NCIA/ACQ/2019/12965
07 Nov 2019

Announcement of pending BOA Competition

Cyber Security Computer Forensics and Investigative Tools

RFQ-CO-115009-FIT

Estimated Value: 3.1M Eur

RFQ Estimated Release Date: December 2019

Estimate Bid Closing Date: January 2020

The NCI Agency is seeking the acquisition and deployment of cyber security computer forensics and investigative tools. These systems are part of the existing NATO Computer Incident Response Centre (NCIRC) which is operated centrally at SHAPE, Mons.

The Prospective Bidder List is attached. Interested companies **already holding an active BOA** with the NCI Agency may contact the below POC for inclusion in the Offeror List.

Principal Contracting Officer: Ms. Rebecca Benson

Point of Contact: Mr Darren Corkindale

E-mail: darren.corkindale@ncia.nato.int

Annexes:

1. Summary of Requirements
2. Prospective Bidder List

Annex A – Summary of Requirements

1. **Introduction**
   To facilitate technology refresh, the NCI Agency is seeking the acquisition and deployment of cyber security forensics and investigative tools. These systems are part of the existing NATO Computer Incident Response Centre (NCIRC) which is operated centrally at SHAPE Mons.

2. **Project Scope**
   Interested and eligible companies may provide quotations for the following requirements:

   a) **Standalone Computer Forensics**
   Software, hardware, and associated implementation services for the delivery of capabilities to extract, process, and analyse data and files from a wide variety of media taken from NATO systems running major operating systems, computer storage technologies, mobile devices, compression formats, email clients, web browsers, and other applications, including specialized tools for password cracking and device analysis.

   b) **Online Computer Forensics**
   Software, hardware, and associated implementation services for the delivery of capabilities to monitor, collect, process and analyse data from a large number of diverse endpoint systems over NATO networks. The future OCF environment will include:
      - Support for major operating systems, virtualisation environments, database systems and cloud providers, all organized in a variety of domains according to NATO organization structure;
      - Support for up to 100,000 nodes in several security domains;
      - Ability to conduct post-incident target investigations as well as post-incident or preventive threat-hunting across NATO networks at large;
      - Secure, centralised management and operation including endpoint agent upgrades, Role Based Access Control (RBAC), and user auditing;
      - Integration to other Information Assurance (IA) and Cyber Defence (CD) capabilities such as log aggregation and Security Information and Event Management (SIEM) systems;
      - Support for multiple and custom Indicator of Compromise (IOC) and threat intelligence feeds;
      - Analysis of targets on low bandwidth and intermittent links;
      - Ability to take action on suspicious endpoints.