CRDF GLOBAL REPRESENTATIVE IN UKRAINE
www.crdfglobal.org

REQUEST FOR PROPOSAL # RFP-28-UA-2023
SEARCHING FOR VENDOR TO DEVELOP AND IMPLEMENT
THE CYBERSECURITY PUBLIC AWARENESS CAMPAIGN

Issue date: 21.12.2023 (December)
Submission Deadline: 18.01.2024 (January), COB EEST

The objective of this tender is to search for and engage proficient Contractor to develop and conduct the Cyber Awareness Campaign scheduled for Febr. – Aug. 2024

CRDF Global invites specialized Bidders to participate in this competitive solicitation and provide proposals.
CRDF Global reserves the right to add, delete, or modify any element of the solicitation at any time without prior notification and with and without any liability or obligation of any kind.
CRDF Global has the right to reject any or all bids received in response to this RFP, to split the award, and to negotiate with any of the bidders or other firms in any manner deemed to be in the best interest of CRDF Global.
This request does not oblige CRDF Global to consider any proposal or to award a contract or to pay any costs incurred in the preparation or submission of proposal, or to procure any services from any bidder.

RFP Estimated Timetable

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

05.01.2024	RFP Questions Due (also available online https://crdfglobal.zoom.us/j/97645102329 Meeting ID: 976 4510 2329 from 2 pm to 3 pm)
12.01.2024	RFP Questions & Answers Released
18.01.2024	RFP Submissions Due
February 2024	Contract start

As a result of this RFP CRDF Global will award a Contract Agreement in line with terms and conditions of this tender. For the additional related services not foreseen in current SOW CRDF Global may place the request/Order in accordance with the terms and conditions of current RFP.

Interested Bidders are invited to submit a proposal.

Bidders shall submit a proposal directly responsive to the terms of this tender. Proposals should include detailed information demonstrating compliance with the requirements and T&C of this tender. It is the responsibility of the Bidder to verify all aspects of the services involved prior to submitting a proposal.

STATEMENT OF WORK
THE CYBERSECURITY PUBLIC AWARENESS CAMPAIGN

INTRODUCTION:

Established in 1995, U.S. Civilian Research and Development Foundation (CRDF Global) is an independent nonprofit organization that promotes safety, security, and sustainability through international development and foreign assistance missions across the globe. A trusted government partner for over 25 years, CRDF Global provides technical assistance, trainings, logistics, and program management in the areas of CBRNE security, global health, cybersecurity, strategic trade controls, international exchanges, and more. The organization is headquartered in Arlington, VA, US, with regional hubs in Amman, Jordan and Kyiv, Ukraine. More details on the CRDF Global website.

CRDF Global runs an impressive portfolio of cybersecurity projects, collaborating with a plethora of stakeholders and meeting the needs of multifarious customers and beneficiaries. An inalienable element of many project activities constitutes communication efforts, which facilitate effective achievement of the goals and outcomes, contribute to impressive long-lasting results, and deliver sought-after impact.

To accomplish required communication tasks, CRDF Global cybersecurity project team seeks for provision of services and support from Communication (Media, PR, production) Agency (hereafter Contractor).

CRDF Global will work with the Vendor, which will provide the creative solutions and general Campaign`s concept development based on the CRDF Global Requirements as well as be able to cover the content part in full by developing communication plan and other implementation services relating to the Cybersecurity Public Awareness campaign (hereafter – Campaign). Due to breadth and nature of the tasks outlined, CRDF Global requires sustainable, agile, and prolific partnership with relevant experts in the field.

BACKGROUND:

Recognizing the risks associated with the increasing digitalization of the world, CRDF Global in 2019 launched a program to **strengthen security in cyberspace in Ukraine, Moldova and the Western Balkans**, aimed at preventing cyber-attacks by creating a reliable cyber infrastructure and professional development of cybersecurity professionals. This program is supported by the U.S. State Department Office of the U.S. Assistance Coordinator for Europe and Eurasia.

