Acquisition Office
NCIA/ACQ/2026/16890

NOTIFICATION OF PROCUREMENT OPPORTUNITY (NPO)
Pre-Solicitation Notice
NATO Competitive Procurement

Open-Source Intelligence (OSINT) Capability

NCIA Reference #: IFB-CO-424330-OSINT

Date of NPO Publication: 13/11/2026

Anticipated Solicitation Release Date: 25/01/2027
Anticipated Solicitation Closing Date: 26/04/2027
Anticipated Contract Award Date: 01/09/2027

Rough Order of Magnitude[1]: Investment: EUR 8,636,325; Operations: EUR 55,328,254

Point of Contact: Nicholas Griffin, Senior Contracting Officer
IFB-CO-424330-OSINT@ncia.nato.int

[1] This Rough Order of Magnitude is informational only and reflects NCIA's estimate. Actual contract value may vary based on competitive submissions.

Introduction

The NATO Communications and Information Agency (NCIA) hereby notifies the following Procurement Opportunity in accordance with the Procedure for NATO Competitive Procurement (link). This notification is issued to foster open and fair competition among eligible vendors from participating nations. This notification does not constitute a commitment to award a contract.

Vendors are invited to review the requirements described herein and to submit their bids in accordance with the instructions provided in this notification and subsequent solicitation documentation. All interested vendors are reminded that timely registration and compliance with eligibility requirements are essential, as deadlines for submission may not be extended. Vendors are advised to regularly check for updates to this notification.

This opportunity reflects NATO's commitment to transparency, equal treatment of suppliers, and the efficient delivery of goods, works, and services in support of NATO missions and participating nations.

All eligible and responsible sources may submit a quotation, bid, or proposal, which shall be considered by the NCIA.

1. Title of Procurement Opportunity

Open-Source Intelligence (OSINT) Capability

2. Description of Requirement

2.1. Background

NCIA requires a common capability for NATO OSINT analysts, with which to collect, process and exploit publicly and commercially available information (PAI/CAI) to produce OSINT. This capability supports NATO's mission to better understand the operational environment, support decision-making and enable cognitive superiority.

2.2. Scope & Deliverables

The OSINT project aims to deliver a capability to NATO analysts from Q1 2028.

NCIA seeks to procure:

- A front-end platform and data broker capability, competed as one contract, which will provide a single point of entry for all OSINT services, processing and exploitation capabilities.
- The successful vendor will act as a broker to provide a best-of-breed solution, harnessing subcontractors and/or consortium partners to provide the full range of required capabilities.
- This front-end platform and data broker capability will be competed as a service, with an industry partner providing the user facing platform, data and analytics required, initially for a period of one (1) year, with options to extend for a further five (5) one-year options (1+1+1+1+1 years).

The target vendor for the Unclassified OSINT capability contract is:

- A vendor acting as a Prime broker that can provide a COTS OSINT software as a service (SaaS) capability on the unclassified domain.
- A vendor that has an established online platform, and B2B contracts with the main commercial data vendors.

2.2.1. **User-Facing/Front-End Platform**

The OSINT front-end platform comprises all required functions to support an OSINT Analyst to search, find, collect, process, and retrieve PAI/CAI in a secure and non-attributable way from sources within the Internet. The following is a list of the required functionalities of the envisioned OSINT front-end platform:

- **Managed Attribution (MA):** The managed attribution service provides a way for the intelligence analyst in the collection phase to browse the Internet while customizing its online presence. This capability will resolve: inconsistencies between operating system language and VPN egress point; keyboard and device layout; and fingerprinting techniques meant to track users, beyond the use of cookies or IP addresses.
- **Secure Unclassified OSINT website:** This will provide forums for discussion; sharing of tradecraft and knowledge; sharing of releasable data; and enable collaboration with wider NATO partners, classification and policy allowing.
- **Collaboration space:** Analysts must have the ability to share data and assessment both within and between teams if required.
- **Report Writing Tool:** Analysts must have the ability to create reports on the unclassified environment. This report creation tool must provide the ability to receive automated summaries, automatic formatting, translation, annotation of embedded data, automated referencing and other tools as requested by analysts.
- **User querying and alerting capability:** Analysts must have the ability to set “indicators and warning”-type queries on topics or areas of interest and to receive regular updates and cueing for further research as required, from all available data sources and services.
- **Tasking tools:** Managers and analysts must have the ability to receive and forward tasks, both up and down the chain, to allow for allocation of tasks according to resources and for quality review prior to release.

The OSINT platform will provide tiered access to users:

Tier 1 Users	Tier 2 Users	Tier 3 Users
Around **400** generalist analysts	Around **300** fusion analysts	Around **120** trained OSINT analysts
• Managed Attribution (MA).	• Managed Attribution (MA); • User querying and alerting capability.	• Managed Attribution (MA); • User querying and alerting capability; • Report Writing Tool;

		• Tasking Tools; • Secure Unclassified OSINT website; • Collaboration space.

