CRDF GLOBAL
REQUEST FOR PROPOSAL
RFP-UA-FK_01-2026

Cybersecurity Subject Matter Expert (SME) Support for Digital Resilience Technical Assistance Activities in Ukraine

Proposals Submission Deadline: Oct 14, 2026

Summary:

CRDF Global is seeking qualified Cybersecurity Subject Matter Expert(s) (SMEs) to conduct a consolidated, case-based assessment of the threat posed by untrusted technologies and concrete, actionable recommendations, namely, priority mitigation steps and the evidence base to inform the subsequent development of Ukraine's Trusted Vendor Framework (TVF).

Scope

CRDF Global, in support of the U.S. Department of State, is implementing Digital Resilience Technical Assistance activities in Ukraine. The objective of this effort is to strengthen the evidence base available to Ukrainian state bodies for addressing risks associated with untrusted technologies and to support the development of a national Trusted Vendor Framework aligned with Ukraine's cybersecurity priorities, EU accession requirements, and relevant international practice.

Untrusted technologies are technologies presenting unacceptable cybersecurity supply-chain risk, including technologies subject to jurisdictions whose laws permit or compel vendor cooperation with state intelligence or security authorities without meaningful independent judicial oversight or legal recourse.

The Contractor shall:

1. Consolidate documented Ukrainian case evidence on risks, dependencies, and incidents associated with untrusted technologies in critical networks and infrastructure;
2. Review foreign (U.S. and European) legislation, regulatory measures, and key incident cases on restricting high-risk / untrusted suppliers, covering no fewer than six European countries, and map these against the U.S. trusted vendor approach as a comparative reference;
3. Develop concrete, actionable recommendations for Ukrainian state bodies on priority mitigation steps and on the policy/regulatory approach for developing the national Trusted Vendor Framework;
4. Support stakeholder engagement and dissemination of findings to relevant Ukrainian institutions and international partners.

The development of the Trusted Vendor Framework itself is a separate follow-on policy effort beyond the scope of this study. The study will provide the analytical foundation and recommendations to inform and de-risk that subsequent process.

The effort may include coordination with Ukrainian cybersecurity stakeholders, including national-level cybersecurity entities, technical teams, and operational partners, as required to support alignment and interoperability objectives.

Period of Performance

- Oct 21, 2026 – February 22, 2027

Work Cadence

- The selected Contractor must be based in Kyiv and able to work in a hybrid format, combining remote support with on-site presence as needed. This includes the ability to promptly attend in-person meetings and provide on-site support upon request.
- Response time expectations for the expert or team of experts should not exceed 24 hours for acknowledging receipt of communications or requests. Subsequent deliverables and actions would then be carried out in accordance with mutually agreed timelines and deadlines.

Tasks and Deliverables

As directed by CRDF the Contractor shall perform tasks including, but not limited to:

Task 1. Ukrainian Threat Landscape Assessment (Case-Based Assessment)

- Conduct desk research on documented real cases and potential threats from untrusted technologies in Ukrainian networks and critical infrastructure;
- Design and administer a survey of up to 10 core actors of the national cybersecurity system and critical infrastructure regarding known cases within their areas of responsibility;
- Conduct up to 5 in-depth interviews with state agencies and critical infrastructure operators;
- Produce a consolidated body of Ukrainian case evidence to ground the analysis and recommendations.

Task 2. Foreign Practice Review

- Review European legislation, regulatory measures, and key incident cases on restricting high-risk suppliers (EU 5G Toolbox terminology) in two phases, covering no fewer than three European countries each as well as U.S. (minimum seven countries in total);
- Map European approaches against the U.S. trusted vendor approach (including references such as the FCC Covered List and related policies) as a comparative reference point;
- Assess areas of convergence and difference between the European and U.S. approaches and their relevance to the Ukrainian context.

Task 3. Recommendations Development

- Provide the evidence base and proposed policy/regulatory approach to inform the subsequent development of the national Trusted Vendor Framework (which may take the form of a package of legislative, regulatory, and policy instruments);
- Identify relevant institutions that should be involved in the Framework's development and adoption.

Task 4. Constant Stakeholder Engagement and Dissemination

- Deliver a dedicated briefing on findings for the donor and partner missions upon request;
- Prepare selected interim findings in concise one-pager format suitable for sharing with international partners upon request.

Task 5 Analytical Report Development and Dissemination

- Finalize the three-part analytical report (Ukrainian threat landscape; foreign practice review; recommendations);
- Prepare public executive summary (Ukrainian and English);
- Prepare presentation materials for state bodies and partners;
- Develop layout of analytical reports suitable for printing;
- Ensure printing of 50 hard copies.

Reporting

Deliverable	Description	Deliver to	Due Date
Technical Report(s)	LOE summary, progress, risks & challenges, next steps	CRDF PM	Per Milestone/as agreed
Invoices	Detailed invoices	CRDF PM	Per Milestone/as agreed

Work Performance Deliverables

Deliverable	Description	Due Date
Initial Data Collection Package	Survey instrument, outreach plan, first contacts with target organizations, interim findings	Milestone 1 (by 16 Nov 2026)
Foreign Practice Alignment Report	Review of U.S. and European (foreign) approaches to untrusted / high-risk suppliers; comparative mapping	Milestone 2 (by 15 Dec 2026)
Analytical Synthesis	Integrated analysis of Ukrainian case evidence and foreign practice; preliminary recommendations	Milestone 3 (by 15 Jan 2027)
Final Analytical Report (3 parts)	Complete three-part analytical report; public executive summary (UKR/ENG); presentation materials	Milestone 4 (by 10 Feb 2027)
Final Submission Package	Final report; presentation to state bodies; donor/partner briefing; invoice	Milestone 5 (by 18 Feb 2027)
Public Executive Summary (UKR/ENG)	Key findings and recommendations framework for broader audiences	With final report
Presentation of Recommendations	Presentation to relevant state bodies (to be confirmed)	Milestone 5
Donor & Partner Briefing	Dedicated briefing on findings	Milestone 5
Interim One-Pagers	Concise findings for Tallinn Mechanism members and international partners	As findings mature (from mid/late Nov 2026)
Layout development and printing	Development of the layout of the analytical report suitable for printing; printing of 50 copies for dissemination	Milestone 5

Milestones

MS	Due Date	Substantive Stage & Key Activities	Milestone Output
1	16 Nov 2026	Initial data collection and stakeholder outreach. Finalize survey instrument; identify and contact core actors of the national cybersecurity system and critical infrastructure operators; launch desk research; establish first contacts with target organizations.	Initial Data Collection Package (survey instrument, outreach plan, first contacts, interim findings) presented
2	15 Dec 2026	Alignment with foreign practice. Complete first phase of Ukrainian evidence gathering (survey responses, initial interviews); conduct systematic review of U.S. and European approaches to non-trusted / high-risk suppliers (first phase, ≥3 European countries); prepare comparative mapping.	Foreign Practice Alignment Report (U.S. and European approaches; comparative mapping)
3	15 Jan 2027	Analytical synthesis. Complete remaining interviews and Ukrainian research; finalize European review (second phase, ≥3 additional countries); integrate Ukrainian case evidence with foreign practice findings; develop preliminary recommendations.	Analytical Synthesis (integrated Ukrainian evidence + foreign practice; preliminary recommendations)
4	10 Feb 2027	Final analytical report. Finalize the three-part analytical report (Ukrainian threat landscape; foreign practice review; recommendations); prepare public executive summary (Ukrainian and English); prepare presentation materials for state bodies and partners.	Final Analytical Report (3 parts) + public executive summary (UKR/ENG)
5	18 Feb 2027	Dissemination and formal closure. Present recommendations to relevant state bodies; deliver donor and partner briefing; design layout and ensure printing of 50 hard copies; submit final report package and invoice.	Final Submission Package (report, presentations, briefing, invoice)

Standards and Framework Alignment

Work performed under this effort should align, as applicable, with:

- NIST Cybersecurity Framework (CSF)
- ISO 27001
- ENISA guidance
- MITRE ATT&CK
- Applicable Ukrainian national cybersecurity frameworks and standards.

Contractor Requirements: Contractor personnel shall demonstrate the following qualifications and capabilities:

- Proven experience in cybersecurity policy research, public policy analysis, and development of practical recommendations;
- Demonstrated expertise in mixed-methods research (desk research, surveys, and in-depth interviews) in the field of cybersecurity or related policy domains;
- Familiarity with Ukrainian national cybersecurity architecture, institutions, and the broader policy context;
- Ability to engage with state bodies and critical infrastructure operators and to handle sensitive information appropriately;
- Experience with European and/or U.S. approaches to high-risk / non-trusted suppliers is highly desirable;
- Advanced English language proficiency required; Ukrainian language fluency required;
- Experience supporting government institutions, public sector entities, or donor-funded programs is highly desired.

Proposal Requirements

Applicants shall submit the following:

- Statement of Interest and Technical Capabilities inclusive of:
    - CV(s)
    - List of recent experience in the RFP subject matter area and applicable references/past performance

- Cost Proposal:
    - Shall be submitted in U.S. dollars and structured as a not to exceed (NTE) Time & Materials (T&M) or Fixed-Price-Level of Effort proposal, at the offeror's discretion, with rationale for the chosen approach.
    - Shall propose daily or hourly labor rates for all proposed personnel, with a fully loaded rate breakdown.
    - Shall propose any other direct costs (ODCs) with brief justification.
    - Shall provide a total not-to-exceed (NTE) ceiling for the Base Period and, separately, for the Optional Extension Period.
    - Cost realism and reasonableness will be evaluated against the proposed scope.

- All submission documents must be in English
- Any Small or Disadvantaged Business Designations (Veteran Owned, HUB Zone, Women Owned, Disadvantaged Businesses)

Proposals will be evaluated based on the qualifications and relevant experience of the proposed expert(s), the quality of the proposed technical approach, demonstrated ability to meet the required scope and deliverables, past performance, and overall price reasonableness. CRDF Global will select the proposal offering the best overall value, considering both technical merit and cost

RFP Timetable:

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

Friday, Oct 09, 2026:	RFP posted and live
Monday, Oct 12, 2026:	RFP Questions due – questions must be submitted in writing
Tuesday, Oct 13, 2026:	RFP Questions & Answers released
Wednesday, Oct 14, 2026	RFP submissions due
Wednesday, Oct 21, 2026	Contract start date

Submission:

Proposals should be submitted to procurement@crdfglobal.org & fkelmendi@crdfglobal.org , **no later than 18:00, October 14, 2026**. Proposals should be submitted as electronic documents in PDF, Word or Excel format.

CRDF Global reserves the right to disqualify any proposal submitted after the submission deadline.

The subject line of the email must read:

[Insert name of submitter] CRDF Global RFP Submission - **Cybersecurity SME Support – Digital Resilience Activities in Ukraine**

Resources Provided by CRDF Global:

CRDF Global will facilitate introductions to the designated Ukraine Government Agency and other relevant Ukrainian cybersecurity stakeholders, and will provide background materials, prior assessment outputs, and program documentation as appropriate and as security classification permits.

Background:

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. With support authorized by the Nunn-Lugar Act of 1991 and the Freedom Support Act of 1992, as well private foundation contributions, CRDF Global embarked on bolstering the global scientific community and fostering alternatives to weapons research.

In the past 25 years, our work has expanded to address ever-changing global concerns, but our commitment to ensuring the success of our partners remains the same. We are 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; Amman, Jordan; Kyiv, Ukraine; Manila, Philippines; Almaty, Kazakhstan; and Warsaw, Poland; CRDF Global's global staff and networks of local community and government stakeholders deliver programs tailored to specific regions that advance U.S. security interests in over 120 countries across the globe.

Vision Statement:
Our world, healthy, safe, and sustainable.

Mission Statement:
Safety, security, and sustainability through science, innovation, and collaboration.

Values:
We do the right thing.
We care about each other and the people we work with.
We work together to deliver excellence

CRDF Global provides equal opportunities to all qualified individuals without regard to age, race, color, religion, sex, sexual orientation, gender identity, national origin, protected veteran, or disabled status. We are committed to prioritizing an inclusive and collaborative space in which diversity and equity is discussed, championed, and

supported. We acknowledge and honor the fundamental value and dignity of all individuals. We pledge ourselves to creating and maintaining an environment that respects diverse traditions, heritages, and experiences.
More information is available at www.crdfglobal.org

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.

Notification. CRDF Global will notify bidders following completion of the evaluation process, as to whether or not bidders have been awarded the contract. The only information regarding the status of the evaluation of proposals that will be provided to any inquiring bidder shall be whether or not the inquiring bidder has been awarded the contract. CRDF Global may, at its sole discretion, inform any inquiring bidder of the reason(s) as to why it was not awarded the contract.

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/RFI, 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/RFI, 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 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/RFI by CRDF Global shall be received for the sole discretion and purpose of enabling the supplier to submit an accurate response to this RFP/RFI. 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/RFI 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.