

Headquarters Supreme Allied Commander Transformation, Norfolk, Virginia, USA



REQUEST FOR INFORMATION

RFI-ACT-SACT-24-22

This document contains a Request for Information (RFI) call to nations, industry and academia in support of HQ SACT Cyberspace Warfare Development and Experimentation Campaign.

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

NATO UNCLASSIFIED RELEASABLE TO THE INTERNET
 HQ Supreme Allied Commander Transformation
 RFI-ACT-SACT-24-22

General Information	
Request For Information No.	RFI-ACT-SACT-24-22
Project Title	Request for Information (RFI) call to nations, industry and academia in support of HQ SACT Cyberspace Warfare Development and Experimentation Campaign.
Due date for questions concerning related information	5:00 pm EST, 22 March, 2024
Due date for submission of requested information	5:00 pm EST, 12 April, 2024
Contracting Office Address	NATO, HQ Supreme Allied Commander Transformation (HQ SACT) Purchasing & Contracting Suite 100 7857 Blandy Rd, Norfolk, VA, 23511-2490
Contracting Points of Contact	<p>Ms. Magdalena Ornat Email: magdalena.ornat@act.nato.int Tel: +1-757-747-3150</p> <p>Ms. Tonya Bonilla E-mail: tonya.bonilla@act.nato.int Tel: +1 757 747 3575</p> <p>Ms. Catherine Giglio E-mail: catherine.giglio@act.nato.int Tel: +1 757 747 3856</p>
Technical Points of Contact	<p>Name: Dr. Alberto Domingo e-mail: Alberto.Domingo@act.nato.int Tel : +1 757 747 3324</p> <p>Name: Mr. Antoine Landry e-mail : antoine.landry@act.nato.int Tel : +1 757 747 3965</p>
All request for clarifications, questions and responses to this RFI must be sent via email to all Points of Contact reported above. Individuals email will not be accepted and should not be sent. Contracting and Technical POCs must be included in any correspondence.	

1. INTRODUCTION

1.1. Headquarters Supreme Allied Commander Transformation (HQ SACT) is issuing this Request for Information (RFI) in order to engage with nations, industry and academia. The objective is to identify existing and under-development cyberspace operations concepts, products or capabilities which HQ SACT can consider for experimentation in support of the implementation of the cyberspace domain.

➔ *This RFI is seeking innovative, tailored and actionable experiment proposals in the area of cyberspace operations to inform HQ SACT cyberspace warfare and capability development efforts. Generic proposals to demonstrate, validate or evaluate commercial product will not be considered.*

1.2. **This RFI does not constitute a commitment to issue a future Request for Proposal (RFP).** The purpose of this request is to invite and involve nations, industry and academia through collaboration to help identify existing or under-development concepts, products or capabilities in the area of cyberspace operations for consideration for experimentation. 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. All information shared with HQ SACT might be shared with contracted third parties in order to support the capability development process as needed. 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.

2. BACKGROUND

2.1. By declaring cyberspace as an operational domain, NATO recognizes that conducting operations in or through cyberspace contributes to the success of the mission in a manner similar to those executed in the traditional domains. This recognition broadens the former approach, limited to defending NATO Communication and Information Systems (CIS) infrastructure, to a wider set of functions required to integrate cyber components into operations and missions.

2.2. Consequently, there are areas where NATO has a very clear understanding of what must be done as a result of the recognition of cyberspace as a domain, however, the how to do it, and what are the required concepts, products or capabilities are constantly evolving. Conversely, there are other aspects are innovative and introduce new warfighting dimensions that are not yet fully understood and which cannot be easily adapted from existing domains.

➔ *This is not a formal request for submissions as part of a procurement; but rather a general request intended to identify existing or under-development solutions that can inform HQ SACT cyberspace domain development activities.*

3. PROJECT DESCRIPTION

3.1. Vision

3.1.1. As demonstrated by recent military conflicts (i.e. Russia's war of aggression against Ukraine, Israel-Hamas conflict), daily criminal activities or even the Covid-19 pandemic, cyberspace remains a vehicle of choice for attackers. Meanwhile, digital society's increasing reliance on technology makes it more susceptible to manipulation, influence and attacks through cyberspace.

