NCIA/ACQ/2024/7392
29 Oct 2024

Market Survey - Request for Information

Identify integrated products for
"Asset discovery, vulnerability remediation for endpoints, application deployment and patching, Security compliance auditing (against vulnerabilities, patching and configuration management)"

NCI Agency Reference: MS-424192-NSATU

NATO Communication and Information Agency (NCI Agency) is seeking information from Nations and their Industry regarding the availability of providers that are able to meet NATO's requirements related to provide Products or an integrated solution for Asset discovery, endpoint vulnerability remediation, application deployment and patching, Security compliance auditing (against vulnerabilities, patching and configuration management).

NCI Agency Points of Contact for this Market Survey
Ms. Estefania Nunez, Principal Contracting Assistant
E-mail: estefania.nunez@ncia.nato.int

To: Distribution List (Annex C)

Subject: **NCI Agency Market Survey**
Request for Information MS-424192-NSATU- Endpoint Configuration Compliance Auditing and Management

1. NCI Agency requests the assistance of the Nations and their Industry to identify providers that are able to meet NATO's requirements related to a requirement for integrated product(s). This Market Survey is being issued to identify possible suppliers and to identify any limitations or conditions that may need to be met before potential suppliers are able to submit bids for similar products.

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

NCIA/ACQ/2024/7392

2. A summary of the requirements is set forth in the Annex A attached hereto. Respondents are requested to reply via the questionnaire at Annex B. Other supporting information and documentation (technical data sheets, marketing brochures, catalogue price lists, descriptions of existing installations, etc.) are also desired.

3. The NCI Agency reference for this Market Survey Request is **MS-424192-NSATU** and all correspondence and submissions concerning this matter should reference this number.

4. In addition to the firms noted in the Distribution List of this letter, Annex D, the NCI Agency requests the broadest possible dissemination by Nations of this Market Survey Request to their qualified and interested industrial base.

5. Responses may be issued to the NCI Agency directly from Nations or from their Industry (to the staff indicated at Paragraph 9 of this Market Survey Request). Respondents are invited to carefully review the requirements in Annex A.

6. Responses shall in all cases include the name of the firm, telephone number, e-mail address, designated Point of Contact, and a description of the capability available and its functionalities (not above NATO Unclassified). This shall include any restrictions (e.g. export controls) for direct procurement of the various capabilities by the NCI Agency.

7. Non-binding product pricing information is also requested as called out in Annex B.

8. Responses are due back to the NCI Agency no later than **15:30 Brussels time 22 Nov 2024**.

9. Please send all responses via email to the following NCI Agency Action Officer:

To Attention of: Mrs. Estefania Nunez

E-mail: Estefania.Nunez@ncia.nato.int

10. Product demonstrations or face-to-face briefings/meetings and technical discussions may take place following the submission of responses with industry after reviewing the proposals with the purpose of clarifying or further augmenting those responses where required.

11. Respondents are requested to await further instructions after their submissions and are requested not to contact directly any NCI Agency staff other than the POC identified above in Paragraph 9.

NCIA/ACQ/2024/7392

12. Any response to this request shall be provided on a voluntary basis. Negative responses shall not prejudice or cause the exclusion of companies from any future procurement that may arise from this Market Survey. Responses to this request, and any information provided within the context of this survey, including but not limited to pricing, quantities, capabilities, functionalities and requirements will be considered as information only and will not be construed as binding on NATO for any future acquisition.

13. The NCI Agency is not liable for any expenses incurred by firms in conjunction with their responses to this Market Survey and this Survey shall not be regarded as a commitment of any kind concerning future procurement of the items described.

14. Your assistance in this Market Survey request is greatly appreciated.

FOR THE CHIEF OF ACQUISITION:

Tiziana Pezzi

Digitally signed by Tiziana Pezzi
Date: 2024.10.29 11:38:01 +01'00'

Ms. Tiziana Pezzi
Principal Contracting Officer

Enclosures:
Annex A: Summary of Requirements
Annex B: Questionnaire
Annex C: Distribution List
Annex D: Potential Industrial Suppliers

ANNEX A
Summary of Requirements

Context

1. NATO is looking for an integrated CIS Security Product to allow principally:
    a. Discovery of Assets connected to the Network;
    b. Vulnerabilities Identification and remediation for endpoints;
    c. Application deployment and patching; and,
    d. Security compliance auditing (against vulnerabilities, patching and configuration management).
2. Additionally and as desirable capabilities NATO would also consider beneficial if the same product could provide:
    a. Endpoint Detect and Response Functionality
    b. Online Computer Forensics Functionality
    c. Threat Hunting and Impact Analysis
    d. Sensitive Data Detection to detect Data leaks
3. This product will be employed in NATO static locations as well as in NATO deployed operations, being the latter the most demanding due to the constrained connectivity available and the frequent disconnections from the central operations centre.
4. Main COTS products are designed for large enterprise environments and fast interconnections. DCIS communication can take place over SATCOM links and utilize various encryption layers. As a result, increase latency and reduced throughput is expected. When the number of assets concurrently trying to receive the same software package increases, the delay can sometimes cause the installation to fail. NATO is looking for a versatile solution that can mitigate these constraints is therefore required.

