NATO Communications and Information Agency

Acquisition

NCIA/ACQ/2024/06544
5 March 2024

Request for Information

Zero Trust Technologies
NCI Agency Reference: MS-423233-ZTC

NCI Agency seeks to identify the availability and technical capability of qualified NATO industry sources for Zero Trust capability (ZTC) that will assist NCIA and its customers at a NATO Enterprise in better understanding their maturity level and determine their future evolution within the Enterprise.

NCI Agency Point of Contact
Ms. Leonora Alushani, Contracting Officer
MS-423233-ZTC@ncia.nato.int

To: Distribution List (Annex A)

Subject: **NCI Agency Market Survey**
Request for Information MS-423233-ZTC

1. Through issuance of this notice, the NCI Agency seeks to identify the availability and technical capability of all qualified NATO nation businesses that believe they can provide the services described in this announcement.
2. This is a Request for Information (RFI). It is NOT a solicitation for proposals nor a pre-solicitation notice.
3. The NCI Agency reference for this RFI is **MS-423233-ZTC**, and all correspondence and submissions concerning this matter should reference this number.
4. The NCI Agency requests the broadest possible dissemination by the Nations of this RFI to their qualified and interested industrial base.

NATO Communications and Information Agency
Agence OTAN d'information et de communication
Avenue du Bourget 140
1140 Brussels, Belgium
www.ncia.nato.int

5. The information resulting from this effort is for planning purposes only and for assisting the NCI Agency in understanding the existing technologies, their maturity level and determining the future evolution of Zero Trust across the NATO enterprise as well as in identifying potential NATO nation based solutions and possible suppliers.
6. Responses may be issued to the NCI Agency directly by eligible NATO industry to the Point of Contact indicated at Paragraph 11 below.
7. Responses shall follow the instructions for submittal at Annex B of this RFI.
8. Interested parties are responsible for adequately marking proprietary or competition sensitive information contained in their response.
9. Technical demonstrations may take place following the submission of responses, with the purpose of showcasing your solution and clarifying or further augmenting those responses where required. Product demonstrations and/or face-to-face briefings/meetings with industry may be considered with companies that have submitted a formal response to this RFI.
10. The NCIA will consider and analyze all information received from this RFI and may use these findings to develop a future solicitation for a Zero Trust capability or a system. Any future solicitation would be advertised on the Agency bulletin board for all eligible companies to respond.
11. Responses are requested to be submitted to Ms. Leonora Alushani via email at MS-423233-ZTC@ncia.nato.int by ~~11~~ 26 March 2024
12. Your assistance in this RFI is greatly appreciated.

For the Chief of Acquisition:

Leonora Alushani
Contracting Officer

Enclosures:
Annex A, Distribution List
Annex B, Instructions & Questionnaire

Distribution List

NATO Delegations (Attn: Military Budget Adviser)

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

Belgian Ministry of Economic Affairs

Embassies in Brussels

(Attn: Commercial Attaché)

Albania
Belgium
Bulgaria
Canada
Croatia

Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Iceland
Italy Latvia
Lithuania
Luxembourg
Montenegro
Netherlands
North
Macedonia
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Turkiye
United Kingdom
United States of America

MS-422233-ZTC Instructions & Questionnaire

Summary of Requirements

1. Zero Trust is an approach to CIS security that aims to prevent unauthorized access to resources[1], requiring strict and granular access control. Zero Trust evolves the traditional perimeter-based to a more resource-centric security paradigm that relies on dynamic risk-based access control.
2. This Markey Survey seeks insight on suitable commercial products to provide the required zero trust capability.

