilities. 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.

1.3 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 - DESCRIPTION OF THE PROGRAMME

2.1 Programme Vision

2.1.1 Today, NATO faces an increasingly diverse, complex, quickly evolving, and demanding security environment than at any time since the end of the Cold War. In particular, the exploitation of cyberspace presents an increasingly growing challenge to the security of the Alliance; a challenge which could be as harmful to our societies and institutions as conventional kinetic attacks.

2.1.2 In this context, HQ SACT – NATO warfare development command – is responsible for leading cyberspace transformation, ranging from cyberspace concept definition to capability development. A particular emphasis is notably put on cyberspace operations, as opposed to CIS security (or cybersecurity), following NATO's declaration of cyberspace as an operational domain back in 2016.

2.1.3 As part of cyberspace transformation, experimentation plays a key role to test and explore existing and underdevelopment solutions, thereby speeding up the deliveries of critical cyberspace capabilities to war fighters. This RFI aims to identify concepts, products, or capabilities; at whatever stage of development; that can be experimented with, potentially adopted and/or adapted to fulfil NATO cyberspace operation's needs.

2.2 Intent/Objectives.

To support cyberspace transformation – and notably feed the development of cyberspace operational capabilities – NATO needs to get a comprehensive overview of existing and under development concepts, products, or capabilities. This Request for Information is intended to provide industry and academia with an opportunity to share with NATO information on their existing and planned solutions that could be further tested/adapted/adopted by the Alliance.

2.3 Expected benefits to respondents

Industry and academia will have the opportunity to share state-of-the-art technologies and products with NATO in the area of cyberspace operations. This RFI is a unique opportunity to boost your business brand/product by establishing a relationship with a highly respected international organization (NATO). Working with HQ SACT on this project will result in increased visibility and international promotion of your brand.

2.4 Expected input from Industry and Academia.

For the purposes of this RFI, participants should distinguish between cyber security and cyber operations. Cybersecurity focuses on the activities or processes, ability, or state whereby information and communication systems and the information contained therein are protected from and/or defended against damage, unauthorized use, modification, or exploitation. Cyberspace Operations, in turn, focus on the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

While HQ SACT is pursuing concepts and products that satisfy both cyber security and cyberspace operations, the headquarters are more interested in concepts and solutions focusing on cyberspace operations. Participants should therefore avoid proposing contributions that focus solely on cybersecurity, unless justified by an element of novelty or technological advantage.

3 - REQUESTED INFORMATION

3.1 **White Paper**

3.1.1 HQ SACT is inviting industry and academia to submit a white paper on existing and under-development concepts, products or capabilities in the areas of **cyberspace operations** (the focus being less on solutions addressing purely cyber-security at technical level). NATO executes the following roles and functions in the area of cyberspace operations:

- Conduct Strategic and Operational Cyberspace Operations Planning;
- Perform Command and Control (C2) of Cyberspace Operations;
- Develop and maintain Cyberspace Situational Awareness;
- Prevent attacks of Alliance Cyberspace;
- Defend Against attacks on Alliance Cyberspace;
- Recover from attacks on Alliance Cyberspace.

3.1.2 As a result, HQ SACT is particularly interested in existing or under-development products that address the following topics:

- Cyberspace situational awareness at operational level;
- Cyberspace Artificial Intelligence/ Machine Learning solutions;
- Cyberspace Decision-support systems;
- Autonomous devices and systems applied to Cyberspace;
- Cyberspace Threat Intelligence Automation;
- Realistic Training in Cyberspace and/or Audacious War gaming;
- Cyber Interoperability Evaluation;
- Cyber Agility;
- Technology Advantage.

3.1.3 The list above is not all encompassing. HQ SACT is open to entertaining other novel ideas, concepts, products, or capabilities. All recommendations should address potential needs to facilitate cybersecurity operations, as well as a clear proposal on how could NATO apply the solutions.

3.1.4 The white papers shall be in Microsoft Word for Office compatible format, and shall not contain classified information. The white papers shall address, at a minimum, the following:

- Type of proposal (idea/concept/product/ or capability);
- Purpose;
- Brief description;
- Examples of potential use;
- Level of maturity/implementation/integration;

- When applicable, brief description of effort/cost requirement to finalize its implementation/adaption/adoption;
- Other relevant information, including constraints or limitation to the adoption of the proposal by NATO.

3.1.5 Information in the white papers may be considered in developing any potential final Statement of Work requirements. HQ SACT will consider selected white paper proposals for developmental contracts and experimentation candidates.

3.2 **Presentation**.
HQ SACT may ask selected RFI respondents to provide a presentation based on their white paper submission. There may be an option to present submissions during the upcoming TIDE Sprint (Cyberspace Track) scheduled for April 4-8 2022. This offer is subject to the general interest of both parties.

3.3 **Answers to the RFI**.
The answer to this RFI may be submitted by e-mail to the contracting and technical Points of Contact listed above.

3.4 **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. HQ SACT will exercise due care to prevent its unauthorized disclosure. Please be advised that all submissions become HQ SACT property and will not be returned**.**

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

3.5.1 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.

3.5.2 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.

3.5.3 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.

4. 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.

5.0 Questions. Questions of any nature, including technical ones, about this RFI announcement shall be submitted by e-mail solely to the contracting and technical POCs. Accordingly, questions in an e-mail shall not contain proprietary and/or classified information. Answers to questions will be posted, for everyone's awareness, on the HQ SACT P&C website at: www.act.nato.int/contracting.

6.0 Response Date. The white papers shall reach HQ SACT PoCs by March 4, 2022.

7.0 Summary. **This is a RFI only. The purpose of this RFI is** to involve industry and academia through collaboration, in an examination of existing and under-development ideas/concepts/products and capabilities in the area of cyberspace operations. 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. It is emphasised that this is a RFI, and not a RFP of any kind.

RFI-ACT-SACT-22-22

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