The Cybersecurity Public Awareness campaign, established with the goal of educating people about online threats and promoting secure practices, is a crucial initiative aimed at enhancing digital safety. The first round of the campaign was launched in September 2022 and lasted until September 2023. The activity was of the all-Ukraine nature and reached country's population of various age groups using wide range of digital and traditional communication channels. To ensure a lasting impact, the campaign is committed to continuous improvement and seeks to be continued, adapting to evolving threats and engaging target audiences for a safer online community in Ukraine. The Campaign was presented using media production, social media, web-development etc.

CAMPAIGN MAIN GOALS ARE:

1. To increase the level of public awareness of cybersecurity threats and vulnerabilities, relevance of cyber hygiene basic rules based on the previously studies results conducted by the CRDF Global team.
2. To design, develop and implement the Cybersecurity Public Awareness campaign using the most effective channels for obtaining information for the targeted group including the suggested types of content.

COMMUNICATION MAIN GOALS ARE:

1. To create and advance an informative digital media agenda focusing on prevalent daily cyber threats, digital safety, and cybersecurity guidelines.

2. To cultivate understanding of the Cyber Hygiene concept as an integral aspect of contemporary digital culture, emphasizing the imperative incorporation of daily cyber hygiene practices to guarantee digital safety and security.
3. To enhance awareness regarding significant cybersecurity threats and vulnerabilities and impart fundamental guidelines for the secure utilization of the Internet.
4. By placing installations (interactive banners and other promotional materials) at public events of various types (exhibitions, presentations, etc.), it is planned to improve the level of public awareness using a basic platform (a set of materials etc.) with key relevant information about the main threats in everyday life, vulnerabilities, and basic rules of cyber hygiene.
5. Additionally, the CRDF Global team is considering creating an animated, viral 15-second video on raising public awareness of cybersecurity threats and vulnerabilities, current basic rules of cyber hygiene and digital literacy. Placement of this video - material is on the main 3D screens.

VENDOR MAIN TASKS ARE:

1. Develop a strategic approach for the Cybersecurity Public Awareness campaign aligned with communication objectives.
2. Create a communication plan with defined media Key Performance Indicators (KPIs) and digital communication tools applicable nationwide in Ukraine.
3. Allocate the preliminary budget according to the proposed strategic approach and communication plan.
4. Devise a creative concept with core messages for the communication campaign and innovative communication solutions.
5. Generate diverse media content such as video graphics, animated reels, audio clips, banners, layouts, and social media posts, aligning with the strategic approach and communication plan.
6. Execute media and PR campaigns as per the proposed strategic approach, communication plan, and budget allocation.
7. Collaborate with opinion leaders, influencers, and bloggers, employing influencer marketing tools to establish a Cyber Safety ambassadors' movement.
8. Engage both national and local/regional mass media for the planning and implementation of the educational aspect of the campaign.
9. Design and development of content and subsequent placement on national and/or regional television or radio.

The potential Vendor offers services associated with executing the suggested strategic approach, communication plan, and budget.

DEFINED TARGET AUDIENCE GROUPS: Geography – all Ukraine.

I. Teenagers, 11 – 17 years old.
II. Young people, 18-25 years old.
III. Adults, 26-59 years old.
IV. Senior adults older than 60 years old.

THE DESIGN, DEVELOPMENT AND IMPLEMENTATION OF THE CYBERSECURITY PUBLIC AWARENESS CAMPAIGN SHOULD BE CARRIED OUT FOR THE PERIOD FEBRUARY-AUGUST 2024.