Instructions for Submitting a Response:

1. Interested and eligible organizations from a NATO nation possessing the capabilities to meet the needs described herein, along with the experience in having supported similar needs should submit one (1) electronic response to MS-423233-ZTC@ncia.nato.int. Responses shall be submitted no later than close of business on 26 March 2024 and shall contain **no classified material**:
    a. **Part I - A cover sheet clearly identifying the following information**:
        - Re: reference control number MS- 423233-ZTC;
        - Organization name, address, and contact information (telephone number and email address of designated Point of Contact);
        - A brief description of your business or organization, including the main products and services it offers and the market or customers it primarily supports, and how your organization will meet the needs of the services required by NATO.

    b. Part II-Capability Package consisting of:
        - Any initial assumptions, constraints, and exceptions regarding this RFI; and
        - A detailed technical response tailored specifically to NCIA's needs, addressing the questionnaire content provided at Annex B of this RFI.
        - The anticipated level of effort required to meet the needs identified in this RFI.
2. Please do not enter any general company marketing or sales material as part of your specific responses within this RFI. Please submit such material as enclosures with the appropriate references within your replies.
3. Responses **are not to exceed two (2) pages per each solution described** in no less than 11 font size. Tables, graphs and other imagery do not count towards the limit.
4. Cost details requested in the questions are not a binding offer. Please include all conditions related to the estimate provided.
5. Other supporting information and documentation specific to this requirement (technical data sheets, marketing brochures, catalogue price lists are also desired).

[1] In the context of this document, a resource is any item in a CIS that can be used or drawn upon when needed, including but not limited to device, data, networks, applications, and services.

Annex B

MS- 423233-ZTC RFI Questionnaire

Part 1: Knowledge/Expertise

1. Please provide the following information regarding your firm's experience in Zero Trust Capability (ZTC). List and codify all Zero Trust solutions, capabilities or services your company offers. After that, technically describe each solution (referring to the ID in the table) and any relevant dependencies (on other solutions) it may have. Use maximum 2 pages per solution.
    - Provide a deployment example (can include a use case, explanation of the solution, including figures, capability…)
    - Define the maturity of your solution following the CISA Zero Trust Maturity Model 2.0 (link): traditional, initial, advanced, optimal).
    - Is there any post-procurement operation and maintenance effort required?

2. Based on the listed solutions in Question 1, fill in the tables below identifying on which pillar, system function and Zero Trust objective your solution touches upon:

    Guidance: You do NOT need to fill in all pillars and objectives, just those which correspond to your company's capabilities. One capability may touch upon several pillars and objectives simultaneously. Please use maximum of 150 words per cell as you are able to add an in-depth description of your capability in Question 1.

    a. Identity/User

	System function	ID	Zero Trust Objective	Identified solution
1.1	Authentication	1.1.1	Maintain one authoritative source of digital identity for the person or NPE	
		1.1.2	Enforce strong authentication	
		1.1.3	Ensure Identity Lifecycle Management	
		1.1.4	Implement Federated Identity	
1.2	Authorization	1.2.1	Least Privileged Access	
		1.2.2	Privileged Access Management	
		1.2.3	Access control per session / Session Management	
		1.2.4	Attribute-Based Access Control /Risk Adaptive Access Control	
1.4	Trust Management	1.4.1	Continuous Trust Monitoring	
1.5	Monitoring	1.5.1	User Behavior Monitoring	
		1.5.2	Continuous auditing	

    b. Device

	System function	ID	Zero Trust objectives	Identified solution
2.1	Authentication	2.1.1	Manage devices	
2.2	Authorization	2.2.1	Enforce Attribute-Based Access Control	
2.3	Policy Management	2.3.1	Define security policies	
		2.3.2	Deploy a device management solution	
		2.3.3	Enforce policies automatically	
2.4	Trust Management	2.4.1	Continuously monitor device trust	
2.5	Monitoring	2.5.1	Continuously monitor device behaviour	
		2.5.2	Continuously audit	
2.6	Threat Protection	2.6.1	Enforce cyber hygiene	
		2.6.2	Perform continuous threat detection	

c. Workloads and Applications Pillar

	System function	ID	Zero Trust objectives	Identified solution
3.1	Authentication	3.1.1	Inventory deployed applications	
3.2	Authorization	3.2.1	Enforce granular access control	
3.3	Policy Management	3.3.1	Secure application development, deployment and testing	
3.4	Trust Management	3.4.1	Trusted software	
		3.4.2	Continuously monitor application trust	
3.5	Monitoring	3.5.1	Continuous threat monitoring	
		3.5.2	Continuous health monitoring	
3.6	Threat Protection	3.6.1	Integrated threat protection	

d. Data

	System function	ID	Zero Trust objectives	Identified solution
4.2	Authorization	4.2.1	Data inventory and categorization	
		4.2.2	Data labelling	
		4.2.3	Enforce data loss prevention	
4.3	Policy Management	4.3.1	Define data access security policies	

