NATO Communications and Information Agency

Acquisition

NCIA/ACQ/2023/07480
8 December 2023

Request for Information

Incident Response Retainer (IRR) Services

NCI Agency Reference: MS-422213-IRR

NCI Agency seeks to identify the availability and technical capability of qualified NATO Industry sources for on-going cyber Incident Response Retainer (IRR) services that will assist NCIA and its customers at a NATO Enterprise level in investigations and remediation activities in the event of a critical cyber security level incident.

NCI Agency Point of Contact
Ms. Rebecca Benson, Principal Contracting Officer
MS-422213-IRR@ncia.nato.int

To: Distribution List (Annex A)

Subject: **NCI Agency Market Survey**
Request for Information MS- 422213 -IRR

1. Through issuance of this notice, the NCI Agency seeks to identify the availability and technical capability of all qualified NATO nation businesses that believe they can provide the services described in this announcement.
2. This is a Request for Information (RFI). It is NOT a solicitation for proposals nor a pre-solicitation notice.
3. The NCI Agency reference for this RFI is **MS-422213-IRR**, and all correspondence and submissions concerning this matter should reference this number.
4. The NCI Agency requests the broadest possible dissemination by the Nations of this RFI to their qualified and interested industrial base.

5. The information resulting from this effort is for planning purposes only and for assisting the NCI Agency in refining its requirement and related acquisition strategy. As a result, the NCI Agency will not pay for any costs incurred in responding to this RFI.

6. Responses may be issued to the NCI Agency directly by eligible NATO industry to the Point of Contact indicated at Paragraph 10 below.

7. Responses shall follow the instructions for submittal at Annex B of this RFI.

8. Interested parties are responsible for adequately marking proprietary or competition sensitive information contained in their response.

9. Product demonstrations or face-to-face briefings/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.

10. Responses are requested to be submitted to Ms. Rebecca Benson via email at MS-422213-IRR@ncia.nato.int by 31 January 2024.

11. Your assistance in this RFI is greatly appreciated.

For the Chief of Acquisition:

Rebecca Benson Digitally signed by Rebecca Benson
Date: 2023.12.08 08:27:27 +01'00'

Rebecca Benson
Principal Contracting Officer

Enclosures:
Annex A, Distribution List
Annex B, Instructions & Questionnaire

Distribution List

NATO Delegations (Attn: Military Budget Adviser)

Albania
Belgium
Bulgaria
Canada
Croatia
Czech
Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Iceland
Italy
Latvia
Lithuania
Luxembourg
Montenegro
Netherlands
North
Macedonia
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Turkey
United Kingdom
United States of America

Belgian Ministry of Economic Affairs

Embassies in Brussels

(Attn: Commercial Attaché)

Albania
Belgium
Bulgaria
Canada
Croatia

Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Iceland
Italy Latvia
Lithuania
Luxembourg
Montenegro
Netherlands
North
Macedonia
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Turkey
United Kingdom
United States of America

MS-422213-IRR Instructions & Questionnaire

Summary of Requirements

Cyber Incident Response Retainer (IRR) services are envisioned to form part of a multi-phase initiative to continue to strengthen the NATO Cyber Incident Response capability and enhance both organizational responsiveness and employee readiness in the event of a major incident.

IRR services will provide NATO with qualified and experienced resources that are capable of delivering both assistance and guidance in a timely manner during a major cyber incident or be utilized for preventative services and employee training/table top exercises.

Instructions for Submitting a Response:

1. Interested and eligible organizations from a NATO nation possessing the capabilities to meet the needs described herein, along with the experience in having supported similar needs should submit one (1) electronic response to MS-422213-IRR@ncia.nato.int. Responses shall be submitted no later than close of business on 31 January 2024 and shall contain **no classified material**:
    a. **Part I - A cover sheet clearly identifying the following information**:
        - Re: reference control number MS- 422213 –IRR;
        - Organization name, address, and contact information (telephone number and email address of designated Point of Contact);
        - A brief description of your business or organization, including the main products and services it offers and the market or customers it primarily supports, and how your organization will meet the needs of the services required by NATO.

    b. Part II-Capability Package consisting of:
        - Any initial assumptions, constraints, and exceptions regarding this RFI; and
        - A detailed technical response tailored specifically to NCIA's needs, addressing the questionnaire content provided at Annex B of this RFI.
        - The anticipated level of effort required to meet the needs identified in this RFI.
2. Please do not enter any general company marketing or sales material as part of your specific responses within this RFI. Please submit such material as enclosures with the appropriate references within your replies.
3. Responses **are not to exceed two (2) pages per each question** in no less than 11 font size.
4. Cost details requested in the questions are not a binding offer. Please include all conditions related to the estimate provided.
5. Other supporting information and documentation (technical data sheets, marketing brochures, catalogue price lists, IRR agreement sample of your company are also desired).

