Acquisition Directorate
dorina.cani@ncia.nato.int
Telephone: +32 (0)2 707 8421

NCIA/ACQ/2021/6724
22 March 2021

Market Survey-Request for Additional Information

Project "Enhanced Security Solution for Oracle e-Business Suite Release 12.1.X and above"

NCI Agency Reference: 115443 Enhanced Security Solution for Oracle e-Business Suite

The NCI Agency is seeking information from Nations and their Industry in order to assess the feasibility of the delivery of a enhance security solution for Oracle e-Business Suite Releases 12.1.X and above.

NCI Agency Point of Contact
Principal contracting assistant: Dorina Cani
E-mail: Dorina.cani@ncia.nato.int

To: See Distribution List

Subject: NCI Agency Market Survey Request enhance security solution for Oracle e-Business Suite

1. NCI Agency requests the assistance of the Nations and their Industry to identify available Commercial-Off-The-Shelf (COTS) solution to meet the requirement for enhance security solution for Oracle e-Business Suite.

2. This Market Survey is being issued to identify potential solutions and possible suppliers.

3. The broadest possible dissemination by Nations of this Market Survey Request to their qualified and interested industrial base is requested.

4. 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.

5. The NCI Agency reference for this Market Survey Request is MS-115443, and all correspondence and submissions concerning this matter should reference this

number.

6. A summary of this emerging requirement is set forth in the ANNEX B attached hereto.

7. Other supporting information and documentation (technical data sheets, marketing brochures, catalogue price lists, descriptions of existing installations, etc.) are also desired.

8. The Market Survey will **ONLY** be assessed on the responses to questions in ANNEX C – Market Survey Questionnaire. 0 provides details of the requirements.

9. Responses are due back to NCI Agency no later than **17:00 hours Brussels time on 12 April 2021**.

10. Please send all responses, via email, using MS-CO-115443-EBA in the title of the email to: dorina.cani@ncia.nato.int

11. The Agency reserves the right to request a solution demonstration of the described solution. However, given the current global landscape, any solution demonstration will be delivered via video conferencing tool at the discretion of the Market Survey Respondent.

12. Any response to this request shall be provided on a voluntary basis. 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 indicative and informational 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 Director of Acquisition

Gael Craver

Digitally signed by Gael Craver
Date: 2021.03.23 14:31:25 +01'00'

Gael Craver
Principal Contracting Officer

ANNEX B.

MARKET SURVEY REQUIREMENTS FOR ENHANCED SECURITY SOLUTION FOR ORACLE e-BUSINESS SUITE

1. Scope

1.1. NCI Agency is performing a market survey in order to identify available enhanced security solutions for Oracle e-Business Suite on the market that fulfil the requirements presented below. At this stage, NCI Agency is willing to evaluate all the available systems on the market which can provide technological, robust, capable and cost effective solution to NATO.

2. Current Solution

2.1. The Agency is currently using Oracle e-Business Suite Releases 12.1.3 and above to manage internal processes.

2.2. For redundancy and failover, multiple web application tiers are used, with an integrated web application firewall/load balancer to manage the redundancy.

2.3. The architecture of the Oracle e-Business Suite COTS product is very complex and very difficult to secure against possible web attacks – when installed it includes all products which is over 25 modules with +/- 20,000 web pages.

2.4. Protection for the Oracle e-Business has been historically implemented using centralized Web Application Firewall (WAF) appliances. The centralized WAF can offer the generic web protection, but require significant effort, knowledge and time in order to develop and maintain dedicated rules and security policies for each of the protected services. The Agency is lacking this expertise and manpower required to develop the rules for e-Business Suite.

3. Requirements/Functionalities

4.1. The NCI Agency's goal is to try and find a specialised COTS product which will further enhance the security of Oracle e-Business Suite.

4.2. Please refer to Annex D and focus on "Must Haves" requirements.

4. Life Cycle information

5.1. The system design should minimise total system life cycle costs, including its future Operations and Maintenance (O&M).

5.2. The software and hardware environment in NATO are in the process of being upgraded by the IT Modernisation project based on a modern data centre approach. However, note that the majority of the NATO systems run on Microsoft/LINUX operating systems and must be capable of running in a virtual environment (VMWare Hypervisor).

