NCIA/ACQ/2026/07399
Friday, 03 July 2026

NCIA Request for Information (RFI)

To: **Industry Partners**

Subject: **MALWARE ANALYSIS AND DETECTION ENGINEERING PLATFORM**
RFI-424358-TSSU-MA-DE

1. The NATO Communications and Information Agency (NCIA) is conducting market research to identify qualified vendors and gather input on potential solutions to support the upcoming acquisition for a Malware Analysis and Detection Engineering Platform. To that end, we are issuing the attached Request for Information (RFI) 424358 to solicit feedback from capable and interested industry partners.

2. This RFI is issued for planning and budgeting purposes only and is not a request for bids. It is part of NCIA's effort to ensure it has a clear understanding of the marketplace, available capabilities, estimated costs and potential acquisition strategies.

3. We value your insight and invite you to:
- **a.** Share relevant corporate capabilities and experience;
- **b.** Review and comment on our draft requirements (Annexes A & B) with a view in providing recommendations for improving performance outcomes, competition, and efficiency; and identifying any risks or concerns that should be considered during planning.

4. Submission instructions and additional details can be found in the enclosure to this RFI.

5. Only companies from a NATO member country can participate in or respond to this RFI (https://www.nato.int/cps/en/natohq/nato_countries.htm).

6. Should you have any questions or need clarification, please contact Leonora Alushani, Contracting Officer at RFI-424358-TSSU-MADE@ncia.nato.int.

7. We thank you in advance for your time and input, and we look forward to engaging with you as we shape this potential acquisition.

For the Chief of Acquisition:

Leonora Alushani
Contracting Officer

Enclosure:

- Request for Information with Annexes A, B & C
- Distribution List

Distribution List

1. NATO Delegation (Attn: Infrastructure Adviser)

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

2. All NATEXs

NATO Communications and Information Agency

Table of Contents

REQUEST FOR INFORMATION 4

A. Introduction 4

B. Purpose 4

C. Background 4

D. Submission Instructions 5

E. Disclaimer 5

F. Use of Information Provided through Responses 6

G. RFI Point of Contact 6

Annex A – Requested Information 7

Annex B – Epics and User Stories ..... **Error! Bookmark not defined.**

Annex C – Response Template ..... **Error! Bookmark not defined.**

REQUEST FOR INFORMATION

A. Introduction

1. The NATO Communications and Information Agency (NCIA) is conducting market research to identify potential sources and gather information regarding industry capabilities to support a Malware Analysis and Detection Engineering Platform. This Request for Information (RFI) is issued solely for informational and planning purposes and does not constitute a Request for Proposal (RFP), Request for Quotation (RFQ), or invitation for bid.

B. Purpose

1. The purpose of this RFI is to obtain input from industry to help inform the NCIA's acquisition planning. Responses to this RFI will assist in refining requirements, identifying capabilities, budget planning and shaping the strategy for any future solicitation.

C. Background

1. Malware analysis within NCIA is performed by the NCSC Cyber Threat Investigation Section. The section provides in-depth cyber threat analysis, malware analysis, and digital forensics in support of incident response activities, as well as proactive efforts to identify and investigate cyber threat activity. Its work supports the development of actionable cyber threat information to strengthen the defensive posture of the NATO Enterprise and NATO Operations and Missions networks.
2. Within this section, the service provides technical analysis capabilities in response to cybersecurity incidents and other cyber investigation requirements. This includes both digital forensics and malware analysis. The service is often engaged where more advanced or specialized technical analysis is required, comparable to a higher-tier technical support function for cyber investigations.
3. In addition to incident response, the team conducts continuous service improvement activities and maintains the specialized skills required to keep pace with evolving adversary techniques, including methods intended to hinder forensic examination, malware reverse engineering, detection engineering, and technical analysis.
4. The current malware analysis capability is supported by a distributed ecosystem of tools and environments. This includes a small cloud-based foothold used to receive suspicious samples, store analysis artefacts, and access general IT capabilities such as team collaboration and source code versioning. Suspicious samples may be received through a dedicated mailbox and are analysed using isolated workstations that are disconnected from NATO networks.
5. Analysis activities are typically performed using purpose-built virtual machines, including static analysis environments, dynamic analysis or victim environments, and anonymization environments used to access external or higher-risk resources where required. The team also makes use of commercial tools, vendor-provided documentation, and capabilities provided by other NATO entities and partner nations, often delivered as Software-as-a-Service.
6. The team also uses an automated malware analysis platform to support the automated detonation, triage, and enrichment of suspicious files and related artefacts. This RFI is not primarily seeking to replace that automated malware analysis capability. Respondents should therefore focus their feedback on the capabilities described in the

attached Epics and User Stories, rather than assuming that the objective is to replace every element of the existing malware analysis ecosystem.

