REQUEST FOR INFORMATION
RFI-ACT-SACT-17-51
Amendment #1

This document contains a Request for Information (RFI) Call for Industry input to NATO’s approach to federated cyber operations which will be discussed during a NATO Industry Forum (NIF)-branded event. Suppliers wishing to respond to this RFI should read this document carefully and follow the guidance for responding.
<table>
<thead>
<tr>
<th>General Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Request For Information No.</td>
<td>17-51</td>
</tr>
<tr>
<td>Project Title</td>
<td>Call for industry input to NATO’s implementation of cyber as domain of operation during event to be held in Virginia Beach, 26 October, 2017.</td>
</tr>
<tr>
<td>Due date for submission of requested information</td>
<td>October 17, 2017</td>
</tr>
<tr>
<td>Contracting Office Address</td>
<td>NATO, HQ Supreme Allied Commander Transformation (SACT) Purchasing &amp; Contracting Suite 100 7857 Blandy Rd, Norfolk, VA, 23511-2490</td>
</tr>
</tbody>
</table>
| 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. Maj James Borst,  
  e-mail: james.borst@act.nato.int  
  Tel: +1 757 747 3787  
  2. Roberto Secco,  
  e-mail: roberto.secco@act.nato.int  
  Tel: +1 757 747 3862 |
1 - INTRODUCTION

1.1 Summary. Cyber-attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. The Wales and Warsaw Summit declarations respectively stated that cyber defence is part of NATO's core task of collective defence and reaffirmed NATO's defensive mandate, recognising cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea.

1.2 These political statements imply the need for NATO to improve its ability to protect and conduct operations across these domains to safeguard the Alliance’s freedom of action and decision, in all circumstances. A specific cyberspace domain will support NATO's broader deterrence and defence: cyber defence will continue to be integrated into operational planning and Alliance operations and missions, and NATO and nations will work together to contribute to their success. Furthermore, it will ensure more effective organisation of NATO's cyber defence and better management of resources, skills, and capabilities. This is part of NATO's long term adaptation, which adheres to the principle of restraint and support, and seeks to maintain international peace, security, and stability in cyberspace.

1.3 The implementation of a new operational domain is no trivial task; it requires a holistic approach across the entire DOTMLPFI\(^1\) spectrum and constant engagement with a significant number of stakeholders, including nations, academia, and industry. In the next years, NATO needs to shift from a quite traditional, well-understood, yet passive role of protecting its CIS infrastructure to a more operational approach, in which cyber capabilities are instrumental to the successful execution of joint operations and to the achievement of the Commander’s objectives.

1.4 Headquarters Supreme Allied Commander Transformation (HQ SACT) is issuing this Request for Information (RFI) in order to engage with industry and academia during a NATO Industry Forum (NIF)-branded workshop that will be held on 26 October 2017 in Virginia Beach, (VA) during the fall edition of the TIDE Sprint (23-27 October 2017). The main topic of the event is “Federated Cyber Operations”.

1.9 Disclaimer. This request for information does not constitutes a commitment to issue a future request for proposal (RFP). The purpose of this RFI is to involve industry through collaboration, in an examination of future capabilities related to the collection, fusion and dissemination of command and control and intelligence, surveillance, and reconnaissance data with a focus on the network capabilities and characteristics which support these activities. 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. 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. RFI respondents would be willing to share their technical knowledge, expertise, and observations with NATO and other attendees participating in the working group and are responsible for complying with national laws regarding transferring information within this NATO forum.

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

---

\(^{1}\) Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, Interoperability
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 website 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.

3 - DESCRIPTION OF THE PROJECT

3.1 Background.
The NATO-Industry Forum is the primary venue for strategic dialogue with the defence and security industry on NATO capability planning and development. The Forum builds upon the Warsaw Summit Communiqué in which NATO Heads of State and Government highlighted that, “A stronger defence industry across the Alliance, which includes small- and medium-sized enterprises, greater defence industrial and technological cooperation across the Atlantic and within Europe, and a robust industrial base in the whole of Europe and North America, remain essential for acquiring needed Alliance capabilities”. Previous NIF events have been held at executive level with attendees at the “four-star” and Chief Executive level. This year, ACT is holding a series of smaller events which will be used to inform the larger event. NIF-branded events are specific workshops involving ACT and industry, which were selected to provide a report as a preparation for the NIF, due to the high level of interest and connection to NATO’s strategic objectives.

3.2 Intent/Objectives.
The main topic of the event is “Federated Cyber Operations”. This RFI is to call for industry to provide its perspective on the topic by designating SMEs to either deliver key note speeches on “Federation Cyber Information” and “Federating Cyber Training” or by participating as panellist in the following “Cyber FMN” panel discussion.

3.3 Expected benefits to respondents
Industry participants will have the chance to expose NATO participants the state of the art technologies and processes and also understand what challenges NATO is facing and how this
will impact future capabilities. By understanding the art of the possible, NATO envisions producing and understanding better the requirements which define future systems.

3.4 **Expected input from industry/academia.**

Expected input to this RFI is an industry perspective on current and future technologies, processes, and capabilities regarding the federation of cyber operations. However, whilst the primary focus is to gather industry perspective on federated cyber operations by designating SMEs as key note speakers or panellist at the NIF-branded workshop, ACT will consider any industry contributions on the subject.

4 - REQUESTED INFORMATION

4.1 **Answers to the RFI.**

This NIF branded event will take place within the bi-annual Think-Tank for Interoperability and Decision and Execution superiority (TIDE) Sprint event that takes place in Virginia Beach every Fall and in Europe every Spring. Industry participants responding to this RFI event will need to register for TIDE Sprint first, indicating that they are only attending the NIF event. Registration for TIDE Sprint requires all participants to have access to the password protected Tidepedia website ([http://tide.act.nato.int](http://tide.act.nato.int)) in order to access the registration portal. Participants without access to Tidepedia can request a user name and password at: tide@act.nato.int. Industry partners wishing to deliver a keynote speech, or participate as part of a panel should register for this event first, then provide an abstract of their keynote or panel contribution to the technical POCs of this RFI.

4.2 **Follow-on.**

The data collected in response to this RFI, at the NIF-branded workshop, and submitted as contribution will be used to develop a report to inform the next high-level NIF forum.

4.3 **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, 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.

4.4 **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. HQ SACT does not guarantee that questions received after 1 October 2017 will be answered. Answers will be posted on the HQ SACT P&C website at: [www.act.nato.int/contracting-procurements](http://www.act.nato.int/contracting-procurements). On the same page, instructions on how to register to the event will be made available after 5 September 2017.

4.5 **Response Date.** 17 October 2017

4.6 **Summary.** This is a RFI only. The purpose of this RFI is to involve industry/academia, through collaboration, in a NATO Industry Forum (NIF)-sponsored event. 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.

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