2.2.2. **Data Sources and Services**

The OSINT data sources and services can be split into two (2) types: foundational PAI/CAI services and more specialist tools and services across Tier 2 and 3 users. The following is a non-exhaustive list of the main categories of required data sources:

Tier 2 & 3 Users	Tier 3 Users
• Traditional media, blogs, forums, periodicals, grey literature; • Social media (e.g. Facebook, X, Instagram, Tiktok, LinkedIn, weibo, Renren, VK, Odnoklassnik).	• Niche social media (e.g. Parler, Mastedon, GAB, Truth Social); • Secure messaging platforms (e.g. Telegram, Whatsapp, weChat, etc.); • Ad-tech data; • Deep and Dark web (Tor); • Internet of Things (IoT) data; • Financial data (including blockchain, crypto etc.); • Cached websites, archived or deleted webpages; • Cyber threat data.

As the OSINT landscape evolves, NCIA will expect its service providers to keep up-to-date with emerging sources and be able to integrate them into the platform as required.

2.2.3. **Analytic Functions**

There is the need to enrich, process and exploit relevant collated PAI/CAI data. The following is a non-exhaustive list of the main categories of required analytic functions, using the latest AI, tools and capabilities:

Tier 1 Users	Tier 2 Users	Tier 3 Users
• Translation and transcription services; • Screen capture service;	• All Tier 1 capabilities; • Query-setting for effective data collection; • Automatic summarization; • Automated geolocation; • Geolocation extraction; • Optical Character Recognition (OCR).	• All Tier 1 & 2 capabilities; • Heatmap/cluster generation; • Anomaly detection; • Data enrichment; • Deepfake recognition; • Named Entity Recognition (NER) and automatic classification; • Network analysis.

As the OSINT landscape evolves, NCIA will expect its service provider to keep up to date with emerging OSINT technologies and advancements in AI tools, and be able to integrate them into the platform as required.

2.2.4. **Non-Functional Requirements**

- As the OSINT landscape evolves, NCIA will expect its service providers to keep up to date with emerging data sources/services and processing capabilities;
- A strong emphasis on cyber security. The potential vendor will have to demonstrate their adherence to the strictest cyber security principles and provide audit reports;
- A user management panel for NCIA and NATO functional administrators, allowing to manage accounts, groups and permissions for the user-facing data-provider(s);
- A documented log for all services, to enable traceability for security and monitoring purposes. allowing secure automation and orchestration of all services features;
- Provision of training, which includes delivery of train-the-trainer, user (and administrator) trainings, and all training documentation.

2.3. Objectives

This OSINT capability will enable analysts, amongst other activities, to:

- Set and receive alerts and notifications based on areas or topics of interest across multiple data sets and services;
- Focus their research and receive alerts on emerging topics of interest;
- Securely conduct their own research directly on the open web without attribution, tailoring their digital footprint effectively;
- Receive and forward tasking;
- Collaborate both within and between teams;
- Draft reports;
- Access an automated source registry capability;
- Automatically enrich data for onward processing and exploitation as needed.

While providing these capabilities, NCIA is aiming to:

- Maximize the participation of the data services market, as opposed to running its own analytic platform;
- Limit custom development to focus on proven industry solutions;
- Have one primary contract covering all capabilities outlined in the Scope.

2.4. Options (Extensions & IDIQ Mechanism)

As noted in section 2.5 below, this project envisages a one-year Base Contract and five (5), one-year options for extension by the Purchaser.

In addition to potential time extensions, the Purchaser intends to include additional Tier 1 to 3 user numbers as part of the evaluated options, as an Indefinite Delivery Indefinite Quantity (IDIQ) mechanism, to include potential scalability of the OSINT capability up to 5,000 users, subject to exercise by the Purchaser.

Please note, the Base Contract will only require the user numbers in section 2.2.1.

2.5. Indicative Project Timelines

Milestone	Milestone Description	Duration	Anticipated Completion Date
T0	Anticipated Solicitation Release Date	N/A	Jan 2027
T1	Anticipated Contract Award	T0 + 8 Months	Sep 2027
T2	Effective Date of Start	T1 + 1 Months	Oct 2027
T3	Initial Operational Capability (IOC)	T2 + 3 Months	Jan 2028
T4	Full Operational Capability (FOC)	T3 + 12 Months	Jan 2029
T5	Operations: Sustainment (Option – Year 1)	T4 + 12 Months	Jan 2029 – Dec 2029
T6	Operations: Sustainment (Option – Year 2)	T5 + 12 Months	Jan 2030 – Dec 2030
T7	Operations: Sustainment (Option – Year 3)	T6 + 12 Months	Jan 2031 – Dec 2031
T8	Operations: Sustainment (Option – Year 4)	T7 + 12 Months	Jan 2032 – Dec 2032
T9	Operations: Sustainment (Option – Year 5)	T8 + 12 Months	Jan 2033 – Dec 2033

3. Vendor Eligibility

3.1. Participation in this Procurement Opportunity is restricted to vendors from participating NATO nations.

3.2. This restriction applies to the eligibility of the vendors only and does not require that the goods, works, or services themselves be manufactured or produced within participating nations.

4. Access to Solicitation Documentation

4.1. Interested vendors may participate to and access the solicitation documentation for this Procurement Opportunity as of the Anticipated Solicitation Release Date as follows:

i. Vendors must obtain a valid Declaration of Eligibility (DoE) through their National Authorities in order to be included in the Bidder's List and to participate should the solicitation be issued.

ii. A template of the DoE is provided in the Annex to this NPO for reference and completion.

iii. The prospective Bidder is responsible for arranging for their National Authority to complete the form. The signed DoE must be transmitted directly by the National Authority to the Point of Contact (PoC) identified in this NPO.

iv. The DoE must be received by NCIA's PoC not later than 11 January 2027.

v. Prospective Bidders are advised to initiate this process early, as NCIA cannot request or obtain a DoE on behalf of a prospective Bidder. Failure to ensure that a valid DoE has been received by the PoC may result in exclusion from the solicitation process.

vi. NCIA will verify the Declaration of Eligibility statements received from the National Responsible Authorities and will invite the nominated qualified and certified companies to access the Solicitation Documentation via email from the OSINT mailbox, **IFB-CO-424330-OSINT@ncia.nato.int**.

5. Security Requirements

5.1. This opportunity is classified as NATO UNCLASSIFIED (NU) and interested vendors are required to meet the above-mentioned security level.

6. Language of Solicitation and Bid Submission

6.1. Solicitation Documentation and Proposal Submission Language(s): English

7. Additional Engagement Opportunities

7.1. The NCIA may organize the following engagement activities:

7.1.1. **Industry Engagement:** 18 Nov 26 – An OSINT Data Exploitation and Visualisation Workshop will be held at NATO Edge, Izmir, Turkiye. For suppliers not able to attend, slides will be published on the NCIA website after the event.

End of Notification

Nicholas Griffin

Digitally signed by Nicholas Griffin
Date: 2026.11.13 14:42:47 +01'00'

Annexes:
Annex 1 to IFB-CO-424330-OSINT Distribution List
Annex 2 to IFB-CO-424330-OSINT DoE Template

ANNEX 1

Distribution List

1. NATO Delegation (Attn: Infrastructure Adviser)

1. Albania
2. Belgium
3. Bulgaria
4. Canada
5. Croatia
6. Czechia
7. Denmark
8. Estonia
9. Finland
10. France
11. Germany
12. Greece
13. Hungary
14. Iceland
15. Italy
16. Latvia
17. Lithuania
18. Luxembourg
19. Montenegro
20. Netherlands
21. North Macedonia
22. Norway
23. Poland
24. Portugal
25. Romania
26. Slovakia
27. Slovenia
28. Spain
29. Sweden
30. Türkiye
31. United Kingdom
32. United States

2. All NATEXs

NATO Communications and Information Agency (NCIA)

Acquisition Office
NCIA/ACQ/2026/16890

ANNEX 2

Date:

Declaration of Eligibility for NATO Competitive Procurement[2]

To: NCIA Procurement Authority

Subject: Declaration of Eligibility for NATO Competitive Procurement

Reference: Solicitation Number:

This Declaration of Eligibility (DoE) must be read in conjunction with the Notice of Procurement Opportunity (NPO), or other applicable solicitation document, which may include opportunity-specific or additional DoE requirements.

1. With reference to the above-mentioned NATO Competitive Procurement (NCP) opportunity, the following *[insert Country of Origin]* vendor has expressed an interest in receiving the solicitation document:

   a. Vendor Name:

   b. Address:

   c. Point of Contact/Title: Mr./Ms.:

   d. Email Address:

   e. Phone #:

2. I certify that this vendor has the necessary financial, technical and professional competence to be admitted by the Government of *[insert Country of Origin]* as a bidder were it responsible for awarding a contract of this nature. The vendor listed above is eligible to initiate the process required to be security cleared to up to *[insert NATO Security Classification]*.

_____

Signature
[Name of National Responsible Authority]
[insert Country of Origin]

[2] The DoE should be substantially similar to this sample. Prospective Bidders should provide the relevant information about their company to their National Authority.