CRDFGLOBAL

Request for Proposals (RFP)

Title of Competition:

Cybersecurity Improvement Grants for Governmental Authorities and Critical Infrastructure State-Owned Enterprises (SOE) in Ukraine

Reference Number: CySIG-06-2026

Competition Opens	June 19, 2026
Submission Deadline	July 10, 2026
Announcement of Results	Grant awards are subject to the availability of funding from program sponsors
Budget Ceiling	Up to USD 50,000 in-kind support per Applicant
Project Duration	Up to 6 months
Eligible Applicant(s)	Governmental Authorities and Critical Infrastructure State-Owned Enterprises (SOE) in Ukraine
Eligible Countries	Ukraine
Eligible Project Scope	Improving the level of cybersecurity and information security in the Governmental Authorities and Critical Infrastructure SOE in Ukraine

TABLE OF CONTENTS

OVERVIEW

CRDF Global is currently accepting proposals from the Governmental Authorities and Critical Infrastructure SOE in Ukraine (hereafter – potential applicants) for the Competition titled "Cybersecurity Improvement Grants for Governmental Authorities and Critical Infrastructure State-Owned Enterprises (SOE) in Ukraine (the Competition). This Competition is organized and administered by CRDF Global, utilizing funding provided by the U.S. Department of State. **Funding will be provided in the form of in-kind support; a grantee is not expected to receive and manage grant funds directly.**

*Governmental Authorities are defined in accordance with the Law of Ukraine "On Central Executive Authorities" and the Law of Ukraine "On Local State Administrations". Critical Infrastructure State-Owned Enterprises (SOE) are defined in accordance with the Law of Ukraine "On Critical Infrastructure".

Goal

Cybersecurity Improvement Grants (CySIG) for Governmental Authorities and Critical Infrastructure SOE in Ukraine 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.

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.

Objectives

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

(1) Increase the level of cybersecurity and the resilience of cybersecurity systems of Governmental Authorities and Critical Infrastructure SOE in 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).

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.

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) Assessment of the cybersecurity posture and audit of protection systems.
(4) Enhancement of professional qualifications and cybersecurity capacities of personnel.

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.
(3) Assessment of the cybersecurity posture and audit of protection systems of Governmental Authorities and Critical Infrastructure SOEs of Ukraine.
(4) Enhancement of qualification skills in the field of cybersecurity for employees of Central Governmental Authorities and Capacity Building Institutions of Ukraine.

Proposed solutions need to address/include the following:

(1) Description of the problem statement and potential solutions that will help to reduce the risk of cyber incidents and enhance cybersecurity systems.
(2) Justification on which critical resources and/or confidential information will be protected and the necessity of protection.
(3) Provide the expected outcomes of the grant implementation.
(4) A results-based monitoring and evaluation framework, including defined KPIs to measure project effectiveness and impact during and after implementation.
(5) Submit a resume (CV) of the Principal Investigator (project coordinator).
(6) Justification of the requested equipment/services/software/materials.
(7) Provide a breakdown of equipment/services/software/materials, specifically:

7.1 Specifications and quantities of services and/or equipment/software with references to relevant models/ brands.

7.2 Cost breakdown:

7.2.1 Equipment/software costs (may include supplementing calculations in Ukrainian Hryvnia with the equivalent amount in US dollars, including value-added tax (VAT) if applicable),
7.2.1 Shipping costs,
7.2.2 Installation costs.

7.3 For each model/brand of equipment/software:

7.2.3 At least one commercial offer from a potential vendor who is ready to supply the services and /or equipment/software.
7.2.4 A list of additional potential vendors, including at least three names and relevant contact information.
7.2.5 If the requested model/brand is supplied by a limited number of vendors or a single vendor, provide substantive and detailed justification for the specific model/brand based on the applicant's experience, technical needs, and the hardware/software previously installed.

