



NCIA/ACQ/2021/06761
25 June 2021

Market Survey Request For Information

WHOIS database provider (WHS)

MS-CO-115492-WHS

The NCI Agency requests information regarding WHOIS database providers, that can provide information on which person and organization register a domain, and that is able to reverse search in order to find related attacker infrastructure, through their application. The purpose of this market survey is to seek WHOIS database providers that meets NCIA minimum requirements.

NCI Agency Point of Contact
Contracting Officer, Frank Iyakaremye and Leonora Alushani
MS-CO-115492-WHS@ncia.nato.int

To: See Distribution List

Subject: NCI Agency Market Survey Request MS-CO-XXXX
WHOIS database provider (WHS)

1. NCI Agency requests the assistance of the Nations to identify industry contacts for an application able to WHOIS services that meets NCIA minimum performance requirements.
2. The NCI Agency reference for this MS is **MS-CO-115492-WHS**, and all correspondence and submissions concerning this matter **must** reference this number within the documentation and email subject line.
3. This Market Survey (MS) is being issued to obtain information on existing product and how they can possibly meet our requirements as well as to identify potential NATO-nation based product and possible suppliers.
4. The MS minimum requirement are provided in Annex A. Each nation is requested to forward this MS to all potential vendors that are WHOIS database providers.
5. Responses shall be submitted to the NCI Agency POC at point 9 of this letter.

Respondents are invited to carefully review the questions within Annex A of this letter to determine interest.

6. Responses shall in all cases include the name of the firm, telephone number, e-mail address, designated Point of Contact, and NATO UNCLASSIFIED responses to the scenarios in Annex A. This shall include any restrictions (e.g. export controls) for direct procurement by NCI Agency.
7. The closing date for this MS is **close of business Monday, August 16, 2021**
8. Please send all responses via email to the following NCI Agency contact:

Mr. Frank Iyakaremye, Contracting Officer
E-mail: MS-CO-115492-WHS@ncia.nato.int

9. Product demonstrations or face-to-face briefings/meetings with industry are not foreseen during this initial stage. 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 in Paragraph 9 above.
10. 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 MS. Responses to this request, and any information provided within the context of this survey, including but not limited to capabilities, functionalities and requirements will be considered as indicative and informational only and will not be construed as binding on NATO for any future acquisition.
11. The NCI Agency is not liable for any expenses incurred by firms in conjunction with their responses to this MS and this survey shall not be regarded as a commitment of any kind concerning future procurement of the items described.

For the Director of Acquisition:

Frank Iyakaremye
Contracting Officer

Attachment(s):

Annex A- WHOIS database provider (WHS) Market Survey

Annex A- WHOIS database provider (WHS) Market Survey

1. Purpose

- 1.1. The NCI Agency requests information regarding potential Vendor that can provide a WHOIS database product, able to meet NCIA minimum requirements.
- 1.2. Issuance of a Market Survey (MS) is viewed as the fastest, most efficient approach in which fairness can be upheld.
- 1.3. For Section 3 below, responders are requested to describe how their product can meet NCIA minimum requirements for a WHOIS database provider. Responses to this market survey must be made in a separate documents answering how the product meets all the listed requirements, in section 3.
- 1.4. In Section 4, a Rough Order of Magnitude in a native MS Excel is requested.

2. Important Notes

- 2.1. The MS is solely a request for information, to support requirements and approvals. It shall not be treated as a request for quotation or an invitation for bids. The Agency will consider and analyse all information received from this MS and may use these findings to develop a future Request for Quote (RFQ).
- 2.2. Any future RFQ would be advertised on the Agency's bulletin board for all eligible companies to respond. Participating in this MS will not benefit, or prejudice, involvement in any future RFQ.
- 2.3. Responders must validate that their product meets all the requirements listed in section 3, below.

3. Market Survey requirements

1. The product must have a searchable data set accessible by Internet containing DNS related data (both current and historical). Please indicate how your product meets this requirement:

- 1.1. Number of historical WHOIS records must not be smaller than 10 billion records. Please indicate how your product meets this requirement:

- 1.2. Number of Domain/IP observations must not be smaller than 15 billion.
Please indicate how your product meets this requirement:

- 1.3. Contain collection of DNS data from the last 15 or more years.

