



NCIA/ACQ/2021/07061
02 August 2021

Notification of Intent to Request Quotations for

**The Cyber Security Framework
NOI-CO-115537-CSF**

Period of Performance:

A basic period of two (2) years plus two 12-month option period.

Overall ceiling amount of 30,000,000 EUR throughout the contract life (of 1 two-year base plus two one-year options (if exercised)). However, the Purchaser reserves the right to unilaterally increase the ceiling amount past 30,000,000 EUR, if this ceiling amount is reached prior to the end of the contract life.

The NCI Agency is seeking to establish a framework agreement which will serve as a preferred vehicle for contractor support for surge cyber security services across all NATO locations.

The Agency anticipates issuing the formal Request for Quote (RFQ) by Q4 2021 with an anticipated Contract Award by Q2 2022.

NCI Agency Point of Contact: Mr. Darren Corkindale

E-mail: RFQ-CO-115537-CSF@ncia.nato.int

To: Distribution List

Subject: Notification of Intent (NOI) to establish an Indefinite Delivery, Indefinite Quantity (IDIQ) framework for cyber security services.

References:

- A.** C-M(2015)0025 – NATO Financial Regulations
- B.** AC/337-D(2016)0014 – NCIO Financial Rules and Procedures
- C.** BC-D(2018)0004 – BC Military Budget Procurement Guidance
- D.** AC/4-D(2019)0004 (INV)

1. In accordance with References A-D, notice is given of the intent of the NATO Communications and Information Agency (NCI Agency) to issue a Request for Quote (RFQ) to establish a Firm Fixed Price (FFP) Multiple Award Indefinite Delivery Indefinite Quantity (IDIQ) framework using multiple funding sources at the NATO Enterprise level.
2. A summary of the requirements of the RFQ are set forth in Annex A attached to this letter. These requirements are currently being refined as part of the preparation of the proposed RFQ.
3. The reference for this RFQ is RFQ-CO-115537-CSF and all correspondence concerning this RFQ should reference this number.
4. The envisaged procurement procedure for this RFQ is Basic Ordering Agreement (BOA) Plus (BOA+). The successful bidder(s), pursuant to the RFQ following this NOI, will be the bid that offers the lowest price and is technically compliant in accordance with the evaluation criteria prescribed in the RFQ.
5. The formal RFQ is planned to be issued December 2021, and Contract Award is planned for no later than June 2022.
6. Attached to this letter at Annex B is a list of potential bidders that may be able to provide the services and equipment required for this project. This list was compiled from the companies that have an active BOA with the Agency.
7. The BOA+ procedures allow National Responsible Authorities to nominate eligible bidders in addition to the companies identified at Annex B. Any such nominations for companies that do not have an active BOA should come from the National Authorities via their Delegation/Mission to NATO, who will provide the requisite Declaration of Eligibility (DoE). Upon receipt of the DoE, the NCI Agency Contracting Officer will add the company to the Bidders List.
8. National Responsible Authorities are kindly requested to provide a list to the NCI Agency with Declarations of Eligibility, not later than **03 September 2021**, of qualified and certified companies which may be interested in receiving a Request for Quote for this project.
 - a. In addition to the certification of the firm's security clearances required under this NOI, the DoE should include the following information for each of the nominated firms:

Name of the Firm

Telephone number

E-mail address

Point of Contact.

- b. This information is critical to enable prompt and accurate communication with prospective bidders and should be sent to the following address:

NATO Communications and Information Agency
Attention: Mr. Darren Corkindale
e-mail: RFQ-CO-115537-CSF@ncia.nato.int

9. Please note that requests for participation in this competition received directly from individual companies cannot be considered, unless they hold a valid BOA with the NCI Agency.
10. National authorities are advised the RFQ package is anticipated to be NATO UNCLASSIFIED; however, the RFQ and the contractual documents could contain references to other NATO documents classified as NATO RESTRICTED.
11. The successful bidder(s) may be required to handle and store classified information up to the level of NATO SECRET. In addition, Contractor personnel may be required to work unescorted in Class II Security areas and therefore, access can only be permitted to cleared individuals. Only companies maintaining such cleared facilities and the appropriate personnel clearances will be able to perform the resulting contract.
12. The Principal Contracting Officer for this RFQ is Rebecca Benson. The NCI Agency point of contact for all information concerning this NOI is Mr. Darren Corkindale, Senior Contracting Officer (Consultant) who can be reached at email: RFQ-CO-115537-CSF@ncia.nato.int
13. Your assistance in this procurement is greatly appreciated.

