Acquisition Office

Boulevard Léopold III
B-1110 Brussels, Belgium

NCIA/ACQ/2024/07509
27 November 2024

Market Survey - Request for Information

Capability Package CP149 Rev 1 "Dragonfly Increment 1"

NCI Agency Reference: MS-423340-ICH-RG

The NATO Communications and Information Agency (NCIA) is seeking information from Nations and their Industry regarding the availability of providing potential solutions for the NATO Information Clearing House – Release Gateway (ICH-RG) project.

NCI Agency Point of Contact (POC) for this Market Survey:

Ms. Estefania Nunez, Principal Contracting Assistant,
E-mail: estefania.nunez@ncia.nato.int

NCIA/ACQ/2024/07509

NATO Communications and Information Agency

To : See Distribution List

Subject : NCI Agency Market Survey - Request for Information
MS-423340-ICH-RG

Reference(s) :
A. NCIA TR-2012-SPW008418-13-4, 2013 Protection Profile For The NATO High-Assurance Attribute-Based Access Control (ABAC) Guard (HAAG) Konrad Wrona (NCI Agency), Nadja Menz (Fraunhofer FOKUS).

B. Ross, A & Oudkerk, S 2011, 'NATO Content Inspection Policy Enforcement Framework Functional Specification', Technical Note, TN-1486, NC3A.

C. NAC AC/322-D/0030-REV6 (INV), C3B, Technical And Implementation Directive For The Interconnection Of Communications And Information Systems, (CIS), 19 July 2023.

1. The NCI Agency requests the assistance of the Nations and their Industry to identify potential solutions for the NATO Information Clearing House – Release Gateway (ICH-RG) from their national providers. Also to determine what could be made available to NATO to support future operations and missions.

2. A summary of the NATO requirement for ICH-RG is set forth in the attached Annex A.

3. Respondents are requested to reply via the questionnaire at Annex B. Other supporting information and documentation of current and future capability programmes is also welcome (technical data sheets, marketing, brochures, non-binding catalogue price lists, descriptions of existing installations, etc.).

4. The NCI Agency reference for this Market Survey Request is **MS-423340-ICH-RG**, and all correspondence and submissions concerning this matter should include this number.

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 summary of requirements in Annex A to determine interest.

6. Responses shall in all cases include the name of the firm, telephone number, email 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 capability by the NCI Agency.

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

8. Responses are requested to reach the NCI Agency no later than by **17:00 Brussels** time on **31 January 2025**.

9. Please send all responses via email to the following NCI Agency Point of Contact:

To Attention of:	Ms. Estefania Nunez, Principal Contracting Assistant,
E-mail:	estefania.nunez@ncia.nato.int

NCIA/ACQ/2024/07509

10. Bilateral meetings with industry are not foreseen during this initial stage, however technical discussions may take place following the submission of responses, with the purpose of clarifying or further augmenting those responses where required.

11. This RFI aims to apply due diligence by 'testing the market' to determine the relevant technologies and products or services which may provide the basis for the ICH-RG capability development strategy, while also evaluating the potential solutions available to NATO which may include "Adopt"-ing (an existing solution already in-service by Nations), commercial "Buy"-ing (acquiring a solution from industry), or "Create"-ing (developing a solution exclusive to NATO needs), or a combination thereof.

12. This Request for Information (RFI) does not constitute a commitment to issue a future request for proposal (RFP).

13. Note that this RFI is not a formal request for submissions as part of a procurement; but rather a general request intended to determine whether any possible solutions exist that should be considered or included in evaluating the options as part of the system requirements development.

14. Respondents are requested to await further instructions after submission of their responses regarding any potential future bidding process, and are requested to contact only the NCI Agency POC identified above in Paragraph 9 above with any further requests for information or clarification.

15. Any response to this request shall be provided on a voluntary basis. Responses to this request will help identifying and selecting firms eligible for any future procurement that may arise from this Market Survey.

16. In accordance with the NATO Management of Non-Classified NATO Information policy (C-M(2002)60), this **MS-423340-ICH-RG** shall not be published on the internet.

17. 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 informational only and will not be construed as binding on NATO for any future acquisition.

18. 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.

