NCIA/ACQ/2026/07313
Thursday, 18 June 2026

NCIA Request for Information (RFI)

DESIGN AND IMPLEMENTATION OF CENTRALISED ENCRYPTED TRAFFIC INTERCEPTION SYSTEM

RFI-424365-CETIS

NCIA Request for Information (RFI)

To: Industry Partners

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 Encrypted Traffic Interception (ETI) solutions. To that end, we are issuing the attached Request for Information (RFI) 424365 to solicit feedback from capable and interested industry partners.

2. This RFI is issued for planning 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, 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 (Annex A) 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 Burak Oguz at RFP-CO-424365-CETIS@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:

Burak Oguz

Digitally signed by Burak Oguz
Date: 2026.06.18 15:18:20 +02'00'

Burak Oguz
Senior Contracting Officer

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**

Table of Contents

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 the requirement to create an accurate and current view of the state-of-the-art Encrypted Traffic Interception (ETI) solutions that can be provided through Commercial of the Shelf (COTS) products, solutions and/or services. This Request for Information (RFI) is issued solely for informational 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, and shaping the strategy for any future solicitation.

C. Background

1. The purpose of this Request for Information (RFI) is to create an accurate and current view of the state-of-the-art Encrypted Traffic Interception (ETI) solutions that can be provided through Commercial of the Shelf (COTS) products, solutions and/or services. The feedback received through the RFI will be used to evolve existing capabilities in NATO and define future needs. The inputs will be used to help NATO define future requirements within these capabilities and to shape future acquisitions. Responses should focus on current mature solutions, products or services, although responders are also provided an opportunity in a separate section to volunteer details of evolutionary plans and future roadmaps.

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 **08 July 2026**.

   b. Responses should be submitted in PDF or Word format and must not exceed **15 pages**, including:
      i. Responses to Annex A
      excluding:
      i. Cover page
      ii. Company brochures or product literature (if included)
      iii. Attachments such as past performance references (optional)

   c. Use the following subject line for submission
      i. "Response to RFI [424365] – [Company Name]"

d. 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. Burak Oguz , Senior Contracting Officer

2. RFP-CO-424365-CETIS@ncia.nato.int

Annex A – Requested Information

1. Respondents are encouraged to provide the following information in their response:

   a. **Company Information**
      - **i.** Legal Business Name
      - **ii.** Address
      - **iii.** Website
      - **iv.** Primary Point of Contact
      - **v.** Email address

   b. **Technical Capability**
      - **i.** Brief summary of relevant capabilities and past performance

   c. **Feedback and Recommendations**
      - **i.** Responses to the following RFI Questions detailed under section 2

2. **Requested Technical Support**

   2.1 Respondents are encouraged to provide the related information in their response under the following categories. Categories are marked with an indicative priority (Priority 1 > Priority 2 > Priority 3). If responses are incomplete due to any constraints on the responder side, this prioritisation indicates NCIA preferred order of completeness and detail level. It is expected to have responses for Categories at least under Priority 1.

   2.2

   2.2.1 **Company overview (Priority 3):** Particular interest goes out to ETI solutions and your experience providing them to Defense industries and international organizations such as the EU and NATO.

   2.2.2 **Solution overview and deployment model (Priority 1):** Overview of ETI products suite, providing details related to the architectural design, central management, the use and deployment of components, scalability and cloud integration.

   2.2.3 **Product features and capabilities (Priority 1):** Functions and capabilities provided by the ETI products suite, detailing unique features, coverage, and performance indicators.

   2.2.4 **Data collection, processing and storage (Priority 1):** Types of data that can be collected, processing methods, and details related to how data is stored and secured.

   2.2.5 **Threat intelligence and threat hunting (Priority 2):** Overview of threat intelligence integration capabilities; of particular interest are (1) feeds provided through your team and solution, and (2) integration of external feeds through industry exchange standards.

   2.2.6 **Policy management (Priority 1):** Overview of policy and playbook management. Specific interest goes out to privilege management, central vs. per site policy application, customization of policies and playbooks, and version control.

   2.2.7 **System integration (Priority 1):** Integration capabilities of the ETI suite with other (security) systems. Please detail both integration with own products and features as well as those provided by other vendors.

2.2.8 **Tool security (Priority 2):** Security functions and measures taken to guarantee the security of the system and its data.

2.2.9 **Management (Priority 2):** The means and mechanisms included to manage the ETI product suite, with a specific interest for large distributed implementations with a large number of stakeholders.

2.2.10 **Support, maintenance and service provisioning (Priority 3):=:** Services provided to ensure an optimal and up-to-date solution.

2.2.11 **Cost and licensing (Priority 3):** Breakdown of indicative pricing and licensing of the ETI product suite, including on-demand scaling requirements.