For the Director of Acquisition:

Rebecca Benson
Principal Contracting Officer

Attachment(s):

Annex A – Summary of Requirements
Annex B – Draft Bidders List

Annex A: Summary of Requirements

1. Introduction

- a. The NATO Cyber Security Centre's (NCSC) mission is to lead the development and delivery of cyber security of cyber security capabilities and services.
- b. Over the past 24 months, the NCSC has been requested to provide services to support various projects across different NCI Agency Service Lines. In doing so, NCSC has utilised a mix of both in-house and external resources to support these projects. Following the expiry of existing contractual agreements, the NCSC is seeking to establish a framework agreement for cyber security services – known as the Cyber Security Framework (CSF).

2. Project Scope

- a. The NCI Agency does not currently have a preferred vehicle for contracted cyber security services. Therefore, through the CSF, NCSC aims to establish an IDIQ framework with up to three (3) suppliers as the preferred vehicle for contractor support for surge cyber security services during the framework's Period of Performance.
- b. The IDIQ will provide an overarching set of terms and conditions and a broad requirement. Up to three suppliers will receive a place on this IDIQ framework.
- c. When the Agency has a requirement for cyber security services, a Statement of Work (SoW) will be developed and a Delivery Order competition will be run among the three suppliers on the IDIQ. The resulting lowest priced, technically compliant offer would be awarded the resulting Task Order to complete the work detailed in the SoW. There is no guarantee of any work through the IDIQ framework.
- d. A place on the IDIQ framework agreement will be awarded through competition. The Agency will issue the IDIQ requirements, alongside a historic Task Order SoW for evaluation purposes only. The three lowest priced, technically compliant bids received for this historic Task Order will be awarded a place on the IDIQ framework. This approach will ensure that the three lowest priced suppliers in the market will competitively be awarded a place on the IDIQ for future Task Orders when a need arises.
- e. The aim of the IDIQ framework is to ensure a broad scope; however, for indicative purposes a non-exhaustive list of potential core services could include:

- I. The extension of NCSC services to Tier 3 Sites¹. The extension may involve the following:
 - Deployment of a dedicated NATO Computer Incident Response Capability (NCIRC) Tier-3 enclave and/or
 - Configuration, tuning and/or testing of existing NCSC centralised services to support the extended NCSC protection and monitoring coverage to the additional site.

NCSC services include the following:

1. Online Computer Forensics (OCF)
 2. Online Vulnerability Assessment (OVA)
 3. Log Aggregation (LOG A)
 4. Firewalls
 5. Network Intrusion Prevention System (NIPS)
 6. Full Packet Capture (FPC)
- II. Subject Matter Expertise (SME) on a level of effort basis for services including, but not limited to, virtualisation, on-site connectivity and firewall integration.
- f. Subsequent Task Orders will define the full scope, although it is envisaged that all services and associated goods procured under this IDIQ shall include delivery to NATO sites.

3. Geographical Implementation

- a. The Contractor shall supply equipment and services to all authorized NATO Command Locations in Europe and North America including any of NATO's Affiliates, upon issuance of Task Orders in accordance with the terms of the Contract. The list of existing affiliates is available at:
<http://www.nato.int/cps/en/natolive/structure.htm>.

¹ Tier-3 encompasses a number of remote locations spread across the NATO Member Nations. Each of these typically include a separate, secure enclave into which NCSC's cybersecurity sensors and systems (for example, full packet capture and log collection) are deployed.