19. Your assistance/participation in this Market Survey request is greatly appreciated.

FOR THE CHIEF OF ACQUISITION:

Estefania Nunez

Digitally signed by Estefania Nunez
Date: 2024.12.13 16:08:52 +01'00'

Estefania Nunez

Principal Contracting Assistant

NCIA/ACQ/2024/07509

Enclosures:

Annex A: Summary of Requirements

Annex B: Questionnaire

Annex C: Distribution List

Annex A

Requirements Summary

A.1. ICH-RG Introduction

[1] NATO's Military information exchange requirements are currently not fulfilled through existing capabilities. The introduction of the Information Clearing House Release Gateway (ICH-RG) is expected to address some of the capability gaps.

[2] The ICH-RG capability will enable information sharing across all NATO security domains[1] and also outside, including domains for Non-NATO entities (NNE) at the lower level since most of the operations currently conducted by NATO require an extensive collaboration between NATO and non-NATO/non-coalition partners, including national governments, the United Nation, the European Union, and non-governmental organizations.

[3] The ICH-RG will enable Mission Commanders afloat and ashore to disseminate or receive critical public information, operational and intelligence documents across all information security classifications. The ICH-RG project aims to develop and provide a security accredited Cross Domain Solution (CDS) with Information Products transfer capabilities to NATO.

A.2. Background

[4] We are building a non-monolithic, modular solution as part of NATO deployable CIS (refer to Figure 1). The full scope of the capability includes mechanisms like Information Catalogues and Information Release/Guard

[1] These network domains are identified by a difference in who manages the CIS in terms of administrative authority, who uses the CIS, the security mode of operation of the CIS and/or the highest security classification level permitted to be processed, stored and/or transmitted by the CIS.

NCIA/ACQ/2024/07509

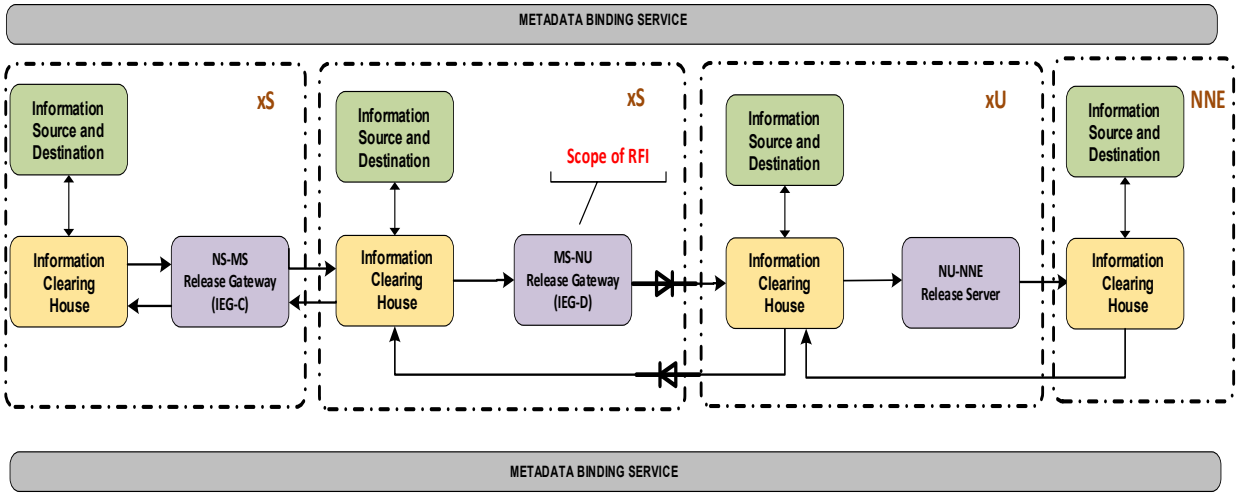

Figure 1. The HAG is a key component enabling the IEG Scenario D.

[5] As per Figure 1, the following should be noted.

1. NATO operates its CIS on various networks (NATO SECRET [NS], NATO RESTRICTED [NR], NATO UNCLASSIFIED [NU], NATO-Led Mission SECRET [MS]) with narrowed capability to exchange information with NNEs.
2. NATO introduced the concept of the Information Exchange Gateway (IEG) to provide a secure solution for cross-domain interconnectivity. Information Exchange Gateway Scenario D (IEG-D) shall support the connection of NATO CIS up to NATO SECRET classification with a NNEs CIS (that is assumed as UNCLASSIFIED).