2.2.12 **Roadmap and future development (Priority 2):** Planned products and features in the near-future with associated timelines.

2.3 Respondents are encouraged to provide answers to the questions under the related categories;

2.3.1 **Company overview (Priority 3)**

2.3.1.1 Can you elaborate on your company's experience and track record in providing cyber security solutions and services to Defense industries and international organizations such as the EU or NATO?

2.3.1.2 What is your experience in providing ETI solutions?

2.3.1.3 Please provide any third-party evaluation of your products suite, if available (e.g. MITRE, Gartner, Forrester, …)

2.3.1.4 Please indicate relevant regulatory compliance standards or industry standards applicable to your solution or company

2.3.2 **Solution overview and deployment model (Priority 1)**

2.3.2.1 Please provide an overview of your product suite relevant to ETI functionality.

2.3.2.2 What does the system architecture of the solution look like (e.g. use of components, centralized control, data collection/feeds, …)?

2.3.2.3 Does the system architecture allow high-availability / redundancy / load-balancing scenarios within a single site or across multiple sites (e.g. two data centres)?

2.3.2.4 What types of platforms and types does your solution support (e.g. network types, hosting models, component types such as physical appliance, container, cloud service)?

2.3.2.5 How does your solution scale, particularly for large dynamic enterprise environments with thousands of endpoints?

2.3.2.5.1 What are the central infrastructural requirements regarding total event throughput and data volume regarding the scalability constraints?

2.3.2.5.2 What are the supported interface scales ? (e.g. 10 Gbps, 100 Gbps)

2.3.2.5.3 How is the solution’s performance affected by the scaling of the number of endpoints / interfaces?

2.3.2.6 What is the estimated size of the team required to manage the solution?

2.3.2.7 Does your solution cover cloud footprints such as Microsoft Azure and Amazon Web Services?

2.3.2.8 Please explain Cloud Deployment categories: SaaS, PaaS, IaaS, etc

2.3.2.9 Does the solution require cloud connectivity? If so, how, and to what extent, does it rely on it?

2.3.2.10 Does the solution allow for air-gapped (non-internet connected) and/or hybrid networks?

2.3.3 Product features and capabilities (Priority 1)

2.3.3.1 Can you elaborate on the specific functions that your ETI solution is able to provide?

2.3.3.2 Which protocols is your ETI solution able to intercept ?

2.3.3.3 What kind of detection / response actions are possible ?

2.3.3.4 Can the solution extract / forward content to other systems for further inspection or storage?

2.3.3.5 What alerting actions does your solution support, and how do you deal with True/False Positive/Negative trade-offs?

2.3.3.6 What manual and what automated response actions does your solution support (e.g. user account actions, file actions, network interface actions, payload modification,…)?

2.3.3.7 What customization does your tool allow for (e.g. custom detection, analysis or response actions)? Please detail the mechanism and available options (e.g. GUI, query language, support for custom scripts/binaries, …)

2.3.3.8 How does the solution handle the detection of both known and unknown (e.g. zero-day) threats?

2.3.3.9 What forensics capabilities does the solution provide (e.g. types of data, analysis capabilities, workflows, playbooks, …)?

2.3.3.10 What are the resource requirements for the solution (per interface type, preferably including performance charts)?

2.3.3.11 What are the correlation abilities or other central analysis capabilities to observe behaviours across multiple (types of) interfaces?

2.3.3.12 What network / session activity does the solution record and use to detect threats? E.g.:

2.3.3.13 Which enforcement / containment mechanisms are available?

2.3.3.14 Is the detection logic provided by the vendor open to review/inspection to better understand the behaviour?

2.3.4 Data collection, processing and storage (Priority 1)

2.3.4.1 What types of data can be collected (e.g. users logs, network connections, browsing history, system logs, …)?

2.3.4.2 Can you expand on how data is collected, processed and stored?

2.3.4.3 Where can or does the tool do its analysis, including correlations: centralized, in the network component, or both?

2.3.4.4 Are there any specific constraints regarding data retention; what parameters can be configured (e.g. time, data size, subset of targets or destinations, …)?

2.3.4.5 What logs are or can be generated in the ETI system itself (e.g. activity logs)?

2.3.4.5.1 Are there features for tracking and documenting actions taken during the incident response process by users/automated playbooks?

2.3.4.6 What anti-tampering measures are used to protect the data integrity?

2.3.4.7 Can all collected data be retrieved from the solution via an API or otherwise?

2.3.5 Threat intelligence and threat hunting (Priority 2)

2.3.5.1 What are the information exchange methods offered to provide threat information updates to the purchaser teams and the implemented solution?

