CRDF GLOBAL

Seeking a Qualified Cybersecurity Assessment Provider for an Independent Assessment of the External and Internal Perimeters of the SE «ICC» Critical Information Infrastructure

Cybersecurity Improvement Grants (CySIG) – State Enterprise «Information and Computing Center of the Ministry of Social Policy, Family and Unity of Ukraine»

REQ26-0909 REQUEST FOR PROPOSAL

Deadline: November 05, 2026 at 23:59 Eastern Time

Summary:
CRDF Global, with support from the United States Department of State, implements the Cybersecurity Improvement Grants (CySIG) program, a competitive program that strengthens the cybersecurity and resilience of central governmental institutions and state-owned critical infrastructure enterprises of Ukraine. Under this program, CRDF Global seeks a qualified and independent cybersecurity assessment provider to perform a comprehensive assessment of the external and internal security perimeters of the State Enterprise «Information and Computing Center of the Ministry of Social Policy, Family and Unity of Ukraine» (SE «ICC»). SE «ICC» is the Administrator of the Unified Information System of the Social Sphere (UISSS) and operates critical information infrastructure that processes large volumes of sensitive personal and social-protection data. This solicitation is organized in four technical tasks: Task One, an external perimeter assessment, including web application and API security testing; Task Two, an internal perimeter assessment; Task Three, a cyber-defense maturity gap analysis against NIST CSF 2.0, CIS Controls v8.1, and ISO/IEC 27001:2022, culminating in a risk-based, prioritized remediation roadmap; and Task Four, validation retesting of remediated vulnerabilities. A fifth task covers coordination and reporting. Offerors must propose for all tasks.

Scope:

The selected contractor will provide an objective, evidence-based picture of the current security posture of the critical information infrastructure administered by SE «ICC». The external assessment will identify how the organization appears to, and can be attacked by, an external adversary. The internal assessment will test the resilience of the internal environment, including network segmentation, privileged access, Active Directory, endpoint detection and response (EDR) coverage, and the completeness of security monitoring. The maturity gap analysis will measure cyber-defense maturity against NIST CSF 2.0, CIS Controls v8.1, and ISO/IEC 27001:2022 and translate the combined findings into a risk-based, prioritized, vendor-neutral remediation roadmap. Finally, validation retesting will confirm whether the vulnerabilities identified have been effectively remediated. The assessment is not intended to serve as the external cyber-protection assessment under CMU Resolution No. 1799 of 31 December 2025.

Indicative scope: based on information provided by SE «ICC», the assessment is expected to cover approximately at least 45 public IP addresses, 1 primary domain, 100 web resources, 150 APIs, 35 physical and 450 virtual servers, approximately 120 workstations, 1 Active Directory domain, and 2 infrastructure hosting sites, including nine core UISSS component deployments across the two sites. These figures are indicative and will be confirmed at kickoff. Detailed asset lists and infrastructure information will be provided to the selected contractor after signing a non-disclosure agreement (NDA).

CRDF Global anticipates executing a three-party agreement among CRDF Global, the selected contractor, and SE «ICC». All testing will be performed only within a scope and under rules of engagement approved

in writing by SE «ICC». Completion of each deliverable will be confirmed by an acceptance certificate signed by SE «ICC» and approved by CRDF Global. CRDF Global reserves the right to make no award.

Period of Performance:
Agreement Execution Date through [●] (anticipated six (6) months from execution).

Assessment Conduct, Data Protection, and Compliance Terms:
The following provisions are conditions of performance and award, not preferences.

- **Independence and conflicts of interest.** The offeror must disclose any current or prior relationship with SE «ICC», including the supply, implementation, or management of security products or services within the environment to be assessed. CRDF Global may find an offeror ineligible where such a relationship would impair the objectivity of the assessment. Remediation recommendations must be vendor-neutral, and the contractor shall not use the assessment to market products or services to SE «ICC» during the period of performance.
- **Authorization and rules of engagement.** No testing may begin until SE «ICC» has approved in writing the in-scope assets, testing windows, test accounts, points of contact, and rules of engagement. Denial-of-service, destructive testing, and social engineering are prohibited unless expressly authorized in writing by SE «ICC». Testing shall be planned and conducted so that the availability of the UISSS and other production services is maintained at all times; the contractor shall immediately stop any activity that affects availability and notify SE «ICC». SE «ICC» has test environments for its production systems. Active exploitation of UISSS components shall be performed in these environments, as agreed in the rules of engagement.
- **Protection of findings and personal data.** All findings, evidence, credentials, and data encountered are confidential. They must be stored and transmitted only in encrypted form, accessed only by named project personnel, and used solely to perform the resulting agreement. Access to personal data must be limited to the minimum needed to demonstrate a finding; if personal or social-protection data is exposed during testing, the contractor shall stop the relevant activity and notify SE «ICC» immediately. The contractor shall comply with Ukrainian legislation on personal data protection and on the protection of critical information infrastructure.Findings and evidence must not be uploaded to third-party cloud services, including cloud-based scanning platforms, without the written approval of SE «ICC».
- **Distribution of reports.** Full technical reports will be delivered to SE «ICC» only. CRDF Global will receive the executive summaries, the remediation roadmap summary, and the acceptance certificates, unless CRDF Global and SE «ICC» agree otherwise.
- **Data destruction.** Within 5 days of final acceptance, the contractor shall securely destroy all data, evidence, and credentials obtained from SE «ICC» and provide a written certificate of destruction.
- **Key personnel.** Personnel named in the proposal must perform the work. Substitutions require the prior written approval of CRDF Global and SE «ICC». Access to SE «ICC» infrastructure will be granted only to personnel who are citizens of Ukraine and have signed a non-disclosure agreement. The contractor shall comply with SE «ICC» requirements for the protection of restricted information, and SE «ICC» may require additional personnel screening under its own security rules.
- **Eligibility and compliance.** Because this activity is funded by the U.S. Government, offerors must not be suspended, debarred, or otherwise excluded from U.S. federal awards; must comply with applicable U.S. and Ukrainian sanctions and export control requirements; and must not use or