[6] The IEG Scenario D should be understood as the interconnection at the equivalent classification level of NATO CIS (or NATO Nation CIS handling NATO information) to NATO Mission CIS at NATO RESTRICTED and below (refer to Ref [C]).

[7] The ICH-RG will provide two main capabilities:

1. Information Catalogues with synchronised repositories serving as the ICH that enables a mission-wide inter-domain information sharing facility, and
2. The Release Gateway (RG) providing a mechanisms for domain protection, high assurance2 separation at system boundaries, and controlled information release between domains, thereby offering a practical solution to some urgent operational needs.

[8] The key concern of this RFI includes the High Assurance Guard (HAG). The HAG is a

[2] The term high assurance is applied to mean that very convincing evidence exists that a system has a given set of properties. Within the Common Criteria (CC), the term high assurance was traditionally reserved for systems providing evidence from formal or semi-formal methods, such as that which would be required for Evaluation Assurance Levels (EAL) greater than or equal to 5 (Ref A).

component within the Release Gateway that supports certain information exchange requirements (IERs) for the ICH-RG, specifically, information exchange between a Classified security domain with high trust and an Unclassified domain, commonly understood as IEG Scenario D (IEG-D), which implements release decisions and security enforcement.

[9] As depicted in Figure 1, in the deployable ICH-RG architecture, all information flows and access control policies are within multiple administrative boundaries under full NATO authority, this authority extends to and includes the direct internet facing Non-NATO Entity (NNE) Information Portal.

[10] The Alliance Information Exchange capability development is an on-going set of activities within NATO, which focuses specifically on the information exchange requirements and issues across security boundaries. The ICH-RG relies on a high-assurance infrastructure for cryptographic Metadata binding, signing or verification of contents and Metadata, and their release.

[11] Nations/industry are requested to state in their response if they can meet the whole, or part of this capability requirement and if they are willing to provide the required capability as stand-alone solution or as part of a consortium of Nations (and/or industry participants).

A.3. ICH-RG Business Process and Use Case Description.

[12] The main high-level use cases of the ICH-RG are related to the following aspects;

1. Mission-wide intra-domain information sharing between security and management domains.
2. Information sharing between information security domains and external partners, connected via the internet, to support the comprehensive approach.

[13] The ICH-RG capability high-level use cases are facilitated by a number of business processes and technical functions in the following ways

1. Information Clearing House (ICH), creates a common, multi-domain mission Information Catalogue, by:
    a. Provision of a mission wide Information Catalogue.
    b. Use of Metadata for information handling.
    c. Use of event management workflows for automated actions, Information Products (IP), message routing instructions and notifications.
    d. Provides the end-user with automated processes workflow tools to support IP transfer from receiving phase to disclosure.
2. Release Gateways (RG), enabling the automated or semi-automated release of information between the various security domains, and with all mission relevant internal and external partners. The Release function provides:
    a. Information release by a Release Authority using Metadata for security aspects.
    b. Use of policies for information protection and information release.
    c. Provide auditing and accounting functions.
    d. Release policy enforcement by Release Authority and technical enforcement of policies using Release Rules.

e. Supporting the administrator level users and the Information Management (IM) team with automated tools.

[14] To support the high level use cases listed above, the ICH-RG allows users from different C2 entities within a mission to access the Information Catalogue. Users can submit Information Products for inclusion into the mission Catalogue in the information security domain they are connected to. The ICH-RG will then facilitate maintenance of the Information Catalogue, and IP sharing between the information security domains and Non-NATO Entities in compliance with the Information Product Metadata classification and related release policies.

[15] In the ICH-RG information handling architecture, content labelling with Metadata is done by the Originator, the "Information Author". Policy maintenance is performed by the policy authorities' "Release Administrator" (not shown in Figure 2) and the validation of the Metadata and IP with the policies is done by the systems providing the guard[3] services within the Release Gateway.

