RFP Released: July 05, 2022
Proposals Due: July 25, 2022, COB (Kyiv time)
Solicitation #: **AM1 to RFP-UA-18-2022_SME_CYBER_Tech experts (p.3; 2.1. GENERAL REQUIREMENTS)**
Solicitation Title: **Technical Expert in Cybersecurity**
Foreseen contract duration: from August 2022 until September 2023

CRDF Global would like to invite you/your organization to participate in our Request for Proposal (hereafter, "RFP") for the provision of **TECHNICAL EXPERTISE TO THE CYBERSECURITY PROJECTS**.

To participate, please review the details below and follow the submission instructions provided in this email.

SUMMARY & PURPOSE:

CRDF Global runs a vast portfolio of projects on various areas and topics of cyber security in a collaborative setting of government, academia, public, and private sector stakeholders to meet the funder's goals.

To implement the projects appropriately and to accomplish projects' tasks, CRDF Global cybersecurity projects teams are seeking local **TECHNICAL CYBER SECURITY SUBJECT MATTER EXPERTS** (hereafter, "SMEs").

Above mentioned SMEs' tasks would be mainly concentrated on **providing certain technical advisory and practical services** on cyber security for the project activities, implemented by coordinating, guiding, and supporting the creation of best practices for the organization's advanced cyber activities. The expert will deliver that in a manner aligned with CRDF Global project goals and objectives and customers' specific requirements.

OBJECTIVE:

CRDF Global programming activities will be centered around but not limited to the following areas for CRDF Global`s Cybersecurity and Cooperative Threat Reduction*:*

- Countering Cyber threats;
- Cyber threat intelligence;
- Security Operations Centers best practices;
- Blue/Red teams trainings;
- Cybersecurity-informed procurement/hardening the supply chain;
- Modern international cyber security trends;
- The U.S., Ukrainian and European cyber security issues;
- Digital Forensics best practices and lab management;
- Cybercrimes investigations and countering;
- European and Euro-Atlantic Integration in the cyber security area;
- Cybersecurity insurance;
- Cyber hygiene for various audiences;
- Cyber security workforce skills development trainings;
- Cybersecurity in IT telecommunication;
- Cyber Range activities;
- OSINT (open-source intelligence);

- Incident Response in cybersecurity;
- Security Architecture (Engineering);
- Big Data Security by Design;
- Digital Forensics and evidence collection;
- National DNS System development and integration;
- Vulnerability disclosure;
- Veterans reintegration trainings;
- Development of new/ adaptation of existing curricula on Cyber security topics for Universities;
- Liaison with governmental agencies, regional government officials, amalgamated communities and educational institutions (universities, institutes, colleges, secondary schools) in Ukraine regarding implementation of CRDF Global Cyber security activities;
- Develop training materials, conduct training/workshops in cybersecurity and cyber-hygiene, and Train the Trainer activities.

As such, CRDF Global requires on-going, flexible, and lasting partnerships with experts in the field.

1. **SCOPE, TASKS, & DELIVERABLES**

- The tentative Period of Performance start date is **from August 2022 until September 2023** (fourteen months)

The selected SME(s) would be expected to provide contracted services such as, but not limited to:

1. Development of training and briefing materials for varied Ukrainian and international audiences in both government and private sectors, educational institutions, and/or civil society.
2. Delivery of virtual and/or face-to-face training, workshops, hackathons, CTF, cluster meetings, and presentations, delivering answers and providing expertise during discussions, and Q&A sessions at CRDF Global events that are to be held in various domestic and international locations.
3. Delivery of an After-Action Report summarizing observations, successes, lessons learned, and recommendations for future programming on the relevant topic.
4. Providing technical advice, guidance, and leadership to CRDF Global colleagues on designing and implementing technical components of cybersecurity and/or CTR projects.
5. Tech consultancy on the best avenues to deliver critical messages on the cyber, safe use of the Internet in digital devices for various age groups.
6. Consultation on the developing Cyber Range scenarios.
7. Collaborating with the Senior Operations Manager, Senior Project Leads, and Project Leads to develop actionable projects based on conceptual policy ideas.
8. Collaborating with CRDF assigned operation staff, relevant stakeholders and partner organizations, to develop content (training modules/ modules content) for new E-learning Cyber hygiene courses for a wide range of stakeholders/adaptation existing E-learning courses.
9. Providing technical development and set-up of virtual servers, virtual competition/CTF/hackathons environments, scoreboard and events participants virtual workstations
10. Providing technical installations of software and/or hardware according to the developed event/competition/workshop/CTF/hackathon network and scenarios

2. **KEY SELECTION CRITERIA:**

Selection will be based on CRDF Global's evaluation of the Contractor's ability to meet CRDF Global's requirements described below, as well as factors such as competitive pricing, quality of the proposal, past performance, and other intangible factors. CRDF Global reserves the right to accept or reject any and all proposals and to negotiate the terms of any subsequent agreements at its own discretion.

Interested Proponents are allowed to submit their proposals as individuals (physical persons) as well as entities/organizations, offering a single expert or a team of experts to cover the tasks of the assignment.

A successful proposal will highlight the following qualifications:

2.1. GENERAL REQUIREMENTS:

- Master's degree in cyber security, computer science, computer networks and other relevant areas required.
- At least 4 years of professional experience in cybersecurity.
- Proven experience in developing/supervision/implementing/moderation cybersecurity-themed seminars/event/competitions/workshops (short portfolio of the projects to be provided)
- Excellent knowledge of the Ukrainian context, including the cybersecurity field.
- Knowledge of the Ukrainian context, including the cybersecurity field is desirable and will be an advantage.
- Strong writing and speaking skills in Ukrainian are required for Ukrainian bidders.
- Strong writing and speaking skills in English are required
- Proven experience working on international donor-funded projects, preferable U.S. government-funded projects or multilateral institutions.