Activities:

- CRDF Global communicates funding decisions to the approved proposals.
- CRDF Global and the Grantee negotiate and execute the Grant Agreement.

- CRDF Global conducts a competitive procurement process based on the specification(s) in the approved Grantee's proposal and in coordination with the Grantee.
- CRDF Global, the Grantee, and the selected Vendor negotiate and execute the three-party Contract Agreement.
- The Vendor delivers goods depending on the delivery terms specified in the Contract Agreement.
- The Grantee and Vendor sign the Delivery-Acceptance Act.
- The Grantee submits to CRDF Global the signed Acknowledgement of Equipment Delivery.
- CRDF Global pays the Vendor.
- Grant close-out: reporting on Grantee side.

ELIGIBILITY REQUIREMENTS

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

(1) Applications are accepted from the Governmental Authorities and Critical Infrastructure SOEs of Ukraine, which may be vulnerable to potential cyber threats or other cyber incidents.
(2) Applicants and all proposed vendors, equipment, software, and services must be in full compliance with all applicable U.S. export control laws and regulations, including the Export Administration Regulations (EAR), 15 CFR Parts 730–774, the International Traffic in Arms Regulations (ITAR), 22 CFR Parts 120–130, to the extent that any proposed items constitute defense articles or defense services under the U.S. Munitions List, and U.S. sanctions programs administered by the Office of Foreign Assets Control (OFAC), 31 CFR Chapter V, including applicable country- and region-specific sanctions. Proposals that include items, entities, or transactions that are prohibited or restricted under these laws and regulations will be deemed ineligible without further review.
(3) Applicants have provided a clear formulation of the problem statement and justified the necessity of acquiring equipment/services/software.
(4) Applicants have presented a clear breakdown of the necessary equipment/services/software.
(5) 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.
(6) Applicants have submitted a list of additional potential vendors, including at least three names and relevant contact information.
(7) 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 that do not meet the 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 award decisions, grant activations, and program activities under this Competition are subject to the availability of funding and the approval of the program sponsors. CRDF Global reserves the right to cancel, suspend, or modify this Competition at any stage, including after the announcement of results, if donor funding is withheld, redirected, or discontinued for any reason. In such cases, CRDF Global shall bear no liability to applicants or selected grantee.

Evaluation

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

1. Proposal's Relevance and Potential Impact	**35 points**

Relevance and impact on cybersecurity: Justification and detailing of how the project will help to improve cybersecurity systems and information resilience, both for the applying institution and for the wider sectoral or regional infrastructure it operates within:

- **Organizational benefit** - how the project advances the institution's long-term cybersecurity maturity, operational continuity, and capacity to deliver its critical functions. This may include improvements to governance, workforce capability, process integrity, or technology posture.
- **Infrastructure benefit** - how the outcomes contribute to shared resilience across the sector, supply chain, or geographic area.

Measurable indicators of success, which may include maturity model progression, incident response capability improvements, employees competency benchmarks, reduction in meantime to detect/respond, etc. need to be defined. Alignment with the institution's Digitalization/Cyber Strategy, legislative requirements or equivalent strategic framework/best practice, showing how cybersecurity investment supports broader transformation goals, critical functions and risk profile is expected.

2. The need for equipment/software and/or provision of services.	**25 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 IT/OT cybersecurity system of the institution, including: technical compatibility with current infrastructure (network architecture, SIEM, SOC tooling).A clear description of the current capability limitation or operational gap the project addresses, expressed in terms of organizational risk, service continuity, or resilience maturity - not solely in technical or procurement terms. The rationale should explain why this gap is a strategic priority at this point in time.

3. Clarity, Feasibility and Sufficient Details of Suggested Activities	10 points

The application has a clearly defined objective in providing resources (equipment/services/software/materials/consultancy /coordination). The proposal should include a clear implementation timeline with milestones, defined roles and responsibilities, identified technical requirements and dependencies.