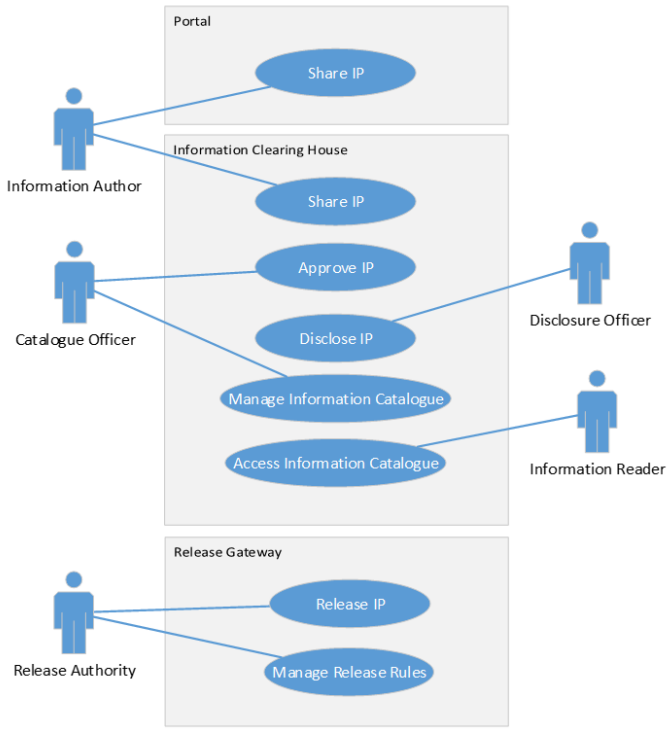

Figure 2. The ICH-RG business process diagram depicting various actors.

[3] By guard, we imply a protection system consisting high assurance software implementing a chain of filters, which examine the content traversing in order to ensure that the classification labels are valid; that they conform to the release policy; and that no covert channel can be established between different network/domains.

[16] The ICH-RG defines a number of basic user roles described below and depicted in Figure 2;

1. Information Author: Generates and submits Information Products to the ICH-RG for inclusion in the Information Catalogue and for sharing/disclosure to other security domains.
2. Information Reader (User): A consumer of IPs published in the Information Catalogue.
3. Catalogue Officer: Apply quality and relevance control to the products submitted to the ICH, and manages the Information Catalogue.
4. Disclosure Officer: Validates the IPs offered for disclosure to a lower security domain complies with Mission Commanders release policies.
5. Release Authority: Executes the final release of the IPs that are transferred from a higher to a lower classification information security domain.
6. Mission Commander: Defines the overall requirements and rules of IP generation, sharing and disclosure, and agreeing MOUs with the various Non-NATO-Entities.
7. The Release Administrator and System Administrator are specific administrative roles with full privileges without restrictions. The System Administrator is a system level access only, to create, edit or delete users (including other System Administrators) and assign or revoke roles to them but no access to the information flow control mechanisms or policy rules creation.

A.4. The Release Gateway High Assurance Guard Description

[17] The main function of the HAG within the Release Gateway on the interface between the High and Low network enclaves (an interconnection defined as IEG Scenario D) is to approve or reject the transmission of Information Products between the Mission S3cr3t and Mission Unclassified network based on a **STANAG**-4774/4778 compliant trusted classification label. The HAG supports bi-directional flow (shown otherwise in Figure 1) and relies on the use of cryptographically bound XML-based content Metadata for making decisions about the processing or the release of information.

[18] The HAG MUST enforce information flow control policy for controlled information sharing and mitigate against two major threats introduced by cross-domain information exchange, specifically, there are two risks, namely;

1. Leakage of confidential information from one information security domain to another information security domain; and,
2. Degradation of the integrity or availability of resources in one information security domain as a result of actions originating from another information security domain.

[19] An implementation of HAG as a part of IEG-D represents a technical solution which could be acceptable for NATO accreditation bodies for the specific case described in this Annex, after having been confirmed by an extensive security risk assessment prior to deployment of this solution.

[20] The HAG envisaged within the Release Gateway is to be used in an information exchange scenario which requires trustworthy release of cryptographically labelled Information Products (IP), mainly comprising of XML based documents (e.g. Office Open XML and Portable

Document Format)[4]. By introducing the HAG, information sharing impediments as a result of security domains are expected to be removed and replaced with a multilevel security service enabled by a Trusted Computing Base platform.

[21] The ICH-RG uses the concept of Information Product (IP) as a generic term. IP is a "package" containing data object(s) in a defined/agreed standard, they are transferred between systems as a "Message" which enables different components within the ICH-RG solution to extract the required information and obtain a common understanding of the packaged IP message in order to execute decisions based on the contents e.g. classification, 'releasable' etc. A data object is a known data of finite size with a given unit of measure (e.g. Byte) and a known structure e.g. UTF-8 encoded XML-based document format.