Functional Objectives

5. The CIS Security Product NATO is looking for shall be an Integrated Product capable of doing in a single glass pane a number of different functionalities. As described in this section.

6. **Asset Discovery Function**: The Asset Discovery Function shall provide visibility of what (assets and devices) is connected to the network. This function shall:

    a. Be OS agnostic;

    b. Be Capable of discovering HW/SW and Infrastructure assets, like e.g. UPSs, physical servers, virtual infrastructure, routers, switches, firewalls, end user devices (phones, MFD, VTC, EUD Workstations)

    c. Identify and create an inventory;

    d. Provide a time accurate picture of the connected assets.

7. **Vulnerability Identification Function**: The Vulnerability Identification Function shall:

    a. Provide Visibility on Open Vulnerabilities of endpoints;

    b. The Vulnerability Identifications Function processes (e.g. active scanning, agents, etc.) shall minimize the WAN traffic and have the option to run locally on endpoints;

    c. Due to the Disperse nature of the Deployable Networks the vulnerability signatures files shall be able to be uploaded locally when network propagation is not possible.

8. **Application deployment, vulnerability remediation and software patching**: The Product shall provide a mitigation and remediation function that shall:

    a. Allow patching of Windows and major Linux distributions (e.g. RedHat, Oracle, Ubuntu, CentOS), as well as container based applications;

    b. Support deployment of software patches for generic use applications (Adobe Reader, Firefox) or custom-made applications.

    c. Allow centralized or user-initiated patching. The patch process can be initiated from the administrator console, or from the endpoint.

    d. The tool shall allow roll-back changes and patches;

    e. Remediation actions shall be initiated as early as possible when the vulnerabilities are identified and executed from the local tool

    f. The remediation (i.e. patches and configurations) shall be able to be triggered from the tool.

    g. The tool shall have the capability of denying specific patches.

9. **Security compliance auditing** (against vulnerabilities, patching and configuration management). This function shall:

    a. Provide endpoint security compliance verification using the Security Content Automation Protocol (SCAP) version 1.3.

    b. The scan engine must support PowerShell Constrained Language Mode or not require PowerShell.

    c. Provide continuous configuration compliance (with potential for automated remediation) of configuration drifts using industry-standard benchmarks such as CIS, DISA STIG, USGCB and PCI-DSS V4.0, as well as custom benchmarks.

Use Cases

10. Today's Deployable Communication and Information Systems (DCIS) environment is under increased pressure of delivering secure CIS services in remote locations.

11. DCIS environments are characterized by reduced link bandwidth and availability. This often results in incomplete/failed software deployment and upgrade process. Therefore the software package transmission shall be resilient and be able to be resumed automatically when the links are re-established.

12. In the deployed space, the main constraints to reach the deployed nodes is the typology of WAN transmission bearers.

    a. Characteristics of the bearers to be analysed are

        i. latency is very high (ca. 500 - 1200 ms)
        ii. Available Bandwidth does not exceed on average 1 Mbps U/D
        iii. Transmission Interruptions can be expected.