Types of records

- 1.3.1. WHOIS
- 1.3.2. WHOIS history
- 1.3.3. Hosting History
- 1.3.4. Reverse WHOIS
- 1.3.5. Brand name
- 1.3.6. Name server change

Please indicate how your product meets these requirements:

- 1.4. The product's data set must contain/support the following data types:

- 1.4.1. ASN
- 1.4.2. Alexa ranking
- 1.4.3. Contact Information (registrant, admin, tech, billing, SOA, etc)
- 1.4.4. Create Date
- 1.4.5. Domain name
- 1.4.6. Email (registrant email)
- 1.4.7. Email address(es)
- 1.4.8. Expiration Date
- 1.4.9. IP address
- 1.4.10. IP Address details (ISP, ASN, Country)
- 1.4.11. IP Address History summary
- 1.4.12. Hosting History for domain (IP and Name Servers)
- 1.4.13. MX (Mail Exchanger) Information
- 1.4.14. Name Server
- 1.4.15. Name Server History summary
- 1.4.16. Redirect Domain
- 1.4.17. Registrant
- 1.4.18. Registrant Organization
- 1.4.19. Registrar
- 1.4.20. Registrar History summary
- 1.4.21. Registrar Status
- 1.4.22. SPF (Sender Policy Framework) rules

- 1.4.23. SSL certificate Country
- 1.4.24. SSL certificate Hash
- 1.4.25. SSL certificate Organization
- 1.4.26. Screenshot on-demand
- 1.4.27. Historical screenshots
- 1.4.28. Status (active or inactive)
- 1.4.29. Tags
- 1.4.30. Website Response
- 1.4.31. WHOIS History summary
- 1.4.32. "Raw" WHOIS record

Please indicate how your product meets these requirements:

2. How many years of collected records, does the product have?

3. The product must support bulk searches. Please indicate how your product meets this requirement:

4. The product must have an alerting by e-mail capability. The alerts must be able to be generated when changes are observed in DNS related data defined below:

- 4.1. IP address values
- 4.2. Brand name values
- 4.3. Domain name values
- 4.4. DNS name server values
- 4.5. Registrant values

Please indicate how your product meets these requirements:

5. Accessibility Web and API:

5.1. The product must be able to query the data set using both:

- 5.1.1. Web interface
- 5.1.2. Application Programming Interface
 - 5.1.2.1. API must support HTTPS queries
 - 5.1.2.2. API must support responses in JSON format

Please indicate how your product meets these requirements:

6. Advanced web search interface:

6.1. Product needs to be equipped with a web based advanced visual search interface being able to query the data set and visualize findings in form of a visual graph.

Please indicate how your product meets this requirement:

6.2. The visual search component must be able to serve as cyber threat intelligence and investigation platform that combines enterprise-grade domain and DNS-based intelligence with an intuitive web interface.

Please indicate how your product meets this requirement:

6.3. The search component must allow to pivot on an attribute/Incident of Compromise to narrow down search results and filter out data which are out of scope of analysis

Please indicate how your product meets this requirement:

6.4. The visual search component must be able to pivot on such data types as:

- 6.4.1. Domain
- 6.4.2. Email (registrant email)
- 6.4.3. Email (SOA)
- 6.4.4. Email domain
- 6.4.5. Name Server
- 6.4.6. IP (Address, ISP, ASN, Country)
- 6.4.7. MX (Mail Exchanger) Information
- 6.4.8. SPF (Sender Policy Framework) rules
- 6.4.9. SSL certificate Hash
- 6.4.10. SSL certificate Organization
- 6.4.11. Dates (create, expiration)

6.4.12. TLD (top level domain)

Please indicate how your product meets these requirements:

6.5. The visual search component must support filter options

6.5.1. Logical operators (AND and OR)

6.5.2. Match rules (they may depend on data types) including

6.5.2.1. Begins With

6.5.2.2. Ends with

6.5.2.3. Matches

6.5.2.4. Exactly Matches (case sensitive)

6.5.2.5. Does Not Match

6.5.2.6. Does Not Exactly Match (case insensitive)

6.5.2.7. Contains (matches if any term in the query is found)

6.5.2.8. Contains All

6.5.2.9. Does Not Contain

6.5.2.10. Does Not Contain All

6.5.2.11. Greater Than

6.5.2.12. Less Than

6.5.2.13. Equal To or Less Than

6.5.2.14. Greater Than or Equal To

Please indicate how your product meets these requirements:

6.6. The visual search component must save previous queries in order to understand the previous steps of pivoting, including the ones that were promising and the ones that were not.

Please indicate how your product meets this requirement:

4. Rough Order of Magnitude (ROM) price data

4.1. Please provide a ROM pricing data for the product. The ROM submission must be in an MS Excel and in a native format.