Request for Proposals (RFP)

Title of Competition:

'Cybersecurity Improvement Grants for Governmental Institutions in Ukraine'

Reference Number: DE-02-2023

Revised: November 17, 2023

Competition Opens	November 3, 2023
Submission Deadline	November 30, 2023
Q&A Session	November 14, 2023
Announcement of Results	On the rolling basis
Grant Amount	Up to USD 54,000
Project Duration	Up to 9 months
Eligible Applicant(s)	Central Governmental Institutions / State-owned enterprises of critical infrastructure of Ukraine
Eligible Countries	Ukraine
Eligible Project Scope	Cybersecurity improvement and capacity building

TABLE OF CONTENTS

TABLE OF CONTENTS 2
BACKGROUND 3
Goals & Objectives 3
SCOPE 4
Problem statement 4
Eligible Scope of Projects 4
ELIGIBILITY REQUIREMENTS 5
REVIEW OF PROPOSALS 5
Review Process 5
Evaluation Criteria 5
PROPOSAL PREPARATION AND SUBMISSION 6
ALLOWABLE COSTS & BUDGETING 8
List of ineligible goods: 8
CRDF GLOBAL POLICIES AND APPLICANT RESOURCES 8
General Terms and Conditions 8

BACKGROUND

CRDF Global is currently accepting proposals from Central Governmental Institutions of Ukraine / State-owned enterprises of critical infrastructure of Ukraine for the Competition titled as 'Cyber Security Improvement Grants for Governmental Institutions in Ukraine' (the Competition). This Competition is organized and administered by CRDF Global, utilizing funding provided by the U.S. Department of State.

Cybersecurity Improvement Grants (CySIGs) are designed to procure solutions to address current and emerging cybersecurity needs with the aim of improving the level of cyber security and information resilience in these institutions, by assigning a cybersecurity expert(s) to ensure a high-level protection of important information resources and networks of these institutions, contributing to the strengthening of cyber defense of Ukraine.

CRDF Global is an independent nonprofit organization founded in 1995 in response to the collapse of the Soviet Union and the threat of large-scale proliferation of weapons technology from the region. In the past 25 years, CRDF Global's work has expanded to address ever-changing global concerns, but the commitment to ensuring the success of the organization's partners remains the same. CRDF Global is a leading provider of flexible logistical support, program design and management, and strategic capacity building programs in the areas of higher education, CBRNE security and nonproliferation, border security, cybersecurity, global health, technology entrepreneurship, and international professional exchanges. With offices in Arlington, VA; Kyiv, Ukraine; Amman, Jordan; and Manila, Philippines, CRDF Global's diverse staff and networks of local community and government stakeholders deliver tailored programs that meet specific regional needs in over 100 countries across the globe.

For more information visit http://www.crdfglobal.org.

Goals & Objectives

As a result of implementation of grants under this Request for Proposals, the following goals and objectives will be pursued:

(1) Analyze current security systems of Central Governmental Institutions of Ukraine / State-owned enterprises of critical infrastructure of Ukraine.
(2) Identify potential threats and further develop the innovative cybersecurity solutions to protect the Central Governmental Institutions of Ukraine / State-owned enterprises of critical infrastructure of Ukraine from such threats.
(3) Enhance cybersecurity and bolster information resilience of the Central Governmental Institutions of Ukraine / State-owned enterprises of critical infrastructure of Ukraine.

SCOPE

Problem statement

In the context of the full-scale war by Russia, Central Ukrainian Governmental Institutions, State-owned enterprises of critical infrastructure have been confronting significant challenges, including cyber-attacks, disinformation campaign that threaten their security and operation stability. These challenges have created a pressing need for Ukraine to bolster its cybersecurity measures and resilience, counter disinformation efforts, and protect critical infrastructure, ensuring the continued functioning and security of governmental institutions and vital sectors during this time of the war. This requires a comprehensive and coordinated approach to safeguarding national security for Ukrainian Governmental Institutions, State-owned enterprises of critical infrastructure. This approach entails protecting sensitive data, conducting diligent analysis of potential threats, and implementing robust security measures to defend against cyberattacks and other security risks.