ANNEX C.

1. Questionnaire

Organisation Name:

Contact Name & Details:

Notes:

1. Please **DO NOT** alter the formatting. 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. Please feel free to make assumptions, ***HOWEVER*** you must list your assumptions in the spaces provided.

3. 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 a continuation sheet and clearly refer to the question being answered

4. Please **DO** try and answer the relevant questions as comprehensively as possible.

5. All questions within this document should be answered in conjunction with the summary of requirements in ANNEX B.

6. All questions apply to Commercial or Government responders as appropriate to their Commercial off the Shelf (COTS) or Government off the Shelf (GOTS) products.

7. Cost details required in the questions refer to Rough Order of Magnitude (ROM) including all assumptions the estimate is based upon.

2. General Questions

1. Do you have an in-service EBS solution that currently meets the requirements as detailed in ANNEX B, 0.

2. Can your solution be implemented on-premise?

3. Provide details of where it is used and deployed and the number of users.

3. Detailed Questions

1. COTS Solution

1.1. Please indicate the areas in 0 where your solution would not meet either entirely or partially.

1.2. Is your proposed system/technology currently in active service as a COTS solution? If so, where and what types of support does your organisation currently provide for such a capability?

1.3. Please provide the following information regarding current and previous uses of your available COTS solution:

1.3.1. Names of customers/users.

1.3.2. UNCLASSIFIED details on the specific programme your COTS solution supported.

1.3.3. Overview of any modifications to the COTS solution necessary to support these customers and the licensing terms applicable to modifications of the COTS product, stating also whether those will be assigned to the NCI Agency (Foreground/Background IPR).

1.4. Please provide us with any additional capabilities of your COTS solution that go above and beyond those included in ANNEX B.

1.5. Advantages & disadvantages of your product/solution/organization.

1.6. Any other supporting information you may deem necessary including any assumptions relied upon.

2. Commercial Aspects

2.1. Are there any restrictions on the use and deployment of the EBS solution within: NATO; NATO nations or NATO Deployed operations?

3. Rough Order of Magnitude (ROM) price data

3.1. Please provide a ROM pricing data for solution.

4. Previous NATO or Equivalent National Defence Experience

4.1. Does your company have experience in achieving Security Certification and Accreditation through the NATO or equivalent national defence process?

Please list applicable past projects where such certifications were achieved.

4.2. Does your company have experience in achieving approval through the NATO Request for Change (RFC) or an equivalent national defence process? Please list applicable past projects.

ANNEX D.
Oracle e-Business Suite Enhanced Security System and User Requirements

Requirements ID	Description	MoSCoW Priority
EBS_TECH_01	Prevent web attacks - protect against Top Ten high-risk security principles set by the Open Web Application Security Project (OWASP) detects and react to SQL Injection, XSS, and known Oracle EBS vulnerabilities.	Must
EBS_TECH_02	Application logging - enhanced application logging for compliance requirements	Must
EBS_TECH_03	Protect web services - detect and react to attacks against native Oracle EBS web services (SOA, SOAP, REST)	Must
EBS_TECH_04	Limit EBS Modules - Able to block unused EBS modules web pages out of the box	Must
EBS_TECH_05	Ability to use multiple 2FA solutions – different solutions between internal (smartcard 2FA) and external facing application tiers (TOTP)	Must
EBS_TECH_06	Ability to protect Mobile Applications - detect and react to attacks against Oracle EBS mobile applications	Must
EBS_TECH_07	Integrate with SIEM software like ArcSight, Splunk etc	Must
EBS_TECH_08	Application aware – able to provide 2FA at different application levels – User/responsibility or function levels	Must
EBS_TECH_09	Regular updates to secure against new vulnerabilities	Must
EBS_TECH_10	Support local EBS authentication, but can be later integrated with SSO solutions	Must
EBS_TECH_11	Preferably no additional hardware to keep TCO down	Should
EBS_TECH_12	Fast solutions for zero day vulnerabilities	Should
EBS_TECH_13		Must
EBS_TECH_14		Must
EBS_TECH_15		Must
EBS_TECH_16		

Table 1 – EBS Technical Requirements