MS- 422213 -IRR RFI Questionnaire

1. Knowledge/Expertise

a. Please provide the following information regarding your firm's experience in Incident Response Retainer (IRR) services:

i. Describe your organisation's experience and expertise in resolving the following:

- Advanced Persistent Threats (APT) and Cyberespionage
- Cybercrime,
- Ransomware/Destructware
- Incidents involving current/former employees
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks
- Disclosure/loss involving intellectual property
- Disclosure/loss of customer or employee information

b. What accreditation does your company hold in the incident response field?

c. What level of experience and accreditation do your responders hold?

d. What prescriptive incident response methodology and/or framework does your company use to plan for and perform incident responses?

e. Does your firm have experience providing IRR services to national defense, public sectors or international organizations? If yes, would you provide your customers name and non-classified details of the services provided?

f. How many cyber incidents with a severity high or critical have your company acted upon in the last 12 months to the customers listed at point e.

g. Based on the methodology/framework your company described at point d, what, if any, delays did your firm experience in engaging in the incident response?

2. Security

a. 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 the services you are including in your questionnaire response (list should also include subcontractors if used in the IRR services your firm provides).

b. Please list all tools your company would require NATO to deploy in the event of a breach to ensure rapid deployment in case of a breach. For each tool listed, please provide the national origin of the tool's parent company.

c. Are any of the tools listed in point b already security certified and/or accredited through NATO or equivalent national defense process? If yes, please list which ones.

d. Are the responders utilized under your IRR services all NATO national citizens?

e. Does your company and responders hold required NATO clearances?

3. IRR Agreements

a. List the terms and conditions of your IRR that are in place ahead of time to allow for quicker response in the event of a cyber security incident.

b. Does your company offer **Pre-Incident Services** such as:

i. Assessment

- Evaluate NATO's current state of information security and cyber-security incident response capability

ii. Preparation

- Provide guidance on requirements and best practices

iii. Developing Cyber-Security Incident Response Plans

- Develop or assist in development of written NATO plans for incident response in the event of a cyber-security incident.

iv. Training

- Provide training for NATO staff from basic user awareness to technical education.
- Information Security Awareness Training

c. Does your company offer **Post-Incident Services** such as:

i. Breach Services Toll-free Hotline

- Provide a scalable, resilient call center for incident response information to NATO
- Does your IRR services include 24/7 detection and response windows?
- Does your company offer 24/7 availability in the event of an incident, providing both remote and on-site support.
  - ○ How quickly does your customer have access to remote support?
  - ○ How quickly does your customer have access to on-site support?

ii. Evidence Acquisition on Mobile devices (including phones), distributed IT systems (laptops, computers, physical and virtualized servers) and Cloud environments (Amazon AWS, Google Cloud, Microsoft Azure) in Infrastructure, Platform and Software as a Service (i.e. Microsoft 365)

iii. Forensic investigations and analysis of malicious activity on the acquired evidence

iv. Malware reverse engineering on the different hardware identified above

v. Support data breach response

vi. Technical information sharing with NATO stakeholders

vii. Communication management (internal/external stakeholders)

viii. Assist with the remediation and recovery from a disruption

ix. Develop incident post-mortems and compromise assessments

x. Threat intelligence analysis

xi. Develop and run incident response table top exercises

xii. Describe the range of assets and environments supported for Digital Forensics and Incident Response Services activities, e.g., endpoints, network devices, applications, infrastructure and platform as a service, software as a service, operational technology, Internet of Things.

d. IRR Agreement Pricing

- **i.** How are your IRR services priced?
- **ii.** What is your annual retainer fee and do you have any terms or conditions associated with it if an incident does not occur during the life of the agreement?
- **iii.** Does your pricing model define response times to incidents and associated costs instead of "best-effort"?
- **iv.** Are the tools required during an incident priced separately or inclusive?
- **v.** Does your pricing model offer a reduced rate for extended contracts beyond one year?
- **vi.** What are your payment terms?

e. Please feel free to add any information you may think that may be of value to NCI Agency.