NCIA/ACQ/2020/6627

27 April 2020

Request For Information

Cyber Security Mobile Device Analysis Tools

Ref: MS-CO-115190-MDA

The NCI Agency requests information regarding the future implementation of a subset of the Standalone Computer Forensics (SCF) scope, more specifically the Mobile Device Analysis (MDA) capability. The MDA facility, allows teams to inspect phones, tablets and other devices suspected to be involved in an internal security incident or to analyse devices recovered as part of allied operations and missions in-theatre. The NCI Agency is looking for a NATO nation based solution that is comprised of one or more products integrated to provide the capability to extract, decode and analyse data from devices.

NCI Agency Principal Contracting Officer: Ms. Rebecca Benson

E-mail: rebecca.benson@ncia.nato.int

Point of Contact: Mr. Darren Corkindale

Email: darren.corkindale@ncia.nato.int

To: See Distribution List

Subject: **Request For Information**

Cyber Security Mobile Device Analysis Tools

1. NCI Agency requests the assistance of the Nations to identify industry contacts for the replacement of Mobile Device Assess tools at the NATO Computer Incident Response Centre (NCIRC), Mons. This Request For Information is being issued to identify potential NATO nation based solutions and possible suppliers.

2. The RFI questions are provided in Annex A. Each nation is requested to forward this RFI to all potential vendors with capabilities in the area of Mobile Device Analysis.

3. The NCI Agency reference for this RFI is **MS-CO-115190-MDA**, and all correspondence and submissions concerning this matter **must** reference this number within the documentation and email subject line.

4. Responses may be submitted to the NCI Agency POC at point 7 of this letter directly from Nations or from their industry vendors. Respondents are invited to carefully review the questions within Annex A to determine interest.

5. Responses shall in all cases include the name of the firm, telephone number, e-mail address, designated Point of Contact, and a NATO UNCLASSIFIED response to the questions in Annex A. This shall include any restrictions (e.g. export controls) for direct procurement by NCI Agency.

6. The closing date for this RFI is **close of business 15 May 2020**.

7. Please send all responses via email to the following NCI Agency contact:

Mr. Darren Corkindale Senior Contracting Officer, Consultant
Email: darren.corkindale@ncia.nato.int

8. 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 above in Paragraph 7 above.

9. 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 RFI. 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.

10. The NCI Agency is not liable for any expenses incurred by firms in conjunction with their responses to this RFI 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:

[*Original Signed By*]

Rebecca Benson
Principal Contracting Officer

Attachment(s):

- Annex A – MDA RFI Questions

Mobile Device Analysis (MDA) Request For Information

Purpose

The purpose of this RFI is to seek industry responses to the Agency's questions regarding the availability of MDA solutions from within NATO nations. In this context, the MDA facility, part of the Standalone Computer Forensics (SCF) environment, allows teams to inspect phones, tablets and other devices suspected to be involved in an internal security incident or to analyse devices recovered as part of allied missions in-theatre.

Issuance of an RFI is viewed as the fastest, most efficient approach in which fairness can be upheld. The Agency is looking for a NATO nation based solution that is comprised of one or more products integrated to provide the capability to extract, decode and analyse data from devices. Each question will request advice from industry about a specific issue and responses are expected to solicit information from vendors about their current solutions. Responses are not to exceed one (1) page for each question in no less than 12 font size. Vendors should include standard brochures as a supplement to demonstrate the capabilities of an interested party.

Important Notes

The RFI 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 RFI and may use these findings to develop a future RFQ for Mobile Device Analysis. Any future RFQ would be advertised on the Agency's bulletin board for all eligible companies to respond. Participating in this RFI will not benefit, or prejudice, involvement in any future RFQ. Any future procurement is likely to request the provision, delivery, installation and configuration of MDA-related hardware, software and associated support. In order to align with other Agency projects, this potential procurement would likely occur in 2020 with a completion date of April 2021. This may be followed by a warranty/support/subscription period of up to five (5) years.

RFI Questions

1. NCIA is seeking a solution based on NATO nation products and/or services. Please indicate the name and national origin of the parent company for each product or service you are including in your survey response.

2. Please detail all export controls on any solutions mentioned in your answers to questions 3-9 below.

3. Can your solution access and extract data from the following Subscriber Identity Modules (SIM) (please mark each applicable item):

- ☐ Mini-SIM
- ☐ Micro-SIM
- ☐ Nano-SIM
- ☐ eUICC

Please describe how your solution does this.

4. Can your solution access, extract and analyse data from the following devices (please mark each applicable item):

- ☐ Smartphones
- ☐ Tablets
- ☐ GPS Devices
- ☐ Smart Watches

Please list other devices covered by your solution.

Please describe how your solution does this.

5. Can your solution access, extract and analyse data from the following platforms (mark each applicable item):

- ☐ iOS
- ☐ Android
- ☐ BlackBerry
- ☐ Windows Mobile

Please list other platforms covered by your solution.

Please describe which versions of those platforms are supported by your solution.

Please describe how your solution does this.

6. Does your solution include all hardware (such as device connectors, plugs, power suppliers and adapters) and software needed to access the SIMs, devices and platforms mentioned in questions 3-5 above?

7. Please describe how your solution can circumvent or break the security protections (such as PINs, passwords and pattern locks) of the SIMs, devices and platforms mentioned in questions 3-5 above.

For each platform and version (e.g. Apple iOS 13.1), please note whether the approach is derived from a publically known exploit or tool, utilizes in-house proprietary 0-days, or a combination thereof.

8. How does your solution provide forensically sound extractions of the intact, hidden and deleted data (and metadata) within the physical, logical, file system elements and any associated storage for the devices and platforms mentioned in questions 4-5 above?

9. Please illustrate how security/forensic analysts are able to utilise your solution to analyse data and metadata recovered/extracted from the devices mentioned in question 4 above and present it in a human-readable format for forensic and intelligence reports.