[22] Content filters are critical for the protection of the integrity and availability of the internal domain by implementing specific filtering (such as virus scanning) of the content transmitted between security domains. Content filters are part of the NATO Content Inspection Policy Enforcement (CIPE) architecture and it is required that the operational environment provide appropriate content filters.

[23] The Content Inspection Policy Enforcement (CIPE)[5] capability is to be provided as a component of the HAG in order to improve the protection for confidentiality, integrity and availability of NATO CIS against malicious software and active content that may be imported from other information systems.

A.5. High-assurance Attribute-based Access Control (ABAC) Guard (HAAG) Concept

[24] The security requirements that apply to the High Assurance Guard are based on the Common Criteria (CC) "Protection Profile for the NATO High-assurance Attribute-based Access Control

[4] Although, NATO operations require the exchange of a wide variety of data, data formats and information between
- a. NATO Consultation, Command and Control (C3) systems and:
- b. National Consultation, Command and Control (C3) systems;
- c. NATO domains and NATO Mission partners (including Non-NATO Troop Contributing Nations) at classified network level; and
- d. Non-NATO Entities.

The Information Exchange in the ICH-RG is primarily concerned with [c] and [d] above (i.e. not between C3 systems, although it may originate from it) to satisfy operational requirements use cases such as (1) Conflict and Natural Disasters IE Use Case, (2) Contamination Ballistic Missile Attack IE Use Case.

[5] Content Inspection Policy Enforcement (CIPE), Ross & Oudkerk, 2011 (Ref[B]) is a capability that enables the inspection of structured data that is to be mediated by the HAAG. The goal is to identify and remove malicious software (such as viruses, network worms and Trojan horses) and active content, combined with a verification of file format type and a white list of allowed file formats.

(ABAC) Guard (HAAG)", ([NCIA TR-2012-SPW008418-13-4, 2013]) developed by the NCI Agency.

[25] The HAAG may be considered a specific implementation specification of an HAG that was developed as part of NATO Scientific Program of Work.

[26] The main purpose of the HAAG Protection Profile (PP) is to formalize the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for the high-assurance attribute-based access control guard solutions to be used within NATO.

[27] The HAAG enables the realisation of a solution for automated cross-domain information exchange which offers the required level of security assurance with respect to the interconnection. The HAAG mediates the flow of data objects between services and user terminals operating in different information security domains. The HAAG is intended for use in information-processing environments, in which a high level of document security, operational accountability, and information assurance is required, without hampering information sharing with coalition partners and external organizations.

[28] The HAAG Protection Profile is to be used as a target specification for the implementation, and/or the Common Criteria evaluation of products providing a HAAG capability for information-sharing use cases, i.e. within the scope of the IEG-D architecture, these aforementioned documents can be made available to the industry for the stated purposes.

[29] A per Figure 3, the security functional requirements (SFR) which are relevant to the scope and implementation of the HAAG concerns information flow policies and content inspection policies.

