Acquisition Directorate
IFB-CO-115579-CSAC@ncia.nato.int

NCIA/ACQ/2021/07319
0 1 F E B R U A R Y 2 0 2 1

Notification of Intent to an Invitation For Bid

Cryptographic Situational Awareness Capability
IFB-CO-115579-CSAC

Estimated Value: 1.2M EUR

This is a notification of an International Competitive Bidding to procure and sustain Cryptographic Situational Awareness Capability (CSAC) that will support cryptography-related business and information management processes within NATO

The Agency anticipates issuing the formal Invitation For Bid (IFB) in Q2 2022 with an anticipated Contract Award by Q1 2023. Please note that the anticipated IFB will likely have a bid closing date of approximately 60 days.

NCI Agency Point of Contact
Contracting Officer, Frank Iyakaremye
IFB-CO-115579-CSAC@ncia.nato.int

To: Distribution List

Subject: **Notification of Intent to an Invitation For Bid**
Cryptographic Situational Awareness Capability (CSAC)

IFB-CO-115579-CSAC

Reference(s): A. AC/4-(PP)D/27921-ADD1
B. AC/4-DS(2021)007 (DS)

1. The NCI Agency, as the Host Nation, hereby gives notice of its intent to issue a Invitation For Bid (IFB) to procure and sustain Cryptographic Situational Awareness Capability (CSAC).

2. The procurement will be conducted under the International Competitive Bidding (ICB) procedures.

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

4. The reference for the IFB is IFB-CO-115579-CSAC, and all correspondence concerning this IFB 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 1.2M.

6. The envisaged procurement procedure for this IFB will be the ICB procedures. The successful bid, pursuant to the IFB following this NOI, will be the bid which is the lowest price and technically compliant in accordance with the evaluation criteria prescribed in the IFB.

7. The formal IFB is planned to be issued in Q2 2022, and Contract Award is planned for no later than Q1 2023.

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. Firms from all 30 NATO Member Nations may respond to future solicitation once issued. Firms that wish to participate in this procurement must be nominated to the NCI Agency through their national delegation to NATO and such nomination must be accompanied by a **"Declaration of Eligibility" (DoE)** and certification of their security clearances executed by their national authorities. Requests for participation received directly from firms shall not be considered.

10. The closing date for additions/ nominations to the Bidders List of qualified and certified firms which may be interested in receiving an Invitation for Bid for this Project is **09 May 2022**. The 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: IFB-CO-115579-CSAC@ncia.nato.int

11. National authorities are advised that the IFB package is anticipated to be **NATO RESTRICTED**.

12. The successful Offeror will be required to handle and store classified information up to the level of **NATO RESTRICTED.** 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 CSAC contract.

13. The NCI Agency point of contact for all information concerning this NOI is Mr. Frank Iyakaremye at email: IFB-CO-115579-CSAC@ncia.nato.int

14. Your assistance in this procurement is greatly appreciated.

For the Director of Acquisition:

Frank Iyakaremye Digitally signed by Frank Iyakaremye
Date: 2022.02.01 11:36:16 +01'00'

Frank Iyakaremye
Contracting Officer

Attachment(s):

Annex A- Summary of the Requirements

Distribution List for Notification of Intent

NATO Delegations (Attn: Investment Adviser):

Albania	1
Belgium	1
Bulgaria	1
Canada	1
Croatia	1
Czech Republic	1
Denmark	1
Estonia	1
France	1
Germany	1
Greece	1
Hungary	1
Iceland	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
Montenegro	1
Netherlands	1
North Macedonia	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Turkey	1
The United Kingdom	1
The United States of America	1

Belgian Ministry of Economic Affairs 1

Embassies in Brussels (Attn: Commercial Attaché):

Albania	1
Bulgaria	1
Canada	1
Croatia	1
Czech Republic	1
Denmark	1
Estonia	1
France	1

Germany	1
Greece	1
Hungary	1
Iceland	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
Montenegro	1
Netherlands	1
North Macedonia	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Turkey	1
The United Kingdom	1
The United States of America	1

Distribution for information (Blind to Potential Industrial Suppliers):

NATO HQ

NATO Office of Resources

Management and Implementation Branch
Attn: Deputy Branch Chief 1

Director, NATO HQ Communications and Information Staff
Attn: Executive Co-ordinator 1

SACTREPEUR
Attn: Infrastructure Assistant 1

SACEUREP

Attn: Investment Assistant 1

Strategic Commands (*as applicable to funding source*)

HQ SACT Attn: ACOS C4ISR 1

ACO Attn: SPT CIS Director 1

NATEXs

All NATEXs 1 Each

Annex A – Summary of the Requirements

1. Description of Project Background

1.1. Cryptographic services protect information at strategic to tactical levels of operations, in static and deployed environments, and are implemented through hardware and software products. It is paramount for NATO to know precisely its cryptographic capability's operational state and that it is maintained to its fullest operational potential.