3.1.2. In this increasingly diverse, complex, quickly evolving, and demanding security environment, and beyond pure cyber security/CIS security activities, NATO needs to be able to operate in cyberspace as effectively that it does in the traditional domains, alongside relevant civilian and military stakeholders. This includes the development and maintenance of operational-level Cyberspace Situational Awareness (CySA), the execution of effective cyberspace Command and Control (C2) and the development of robust and realistic Education, Training and Exercise (ETE) solutions for cyber operators, to name a few.

3.1.3. In this context, HQ SACT – NATO warfare development command – is responsible for leading cyberspace transformation, ranging from cyberspace concept definition to capability development. As explained above, a particular emphasis is put on cyberspace operations, as opposed to cyber security/CIS security, following NATO's declaration of cyberspace as an operational domain.

3.2. Objectives.

3.2.1. As part of cyberspace transformation, warfare development and experimentation plays a key role to test and explore concepts, products or capabilities with a view to speeding up the delivery of critical cyberspace capabilities to war fighters. To support cyberspace transformation through experimentation – 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.

3.2.2. This RFI is intended to provide nations, industry and academia with an opportunity to share with HQ SACT experiment proposals related to their existing and planned concepts, products, or capabilities in the area of cyberspace operations.

3.3. Expected Benefits to Respondents

3.3.1. Nations, industry and academia will have the opportunity to inform and shape HQ SACT cyberspace warfare and capability development activities,

which can result in potential collaboration opportunities (e.g. experiments as part of NATO's flagship exercise Cyber Coalition). Working with HQ SACT on this project will contribute to increased visibility and international promotion of your solutions, while helping respondents understand and focus efforts on essential cyberspace capabilities, which are needed to further operationalize the cyberspace domain.

3.4. Expected Benefits to NATO

3.4.1. By identifying experiment proposals related to innovative and forward-looking concepts, products or capabilities in the area of cyberspace operations, HQ SACT will feed cyberspace transformation, notably through experimentation, with a view to delivering, at the time of relevance, cyberspace operations capabilities to NATO war fighters. Through this effort, NATO expects to rationalize efforts, encourage synergies, improve interoperability and creates Communities of Interest.

4. REQUESTED INFORMATION

4.1. White Papers – topics/area of interest

- ➔ *HQ SACT is inviting nations, industry and academia to submit a white paper containing experiment proposals related to existing or under-development concepts, products or capabilities in the area of cyberspace operations.*
- ➔ *Cyberspace operations include defensive, offensive and cyber intelligence operations, and utilize enablers like cyberspace Command and Control (C2), Cyberspace Situational Awareness (CySA) and cyberspace operations Education, Training, Exercises and Evaluation (ETEE). These are the areas of interest of ACT, for the purposes of this RFI.*
- ➔ *Cyberspace operations are underpinned by strong cyber security. However, cyber security is not in the scope of this RFI. Proposals based on the consideration, evaluating or experimentation with technical level cyber security concepts and products will not be considered.*

4.1.1. Topics/areas of interest. The diagram and paragraphs below identify, with more details, the topics and areas of interest that HQ SACT wishes to explore through experimentation based on feedback from this RFI.