In light of the challenges outlined above, this Request for Proposal seeks to address the outlined challenges faced by the Central Ukrainian Governmental Institutions, State-owned enterprises of critical infrastructure. It aims to provide cybersecurity support for grantees to identify vulnerable areas and protect their systems against potential cyber incidents, by improving the level of cyber security and information resilience in these institutions, by assigning a cybersecurity expert to ensure a high-level protection of important information resources and networks of these institutions, contributing to the strengthening of cyber defense of Ukraine.

Eligible Scope of Projects

For the purposes of this Competition, applicants should propose projects in the following areas:

(1) Cybersecurity.
(2) Cyber hygiene.
(3) Data protection.
(4) Threat analysis.
(5) Grantees' capacity building in areas outlined above.

Given the areas outlined above, project activities may include, but are not limited to:

(1) Conducting the analysis of Grantee's vulnerable areas that may be exposed to potential cyberattacks and cybersecurity incidents.
(2) Development of strategic/operational solutions to prevent and respond to potential cyberattacks and cybersecurity incidents.
(3) Optimization and cybersecurity processes improvement for Grantee in the areas identified above.

Proposed solutions/project activities need to address/include the following:
Specify the number of cybersecurity experts.
Specify the general scope of work for each cybersecurity expert(s) and vulnerability area that the Government Institution is facing.

The curriculum vitae (CV) of Principal Investigator (project coordinator responsible for project implementation) to be submitted.
Applicants have named potential gaps in cybersecurity perimeter that the grantee intends to cover for the period of up to nine (9) months.

ELIGIBILITY REQUIREMENTS

All applicants and proposals must meet **each** of the following eligibility criteria:

(1) The Applications are accepted from Central Governmental Institutions of Ukraine / State-owned enterprises of critical infrastructure of Ukraine who demonstrated susceptibility to potential cyber threats and/or cyber incidents.
(2) Applicants have provided a clear problem statement and identified key requirements for cybersecurity expert(s) to be later engaged to the project.
(3) Applicants have submitted a full proposal package.

NOTE: CRDF Global reserves the right to decline review and evaluation of the applications which do not meet eligibility requirements stipulated above.

REVIEW OF PROPOSALS

Review Process

All proposals and information contained therein will remain confidential prior to the award and will be screened for eligibility and completeness upon receipt by CRDF Global. All eligible proposals will be subjected to a technical review process. CRDF Global will use the criteria described below to evaluate the merit of each proposal and make award recommendations. CRDF Global will select finalists based on the proposal's overall rating and these recommendations.

CRDF Global will conduct a review of eligible proposals in accordance with local legislation and established policies of the organization. Following these reviews, CRDF Global will select proposals for award and notify PIs and/or designated contact point of award results via e-mail.

NOTE: All awards are subject to the availability of funding from program sponsors. All decisions by CRDF Global are final.

Evaluation Criteria

The following evaluation criteria will be applied while review and evaluation of each proposal:

1. Proposal's Relevance and Potential Impact	**30 points**

- **Technical Merit.** Whether the project aligns the necessary areas of improvement in cybersecurity area and how well the individual elements of the scope of work fit with the overall project goal. Evaluating the feasibility of completing the project within the up to 9-months timeline.
- **Cyber security relevance and impact**: The probability that the project will help to analyze and improve the cyber security systems and information resilience of grantees.

- **Benefit to Central Governmental Institutions of Ukraine / State-owned enterprises of critical infrastructure of Ukraine.** Whether the proposal has demonstrated a clear and reasonable timeline, strong motivation, areas of improvement for the grantees.

2. Cybersecurity Expert Needs and Scope of Work	30 points

- Align the reasons for assigning the cybersecurity expert(s) for the Central Governmental Institutions of Ukraine / State-owned enterprises of critical infrastructure of Ukraine.
- Specify the current cybersecurity issues that are relevant and important to analyze, solve and enhance for grantees, considering up to 9-months timeline.
- The Scope of Work is detailed, sufficient and embrace all the problematic cases related to cybersecurity that the grantee is currently facing with.

3. Clarity, Feasibility and Sufficient Details of Suggested Activities	15 points

- Ensure that successful applications have a well-defined objective, along with a justification for the need of a cybersecurity expert(s).
- **Project Plan.** The technical soundness of the proposed Scope of Work, feasibility of suggested workplan, and adequacy of the needs to be analyzed and improved by cybersecurity expert(s).