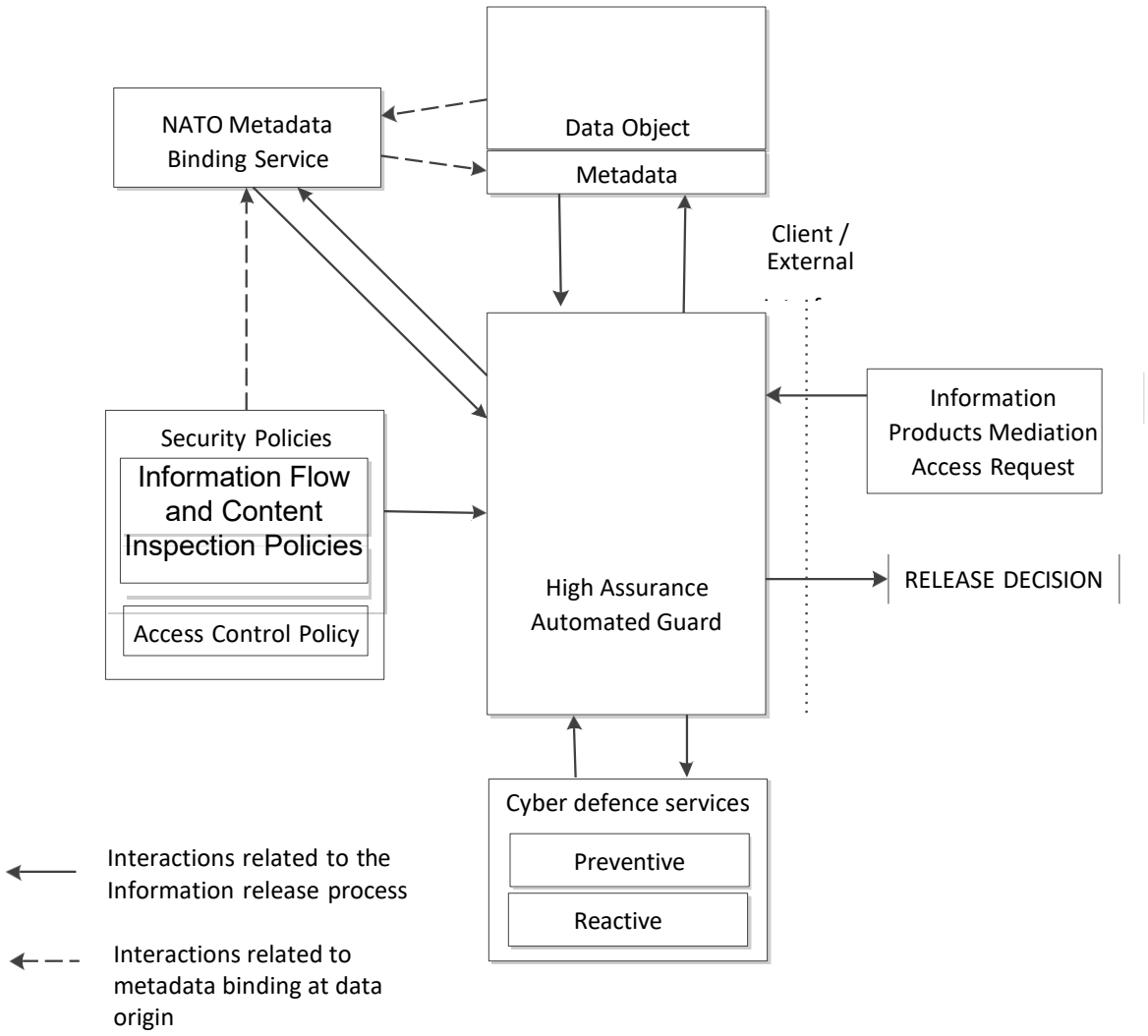

Figure 3 Design Principle for the HAAG

A.6. HAG Countermeasure Characteristics

[30] To mitigate the two mains risks identified in [18], the operating environment and the design of the MUST provide a number of countermeasures by means of the following;

1 Physical protection (the system will be located in areas with Restricted Access).

2 The guard application shall be able to provide, with a specified assurance level, the following functionalities

2.1 Control/mediate the direction of traffic flow through the Information Flow Control (IFC) policies enforcement based on Metadata labelling; and

2.2 Implement domain separation with effective and high assurance separation interfaces/networks for restricted system interconnections; and
2.3 Able to perform Content Inspection and mediation functionality based on protection policies including XML payload schema validation; and
2.4 Implement full HTTP Proxy with HTTP header control/re-write; and
2.5 Perform verification of digital signature based on XMLDSIG for labelled content conforming to a given Metadata label specifications; and
2.6 Perform release decisions for labelled HTTP content/ payload based on security policy; and
2.7 Provide the capability to detect and create records of security-relevant events associated with users.

3 High Assurance Guards shall typically have the following characteristics:

3.1 **Non-By-passable**: Only explicitly controlled channels can be used to exchange information (two ways) between domains having different security level. The Information Flow Control policy, based on security labels and content inspection, is enforced by means of a non-by passable Security Monitor.

3.2 **Evaluable**: Each component is to be designed and implemented in a clear and effective way, in order to be evaluated by a third party with any specified assurance level (e.g. Common Criteria Evaluation Assurance Level (EAL)).

3.3 **Always Invoked**: All accesses and policy enforcement shall always (every time) be mediated by the Security Monitor.