1.2. To meet this intent, NATO currently leverages two authoritative data sources (ADS), the Communications Security (COMSEC) Accounting, Reporting and Distribution System (CARDS) and the NATO Information Assurance Product Catalogue (NIAPC). There is typically manual correlation between the two ADS with additional inputs to produce ad-hoc COMSEC reports. This contract will provide the capability to enhance the effectiveness and efficiency of stakeholders to track, update, query and report on operational COMSEC status.

1.3. Although there are a variety of operational staff user entities, the CIS platform that is delivered by this project is to be deployed within the standard NCI Agency data centre environment and maintained at the technical level by NCI Agency staff.

1.4. As per NATO acquisition rules, NATO seeks to expand availability of the opportunity through an International Competitive Bid.

2. Description of Project Scope

2.1. The principal output of the Cryptographic Situational Awareness Capability (CSAC) will be a logical dataset, the "Allied Cryptographic Repository" (ACR). The composition of the CSAC will reflect the maturity of the Alliance's data gathering capability and shall therefore exploit the ACR and provide dashboards and reports on the following topics:

a) Cryptographic items (devices, software, personalities, keys, algorithms), including dashboards and detailed reports on their inventory (by network/operation), effectiveness, efficiency and life-expectancy;
b) Products that are or may become available for NATO usage including approval status;
c) Issues and risks (and related mitigation plans) connected with any cryptographic item in use or combination of thereof;
d) Crypto management decisions and actions, along with issue owners, actioners and deadlines;
e) Crypto device interoperability matrix; and
f) Impact analysis of planned or actual non-availability of cryptographic items and mitigation options based on availability of alternative cryptographic solutions.

2.2. The scope of work supplied in this contract shall include:

a) The establishment of an appropriate Information Management Application, called the Cryptographic Situational Awareness Tool (CSAT), that will interface with relevant authoritative data sources;
b) The development of the solution according to a pre-agreed project methodology;
c) The conduct of the testing, providing supporting evidence that the solution meets the requirements;
d) O&M years 1 through 5 exercisable at the discretion of the Host Nation;
e) System documentation; and
f) Training material.

3. Description of Operational/Functional Requirements

3.1. Data entry and manipulation interfaces including import and export from database tables and generation of local copies to be distributed to users without direct access to the CSAC.
3.2. Detailed access controls to map authorization of individual users to allow tailored user identification and authentication.
3.3. Flexible modification and configuration of the data model.
3.4. Availability of standard (pre-configured) and customizable queries, views and reports.
3.5. Process to tracking risks, issues, actions and management decisions including notification to the stakeholders about assigned tasks and actions.
3.6. Document storage that allows to store internal to CSAC and linking to documents both internally and externally.
3.7. Provides product catalogue including products that are approved or under assessment, and details their current or planned usage (e.g. network, systems, operations, etc.).

4. Implementation Strategy

4.1. To the greatest extent possible, the Contractor will design the solution leveraging existing applications on the Approved Fielded Product List (AFPL). An overall architecture will be proposed by the Contractor and agreed with the NCI Agency.
4.2. The solution will be designed by the Contractor and will be subject to intermediate reporting and a Factory Acceptance Test (FAT), before being accepted by the NCI Agency for implementation.
4.3. The capability will be installed and hosted on existing Core Enterprises Services virtual platform infrastructure.
4.4. Vulnerability testing and any remediation will be carried out as part of the Change Management process.
4.5. The solution will be procured and maintained by NATO as per a NATO Owned / NATO Operated (NONO) scenario.
4.6. Contractor’s internal Life Cycle Management (LCM) process and system will be required to comply with STANAG 4728 “System Life Cycle Management (SLCM)”.