13. Following picture represents an archetypical deployment:

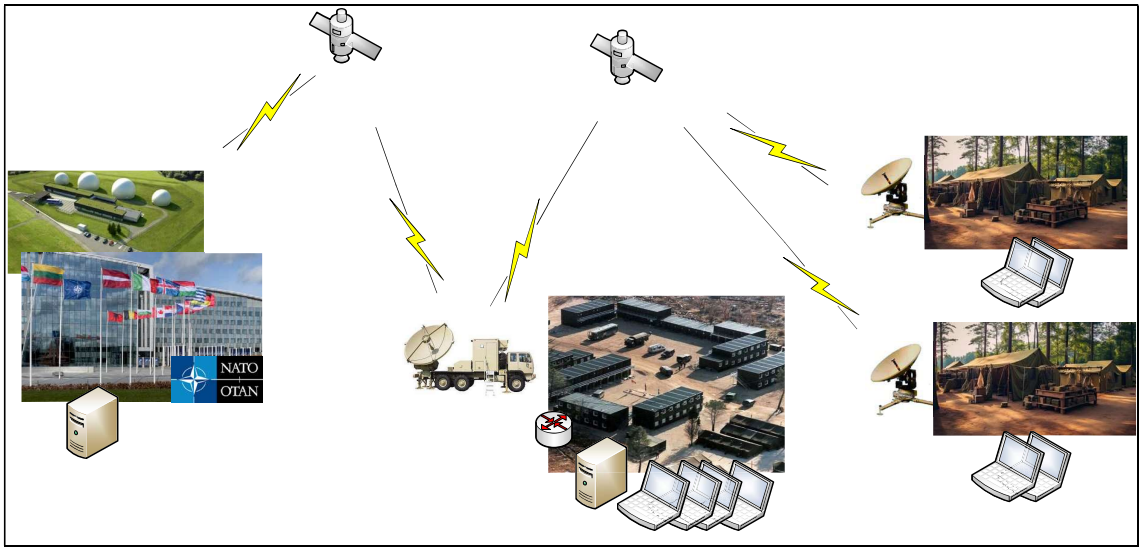

Figure 1 – Deployable CIS concept

14. In NATO HQ (left) the Network and Cyber Security Management and Control is performed from the Network and Cyber Security Operating Centres. The technical services enabling this functions are installed in the static data centres.

15. Over SATCOM links (as described above) the Deployed HQ (centre) is reached. This Deployed HQ is a deployable data centre extending services from the static data centre for the users or, if needed, providing these locally. This Deployed HQ is also able to perform a Network and Cyber Security Management and Control function for itself and for the downstream Remote Nodes (right).

16. Over a second SATCOM link the Deployed HQ is able to reach the Remote Nodes. Remote Nodes are smaller entities supporting the subordinated units from the Deployed HQ by extending the network services provided from the Deployed HQ, but not hosting the services locally.

Constrains and general requirements for the product

17. For the Deployable CIS landscape the architecture has to support a hierarchical approach, with minimum WAN traffic utilization between deployment sites and rather promoting LAN traffic.

18. The proposed system shall be able to work in an air-gapped environment, without connection to public networks.

19. The tool shall provide traffic encryption of all communications (including software distribution) between the components of the system (i.e. servers, agents, etc.).

20. The tool shall support multi-factor authentication for the management interface.

21. The tool shall be able to integrate with an external credential store solution.

22. The product functionality shall be able to be managed both centrally and locally.

23. The tool shall be capable of feeding the Configuration Management System (CMS) and IT Service Management (ITSM)

ANNEX B
Questionnaire

Organisation Name:

Contact name & details within organisation:

Notes

- Please **DO NOT** alter the formatting. Please use the 'Answer Sheet' at the end of this Annex and reference the question to which the text relates to.
- Please feel free to make assumptions, *HOWEVER* you must list your assumptions in the spaces provided.
- Please **DO NOT** enter any company marketing or sales material as part of your answers within this market survey. But please submit such material as enclosures with the appropriate references within your replies.
- Please **DO** try and answer the relevant questions as comprehensively as possible.
- All questions within this document should be answered in conjunction with the summary of requirements in Annex A.
- All questions apply to Commercial or Government respondees as appropriate to their Commercial off the Shelf (COTS) or Government off the Shelf (GOTS) products.
- 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 product/solution/organisation,
    - Any other supporting information you may deem necessary including any assumptions relied upon.

Questions

1. **Do you currently provide any product/services similar to Asset discovery, vulnerability remediation for endpoints, application deployment and patching, Security compliance auditing (against vulnerabilities, patching and configuration management) as described in Annex A?**

2. **If you already provide a similar product can you please:**
    a. **Attach all related information and a brochure?**
    b. **Confirm if the product is accredited by NATO or a NATO Nation?**
    c. **Provide further information on the Nations where it is provided and the relevant use cases?**

3. **If you do already provide a similar product can you please:**
    a. **Provide further information about the deployment architecture?**
    b. **Provide further information about the bandwidth consumption between sites and endpoints?**
    c. **Provide further information about behaviour during disconnections from the management nodes and re-connection?**
    d. **What packing formats are supported for software and patch deployment?**
    e. **Does the system support an on premise installation without connectivity to any public network?**

4. **If you do already provide a similar product can you please:**
    a. **Indicate which of the Functions and features captured in Annex A this product is providing; and,**
    b. **Indicate other Cyber Security features for Endpoints it offers additionally?**

5. **If you do already provide a similar product can you please:**
    a. **Provide further information about the support and training concepts you offer.**
    b. **Provide further information about the different training levels.**
    c. **Can you provide on-site technical support?**

6. **Would your company be able to make an on premise demonstration of this tool/product?**

7. **What is the pricing scheme or licencing model applied for the proposed product?**

Answer Sheet Template 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 __