2.3.5.1.1 What is the frequency of such communications?

2.3.5.1.2 How are isolated networks kept up to date?

2.3.5.2 What threat intelligence feeds are readily supported by the solution (e.g. existing feeds and supported standards such as MISP, STIX or TAXII)?
2.3.5.3 What are the options for creating custom threat intelligence feeds, importing indicators of compromise (IOCs) and adding new standards?
2.3.5.4 What methodologies does your solution employ to detect and identify new threats (threat hunting)?

2.3.6 Policy management (Priority 1)
2.3.6.1 Please explain the different roles available in your solution for policy management hierarchy / delegation model (e.g. central policy definition vs. per site policy application).
2.3.6.2 Can you explain the process of centrally managing policies, including dealing with site or component specific deviations compared to a standard baseline configuration?
2.3.6.3 How can a user specify custom policies and/or playbooks?
2.3.6.4 How does your tool deal with version control of policies? In the case of site or endpoint specific deviations, would changes be overwritten with the next content update?

2.3.7 System integration (Priority 1)
2.3.7.1 Please explain the integration / interfacing capabilities (e.g. API, data formats) of your solution to:
2.3.7.1.1 External Identity and Access Management (IAM) (e.g. Microsoft AD)
2.3.7.1.2 External Reporting Systems / Dashboards
2.3.7.1.3 External automation / management systems
2.3.7.1.4 External complementary cyber security solutions (e.g. firewalls, forensic solutions, …)
2.3.7.2 How does your solution facilitate integration to external SIEM solutions (e.g. Splunk)?
2.3.7.3 How does your solution facilitate integration to external SOAR solutions?
2.3.7.4 How does your solution facilitate integration with external PKI solutions?
2.3.7.5 For all questions above: which of these are supported by default and which require custom connectors?
2.3.7.6 Does the solution allow for integration with any of the following tools?
2.3.7.6.1 Splunk; Zeek; MISP; Palo Alto Panorama; Cloudflare; BlueCoat; Netscout Packet Broker; PKI Infrastructure
2.3.7.7 Does your solution support Sandbox integration? If so, does it have native Sandbox available for purchase and integrated with the ETI solution?

2.3.8 Tool security (Priority 2)
2.3.8.1 What security functions and measures are included to protect the system and its data?
2.3.8.2 What measures are taken to avoid bypassing or tampering of the system (e.g. hunting on telemetry)?
2.3.8.3 Do you have a dedicated team to assess and respond to security vulnerabilities in the product suite?

2.3.9 Management (Priority 2)
2.3.9.1 What is the central management method for the solution?
2.3.9.2 What are the management roles to distribute the management privileges?

2.3.9.3 Is there a single management console controlling all the solution components?
2.3.9.4 Are there functional limitations of the management console that requires use of external interfaces such as CLI?
2.3.9.5 What is the compatibility / integration for the management component for on-premises and cloud related modules?
2.3.9.6 What reporting capabilities are available for auditing, compliance, and executive reporting purposes?

2.3.10 Support, maintenance and service provisioning (Priority 3)
2.3.10.1 How is the product ensured to be up to date with the latest developments, both functionally and to mitigate new risks?
2.3.10.2 What parts of the solution are expected to be operated by the purchaser and which can be provided as a service?
2.3.10.2.1 Can you specify what service level guarantees can be provided through these services?
2.3.10.2.2 Are you able to provide any examples of service support models for any managed services that you currently operate?
2.3.10.3 What levels and type of support do you offer for the products identified in this questionnaire (e.g. Support Portal; Help Desk 24x7 / 9x5; Technical Account Manager; Development Team access; Onsite Professional Services …)?
2.3.10.4 What system diagnostic information needs to be provided with support cases?
2.3.10.5 Are you able to provide any guaranteed response and/or resolution times for support cases raised by a Customer?
2.3.10.6 What onsite consultancy services are you able to provide (e.g. deployment; integration; configuration, tuning, optimisation; policy management …)?
2.3.10.7 Are you able to provide Training on your products and services? If so, in what form (e.g. Face-To-Face at purchaser / vendor site?; Online or CBT; Training material …)
2.3.10.8 What are your policies and procedures regarding notification of security vulnerabilities which may be identified in your products (e.g. through internal release testing)?

2.3.11 Cost and licensing (Priority 3)
2.3.11.1 Can you provide an breakdown of your indicative pricing and licensing structure for the ETI solution and related support?

2.3.12 Roadmap and future development (Priority 2)
2.3.12.1 Can you provide an overview of the relevant near-future product roadmap?
2.3.12.2 Are there any announced End of Life / End of Support point for the products described in the solutions provided ?
2.3.12.3 Any Post Quantum Encryption solutions on the Roadmap?