CORE TASKS/SUB-MILESTONES OF EACH CAMPAIGN STAGE/MILESTONE:

1. **CONCEPT DEVELOPMENT:** To design, develop and implement the concept of the Campaign using the most effective channels for obtaining information for targeted groups.
2. **MATERIALS AND SOURCES DEVELPPMENT&WORKED OUT:** To design, develop and disseminate media content for the segmented audience groups to raise knowledge of cybersecurity threats, vulnerabilities, and relevance of cyber hygiene basic rules based on the agreed concept and in close cooperation with the CRDF Global in Ukraine team.
3. **PROGRAM(S) IMPLEMENTATION BY MILESTONES:** To raise the level of awareness of cyber threats and the basics of cyber hygiene among residents of Ukraine.
4. **CROSS-SECTION OF KNOWLEDGE(s), RESULTS EVALUATION:** To evaluate effectiveness and coverage of the Cybersecurity Public Awareness campaign among the general population of Ukraine.
5. **STUDY SUMMARY**

The Midterm study conducted as part of the first round of the Cybersecurity Public Awareness campaign has provided valuable insights into the public's understanding of crucial cybersecurity aspects. This research embarked on multiple waves: the first one, in August-September 2021, explored target groups' awareness of cybersecurity fundamentals. In March 2023, the interim study presented pivotal results, showing the dynamic of the indicators. The obtained results underlined the Campaign's success in educating people about online threats and promoting secure practices. The awareness of Ukrainians regarding concepts like "cybersecurity" and "cyber hygiene rules" has increased since 2021, with 19% and 14% confidently claiming knowledge about these concepts. Specifically, 69% have a general idea about cybersecurity, and 55% have a similar understanding of cyber hygiene rules. Overall, there's positive progress in awareness, but there's room for improvement, especially in understanding cyber hygiene rules.

THE MAIN GOAL:

The main goal of the campaign is to continue to improve public awareness of cybersecurity threats and cyber hygiene rules among the target audience groups in Ukraine with the objective to make cyber hygiene routine a normal practice in audiences` everyday life.

The Campaign should be targeted at four age category groups:

I. Teenagers 11 – 17 years old;
II. Young people, 18-25 years old;
III. Adults, 26-59 years old;
IV. Senior adults older than 60 years old.

TYPES OF CONTENT INCLUDED BUT NOT LIMITED WITH:

1. Targeted social media content for various age groups with CRDF Global in Ukraine Facebook page being the main distribution channel.
2. YouTube material(s) with one or more content developers who deliver interview/documentary videos with a minimum of 500 000 subscribers.
3. Brief awareness raising video content to be broadcasted on the national television of Ukraine.
4. Outdoor advertising in major Ukrainian cities.
5. Interactive installation in museum or art gallery or through any other public location available to draw public`s attention to the importance of cyber hygiene (optional).
6. Online thematic flashmobs (optional).

All the products delivered under the campaign should be of a consistent and distinctive nature for the audience to be able to create associations with the key objective of the activity regardless of the content they are consuming.

The Campaign is suggested to be implemented in stages, considering the specifics of each target group. **HOWEVER, VENDORS ARE ENCOURAGED TO PROVIDE THEIR OWN CREATIVE VISION OF EFFECTIVE CONTENT DELIVERY AS LONG AS IT MEETS THE BASELINE REQUIREMENTS AND OBJECTIVES.**

SUGGESTED STAGES:

Stage 1. The Cybersecurity Public Awareness campaign for adults, 26-59 years old (reaching a minimum coverage of 10 million individuals within the campaign duration). Scheduled for February/March 2024

Stage 2. The Cybersecurity Public Awareness campaign for young people 18-25 years old (reaching a minimum media audience of 10 million individuals within the campaign duration). Scheduled for March - April 2024

Stage 3. The Cybersecurity Public Awareness campaign for teenagers, 11-17 years old (reaching a minimum media audience of 5 million individuals within the campaign duration). Scheduled for April-May/June,2024

Stage 4. The Cybersecurity Public Awareness campaign for senior adults older than 60 Scheduled for years old (reaching a minimum media audience of 5 million individuals within the campaign duration). Scheduled for June- July 2024

Assessment on the Campaign results and impact launched.
Assessment report on the Campaign results and impact ready - August 2024

This delivery Schedule may be revised and updated by CRDF Global and/or the Contractor during the period of performance if mutually approved.

