Acquisition Directorate
RFQ-CO-115300-CSSR@nr.ncia.nato.int

NCIA/ACQ/2020/7085
16 November 2020

Notification of Intent to Request for Quotations

Cyber Security System Refresh
RFQ-CO-115300-CSSR

Estimated Value: 27.1MEUR

The NCI Agency is seeking the acquisition and deployment of cyber defense systems as replacement for those that are at, or near, End-of-Life (EoL) within three environments at the NATO Computer Incident Response Centre (NCIRC) located in SHAPE, Mons, Belgium.

The Agency anticipates issuing the formal Invitation for Bid (IFB) in Q3 2021 with an anticipated Contract Award by Q4 2021. Please note that the anticipated IFB will likely have a bid closing date of approximately 30 days.

NCI Agency Point of Contact
Contracting Officer, Frank Iyakaremye
RFQ-CO-115300-CSSR@ncia.nato.int

To: Distribution List

Subject: **Notification of Intent to Requests for Quotations**
Cyber Security System Refresh (CSSR)

RFQ-CO-115300-CSSR

Reference(s): A. AC/4-D(2019)0004 (INV)
B. AC/4-DS(2020)0015 (DS)

1. The NCI Agency, as the Host Nation, hereby gives notice of its intent to issue a Request for Quote (RFQ) to acquire and deploy cyber defense systems as replacement for those that are at, or near, End-of-Life (EoL) within three environments at the NATO Computer Incident Response Centre (NCIRC) located in SHAPE, Mons, Belgium.

2. The procurement will be conducted under the Basic Ordering Agreement Plus (BOA+) procedures.

3. A summary of the requirements of the anticipated RFQ is set forth in Annex A of this letter. The NCI Agency is refining the requirements and will include more

details when the RFQ is released.

4. The reference for the RFQ is RFQ-CO-115300-CSSR, and all correspondence concerning this RFQ must reference this number.

5. For the purpose of planning, the estimated cost for the services and deliverables included within the scope of the intended contract is approximately EUR 27.1M.

6. The envisaged procurement procedure for this RFQ will be the BOA+ procedures. The successful quote, pursuant to the RFQ following this NOI, will be that quote which is the lowest price and technically compliant in accordance with the evaluation criteria prescribed in the RFQ.

7. The formal RFQ is planned to be issued in Q3 2021, and Contract Award is planned for no later than Q4 2021.

8. It is planned to award a single firm-fixed price contract for the entire scope of work. No partial bidding will be accepted.

9. A draft Bidders list extracted from those companies who currently have an active BOA with the NCI Agency is attached at Annex B.

10. Companies that have a signed and activated BOA and are not listed in Annex B, may contact the NCI Agency's POC at paragraph 12 of this letter enabling the Company to be added to the Bidders list.

11. In addition, national responsible authorities are kindly requested that the NCI Agency be provided with Declarations of Eligibility (DoE) **not later than 35 days from the date of this Notification of Intent (NOI)** of qualified firms which are interested in participating in this procurement but do not possess a BOA.

12. The declarations of Eligibility (DoE) should include the following information for each of the nominated companies:

- Company Name and Address
- Point of Contact, Telephone number and E-mail address.

This information is critical to enable prompt and accurate communication with prospective Bidders. The DoE should be sent to the following point of contact:

NATO Communications and Information Agency
Attention: Frank Iyakaremye, Contracting Officer
E-mail: RFQ-CO-115300-CSSR@ncia.nato.int

13. National authorities are advised that the RFQ package is anticipated to be NATO UNCLASSIFIED. However, the RFQ and the contractual documents may contain references to other NATO documents classified as NATO R3STRICTED.

14. The successful Offeror will be required to handle and store classified information up to the level of NATO S3CRET. In addition, Contractor personnel will 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.

15. The NCI Agency point of contact for all information concerning this NOI is Mr. Frank Iyakaremye at email: RFQ-CO-115300-CSSR@ncia.nato.int

16. Your assistance in this procurement is greatly appreciated.

For the Director of Acquisition:

Ijeoma Ike-Meertens
Principal Contracting Officer (Acting)

Attachment(s):

Annex A- Summary of the Requirements
Annex B- Draft Bidders List

Annex A – Summary of the Requirements

1 Introduction

1.1 To address an obsolescence management requirement and facilitate technology refresh, the NCI Agency is looking for an integrator(s) from industry to provide, and commission into service, a list of systems.

1.2 A technology refresh is required to consolidate the capabilities referenced in section 2.1, modernize them where newer techniques and technologies exist, and to replace elements that are otherwise losing reliability due to obsolescence, in order to improve Computer Information Systems (CIS) security within the NATO Enterprise. The aim also includes the provision of engineering and design work to adapt the new technologies with the NATO architecture.

1.3 The components will be deployed both at the NCIRC operations based in SHAPE, Mons, Belgium as well as at various NATO sites.

2 Project Scope

2.1 The main systems in scope of refresh are:

2.1.1 Firewalls – A vital component in the protection of network enclaves. NATO Cyber Security Centre (NCSC) seeks to leverage advances in firewall technology by deploying feature sets common to Next Generation Firewall systems. A firewall outage can potentially disrupt all CIS services.
2.1.2 Network Intrusion Detection/Prevention Systems (NIPS) with Anomaly Based Detection– Considered an essential device for the purpose of detecting / monitoring potential threats on networks. This capability is hardware-intensive and is required to adapt to increasing network bandwidth. A NIPS outage can potentially disrupt all CIS services.
2.1.3 Log Aggregation (LogA) - Key data source for the SIEM.
2.1.4 Equipment TEMPEST Level Testing tools - System no longer supported by vendor post-2018.
2.1.5 NCIRC Tier-3 Enclave - Platform to support and connect all deployed sensors at remote sites.
2.1.6 Data Diodes
2.1.7 Guards (Mail / Web)
2.1.8 Forensics Evidence Management (FEM) system
2.1.9 Malware Analysis (MA) system
2.1.10 NCIRC Operational Deployment Support & Exercise Reference System (NODCERS)
2.1.11 Cyber Threat Assessment Cell (CTAC) systems
2.1.12 Rapid Reaction Team Kits (RRTK)
2.1.13 Penetration Testing tools
2.1.14 Website Vulnerability Assessment tools
2.1.15 Onsite Vulnerability Assessment tools

2.2 The systems listed in paragraph 2.1 above will be deployed in independent architectures for NATO R3STRICTED, NATO S3CRET, and a Test/Reference environment.

3 Geographical Implementation

3.1 The NCIRC capability is operated centrally from SHAPE Mons. Additional components are deployed within NCIRC enclaves to support monitoring at the following geographical locations:

3.1.1 Mons, Belgium
3.1.2 Brussels, Belgium
3.1.3 Lago Patria, Italy
3.1.4 Pogio Renatica, Italy
3.1.5 La Spezia, Italy
3.1.6 Brunssum, Netherlands
3.1.7 The Hague, Netherlands
3.1.8 Izmir, Turkey
3.1.9 Northwood, UK
3.1.10 Norfolk VA, USA
3.1.11 Aix en Provence, France
3.1.12 Munich, Germany
3.1.13 Uedem, Germany
3.1.14 Ramstein, Germany
3.1.15 Geilenkirchen, Germany
3.1.16 Capellen, Luxembourg
3.1.17 Betzdorf, Luxembourg
3.1.18 Torrejon, Spain
3.1.19 Stavanger, Norway
3.1.20 Monsanto, Portugal
3.1.21 Bydgoszcz, Poland