HQ Supreme Allied Commander Transformation

RFI-ACT-SACT-22-130

Headquarters Supreme Allied Commander Transformation Norfolk Virginia

REQUEST FOR INFORMATION
RFI-ACT-SACT-22-130

Amendment 1

This document contains a Request for Information (RFI) call to industry and academia in support of the NATO Classified Cyber Range (NCCR), 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-22-130

HQ Supreme Allied Commander Transformation RFI 22-130 General Information	
Request For Information No.	22-130
Project Title	Request for Information (RFI) call to industry, academia and Nations in support of NATO Classified Cyber Range (NCCR).
Due date for questions concerning related information	23:59 hours EST on 10 October 2022
Due date for submission of requested information	9:00 a.m. EST on ~~31 October 2022~~ 11 November 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	Ms Magdalena Ornat Email: magdalena.ornat@act.nato.int +1-757-747-3150 Ms Tonya Bonilla E-mail : tonya.bonilla@act.nato.int Tel : +1 757 747 3575 Ms Catherine Giglio E-mail : catherine.giglio@act.nato.int Tel :+1 757 747 3856
Technical Points of Contact	Ms. Manisha Parmar, E-mail : Manisha.parmar@act.nato.int Tel : +1 757 747 3413 OF-4 Sven Rieche, E-mail : sven.rieche@act.nato.int Tel : +1 757 747 3155

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, academia and Nations. 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 NATO Classified Cyber Range (NCCR). 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 Programmes

2.1. Programme Vision (NCCR)

2.1.1. The NCCR shall provide a secure classified environment able to:

- Support live Collective Training and Exercises
- Support the development and testing of classified TTPs
- Mission rehearsal by using real data and classified tools without corrupting the operational classified network
- Development and testing of capabilities (software, tools, virtual twins) without corrupting classified networks
- Run investigation on malicious code without corrupting the classified networks (soft requirement, only counts if it does not endanger the accreditation)
- Execute Vulnerability testing using virtual twins or system mock-ups

3. Scope of Capability (NCCR)

3.1. The NCCR shall be able to provide the following:

3.2. Physical Architecture:

- Operate within physical and virtual environments
- Provide remote access within classified networks (allow distributed live participation)
- Capability to be used in classrooms with physical security in place according to the foreseen security level
- Isolated to NATO classified network with only inbound data flow allowed
- Be a scalable system in order to get connected to other (national CCR) to host more user and/or to provide more functionalities

3.3. Non Functional Requirements:

- Have quality features with regard to scalability, capacity, availability and security
- Be able to change its configuration according to the training needs
- Be able to train at least 25 people simultaneously
- Be available at all times/on demand
- Meet the requirements for the accreditation on a NATO classified network
- Operate with respect to confidentiality and integrity of data

3.4. User Management & Authentication:

- Management of internal/external users
- Provide an authentication mechanism to log in
- Ensure Role-Based Access Control (RBAC)
- Import a list of users
- Access directory information services through Lightweight Directory Access Protocol (LDAP)

3.5. Internal & External Entities:

- Connect to internal and external providers
- Interface Cyber Situational Awareness capability
- Connect secure to other NATO entities, e.g. Cyberspace Security Centre and Cyber Operations Centre
- Import/ Exchange data with different sources, e.g. Intelligence sources
- Allow access remotely for Nations through a complete trusted isolated virtual environment
- Import real operational data from NATO classified networks

3.6. Input Sources:

- Import data from several trusted sources
- Accept pre-defined scenario's as a framework
- Use data from the current exercise
- Run user-injected events
- Import configuration settings

3.7. Functions:

- Provide a set of functionalities able to provide collective training and exercises in a classified accredited network using real data and tools up to NATO SECRET
- Allow the creation of scenarios based on realistic situations
- Allow TTPs development, execution and outcome analysis
- Provide data for further deeper analysis
- Allow the execution of scenario-driven exercises
- Allow the testing of capabilities (software, tools, virtual twins) in an operational-like environment
- Allow the execution and investigation of malicious code in an operational-like environment (soft requirement, only counts if it does not endanger the accreditation)
- Allow the modelling of the current scenario according to the needs of the Training Audience
- Collect data and provide reports upon request
- Run simulated operational scenarios
- Support an auditing functionality
- Provide an operation execution review
- Perform mission rehearsals
- Analyse data from a cyber-incident
- Be able to train the investigation, analysis and actions in response to an attack
- Be able to sanitize the training environment after exercise, resetting to the pre-exercise status

- Support Joint Cyber operation exercises
- Provide User Awareness Training
- Allow Incident Response information sharing
- Allow/Support the evaluation of the effectiveness and efficiency of the actors involved in an exercise

3.8. Output:

- Provide data for further analysis, future exercises, lessons learned, roles, scenarios and reports
- Produce, maintain and archive real operational-like scenario
- Capability to extract sample data and/or execution data from a mission
- Export of system configuration settings
- Capability to create models based on roles definition
- Visualize and export mission execution reports
- Export mission execution data and lessons learned
- Identify and report potential vulnerabilities
- Support the analyse and identification of training needs

4. Requested Information

4.1. White Paper

4.1.1. HQ SACT is inviting industry, academia and Nations to submit a white paper on existing and under-development concepts, products or capabilities in the area of NCCR.

4.1.2. 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 with underlying Capability Requirements;
- 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.

4.1.3. 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.

5. Presentation

5.1. HQ SACT may ask selected RFI respondents to provide a presentation based on their white paper submission.

6. Answers to the RFI

6.1. The answer to this RFI must be received by 9:00 a.m. EST on ~~31 October 2022~~ 11 November 2022 to the contracting and technical Points of Contact listed above (page 2).

7. Handling of Proprietary Information

7.1. 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.

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

8.1. 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:

8.2. 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 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.

9. Exceptions to Obligations

9.1. 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.

9.2. 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.

10. Questions

10.1. Questions of any nature, including technical ones, about this RFI announcement shall be submitted by e-mail solely to the contracting and technical POCs by 23:59 hours EST on 10 October 2022. 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.

11. Response Date.

11.1. The white papers shall reach HQ SACT PoCs by ~~Oct 31, 2022~~ 9:00 a.m. EST 11 November 2022.

12. Summary.

12.1. This is a RFI only. The purpose of this RFI is to involve industry, academia and Nations through collaboration, in an examination of existing and underdevelopment 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.