Example of approach…

Stage 1. The Cybersecurity Public Awareness campaign for adults, 26-59 years old

The period of development and implementation of the Campaign is February-August 2024.
Stage breaks down per Milestones set up to be reached out during the defined period:

A. ..
B. ..
C. .. etc.

All documents should be prepared in English in formats pdf, word, ppt, excel.
Applicants should be ready to present their tender offer to CRDF Global tender committee via online meeting in English.

REQUIREMENTS FOR APPLICANTS, to be proved with appropriate documents submission:

Only applications from possible Vendors who meet the following requirements will be considered.

1. The Applicant must be founded and provide communication, media placement and PR services for at least three years.
2. The Applicant must have proven work experience with international organizations, international funds, international non-profit organizations over the past three years.

3. The Applicant must have proven work experience with social impact projects and social advertising campaigns in partnership with Ukrainian Governmental agencies (local authorities, regional state administrations, Ministries, others) over the past three years.

4. The Applicant must have experience in the development and implementation of social impact communication campaigns with national coverage over the past three years.

VENDOR SELECTION CRITERIA, to be proved with appropriate documents submission:

CRDF Global will select the Contractor that provides the best total value in terms of the best approach and experience on the project implementation and cost for the project implementation.

The selection of the company will be carried out by the CRDF Global tender committee based on the next criteria according to the specific scope weight:

The most significant criterion for evaluation would be - completeness and filling of the program deliberate and accountable steps to achieve the goal the possibility of obtaining a qualitative result in a quantitative measurement when conducting a cross-section of knowledge and preparing a report the most efficient use of funds breakdown of goals and budget according to milestones.

We expect to receive the BEST VALUE FOR MONEY through appliance of above listed approached.

1. Efficiency of proposed strategic approach, proposed communication plan and planned KPIs – 3 points.
2. Economic efficiency of proposed budget split (correl. between activities/tools and budget) – 4 points.
3. Applicant's technical and professional capabilities, team members expertise which Applicant can provide for the Cybersecurity Public Awareness campaign development and implementation given the complexity of the project and the involvement of a Ukrainian government partners – 3 points.

Vendors may contact the team in case of any clarifying questions related to the campaign`s implementation before the application deadline. The deadline for questions receiving is (10 days before the submission deadline).

CAMPAIGN BUDGET:

The Cybersecurity Public Awareness campaign preliminary total budget is **USD 190,000** for all target groups, for the period **February-August 2024.** The budget includes all creative services, production, media placement expenses, fees, including taxes or any other expenses required for campaign development and implementation.

The final campaign budget can be changed according to the changes of campaign objectives.

IMPORTANT NOTES:

Considering CRDF Global cybersecurity policies, the Vendor must consider and follow the next rules:

1. All communication campaign materials should include U.S. Department of State, CRDF Global and Ukrainian Government Partners brand identity elements (logos) and disclaimers.
2. It is not allowed to use Russian Federation web builders (like Tilda, or any others) or any other Russian Federation digital platforms and media tools.
3. It is not allowed to conduct advertising campaigns in TikTok social networking services. It is allowed to use TikTok social networking service as communication channels by third parties.
4. All developed materials, ideas, reports, hand-outs, postings etc. that resulted from the project implementation remain sole property of CRDF Global and cannot be transferred/shared with a third party. For the leak of any information the Contractor agrees to be responsible and bear penalties and fine(s).

