Request for Proposals (RFP)

Title of Competition:

'Cybersecurity Improvement Grants for Central Governmental Authorities and Capacity Building Institutions of Ukraine'

Reference Number: DE-04-2024

Competition Opens	May 29, 2024
Submission Deadline	June 19, 2024
Q&A Session	June 07, 2024
Announcement of Results	On the rolling basis
Project Duration	September 13, 2024
Budget Celling	45 000 USD per 1 Application
Eligible Applicant(s)	Central Governmental Authorities and Capacity Building Institutions of Ukraine
Eligible Countries	Ukraine
Eligible Project Scope	Improving the level of cybersecurity and information security in Central Governmental Authorities and Capacity Building Institutions of Ukraine

TABLE OF CONTENTS

BACKGROUND

CRDF Global is currently accepting proposals from Central Governmental Authorities and Capacity Building Institutions of Ukraine (hereafter – potential applicants) for the Competition titled as 'Cybersecurity Improvement Grants for Central Governmental Authorities and Capacity Building Institutions of 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 for Central Governmental Authorities and Capacity Building Institutions of Ukraine (CySIG) are designated to address current and emerging challenges in the cybersecurity field. Their aim is to improve cybersecurity measures, resilience of cybersecurity systems within these institutions, ensure the reliability, confidentiality, and accessibility of information, and mitigate the risks of cyberattacks and other cyber threats. These grants target strengthening cybersecurity in government institutions by implementing cutting-edge technologies, providing support services to potential applicants to identify and prevent potential cyber threats, instilling confidence in the resilience of their information systems and networks against possible cyberattacks, and contributing to the enhancement of infrastructure and protective methods. They involve creating or enhancing existing information protection systems, as well as providing professionals working in the cybersecurity field of these institutions with opportunities to acquire skills and knowledge for engaging with international communities and key donors. This includes exchanging best practices, studying international standards, allowing more effective collaboration, and implementing advanced approaches in partnership with these entities. This component will expand the utilization skills of available international resources, contributing to the elevation of cybersecurity levels in

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 goalsand objectives will be pursued:

(1) Increase the level of cybersecurity and the resilience of cybersecurity systems of Central Governmental Authorities and Capacity Building Institutions of Ukraine.
(2) Contribute to the development and/or improvement of existing information and cyber infrastructure

of these institutions by providing necessary resources (services, equipment, hardware, and software).

(3) Enhance the skills and knowledge level of professionals involved in the field of cybersecurity of these institutions to study international standards in the sphere of cybersecurity and cyber defense and utilize available international professional information resources.

SCOPE

Problem statement

In the context of the full-scale war by Russia, Ukrainian governmental institutions and authorities of Ukraine 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.

In the context of this competition, it is important to note the significant shortage of technical equipment and software in Ukrainian governmental institutions, which significantly complicates the process of protecting these institutions from cyber threats and other cyberattacks. The absence of adequate tools and programs can compromise the resilience and effectiveness of data and infrastructure protection, thereby increasing vulnerability to modern cyber threats.

It's worth mentioning that such a critical need exists not only in improving cybersecurity systems but also in developing communication skills among professionals working in state institutions and critical enterprises. The lack of these key skills limits their ability to effectively communicate with international representatives and adapt to modern cybersecurity requirements, which can complicate the successful protection of crucial systems in the face of contemporary threats.

Addressing these issues requires a comprehensive and coordinated approach to ensuring the national security of Ukrainian governmental institutions and state-owned critical infrastructure enterprises. Such an approach will not only develop the technical aspects of cybersecurity but also ensure effective communication and collaboration with international experts, which is crucial for successfully protecting critical infrastructure in the current landscape of cyber threats.

Eligible Scope of Projects

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

(1) Cybersecurity and improvement of the material-technical base for its provision.
(2) Data protection and threat analysis.
(3) Coordination and enhancement of access to international analytical resources for information exchange.
(4) Legislative work and standardization in the cybersecurity field.

