Acquisition
sven.schumacher@ncia.nato.int

NCIA/ACQ/2025/06651
12 March 2025

Request for Information

Cloud-based Online Cybersecurity Training Solutions

NCI Agency Reference: RFI-424245-ACAD

The NATO Communications and Information Agency is seeking information from Nations and their qualified Industry in order to assess the availability of Cloud-based Online Cybersecurity Training Solutions within all NATO Nations.

NCI Agency Point of Contact (POC):

Senior Contracting Officer: Sven Schumacher

Email: Sven.Schumacher@ncia.nato.int

To : Distribution List (Annex A)

Subject : **NCI Agency Request for Information: RFI-424245-ACAD**

1. The NATO Communications and Information Agency (NCI Agency) requests the assistance of the Nations and their Industry to identify within all NATO Nations the availability of Cloud-based Online Cybersecurity Training Solutions. This Request for Information (RFI) is being issued to identify potential solutions and possible suppliers.

2. The broadest possible dissemination by Nations of this Request for Information to their qualified and interested industrial base is requested.

3. A summary of the requirements is set forth in the Annex B attached hereto. Respondents are requested to reply via the Questionnaire at Annex C. Supplementary information and documentation (technical data sheets, marketing brochures, catalogue price lists, descriptions of existing installations, etc.) are welcome.

4. Responses to this request, and any information provided within the context of this RFI, including but not limited to pricing, quantities, capabilities, functionalities and requirements will be considered as indicative and informational only and shall not be construed as

NATO Communications and Information Agency
Boulevard Leopold III
1110 Brussels
Belgium
www.ncia.nato.int

binding on the participant or on NATO for any future acquisition. Respondents are responsible for adequately marking proprietary or competition sensitive information contained in their response.

5. Responses shall in all cases include the name of the firm, telephone number, e-mail address, designated Point of Contact, and a NATO UNCLASSIFIED description of the capability available and its functionalities. This shall include any restrictions (e.g. export controls) for direct procurement of the various capabilities by NCI Agency. Non-binding pricing information is also requested as called out in Annex C.

6. The NCI Agency reference for this Request for Information is **RFI-424245-ACAD**, and all correspondence and submissions concerning this matter must reference this number within the documentation and email subject line.

7. Responses are due to NCI Agency no later than **23:59 hours Central European Time (CET) on 18 April 2025** and may be submitted to NCI Agency directly from Nations or from their Industry.

8. Please send all responses via email to the following NCI Agency POC:

   For attention of:

   Mr Sven Schumacher

   Senior Contracting Officer

   Email: Sven.Schumacher@ncia.nato.int .

9. Technical discussions and/or demonstrations may take place following the submission of responses, with the purpose of clarifying or further augmenting those responses where required. Respondents are requested to await further instructions after their submissions and are requested not to contact any NCI Agency staff directly other than the POC identified at paragraph 8 above.

10. Any response to this request including follow-on technical discussions and/or demonstrations shall be provided on a cost-free and voluntary basis. Not responding will not prejudice or cause the exclusion of companies from any future procurement that may arise from this Request for Information.

11. The NCI Agency is not liable for any expenses incurred by firms in conjunction with their participation in this Request for Information and this RFI shall not be regarded as a commitment of any kind concerning future procurement of the items described therein.

12. Your assistance in this Request for Information is greatly appreciated.

For the Chief of Acquisition:

Sven Schumacher

Digitally signed by Sven Schumacher
Date: 2025.03.12 10:43:57 Z

Sven Schumacher
Senior Contracting Officer

Enclosures:
Annex A (Distribution List)
Annex B (Request for Information - Summary of Requirements)
Annex C (Request for Information - Questionnaire)

ANNEX A

Distribution List for Request for Information
RFI-424245-ACAD
Cloud-based Online Cybersecurity Training Solutions

All NATO Delegations (Attn: Investment Adviser)

NATO Members Embassies in Brussels (Attn: Commercial Attaché)

NCI Agency – All NATEXs

NCI Agency – (reserved)

ANNEX B

SUMMARY OF REQUIREMENTS

Request for Information
RFI-424245-ACAD
Cloud-based Online Cybersecurity Training Solutions

1. Introduction

1.1. The NATO Office of the Chief Information Officer (OCIO) is mandated to raise the maturity of the NATO Enterprise cybersecurity (CS) posture through the delivery of bespoke Education and Training (E&T).

1.2. The associated cybersecurity E&T initiatives can include the development and delivery of frameworks, tools, content, practices, support to NATO Education and Training Facilities (NETFs), and outreach activities.

1.3. E&T initiatives can be achieved by focusing on two themes and distinct target audiences within the NATO Enterprise:

1.3.1. Cybersecurity Hygiene (Cyber-hygiene) for the generic, non-technical NATO ICT user, which includes any NATO staff member that uses information technology/CIS in the execution of their day-to-day function

1.3.2. Cybersecurity Skills Development for the NATO Cyber Security professional, which includes any NATO staff member that incorporates cybersecurity activities in the execution of their day-to-day function.

1.4. To operationalize both of the above E&T categories and to support NATO's journey towards an improved Organisational Cybersecurity maturity, the OCIO has requested the NATO Communications and Information (NCI) Academy to develop a plan for a "NATO Enterprise Cybersecurity Learning and Development Uplift" (NATO CS L&D Uplift).