   *"**INTELLECTUAL PROPERTY.** "Intellectual Property" means all (i) patents, patent applications, patent disclosures and inventions, (ii) trademarks, service marks, trade dress, trade names, logos,*

(iii) copyrights (registered or unregistered) and copyrightable works and registrations and applications for registration thereof, (iv) computer data, data bases and documentation thereof, (v) trade secrets and other confidential information including, without limitation, ideas, formulas, compositions, inventions (whether patentable or un-patentable and whether or not reduced to practice), know how, processes and techniques, research and development information, drawings, specifications, designs, plans, proposals, technical data, copyrightable works, moral rights, financial and marketing plans. CRDF Global shall be the sole and exclusive owner of all of the Intellectual Property produced or adopted by the Contractor in fulfilling its obligations under the terms of this PO. The Contractor shall cooperate and assist in all reasonable manners to ensure that CRDF Global has the valid right or license to use, possess, develop, sell, license, copy, distribute, market, advertise, and/or dispose of any or all of the Intellectual Property."

5. The **NON-Disclosure Agreement** shall be signed by the parties.

PROPOSAL STRUCTURE:

1. Applicant short description
2. Statement of Interest and Technical Capabilities
3. Proposed approach for the project implementation
   3.1. The strategic approach proposal for Stages 1-4. The strategic approach is proposal with demonstration of the common vision and ideas that will meet communication challenges and achieve project's KPIs.
4. Main team characteristics
5. List of recent experiences
   5.1. Applicant's credentials with demonstration of experience and cases related to social impact communication projects.
   5.2. Applicant's credentials with demonstration of experience and cases related to digital media campaigns.
   5.3. The list of social impact communication projects implemented for international organizations, international funds and international nonprofit organizations. The list should include the short description of the project, period of implementation, summary of results, efficiency of the project. The document should be submitted on the Applicant's branded template with signature(s) and official stamp of the Applicant.
   5.4. Team members profiles, CVs, who will work on the Cybersecurity Public Awareness campaign project.
6. Cost proposal
   6.1. The commercial offer must include all creative services, production, media placement expenses, fees, including taxes or any other expenses required for campaign development and implementation. The commercial offer must be prepared according to Table 1. The Cybersecurity Public Awareness campaign budgeting framework. The document should be submitted on the Applicant's branded template with signature(s) and official stamp of the Applicant.
7. Annexes

PRICE SCHEDULE:

The prices provided shall be all-inclusive and include all additional expenses, e.g. travel, accommodation, management of a project, project overheads, etc. All prices shall be **GROSS** and provided **in USD.**

Kindly mind that the submitted quotes shall be fixed under the **Fixed-Price (FFP) Contract.** That type of Contract foresees prices schedule that is not subject to any adjustment. Firm prices shall be kept based on

the contractor's cost experience in fulfilling the contract. This contract type places upon the contractor maximum risk and full responsibility for all costs and resulting profit or loss.

Table 1. The Cybersecurity Public Awareness campaign budgeting framework

Service	Budgeting Framework, Stage 1 adults 26-59 y.o., USD	Budgeting Framework, Stage2 young people 18-25 y.o. USD	Budgeting Framework, Stage 3 teenagers, 11-17 y.o., USD	Budgeting Framework, Stage 4 senior adults, 60+ y.o., USD
Media Production (video, radio reels, banners, social media content, leaflets, etc)				
Media placement				
Social Media Marketing campaign				
Installations at public events etc.				
PR activities (work with Mass Media, etc.)				
Work with campaign's ambassadors, bloggers, influencers				
Outdoor activities (3D screen Animation)				
Other activities (*please specify every issue)*				
Creative services				
Agency Fee				

** In case needed, the table may be supported with extra lines to reflect extra services being charged.*

TOTAL Budget: USD _____

PAYMENT:

The Bidder shall submit a notional deliverable schedule with their submission that includes the acceptance criteria for each deliverable and expected implementation.

Proposed payments schedule – upon competed and accepted milestones. Reporting milestones are subject to mutual agreement and shall be set prior to the campaign startup. Milestones shall be set as per the vendor's proposal under RFP.

Standard payment terms – it's a post payment within 30 calendar days after acceptance of delivery. In some cases, deliverables may have to be approved by the US Government prior to CRDF Global acceptance.