4. Cost Effectiveness	10 points

- Sufficient level of details in provided budget and justification in the budget narrative.

5. Sustainability of Suggested Approach / Activities	15 points

- How can the proposed activities contribute to enhancing the cybersecurity systems of grantees?
- Clear deliverables for each Milestone in Scope of Work.

TOTAL SCORE	100 points

PROPOSAL PREPARATION AND SUBMISSION

Full Proposal Submission

All proposals must be submitted no later than **November 30, 2023.**

All proposals must be submitted electronically, using CRDF Global's proposal package template via email: vsheliekhova@crdfglobal.org

Email's subject line should indicate RFP# and name of the applicant in the following format provided with an example:

"DE-02-2023_RedCrossAssociation".

At the conclusion of the electronic submission process, applicants will receive a confirmation message from CRDF Global.

Proposal application materials submitted to CRDF Global must be prepared in English or Ukrainian and compiled in the **proposal package template**. Acceptable file formats are MS Excel (.exsm) and pdf when directly requested in instructions.

Proposal package template contains the following sections (tabs):

Required:

(1) Proposal Cover Page
(2) Institutional Data Form
(3) Project Proposal Overview
(4) Scope of Work
(5) Workplan
(6) Budget
(7) Budget Narrative

Additional, as specified below:

(1) CV of Principal investigator (project coordinator responsible for project implementation).

For questions about the submission process, please contact the CRDF Global Staff at: vsheliekhova@crdfglobal.org

Q&A session

CRDF Global will arrange an on-line Q&A session in order to address any questions related to the Competition and this RFP's provisions, including eligibility requirements, submission and review of proposals and other related matters.

NOTE: CRDF Global will not review, assess, or advise on actual proposals by the applicants, or anyhow support development of implementation approaches and activities. The purpose of the Q&A session is to give guidance to the applicants and answer pertinent questions to improve the overall quality of submitted proposals.

The Q&A session will be recorded and posted on CRDF Global's website.

Please find details of the upcoming Q&A session below:

Date: November 14, 2023
Time: 12 am, Kyiv time
Meeting Platform: Zoom.
Participants need to register in advance to participate in the Q&A session. Please use this link below to access the registration form. Applicants will be provided with an invitation to a Zoom meeting in advance of the Q&A session.

Registration link: https://forms.office.com/r/5K8AaBmyr5.

ALLOWABLE COSTS & BUDGETING

Grant Ceiling. The maximum total award is up to **USD 54,000** disbursed over grant's period of performance.

In the case of an award, a project budget may be subject to revision by CRDF Global staff.

CRDF Global will disperse award funds using an in-kind grant mechanism.

The following costs are permitted under CRDF Global's guidelines for this Competition:

1. **Services:** This includes provision of information and consultation services to the grantees by the local services providers who are experts in cybersecurity matters. Such experts need to correspond to requirements provided by the applicants.

List of ineligible goods:

The following goods cannot be budgeted by the applicants within the scope of this Competition:

1. Weapons and explosives;
2. Alcohol beverages;
3. Illegal and/or restricted substances, such as drugs;
4. Surveillance equipment;
5. Luxury goods and jewelry;
6. Gambling equipment;
7. Sports equipment.

CRDF GLOBAL POLICIES AND APPLICANT RESOURCES

General Terms and Conditions

CRDF Global's General Terms and Conditions are incorporated herein by reference and published together with this RFP on CRDF Global's website.

Applicants must review applicable Terms and Conditions prior to submission of their proposals under this Competition.

Specific Terms and Conditions

1. Each applicant - Central Governmental Institutions of Ukraine / State-owned enterprises of critical infrastructure of Ukraine - is allowed to submit **only one application** per this Competition.
2. After the announcement of results of this Competition, each selected applicant will be informed directly by CRDF Global via e-mail. Applicants will have **no more than 10 calendar days** to sign provided Grant Agreements. If applicant fails to comply with the stipulated term, CRDF Global reserves the right to deny any award unilaterally.
3. Each selected and awarded grantee is expected to provide Final Progress Report upon completion of the Grante Agreement in accordance with the reporting schedule in Grant Agreement.