3.4 **Tamper Resistant and Tamper Evident**: Any attempt to circumvent, modify or bypass the security configuration and the Security Monitor shall be detected and blocked if possible.

3.5 High assurance software engineering process (es) or practices observed as part of the software lifecycle development, with a formal framework employed during the design and implementation of this solution.

4 Secure design and implementation:

4.1 Use of Defence in Depth, Zero trust design paradigm, minimal configuration, redundancy, self-protection, isolation, heterogeneity (e.g. Boundary Protection Device (BPD) from different vendors), out-of-band management, etc.

4.2 All software application(s) enabling the information flow, content inspection, access control, content policy enforcement and release of information subject to high assurance software engineering process during the design and implementation of those services.

4.3 De-Militarised Zone (DMZ) to provide IES.

4.4 Use of High Assurance Common Criteria certified firewall, IDS/IPS, etc., properly configured in accordance with the certification report.

5 Cyber Defence services:

5.1 Content management, Host-based and Network-based Anti-Malware, Intrusion Detection Systems (IDS),

5.2 Privilege management, Auditing, process accounting, Security Information Event Management, and Logging

5.3 Vulnerability Management/attack surface reduction.

5.4 Application-level firewalls.

5.5 Patching services and periodical security assessment and security hardening.

NCIA/ACQ/2024/07509

Annex B

Questionnaire

Organisation Name:

Contact name & details within organisation:

Notes

- Please **DO NOT** alter the formatting. If you need additional space to complete your text then please use a 'Continuation Sheet' which you can append at the end of this Annex and please 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. If you need additional space, please use the sheet at the end of this Annex.
- 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 B.
- 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

B.1. Information Clearing House Release Gateway Solution

A. Do you currently have a solution, planning to or currently working to deliver an operational ICH-RG capability similar to the description provided in Annex A? If so, when can such solution be made available to NATO, and for how long?
   1. If so, please specify if your solution can be made available to NATO for evaluation or use.
   2. If your solution can be made available for NATO use, can you specific any restrictions of use, including but not limited to Intellectual Property rights.
   3. If your existing solution cannot be adapted or made available directly to NATO for use and evaluation, can you provide an alternative technology or solution? Please state any relevant condition(s) necessary for you to provide an alternative solution.

Answer:

B. Do you currently have the entirety of the solution that may provide (or be adapted) the capability requirements as described in Annex A or part of it? This implies you have a solution with functional and security characteristic similar to the Information Clearing House only, the Release Gateway only or both.

Answer:

C. Can your solution be demonstrated to NATO staff members within a month notice?

Answer:

D. Is your solution currently used as a deployable capability or used from a static Data Centre setting only?

Answer:

E. Can you describe at what capability lifecycle stage is your ICH-RG-like solution for example, is it at exploratory, experimental, development, operational or deprecated stage.

Answer:

F. Are you able to share information on the system description including high-level architecture, of this solution? If so, can you provide this information in your response?

Answer:

G. Are you able to share any information that may enable the evaluation of completeness and appropriateness of your solution to meet our requirements?

Answer:

H. Can you state/describe if a specific high assurance software engineering process(es) or practices was observed as part of the software lifecycle development, and describe the framework (if formal), employed during the design and implementation of this solution?

Answer:

B.2. High Assurance Guard Products/Solution

This section of the RFI is seeking information on guard solutions that can fill the requirement goals of a non-monolithic modular componentized solution. NCIA is inviting industry, and Nations to submit information/white paper on existing and under-development concepts, products or capabilities in the area of High Assurance Guard (HAG).

The RFI is expected to address the following questions;

A. Do you currently have a High Assurance Guard solution that mediates the information exchange between different security levels of information classification?

Answer

B. Can you describe some of the use cases for which your HAG solution is currently employed and other foreseen potential use(s) to protect high-value resources?

Answer

C. Is your HAG solution a Commercial of-the-Shelf solution or a special purpose development effort that was built for Nation own use?

Answer

D. Can you provide (or describe) the functional and security basis (e.g. including a Common Criteria Protection Profile) for your High Assurance Guard technology. This is to establish evidence or evaluate that your guard services or application meets NATO requirements specification or comparable to it.