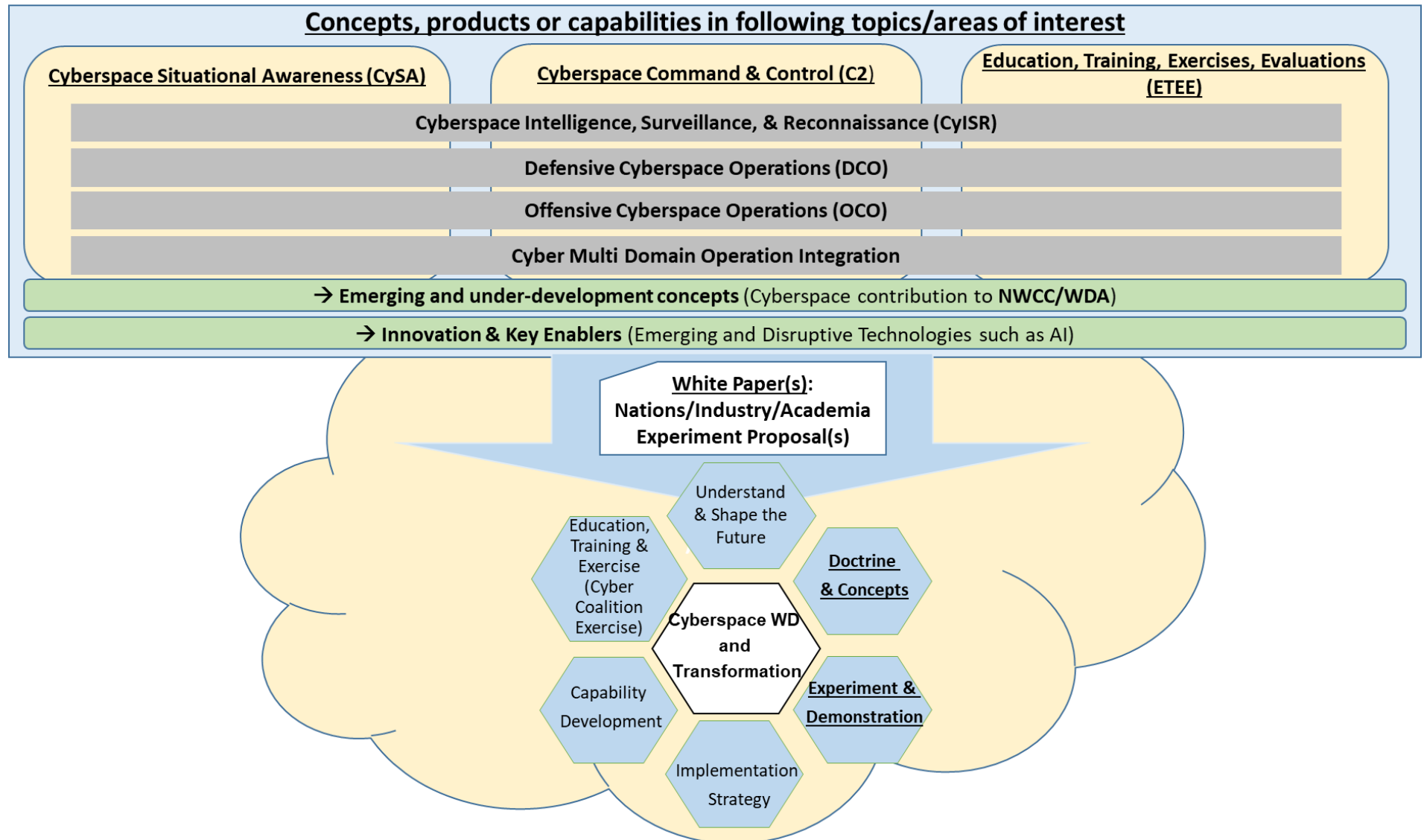


Figure 1 HQ SACT main topics/areas of interest

4.1.2. Whilst fostering the cyber security and resilience of CIS infrastructure and networks remains key, HQ SACT focuses efforts on the continuous development of the **cyberspace domain at military/mission-level**. HQ SACT therefore seeks concepts, products or capabilities addressing the following key functions (a number of potential experimentation areas are also highlighted in blue, but they are by no means exclusive):

- a) **Cyberspace Situational Awareness (CySA)**. This refers to the need to develop and maintain CySA at the operational-level, combining cyberspace threat awareness, network/CIS awareness and mission awareness to inform Commanders' decision-making.

→ *Potential experimentation areas include: Cyber key terrain; Cyber Prioritized Asset List (CPAL); Critical Information Requirement integration in CySA; Recognized Cyber Picture (RyCP); CySA distribution, federation and sharing; Cyber Battle Damage Assessment (BDA).*

- b) **Cyberspace Command and Control (C2)**. This refers to the Commander's need to maintain C2 of the operation and ensure that effects delivered in or through different domains are orchestrated to achieve mission objectives. By recognizing cyberspace as a domain, cyber should be fully integrated into existing operations and C2 functions.