7. On premises, the team uses Jira to receive, manage, and report on malware analysis tasks; Confluence to document procedures, findings, and threat knowledge; and Splunk to support case-by-case research of logs and other telemetry, particularly in proactive investigation scenarios.
8. This RFI seeks industry feedback on how a future Malware Analysis and Detection Engineering capability could be delivered primarily as a fully managed service, implemented and maintained by the Contractor. The intended outcome is to enable Purchaser personnel to perform secure malware analysis, detection engineering, and related workflows with minimal administrative effort, while making use of Commercial-Off-The-Shelf products, standard service capabilities, and limited customization wherever feasible.

D. Submission Instructions

1. Interested parties are invited to respond in accordance with the instructions below:

   a. Submit responses via the email address in section G no later than **12:00 hours Central European Time (CET)** on **17 July 2026**.

   b. Responses should be submitted using the Excel Response template provided in Annex C

   c. The following can be included as a reference in your responses and attached as separate documents:
      i. Company brochures or product literature (optional)
      ii. Attachments such as past performance references (optional)

   d. Use the following subject line for submission
      i. “Response to RFI [424314-NPKI-TPT] – [Company Name]”

   e. All responses should address the items listed in Annex A – Requested Information.

E. Disclaimer

1. This RFI is for planning and informational purposes only and shall not be construed as a solicitation or obligation on the part of the NCIA. The NCIA does not intend to award a contract based on responses to this RFI. Respondents are solely responsible for all costs incurred in responding to this RFI. The NCIA will consider and analyse all information received from this RFI and may use these findings to develop a future solicitation. The NCIA will consider all responses as confidential commercial information and will protect it as such.

2. NCIA reserves the right, at any time, to cancel this informal market survey, partially or in its entirety. No legal liability on the part of NCIA for payment of any sort shall arise and in no event will a cause of action lie with any prospective participant for the recovery of any costs incurred in connection with the preparation of documentation or participation in response hereto. All effort initiated or undertaken by prospective informal market survey participants shall be done considering and accepting this fact.

F. Use of Information Provided through Responses

1. Confidentiality of Responses

The NCIA may incorporate industry comments and responses, in part or in whole, into a future release of a solicitation. Should respondents include proprietary data in their responses that they do not wish to be disclosed to the public for any purpose, or used by NCIA (except for internal evaluation purposes), they must:

a. Mark the title page with the following legend:

This document includes data that shall not be disclosed outside NATO and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than for NCIA internal evaluation purposes, unless otherwise expressly authorised by [insert company name]. This restriction does not limit the NCIA's right to use information contained in this data without restriction if it is obtained from another source. The data subject to this restriction are contained in sheets [insert numbers or other identification of sheets]

b. Mark each sheet of data it wishes to restrict with the following legend:

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

G. RFI Point of Contact

1. Leonora Alushani

2. RFI-424358-TSSU-MADE@ncia.nato.int. .

Annex A – Requested Information

A.1 Purpose and Desired Outcome
The purpose of this Request for Information is to obtain industry feedback on the attached draft Epics and User Stories for a Malware Analysis and Detection Engineering capability, provided in Annex B.

The Purchaser's intent is to validate whether the required operational outcomes can be achieved primarily through existing Commercial-Off-The-Shelf products, standard managed service offerings, configuration, and limited integration wherever possible. The Purchaser does not intend to drive the requirement toward a fully custom-developed solution unless industry feedback demonstrates that this is necessary to achieve the required operational outcomes.

The desired outcome of this RFI is to help the Purchaser refine the attached Epics and User Stories before any potential future solicitation. Industry feedback should help determine whether the required capability can be achieved through existing products and standard managed service offerings, whether the requirements should be adjusted to better align with market capabilities, and where customization or bespoke development may create avoidable cost, complexity, or risk

Respondents are requested to review the Epics and User Stories provided in Annex B and provide structured feedback using the response template in Annex C. Response should focus on practical product capability, managed service delivery, implementation approach, risks, constraints, and recommendations.