The invoice shall be issued together with detailed specifications on the list of services and goods provided.

Other payments terms and schedule may be discussed additionally. Preference will be given to Bidders, that confirm standard payment terms.

Payment shall be affected in USD from CRDF Global bank account located in the USA, Arlington. Requisites of USD bank account shall be available and provided.

SUBMISSION:

The proposals should be submitted only in English to procurement@crdfglobal.org,

CC to: ynikolova@crdfglobal.org and: akurylenko@crdfglobal.org, no later than **18.01.2024 (January), COB EEST.** The proposal should be submitted as a single electronic document in **PDF and Word or Excel format**, except annexes that can be archived and attached to the proposal as a separate archive.

In case of a huge volume of an electronic document, it should be archived and submitted in parts. Indicate the letter`s subject - **RFP-28-UA-2023**. CRDF Global reserves the right to disqualify any proposal submitted after the submission deadline.

All applications that do not meet the mandatory requirements mentioned in this RFP will not be considered.

I. Period of Validity

Proposals and all price offers shall remain valid and open for acceptance for at least sixty calendar days (60 days) from the date the tender closes.

II. Questions:

Any questions pertaining to this RFP and any issues submitting your Bid Email shall be addressed in writing by email to procurement@crdfglobal.org; CC: ynikolova@crdfglobal.org and akurylenko@crdfglobal.org

III. Evaluation of Proposals:

Only proposals that provide all the necessary evidence required in the RFP will be considered for evaluation. The proposals will be evaluated according to the following criteria: Technical is more important than past performance.

IV. Solicitation Terms & Conditions:

Right to Select Suppliers. CRDF Global reserves the right to negotiate with and select all qualified suppliers at its own discretion and is not obligated to inform suppliers of the methods used in the selection process. CRDF Global reserves

the right to dismiss any and/or all suppliers from the bid process and reject any and/or all proposals.

Obligation. This RFP does not bind nor obligate CRDF Global in any way. CRDF Global makes no representation, either expressed or implied, that it will accept or approve in whole or in part any proposal submitted in response to this RFP. CRDF Global may reward, in whole or in part, the proposal at its sole discretion.

Binding Period. Following the due date of submission of this Proposal, the pricing included in this RFP shall be binding upon the supplier for the duration of the contract.

Hold Harmless. By submitting a response to the RFP, bidder agrees that CRDF Global has sole discretion to select any and/or all suppliers. During or following the conclusion of this process, bidders waive their rights to damages whatsoever attributable to the selection process, materials provided, supplier selection, or any communication associated with the RFP process and supplier selection.

Transfer to Final Contract. The terms and conditions of the RFP, including the specifications and the completed proposal, will become at CRDF Global's sole discretion, part of the final contract (the "Agreement") between CRDF Global and the selected bidder. In the event that responses to the terms

and conditions will materially impair a bidder's ability to respond to the RFP, bidder should notify CRDF Global in writing of the impairment. If bidder fails to object to any condition(s) incorporated herein, it shall mean that bidder agrees with, and will comply with the conditions set forth herein.

Exceptions. Any exceptions to the terms and conditions or any additions, which the bidder may wish to include in the RFP, should be made in writing and included in the form of an addendum to the applicable Section in the RFP.

CRDF Global Proprietary Information. Supplier agrees that all non-public information contained in this document and communicated verbally in reference to this RFP by CRDF Global shall be received for the sole discretion and purpose of enabling the supplier to submit an accurate response to this RFP. The information contained in this RFP and disclosed during the course of negotiations and communications are proprietary in nature and under no circumstances to be disclosed to a third party without prior written consent from CRDF Global.

Supplier Proprietary Information. Information contained in the response to this RFP will be considered proprietary in nature if marked "confidential" or "proprietary". Such marked documents will not be disclosed to third parties outside CRDF Global with the exception of retained consultants under contractual confidentiality agreements.

Company name:
Authorized representative's name and signature:
Address:
E-mail: