CRDFGLOBAL

CLARIFICATIONS NO. 1

RFP-UA-FK_01-2026 – Cybersecurity Subject Matter Expert (SME) Support for Digital Resilience Technical Assistance Activities in Ukraine

Dear Prospective Offerors,

With reference to the Request for Proposals (RFP) published on October 9, 2026, please find below the Contracting Authority's responses to the clarification questions received by the applicable deadline.

These clarifications form an integral part of the RFP and should be considered when preparing and submitting proposals. In the event of any inconsistency between these clarifications and the original RFP, the information provided in this document shall prevail.

The Contracting Authority acknowledges that the proposal submission period is relatively short and appreciates the request received for an extension.

However, due to the urgent nature of the requirement and the pre-established project deadlines, it is unfortunately not possible to extend the submission deadline. Prospective Offerors are therefore kindly requested to prepare and submit their proposals within the timeframe specified in the RFP.

#	Question	Clarifications by the Contracting Authority
1. Access to stakeholders and critical infrastructure operators		
1.1	The Scope of Work includes conducting surveys and interviews with representatives of national cybersecurity authorities and critical infrastructure operators. Will CRDF Global facilitate introduction and engagement with the identified stakeholders, including critical infrastructure entities and relevant government institutions?	CRDF Global may facilitate selected introductions where such support is required. However, the Vendor is expected to maintain established relationships with key entities and to demonstrate a solid understanding of the research topic.
1.2	Does CRDF Global already have a predefined list of organizations that are expected to participate in the survey and interview process, or is the Contractor expected to identify and engage these stakeholders independently?	CRDF Global expects the Vendor to identify and focus on key institutions within the sector. The final list of stakeholders will be reviewed and approved jointly by CRDF Global and the Vendor.
1.3	In the event that certain organizations are unable or unwilling to participate, how will this affect the expected scope of evidence collection?	Non-participation will itself be regarded as a valid response and a valuable insight for the assessment.

2. Expected coverage of Ukrainian case evidence		
2.1	Is the intention to focus primarily on documented and publicly available cases, or does CRDF Global expect the collection and analysis of non-public information obtained through stakeholder engagement?	Given the sensitive nature of the subject and the limited availability of public information, which may not fully reflect the actual situation, the Vendor is expected to analyze both publicly available and non-public (but non-classified) information.
2.2	Are there any priority technology domains or categories of suppliers that should receive particular attention within the assessment (e.g., telecommunications, networking equipment, cloud services, industrial control systems, surveillance technologies)?	No specific priorities have been set. The assessment should cover the domain as comprehensively as possible.
3. Scope of the foreign practice review		
3.1	Beyond the requirement to review U.S. approaches and at least three European countries, does CRDF Global have any preferred jurisdictions that should be included in the analysis?	The Vendor is invited to propose mature jurisdictions that have established effective Trusted Vendor Frameworks.
3.2	Is the expectation to conduct a legal and regulatory review only, or also to assess implementation practices and enforcement mechanisms where information is available?	The review should cover both the legal and regulatory framework and, where information is available, implementation practices and enforcement mechanisms.
4. Recommendations for Trusted Vendor Framework		
3.3	*The RFP notes that development of the Trusted Vendor Framework itself is outside the scope of the assignment.* Could CRDF Global further clarify the expected level of detail for the policy and regulatory recommendations?	Recommendations should be high-level, highlighting key directions for further development of the domain
3.4	Should the recommendations include proposed criteria, governance principles, and institutional roles for a future Trusted Vendor Framework, or should they remain at the strategic and policy level?	Recommendations should remain at the strategic and policy level.

5. Deliverables and reporting expectations		
5.1	Is there an expected format, template, or approximate length for the analytical report, executive summary, presentation materials, and interim one-pagers?	No specific template is prescribed; the emphasis is on the quality and substance of the content.
5.2	Are there specific donor, governmental, or program reporting standards that should be followed when preparing the deliverables?	Deliverables must be provided in both English and Ukrainian.
6. Deliverables and reporting expectations		
6.1	For the stakeholder briefings and dissemination activities, does CRDF Global anticipate organizing and coordinating these sessions, or is the Contractor expected to manage the participant engagement?	The Vendor is expected to manage stakeholder engagement in close coordination with CRDF Global.
6.2	Are interpretation, translation, and meeting facilitation services expected to be included in the Contractor's scope?	Yes. The Vendor must be able to conduct meetings in the working language of the interviewees, organize and hold both in-person and online meetings, and provide translation of materials from Ukrainian into English.

***