Marketing material may be included as supporting information; however, respondents are invited to complete the response template in Annex C to allow consistent comparison of industry responses.

A.2 Scope of Requested Feedback
Respondents are requested to provide feedback on the degree to which their proposed product, platform, service, or combination thereof aligns with the attached Epics and User Stories.

The Purchaser is particularly interested in understanding:

1. Which Epics or capability areas are well supported by the respondent's existing Commercial-Off-The-Shelf products or standard managed service offerings.
2. Which capabilities can be achieved through standard configuration.
3. Which capabilities would require customization, integration, professional services, or bespoke development.
4. Which capabilities are not supported.
5. Which User Stories may be too specific, unnecessarily complex, or misaligned with common product or managed service capabilities.
6. What alternative approaches the respondent would recommend where a User Story is not supported, and why the alternative would better achieve the underlying operational intent.
7. Whether there are industry-standard capabilities, workflows, or product features that should be considered but are not currently reflected in the Epics and User Stories.
8. How the capability would be implemented, operated, maintained, upgraded, and supported by the Contractor.

9. How licensing, renewal, sustainment, support, and service management would typically be structured.

A.3 Response Approach

To reduce response burden and support meaningful comparison across submissions, respondents should first provide feedback at the Epic or capability level.
Detailed User Story-level responses are only required where:

- the capability is not supported natively by the proposed product, platform, or service;
- the capability would require customization;
- the capability would require significant integration;
- the respondent recommends an alternative approach;
- the User Story creates implementation complexity, cost, risk, vendor lock-in, or technical constraints; or
- the User Story should be clarified, consolidated, removed, reprioritized, or reframed.

Respondents should avoid treating the attached User Stories as a compliance matrix. The Purchaser is seeking industry feedback on the feasibility, maturity, and suitability of the required capabilities, including whether the User Stories should be adjusted to better align with existing Commercial-Off-The-Shelf products and standard managed service models.

A.4 Areas of Interest

Respondents are requested to address the following areas in their response and to prioritize responding to A.4.1 through A.4.4, responding to the other areas when applicable and time permitting.

A.4.1 Overall Fit

Respondents should provide a summary of the overall fit between the attached Epics and User Stories and their proposed solution or service. This should include areas of strong alignment, areas of partial alignment, and areas that are not supported or would require significant adaptation.

A.4.2 COTS and Managed Service Alignment

Respondents should identify which capabilities are available through existing Commercial-Off-The-Shelf products, which are available through standard managed service offerings, and which would require configuration, integration, customization, or professional services.

A.4.3 User Story Exceptions, Gaps, Risks, and Recommended Changes

For User Stories that are not fully supported, or where the respondent recommends a different approach, respondents should identify the relevant User Story, describe the issue or gap, and provide a recommended approach.
Relevant feedback may include, but is not limited to:

- the User Story is not supported;
- the User Story is partially supported;
- the User Story requires configuration;
- the User Story requires customization;
- the User Story requires third-party integration;
- the User Story assumes a custom workflow rather than a standard product or service workflow;

- the User Story may introduce unnecessary cost, complexity, risk, or vendor lock-in;
- the User Story should be clarified, consolidated, removed, or reprioritized; or
- the operational intent could be achieved through an alternative product capability, workflow, or managed service approach.

A.4.4 Recommended Additional Capabilities
Respondents should identify any industry-standard capabilities, workflows, or service features that are not reflected in the attached Epics and User Stories but should be considered by the Purchaser.

A.4.5 Implementation, Operation, and Sustainment
Respondents should describe how a comparable capability would typically be implemented, transitioned into service, operated, maintained, and upgraded. This should include key Purchaser responsibilities, key Contractor responsibilities, common dependencies, implementation risks, training considerations, and sustainment considerations.

A.4.6 Configuration, Customization, and Integration
Respondents should describe which capabilities can typically be configured by the Purchaser or Contractor, which changes would require vendor professional services, which changes would require custom development, and how customizations or integrations are maintained through upgrades.
Respondents should also identify relevant APIs, connectors, import/export mechanisms, and integration patterns applicable to the proposed solution or service.

A.4.7 Licensing, Renewal, and Support Model
Respondents should describe the typical licensing, renewal, support, and service model for the proposed capability. This should include relevant licensing metrics, support tiers, software update arrangements, renewal model, optional modules or add-ons, and any separate costs for implementation, migration, training, integration, or sustainment.