MS-423244-DCO Instructions & Questionnaire

Summary of Requirements

Defensive Cyberspace Operations (DCO) Retainer services are required to ensure appropriate resources and capabilities are available on demand, in order to support DCO activities on NATO networks. These services are aimed at augmenting the NATO Enterprise capacity of planning and conducting DCO, under circumstances where expert-level support is required urgently.

DCO Retainer services will provide NATO with qualified and experienced resources that are capable of delivering both assistance and guidance in a timely manner during DCO planning and execution or be utilized for preventative services and employee training/table top exercises. The aim will be to provide services and expertise, not appliances nor hardware solutions.

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-423244-DCO @ncia.nato.int. Responses shall be submitted no later than close of business on 16 April 2024 and shall contain **no classified material**:
    a. **Part I - A cover sheet clearly identifying the following information**:
        - Re: reference control number **MS-423244-DCO**;
        - 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. I**f there are sub-sections to the question, 2 pages per sub-section will be permitted.**
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, DCOR agreement sample of your company are also desired).

MS-423244-DCO RFI Questionnaire

1. Knowledge/Expertise

a. Please provide the following information regarding your firm's experience in providing Defensive Cyberspace Operations (DCO) Retainer services:

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

- Responding to Web defacement attacks;
- Preventing and detecting typo-squatting campaigns;
- Spear-phishing campaigns simulation;
- Detecting and notifying of targeted data leaks ;
- Conducting cyber security vulnerability assessments;
- Conducting cyber threat hunting activities;
- Producing actionable cyber threat actor tactics, techniques and procedures;
- Conducting sentiment analysis of hacktivist groups intents to execute targeted cyber-attacks;
- Conducting cyber security forensics investigations;
- Conducting adversary emulation activities (red and purple teaming, and breach and attack simulation);
- Adversary Deflection by means of active and passive digital breadcrumbs to attract an adversary into a deception environment and away from production assets;
- Adversary Management by means of but not limited to deploying active and/or passive breadcrumbs, thwarting the adversary's efforts, or shutting down the adversary's access, and providing the broader deception management capability to manage an adversary in real-time.

b. What certification does your company hold in the incident cybersecurity field?

c. What level of experience and certification do your experts hold?

d. What prescriptive cyber defence methodology and/or framework does your company use to plan for and conduct defensive cyberspace operations and activities (including advanced technical operations, cyber incident response, threat hunting, adversary emulation, deception technologies, etc.)?

e. Does your firm have experience providing DCO Retainer or similar retainer (e.g. Incident Response Retainer) services to national defence, public sectors or international organizations? If yes, would you provide your customers name and non- classified details of the services provided?

f. How many DCO (including advanced technical operations, cyber incident response, threat hunting, adversary emulation, deception technologies, etc.) has your company planned and conducted in the last 12 months to the customers listed at point e? Please provide examples.

g. How many cyber incidents with a severity high or critical has your company acted upon in the last 12 months to the customers listed at point e? Please provide examples.

h. Based on the methodology/framework your company described at point d, what, if any,

delays did your firm experience in planning and executing DCO or engaging in the cyber 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 DCO Retainer services your firm provides).

   b. Please list all tools your company would require NATO to deploy to support a DCO and in the event of a cybersecurity breach to ensure rapid deployment of cyber incident response support. 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 defence process? If yes, please list which ones.

   d. Are the experts utilized under your DCO Retainer services all NATO national citizens?

   e. Does your company and responders hold required NATO clearances? If yes, please specify up to which level.

3. **DCO Retainer Agreements**

   a. List the terms and conditions of your DCO Retainer that are in place ahead of time to allow for quicker response in the event of a cybersecurity incident.

   b. Does your company offer **DCO Planning services** such as:

      i. Assessment

      - Evaluate NATO's current state of DCO capabilities.

      ii. Preparation

      - Provide guidance on requirements and best practices for DCO planning and execution.

      iii. Developing DCO Plans

      - Develop or assist in development of written DCO plans.

      iv. Training

      - Provide training for NATO staff from basic user awareness to technical education.
      - DCO best practice training.

   c. Does your company offer **DCO Execution and Reporting Services** such as:

      i. Breach Services Toll-free Hotline

      - Provide a scalable, resilient call centre for DCO execution and cyber incident response information to NATO.
      - Does your DCO Retainer services include 24/7 cyber incident detection and response windows?
      - Does your company offer 24/7 availability in the event of a cyber incident while conducting a DCO, 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. Support data breach response

iii. Technical information sharing with NATO stakeholders

iv. Communication management (internal/external stakeholders)

v. Assist with the remediation and recovery from a cyber incident

vi. Develop cyber incident post-mortems and compromise assessments

vii. Develop adversary emulation activities (red and purple teaming, and breach and attack simulation)s assessments and execution reports

viii. Develop threat hunting assessments and execution reports

ix. Develop adversary detection and management assessments and execution reports

x. Develop deception techniques assessments and execution reports

xi. Threat intelligence analysis

xii. Develop and conduct DCO table top exercises

xiii. Develop and conduct cyber incident response table top exercises

d. DCO Retainer Agreement Pricing

i. How are your DCO Retainer services priced?

ii. What is your annual retainer fee and do you have any terms or conditions associated with it if a DCO does not occur during the life of the agreement?

iii. Does your pricing model define response times to DCO and cyber incidents and associated costs instead of “best-effort”?

iv. Are the tools required to plan and execute a DCO and to respond to a cyber 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.