2.2. TECHNICAL REQUIREMENTS:

Candidate must meet the following technical desirable and optional requirements, skills, experience, and knowledge:

2.2.1. DESIRABLE REQUIREMENTS, SKILLS, EXPERIENCE, AND KNOWLEDGE:

- Understand and apply security concepts:
  - Confidentiality, integrity, and availability, authenticity and nonrepudiation.
- Understand and apply threat modeling concepts and methodologies;
- Identify and classify information and assets;
- Understand fundamental concepts of security models;
- Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption);
- Understand methods of cryptanalytic attacks;
- Implement secure design principles in network architectures;
- Implement secure communication channels according to the design;
- Deep knowledge in Secure network components;
- Proven experience in protocols like LDAP, SAML, OAuth, OpenID, Kerberos;
- Experience in Networks and Applications Testing Conduct;
- Understand all Incident response phases (which tasks occur at each phase: identification, containment remediation, recovery, after action reporting/lessons learned);

- Malware campaigns and malware analysis, including Static, Dynamic, and Reverse analysis
- Threat hunting;
- Host/network access control mechanisms (e.g., access control list);
- System and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code);
- Understand all general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks);
- Network security architecture concepts (including topology, protocols, components, and principles (e.g., application of defense-in-depth);
- Penetration testing principles, tools, and techniques;
- Threat actor classification (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored);
- Understand and implement the concepts of Cyber threat intelligence, methods, procedures, and information gathering techniques ;
- Understand the principles of agile and secure SDLC;
- Understand and be able to work with a wide range of Cyber Security related toolsets, SIEM, EDR/MDR, Vulnerability management, Microsoft and Linux operating systems, Firewalls, Networks, Deception tech, UEBA, IDS/IPS to name a few;
- Understand and implement MITRE ATT&CK/D3FEND frameworks and MITRE TTPs.

2.2.2. OPTIONAL REQUIREMENTS, SKILLS, EXPERIENCE, AND KNOWLEDGE:

- Evaluate and apply security governance principles:
  - Alignment of the security function to business strategy, goals, mission, and objectives;
  - Security control frameworks.
- Determine compliance and other requirements:
  - Contractual, legal, industry standards, and regulatory requirements;
  - Privacy requirements.
- Understand requirements for investigation types;
- Contribute to and enforce personnel security policies and procedures;
- Understand and apply risk management concepts:
  - Identify threats and vulnerabilities;
  - Risk assessment/analysis;
  - Applicable types of controls;
  - Monitoring and measurement;
  - Risk frameworks.
- Understand data lifecycle management and apply data security controls and compliance requirements;
- Design site and facility security controls;
- Experience with Zero Trust conceptual knowledge;
- Experience in Security Audits Conduct;
- Experience in Security Policies Analysis;
- Technical forensics (including computer, memory, mobile, and network forensics);
- Understand ethical hacking principles and techniques;
- Hands-on experience in the OWASP WSTG, ASVS, SAMM standards implementation;

- Develop/improve the security incident response framework, including related standards and processes, and ensure effective implementation;
- Develop/improve process of cyber threat information sharing. Support of information sharing platform (MISP, STIX).

3. **SUBMISSION REQUIREMENTS & INSTRUCTIONS:**

! Each proposal must include:

3.1. Statement of Interest and Technical Capabilities (including the list of RFP related capabilities, applicable experience and references):
  - Detailed description of the services offered in correlation with this RFP section for: **SCOPE AND TASKS AND DELIVERABLES (p.2)**
  - List of recent experiences/samples working with the US Government and/or other donors' organizations

3.2. CVs (no more than 2 pages) of the bidders specialists offered for the assignment

3.3. Cost proposal – description of the pricing and cost factors **(hourly rates)** that the Bidder would be willing to negotiate under the GSC;

3.4. Completion & online submission of CRDF Global's Contractor Data Form/Formstack.

Submissions should be sent to Yuliia Nikolova ynikolova@crdfglobal.org & CC Anastasiia Kurylenko, kurylenko@crdfglobal.org no later than **July 25, 2022, COB (Kyiv time)**. Proposals should be submitted as electronic documents **in PDF** and **Word,** and/or Excel formats.

4. **TIMETABLE:**

CRDF Global reserves the right to make changes to the RFP Timetable without providing explicit notification ahead of time.

RFP issued:	July 05, 2022
Proposals Submissions Due:	July 25, 2022, COB (Kyiv time)
Contractor Selection:	August 2022

For any questions regarding this RFQ, please reach out directly. We thank you for your time and consideration and look forward to hearing from you.

CONTRACT FOR SERVICES:

Following selection, CRDF Global will negotiate a General Services Contract (hereafter "GSC") with the selected SME(s).

While the GSC is not a guarantee of any work, the selected SME(s) on a GSC can be engaged by CRDF Global staff with an abbreviated selection process. This allows CRDF Global to potentially leverage the partnership with the SME for strategic initiatives, proposal submissions, and programmatic responses to urgent timelines.

The GSC will be structured to allow CRDF Global Agreement Officer(s) to issue task orders to the SME upon successful negotiation of scope and budget.

The specific duration of the GSC foreseen from July 2022 until September 2023.
The GSC would seek to negotiate and lock in elements of pricing and cost that are agreeable to both parties.

Sincerely,

Yuliia Nikolova,
Procurement specialist