→ *Potential experimentation areas include: Mission decomposition and analysis; Request for Information (RFI) and Commander's Critical information Requirements (CCIR) management (fusion, correlation, dissemination, etc.); Course of Action (CoA) and "What-if scenario" development; cyber effects modelling, cyber effect orchestration; Joint- and cross-domain operations.*

- c) **Education, Training, Exercises and Evaluations (ETEE)**. This refers to the need to enable the force, through Education, Training, Exercises and Evaluations (ETEE) solutions, to know how to operate together and then to execute in concert with one another cyberspace operations.

→ *Potential experimentation areas include: Digital twins and synthetic environments; cyberspace operational-level scenarios; digital library implementation in Cyber Ranges; strategic and operational level war-games.*

4.1.3. Those functions need to support the **full spectrum of cyberspace operations**, which include, according to NATO cyberspace high-level taxonomy, the following:

- a) **Cyberspace Intelligence, Reconnaissance, Surveillance (CyISR)**. This refers to activities whereby intelligence is derived in or through cyberspace.

→ *Potential experimentation areas include: Cyber Threat Intelligence (CTI) integration into CySA; CyISR collection, fusion and dissemination; CyISR integration into intelligence lifecycle.*

- b) **Defensive Cyber Operations (DCO).** This refers to defensive actions in or through cyberspace to preserve friendly freedom of action in cyberspace.

→ *Potential experimentation areas include: Resilience and mission assurance frameworks; cyber threat hunting; deception techniques to inform operational-level CySA.*

- c) **Offensive Cyber Operations (OCO).** This refers to activities in or through cyberspace that project power to create effects which achieve military objectives.

→ *Potential experimentation areas include: OCO integration into joint targeting; operational risk analysis; de-confliction mechanisms; Battle Damage Assessment (BDA).*

- d) **Cyber Multi-Domain Operation Integration.** This refers to the need to integrate and orchestrate military activities across all operating domains and environments, while ensuring synchronization with non-military activities and stakeholders. As cyberspace is a domain mainly owned and operated by commercial providers, fostering civilian-military collaboration is essential.

→ *Potential experimentation areas include: Integration of cyberspace operations into information/cognitive warfare operations; civilian-military integration; cross-domain/cross command information sharing.*

4.1.4. In support of the afore-mentioned functions and operations, HQ SACT is also particularly interested in:

- a) **Emerging and under-development concepts.** This includes experiments that support warfare development efforts and elicitation and identification of capabilities in the most current HQ SACT's Warfare Development Agenda (WDA).

→ *Potential experimentation areas include: Cyberspace integration with Electronic Warfare (EW); cyberspace support to Cognitive Warfare (CW), Multi-Domain Operations (MDO) and Digital Transformation (DT).*

- a) **Innovative solutions and key enablers**, notably related to the use of Emerging and Disruptive Technologies (EDTs), provided that proper use cases in support of cyberspace operations can be articulated.

→ *Potential experimentation areas include: Artificial Intelligence (AI) and Machine Learning (ML) use for risk analysis; AI-techniques in support of CySA development.*

4.1.5. The list above is not all encompassing. HQ SACT is open to experiment proposal(s) addressing other novel ideas, concepts, products, or capabilities that can feed HQ SACT cyberspace transformation efforts.

4.2. White Papers – format

4.2.1. The white paper shall address, at a minimum, the following:

- a) **Experiment proposal(s)** formulated in terms of objectives, hypotheses, success criteria, technical set up, metrics, etc.
- b) **Brief description** (maturity, use cases, etc.) of the concept, product or capability to be experimented with.
- c) **Effort/cost (ROM¹)** required to conduct the proposed experiment.
- d) Other relevant information, including constraints or limitation related to the experiment proposal.
- e) Name, mailing address and designated point of contact (phone, e-mail).

