

Notification of Intent to Request Quotations for

**SIEM Infrastructure Refresh
RFQ-CO-15569-SIEM**

EUR 17,000,000 (Estimated value)

The NCI Agency is seeking the acquisition and deployment of cyber security logging and Security Information and Event Management (SIEM) hardware and software 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.

Principal Contracting Officer: Ms. Rebecca Benson

Point of Contact: Mr Darren Corkindale

E-mail: darren.corkindale@ncia.nato.int

To : Distribution List

Subject : **Notification of Intent to Invite Requests for Quotations for SIEM Infrastructure Refresh**

Reference(s) : A. AC/4-D(2019)0004 (INV)
B. AC/4-DS(2019)0015 –COR1
C. AC/4-DS(2019)0024 (INV)

1. In accordance with References B and C, notice is given of the intent of the NATO Communications and Information Agency (NCI Agency), as the Host Nation, to issue a Request for Quotation (RFQ) to Refresh SIEM Infrastructure Equipment and Systems under the Basic Ordering Agreement Plus (BOA+) procedures outlined in Reference A.
2. Annex A of this Notification of Intent (NOI) is a summary of the project's requirements. To address an urgent obsolescence management requirement and facilitate technology refresh, the NCI Agency is seeking the acquisition and deployment of cyber security logging and Security Information and Event Management (SIEM) systems. These requirements are being refined and detailed

as part of the preparation of the SIEM Infrastructure Refresh proposed BOA+ Award.

3. The reference for the RFQ is RFQ-CO-15569-SIEM, and all correspondence concerning this RFQ must reference this number.
4. The estimated investment cost for the services and deliverables included within the basic scope of the intended contract(s) is EUR 17,000,000. Funding for this project is provided by the Investment Committee as per References B and C.
5. 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.
6. The formal RFQ is planned to be issued early December 2019, and Contract Award is planned for no later than April 2020.
7. The draft Vendor list extracted from those companies who currently have active BOAs with the NCI Agency and who may be interested is attached at Annex B. Companies that have a signed and activated NCI Agency BOA and are not listed in Annex B may also contact the NCI Agency's POC at point 7b of this letter enabling the Company to be added to the Vendor list. In addition, national responsible authorities are kindly requested that the NCI Agency be provided Declarations of Eligibility (DoE) not later than **22 Nov 2019**, of qualified and certified firms which are interested in quoting against this project and of which currently do not possess an active NCI Agency BOA.
 - 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 Offerors and should be sent to the following address:

NATO Communications and Information Agency

Boulevard Leopold III, 1110, Brussels, BELGIUM

Attention: Mr. Darren Corkindale – Sr. Contracting Officer (Consultant), S2/2027

E-mail : darren.corkindale@ncia.nato.int

8. Offerors will be required to declare a Quotation validity of six (6) months from closing date for receipt of quotes, supported by a Quotation Guarantee of EUR 300,000 (three hundred thousand Euro), should it be decided the guarantee will be a different amount the RFQ will detail the values. Should the selection and award procedure exceed the RFQ Closing Date by more than six (6) months firms

will be requested to voluntarily extend the validity of their Quotations and Quotation Guarantee, accordingly. Offerors may decline to do so, withdraw their Quote and excuse themselves from the RFQ process without penalty.

9. 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.
10. The successful Offeror will be required to handle and store classified information up to the level of NATO SECRET. 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.
11. Requests for participation in this competition directly from firms without an active NCI Agency BOA cannot be considered and point 7 of this letter applies.
12. The Principal Contracting Officer for this RFQ is Rebecca Benson. The NCI Agency Point of Contact (POC) for all information concerning this RFQ is Mr. Darren Corkindale, Senior Contracting Officer (Consultant) and can be reached at email: darren.corkindale@ncia.nato.int.
13. Your assistance in this procurement is greatly appreciated.

FOR THE DIRECTOR:

[Original Signed By]

Rebecca Benson
Principal Contracting Officer

Attachment(s):

Annex A- Summary of the Requirements

Annex B – Draft Vendor List

Annex A – Summary of the Requirements

1. Introduction

To address an urgent obsolescence management requirement and facilitate technology refresh, the NCI Agency is seeking the acquisition and deployment of cyber security logging and Security Information and Event Management (SIEM) systems that are at or near End-of-Life (EoL). These systems are part of the existing NATO Computer Incident Response Centre (NCIRC) which is operated centrally at SHAPE Mons.

The objective of this acquisition is to ensure continuity of service and support by refreshing the existing logging and SIEM components of the NCIRC capability that are nearing EoL, and to enable transition to an enterprise logging solution.

2. Project Scope

The intent is to award a single contract. Interested and eligible companies may provide quotations for the requirement as a whole as follows:

- a) Partial refresh and transition of the currently deployed ArcSight Security Information and Event Management (SIEM) system to provide continuity of service until replacement of remaining ArcSight components in a future project. Activities include:
 - Upgrading and migrating existing ArcSight Enterprise Security Manager (ESM) to new hardware;
 - Deployment and configuration of ArcSight Management Center (ArcMC) to manage the ArcSight infrastructure;
 - Tuning of event management as necessary;
 - Corresponding implementation services.
- b) Deployment and configuration of Splunk Enterprise and Splunk Enterprise Security (ES), including corresponding hardware.
- c) Migration of ArcSight SIEM back-end to Splunk, including:
 - Migrating existing ESM use-cases and integrations to Splunk.
 - Configuring event transit and ingestion from ArcSight Loggers to Splunk.

The scope items above will be deployed in independent architectures for NATO Restricted, NATO Secret, and a Test/Reference environment.

3. Geographical Implementation

The NCIRC SIEM and central logging capability is operated centrally from SHAPE Mons. All scope items are wholly deployed and operated from SHAPE Mons.