4. Cost Effectiveness	10 points

Sufficient level of details in provided budget and justification in the budget narrative. Proposed costs should be reasonable and benchmarked against market rates. The strategic document should demonstrate how proposed resources are allocated in direct proportion to expected outcomes, Total Cost of Ownership considerations (licensing, maintenance, training), and how the institution will maximize the long-term value of grant funding beyond the initial investment period.

5. Alignment with U.S. Strategic Cybersecurity Priorities	15 points

The extent to which the proposed project advances U.S. strategic cybersecurity priorities and supports market-based technology partnerships with allied nations. Reviewers will score each sub-criterion independently:

(a) Standards Alignment — 5 points: Identify the U.S.-originated cybersecurity frameworks applicable to your institution's operational environment — NIST CSF 2.0, NIST SP 800-53, CIS Critical Security Controls. For each framework identified, describe specifically how the proposed project advances conformance or implementation. If a particular framework does not apply to your context, provide a written explanation of why.

(b) Technology Origin — 5 points: Specify whether proposed equipment, software, and services are of U.S. or allied-partner origin and reference applicable NIST-conformant or allied-equivalent product standards in your technical requirements. Include at least one commercial offer from a U.S. or allied-partner supplier. If U.S. or allied-partner origin products are not technically feasible for a specific component, provide written justification. *Note: Applicants are not scored on the outcome of CRDF Global's competitive procurement process, which is conducted independently by CRDF Global following award.*

(c) Strategic Cooperation Alignment — 5 points: Describe how the proposed project advances relevant objectives reflected in current U.S. cyber and foreign policy guidance, including the White House's 2026 Cyber Strategy for America, the 2023 U.S. National Cybersecurity Strategy where applicable, and the U.S. Department of State Agency Strategic Plan for FY 2026–2030. Strong responses should explain how the project strengthens Ukraine's cyber resilience, improves interoperability with trusted partners, supports secure and market-based technology partnerships, and advances operational cooperation consistent with the applicant's mission and authorities. This may include participation in threat-sharing mechanisms, communities, or platforms such as MISP, FIRST, sectoral ISACs, or other trusted cyber defense exchanges, where these serve the applicant's operational needs. If a specific mechanism, platform, or partnership model does not apply to the applicant's institutional context, explain why and identify any alternatives.

6. Sustainability and Institutional Capacity	5 points

The proposal demonstrates how the institution will maintain and operate the acquired cybersecurity capabilities beyond the grant period. This includes evidence of trained personnel, maintenance plans, and institutional commitment to continued investment in cybersecurity resilience

TOTAL SCORE	100 points

PROPOSAL PREPARATION AND SUBMISSION

Full Proposal Submission

All proposals must be submitted no later than **July 10, 2026.**

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

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

"CySIG-06-2026_YourOrganization".

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 consist of the following documents:

Required:

I. Proposal Cover Letter (PDF, signed) and Proposal Application (PA) Form (Excel spreadsheet) that includes the following sheets:
   (1) Institutional Data Form (IDF)
   (2) A. Project Overview
   (3) B. Scope of Work (SOW)
   (4) C. Workplan (WP)
   (5) D. Budget
   (6) E. Budget Narrative

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

III. One Commercial Offer from a potential vendor.

IV. A list of additional potential vendors.

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

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:

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

II. **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
(8) Information and communications technology (ICT) products, software, or services of Russian origin, including but not limited to products subject to U.S. federal procurement prohibitions.
(9) ICT products, software, or services from entities designated as covered telecommunications equipment or services producers under U.S. law, including equipment manufactured by Huawei Technologies, ZTE Corporation, Hikvision, Dahua Technology, and their subsidiaries or affiliates.

CRDF GLOBAL POLICIES AND APPLICANT RESOURCES

General Terms and Conditions

CRDF Global's General Terms and Conditions are incorporated in the Proposal Application (PA) Form 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 - Governmental 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 equipment received.