→ *This RFI is seeking innovative, tailored and actionable experiment proposals in the area of cyberspace operations to inform HQ SACT cyberspace warfare and capability development efforts.*

- *Cyber security-focused proposals will in general not be considered.*
- *Generic proposals to demonstrate, validate or evaluate commercial products will not be considered.*

→ *HQ SACT will exceptionally consider concept development and experimentation design short studies and research efforts, should be the topic be of primary relevance for HQ SACT and the maturity of the experiment requires a preliminary research phase.*

4.2.2. Responses to this RFI **shall not be classified above NATO UNCLASSIFIED.**

4.2.3. The white paper (main document and enclosures) should not exceed **10 pages**. It should be single-spaced, have one-inch margins, assume US letter-size (8 1/2 by 11 inches) page, use 12-point font, and be formatted for compatibility with Microsoft Word or Adobe Acrobat Reader (current versions).

4.2.4. Submissions should be named according to the following convention: <Respondent company name; maximum of 12 characters>_CYBER-EXP-

¹ HQ SACT seeks non-binding Rough Order Magnitude (ROM) price estimates for the sole purpose of estimating programmatic costs and planning funding for future programme proposals/bids. Provision of data, or lack of, will not prejudice any respondent in the event that there is a competitive bidding process later on, as part of NATO Budget and NATO Common Funded Capability Development policies.

RFI_<date in YYYYMMDD format>.<filename extension of 3 or 4 characters>.

4.2.5. The response(s) to this RFI shall be submitted by e-mail. Submissions must include both the Contracting and Technical POCs listed on page 2. The responses shall not contain proprietary and/or classified information. HQ SACT reserves the right to seek clarification on submissions.

4.2.6. Eligibility to Respond. Only NATO nations, and industry and academia that originate or are chartered/incorporated within NATO nations are eligible to respond to this RFI. Companies from Partner Nations who want to participate should collaborate with a primary company headquartered within a NATO Nation.

4.2.7. Respondents can collaborate with other providers, but all companies/organizations must be clearly identified and their role/services clearly stated.

4.2.8. The information may be considered in developing any future potential Statement of Work requirements. HQ SACT will consider selected information for developmental contracts and experimentation candidates.

4.3. Response Due Date. Responses to this RFI must be received by **5:00 pm EST 12 April 2024**. The responses shall not contain any classified information. HQ SACT reserves the right to seek clarification on submissions.

5. CLARIFICATIONS AND QUESTIONS

5.1. All questions should be submitted by e-mail solely to the aforementioned POCs by **5:00 pm EST 22 March, 2024** to allow for appropriate response time prior to the **5:00 pm EST 12 April 2024** response due date.

5.2. 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://act.nato.int/contracting>

6. ADDITIONAL INFORMATION

6.1. Non-disclosure Principles and/or Non-disclosure Agreement (NDA) with Third Party Company.

6.1.1. Please be informed that HQ SACT may contract a company to conduct investigation or analysis in support of this project. HQ SACT will follow nondisclosure principles and possibly conclude 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.

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

- a) Discuss, disclose, publish or disseminate any Proprietary Information received or accessed under nondisclosure principles and subject to an NDA, if an NDA is concluded;
- b) 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
- c) Mention the other Party or disclose the relationship including, without limitation, in marketing materials, presentations, press releases or interview.

6.2. Organizational Conflicts of Interest.

6.2.1. 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.

6.2.2. 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 Interests (OCI). Similarly, companies responding to an HQ SACT RFI may create a subsequent OCI determination when pursuing future NATO contracts generated from that RFI.

6.2.3. Each individual contracting situation will of course 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.

6.2.4. 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.

6.3. 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.

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

- a) 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);
- b) 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, or
 - already in the possession of the company receiving the information without obligation of confidentiality, prior to the date of receipt from HQ SACT, or
 - 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.

6.5. 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.

7. SUMMARY. This is a RFI only. The purpose of this RFI is to involve nations, industry and academia through collaboration to collect experiment proposals to feed cyberspace transformation. 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 emphasized that this is a RFI, and not a RFP of any kind.