4.5	Monitoring	4.5.1	Continuously monitor data access	
4.6	Threat Protection	4.6.1	Protect data at rest and in transit	
		4.6.2	Perform continuous threat detection	

e. Network

	System function	ID	Zero Trust objectives	Identified solution
5.1	Authentication	5.1.1	Network Inventory	
5.2	Authorization	5.2.1	Network segmentation	
5.3	Policy Management	5.3.1	Network Traffic management	
5.4	Trust Management	5.4.1	Continuously monitor traffic trust	
5.5	Monitoring	5.5.1	Continuous threat monitoring	
		5.5.2	Continuous health monitoring	
5.6	Threat Protection	5.6.1	Traffic Encryption	

f. Visibility and Analytics

	System function	ID	Zero Trust objectives	Identified solution
6.1	Identity	6.1.1	Analysis of user (person and device) activity, including behavior-based analytics.	
6.2	Devices	6.2.1	Status collection, endpoint monitoring, anomaly detection, etc.	
		6.2.2	Automatic correlation of connected assets (devices and virtual ones) with identities	
6.3	Networks	6.3.1	Network monitoring, telemetry, correlation from different sources, threat hunting, etc.	
6.4	Applications and Workloads	6.4.1	Monitoring of applications including security, performance, trends identification, impact, etc.	
6.5	Data	6.5.1	Detection of data breaches	

g. Automation and Orchestration

	System function	ID	Zero Trust objectives	Identified solution
7.1	Identity	7.1.1	Orchestration of identities within environments	

7.2	Devices	7.2.1	Automatic vulnerability scanning of devices	
		7.2.2	Automatic remediating, and deprovisioning of devices and virtual assets.	
7.3	Networks	7.3.1	Automatic configuration and resource lifecycle of networks and environments	
7.4	Applications and Workloads	7.4.1	Automatic configuration of applications (e.g. for security and performance optimization).	
7.5	Data	8.5.1	Automated labelling of data	
		8.5.2	Policy- based data handling processes.	

3. Please identify if any of your already listed Zero Trust solutions touches upon any of the technical areas described below. Describe the solution giving deployment scenario or relate to relevant description from Question 1:

Technical Area	Supported (Y/N)	Identified solution
Cognitive approach to environment monitoring, which enables to create understanding of security posture and risk level in all ZT pillars: User, Device, Applications/Workloads, Network & Environment. This also includes advanced data analytics (including behavioral analysis), being able to understand impact of the observed system security posture on the business processes, and visualization of this to the stakeholders (interested parties).		
Risk Adaptive access control based on a broad range of parameters and identity attributes, in one domain and in cross-domain approach (federated scenarios).		
Support for automated data classification and labelling based on understanding of the content and explainable AI.		
Data protection at rest and in processing, enabling to carry operations on encrypted data		

(e.g. homomorphic encryption), enabling enhanced data protection for cloud environments, collaborative data analysis and private machine learning.		
Automation of the activities related to threat and intrusion detection and network protection.		

Description: Max 2 pages per solution

Part 2: Cost Model – ZTC Agreement Pricing

1. How are your Zero Trust capability/services priced
2. What is your licensing model (payment per user/ virtual machine/ server/ amount of data processed/ physical component)?
3. Describe service/capability pricing.
4. Are there any tools required during an incident? If so, are they priced separately or inclusive?
5. Does your pricing model offer a reduced rate for extended contracts beyond one year?
6. What are your payment terms?

Please feel free to add any information you think that may be of value to NCI Agency.