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

(1) Provision of necessary resources (equipment, services, hardware, and software).
(2) Optimization and improvement of processes/systems of cybersecurity for the grantee in the aforementioned areas.
(4) Implementation of recommended updates and/or security measures in Central Governmental Authorities and Capacity Building Institutions of Ukraine.
(5) Enhancement of qualification skills in the field of cybersecurity for employees of Central Governmental Authorities and Capacity Building Institutions of Ukraine.

Proposed solutions/project activities need to address/include the following:

- Provide a detailed description of the problem statement and potential solutions that will help to reduce the risk of cyber incidents and enhance cybersecurity systems.
- Identify which critical resources and/or confidential information will be protected as a result of implementing activities under this grant and provide justification for the necessity of protection.
- Provide the expected outcomes of the grant implementation.
- Provide a breakdown of equipment/services/software/materials, specifically: key specifications and quantities of each product with references to similar models and brands of equipment.
- Specify cost breakdowns, justifying the suitability of this brand and product model (calculations in Ukrainian Hryvnia with the equivalent amount in US dollars, including value-added tax (VAT), shipping costs, and installation expenses).
- Provide at least one (1) commercial offer from a potential vendor who is ready to supply the services and /or equipment within the requested items as specified in your application.
- Submit a resume (CV) of the Principal Investigator (project coordinator).

* If potential applicants require a specific brand and model of equipment based on their experience and understand that only this model can meet their technical needs, they should provide substantive and detailed justification for this requirement. Provide examples of the technical advantages of this equipment specifically for accomplishing the tasks outlined in the applicant's project.

ELIGIBILITY REQUIREMENTS

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

(1) Applications are accepted from Central Governmental Authorities and Capacity Building Institutions of Ukraine which may be vulnerable to potential cyber threats or other cyber incidents.
(2) Applicants have provided a clear formulation of the problem statement and justified the necessity of acquiring equipment/services/software.
(3) Applicants have presented a clear breakdown of the necessary equipment/services/software.
(4) Applicants have submitted at least one commercial offer from a potential vendor who is ready to supply the services and/or equipment as specified in your application.
(5) Applicants have submitted a complete set of required documents **in English only.**

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 Impact	Potential	30 points

- Relevance and impact on cybersecurity: Justification and detailing of how the project will help to improve cybersecurity systems and information resilience.

2. The need for equipment/software and/or provision of services.	30 points

- Specify a clear formulation of the problem and rationale for the necessity of acquiring specific equipment/services/software for the grant recipient. Explain how this assistance will be integrated into the existing cybersecurity system of the institution.

3. Clarity, Feasibility and Sufficient Details of Suggested Activities	20 points

- The application has a clearly defined objective in providing resources (equipment/services/software/materials). How the provided assistance will impact the cost-effectiveness of the institution's cybersecurity system in the future.

4. Cost Effectiveness	20 points

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

TOTAL SCORE	100 points

PROPOSAL PREPARATION AND SUBMISSION

Full Proposal Submission

All proposals must be submitted no later than **June 19, 2024.**

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 and the proposal package should consists of the following documents:

I. Proposal Application (PA) Form (Excel spreadsheet) that includes:

1. Proposal Cover Page
2. Institutional Data Form
   - A. Project Overview
   - B. Scope of Work
   - C. Workplan
   - D. Budget
   - E. Budget Narrative

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

III. One Commercial Offer from potential vendor.

For questions about the submission process, please contact the CRDF Global Staff at: nonpro-grants@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: 07 June, 2024
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/0nLAGeyr9P

ALLOWABLE COSTS & BUDGETING

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:

Services: This includes provision of information and consultation services to the grantees by the local and international services providers.

Procurement of equipment and materials: for the building and/or enhancing of existing information and cyber infrastructure.

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 Authorities and Capacity Building Institutions of Ukraine - is allowed to submit **only one application per this Competition.**
2. After the announcement of the results of this Competition, each selected applicant will be informed directly by CRDF Global via e-mail.
3. Each selected grantee must provide the Final Program Report within 1 month after receiving the grant assistance.
4. Each selected grantee must provide a signed Acceptance Certificate for the received equipment.