2. Scope

2.1. In support of OCIO's endeavours regarding Cybersecurity Skills Development, NCI Academy is currently exploring cloud-based, online cybersecurity training solutions that provide realistic, hands-on virtual environments for both individual and small team-based training. We are particularly interested in platforms that offer simulated cybersecurity threats to enhance practical skills in threat detection, incident response, and mitigation strategies.

2.2. This COTS cloud-based, online cybersecurity training solution would complement NATO cybersecurity learning solutions by focusing on individual and small team cybersecurity skills development via realistic simulations and hands-on practice.

3. Eligibility

3.1. Eligible suppliers must be from Participating NATO Nations (ALBANIA, BELGIUM, BULGARIA, CANADA, CROATIA, THE CZECH REPUBLIC, DENMARK, ESTONIA,

FINLAND, FRANCE, GERMANY, GREECE, HUNGARY, ICELAND, ITALY, LATVIA, LITHUANIA, LUXEMBOURG, MONTENEGRO, THE NETHERLANDS, NORTH MACEDONIA, NORWAY, POLAND, PORTUGAL, ROMANIA, SLOVAKIA, SLOVENIA, SPAIN, SWEDEN, REPUBLIC OF TÜRKIYE, THE UNITED KINGDOM and THE UNITED STATES), unless otherwise specifically authorized by the NCI Agency.

ANNEX C

QUESTIONNAIRE

Request for Information
RFI-424245-ACAD
Cloud-based Online Cybersecurity Training Solutions

Organisation name:

Contact name & details within organisation:

Notes:

1. Please DO NOT alter the sequence and numbering of questions. It is recommended to copy the questions into your response and provide your answers under each question. If you need additional space to complete your text then please use the 'Continuation Sheet' at the end of this Annex and reference the question to which the text relates to.
2. A MS Word version of the questionnaire can be made available to interested parties upon request to the NCI Agency POC identified in paragraph 8 of the cover letter.
3. Please feel free to make assumptions, *HOWEVER* you must list your assumptions in the spaces provided.
4. Please DO NOT enter any company marketing or sales material as part of your answers within this Request for Information. Such material should be submitted as enclosures with the appropriate references within your replies. If you need additional space, please use the 'Continuation Sheet' at the end of this Annex.
5. Please DO try and answer the relevant questions as comprehensively as possible.
6. All questions within this document should be answered in conjunction with the summary of requirements in ANNEX B.
7. All questions apply to Commercial or Government responders as appropriate to their Commercial off the Shelf (COTS) or Government off the Shelf (GOTS) products.
8. Cost details required in the questions refer to Rough Order of Magnitude (ROM) Procurement & Life Cycle cost, including all assumptions the estimate is based upon:
    - Advantages & disadvantages of your service/solution/organisation,
    - Any other supporting information you may deem necessary including any assumptions relied upon.

Request for Information - Questionnaire

To better understand your offerings, we would appreciate it if you could provide information on the following:

1. **Virtual Training Environment Capabilities**
    a. Do you offer COTS[1] cloud-based and/or on-premise virtual labs?
        i. Can they be deployed on-premise, isolated from the internet?
    b. What types of cybersecurity threats and attack scenarios are simulated?
    c. Are your training environments customizable to match specific use cases?
    d. Does your environment include (self-)assessment tools to ascertain a learner's level before engaging with the content?
    e. Can NATO be given access to your environment in order to get a 'hands-on' perspective?

2. **Training Modules and Content**
    a. Which cybersecurity topics and skill levels do your training programs cover?
    b. Do you provide guided exercises, red team/blue team simulations, or capture-the-flag (CTF) challenges?
    c. How many training scenarios can you offer Off-the-Shelf?
    d. How is your content offering updated / how can it stay abreast with continuous developments in the Cybersecurity domain?
    e. How quickly can new training scenarios be developed and made available to training audiences via the platform?
    f. Is it possible to add NATO specific training scenarios to the platform (e.g., NATO team develops the storyline of a training scenario, your company implements the virtual machines and all other requirements for deployment)?
    g. Are there options to deploy self-paced theoretical training (e.g. eLearning) on the same platform?

3. **Team Training and Collaboration Features**
    a. Can teams train collaboratively in a shared environment?
    b. Can various teams train in the same environment without impacting each other?
    c. Do you offer competitive team-based exercises or adversarial simulations?
    d. What features exist for performance tracking, analytics and granular reporting?

[1] COTS – Commercial-off-the-shelf

4. **Technical and Security Requirements**
    a. What are the system requirements for accessing your virtual training environment?
    b. How is data security and user privacy ensured within your platform?
    c. Has your platform already been accredited for use in other environments (e.g. a National MoD or other government organisation) and to what level of security classification?
    d. Is it platform certified by entities like FedRAMP or SOC2 Type2?
    e. Can you confirm that all your servers reside in a NATO country?

5. **Pricing and Licensing Models**
    a. What are your pricing structures for individual and team training?
    b. Do you offer enterprise or volume-based licensing options?
    c. Are there any additional costs for customization or dedicated support? If so, what is the pricing structure for that?

Continuation Sheet Please feel free to add any information you may think that may be of value to NCI Agency in the space provided below. Should you need additional space, please copy this page and continue with the appropriate page numbers.	Page # __ of __