Answer

E. Can you provide the details of the Operating System on which your High Assurance Guard was built?

Answer

F. Does the Trusted Base Platform consisting of the Operating System (OS), tools and applications implement a security model that employs any of the following security engineering approaches;
   i. A system-wide Mandatory Access Control (MAC);
   ii. A Role-based Access Control (RBAC) or/and an Attribute-based Access Control (ABAC);
   iii. Multilevel security (MLS) service and;
   iv. A Reference Monitor?

   If so, provide further information describing the organization of security components throughout the system.

Answer

G. Are there export restrictions attached to your HAG solution in part or whole that cannot be circumvented or requires sale authorisation from National competent authorities.

Answer

H. Are you able to share information concerning functional decomposition of the system, any high level formal specification and formal analysis tools which may provide the basis for formal verification

Answer

I. Please share your HAG high-level solution architecture about the following major security aspects.
   i. Authentication and authorization mechanism(s) for users/applications on both the low and high network sides
   ii. Audit capability, accounting capability for processes and users, and configuration monitoring.
   iii. Access control mechanisms or paradigm including support for separation of duties and least privilege.
   iv. Cryptographic functions support including PKI and key management.
   v. Information Flow Control
   vi. Describe the content filter capability of the HAG including supported data formats, extensibility options and support for plug-ins.
   vii. Metadata binding including support for binding, verification of STANAG-4774[6] and STANAG-4778[7] complaint labels.
   viii. Security management[8] including security information management emanating from services (such as Identity, Configuration, Audit, Metadata, Policy and Credential) and Information assurance services (such as Confidentiality, Integrity, Availability, Authentication and Non-repudiation).
   ix. External cyber defence capability for reactive/proactive security services.
   x. File system support for full-disk encryption for data-at-rest.

Answer

[6] STANAG-4774, "Confidentiality Metadata Label Syntax"
[7] STANAG-4778, "Metadata Binding Mechanism"
[8] These security management services are expected to be a set of comprehensive and integrated services and not to be understood as separate entities in practice.

J. Is your HAG registered as an approved product/solution under any national (or international bodies) such as NATO Information Assurance Product Catalogue (NIAPC or a national equivalent)?
If so, please provide further information.

Answer

K. Describe if your HAG product/technology has been subject to IT security evaluation or validation by an independent testing laboratory (such as an accredited Common Criteria Testing Laboratories or similar bodies in other non US jurisdictions) for compliance (or conformance) to applicable Protection Profile as those found in International Standard ISO/IEC 15408 series, Common Criteria for Information Technology Security Evaluation or national equivalents.

Answer

L. If yes (to [K]), if you can share the evaluation test report, kindly furnish it.

Answer

M. Can you share publicly available product/solution documentation manuals including administration guide and other applicable reference materials for your HAG technology?

Answer

N. Please provide a Rough Order of Magnitude (ROM) cost for the yearly use of the HAG solution, based on the quantity and period of commitment that you are able to offer. Please include any assumptions that this ROM is based upon, including management fees for operating and supporting the capability, if and where applicable.

Answer

O. To help us understand how the assurance gained from an evaluation will be maintained, and how continuous product development and changes to the HAG solution may be analysed to determine security impact, provide us with information regarding the product life-cycle model, life-cycle management and support including release cycle. This life-cycle model should describe the procedural aspects regarding the development of the guard solution, such as design methods, code and documentation reviews, and how changes are reviewed and accepted or rejected.

Answer

NCIA/ACQ/2024/07509

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 __

NCIA/ACQ/2024/07509

Annex C

Distribution List for Market Survey

MS-423340-ICH-RG

NATO Delegations (Attn: Investment Committee Adviser):

Albania	1
Belgium	1
Bulgaria	1
Canada	1
Croatia	1
Czechia	1
Denmark	1
Estonia	1
France	1
Germany	1
Greece	1
Hungary	1
Iceland	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
Montenegro	1
Netherlands	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Türkiye	1
United Kingdom	1
United States	1

Belgian Ministry of Economic Affairs 1

Embassies in Brussels (Attn: Commercial Attaché):

Albania	1
Belgium	1
Bulgaria	1
Canada	1
Croatia	1
Czechia	1
Denmark	1
Estonia	1
France	1
Germany	1

Greece	1
Hungary	1
Iceland	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
Montenegro	1
Netherlands	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Türkiye	1
United Kingdom	1
United States	1

NATEXs

All NATEXs	1 Each