provide covered telecommunications equipment or services as defined in Section 889 of the FY2019 National Defense Authorization Act (2 CFR 200.216), or any hardware, software, or services developed or provided by Kaspersky Lab or its affiliates. All testing tools must be legitimately licensed.

- **Taxes.** The services procured under this RFP are exempt from Value Added Tax (VAT). CRDF Global will provide the selected contractor with an official tax exemption letter confirming this status. All prices must therefore be quoted in U.S. dollars, exclusive of VAT. Offerors should state in their proposal any obstacle they foresee to applying the exemption.
- Goods and/or services under this RFP are procured using funds allocated exclusively for the implementation of an international technical assistance project registered in Ukraine in accordance with the procedure established by applicable legislation.

Task One: External Perimeter Assessment, including Web Application and API Security

Objective: Identify and validate the vulnerabilities and exposures of SE «ICC» that are visible to, and exploitable by, an external adversary.

Example Activities include:

- Discover the external attack surface, including domains, subdomains, public IP ranges, exposed services, and cloud-hosted assets, and confirm the in-scope asset list with SE «ICC».
- Conduct open-source intelligence (OSINT) reconnaissance, including exposed technical information and publicly available leaked credentials associated with the organization.
- Perform vulnerability scanning of public-facing services and infrastructure.
- Test in-scope web applications and APIs, including authentication, session management, access control, input validation, and business logic, in accordance with the OWASP Web Security Testing Guide (WSTG) and the OWASP API Security Top 10.
- Validate exploitable findings in a controlled, non-destructive manner within the approved rules of engagement.
- Review the security configuration of external-facing encryption (TLS), DNS, email security (SPF, DKIM, DMARC), and remote access services.

Task One Deliverables:

- External perimeter assessment report, including a dedicated web application and API security section, with an executive summary, risk-rated findings (including CVSS v4.0 scores), supporting evidence, and remediation recommendations.
- Immediate written notification to SE «ICC» of any critical finding, without waiting for the final report.

Task Two: Internal Perimeter Assessment

Objective: Assess the resilience of the internal environment of SE «ICC» against an adversary who has gained an initial foothold, and verify the completeness of its detection and monitoring capabilities. Internal testing shall be performed exclusively on-site at the SE «ICC» office. The provision of test accounts and a workstation, and the conditions for their use, will be agreed in the rules of engagement.

Example Activities include:

- Test network segmentation between user, server, management, and critical system zones.

- Review privileged access management, including privileged accounts, administrative paths, and credential hygiene.
- Review Active Directory security, including privileged groups, delegation, authentication configuration, password policies, Active Directory Certificate Services (ADCS), and attack paths to domain dominance.
- Verify EDR coverage across in-scope endpoints and servers and identify unprotected assets.
- Assess the completeness of security logging and monitoring (SIEM), including log source coverage and whether agreed test activities were detected and escalated.
- Validate high-impact findings in a controlled, non-destructive manner within the approved rules of engagement.

Task Two Deliverables:

- Internal perimeter assessment report with an executive summary, risk-rated findings (including CVSS v4.0 scores), attack path analysis mapped to MITRE ATT&CK, supporting evidence, and remediation recommendations.
- Detection coverage summary identifying monitoring and EDR gaps.
- Immediate written notification to SE «ICC» of any critical finding, without waiting for the final report.

Task Three: Cyber-Defense Maturity Gap Analysis and Remediation Roadmap

Objective: Measure the cyber-defense maturity of SE «ICC» against NIST CSF 2.0, CIS Controls v8.1, and ISO/IEC 27001:2022, and deliver a risk-based, prioritized remediation roadmap that integrates the results of Tasks One and Two.

Example Activities include:

- Review policies, procedures, and technical documentation, and conduct interviews with relevant SE «ICC» staff.
- Assess current maturity against the six NIST CSF 2.0 functions (Govern, Identify, Protect, Detect, Respond, Recover) and define a target profile with SE «ICC».
- Map implementation of CIS Controls v8.1 safeguards for Implementation Group 2 (IG2).
- Assess the status of the information security management system and Annex A controls against ISO/IEC 27001:2022, identifying gaps relative to the current and target profiles.
- Consolidate all findings into a risk-based, prioritized, vendor-neutral remediation roadmap, ranking actions by risk to SE «ICC» (likelihood and impact), with short-, medium-, and long-term actions and an indicative level of effort for each.
- Within the roadmap, identify the categories of protective solutions recommended for future procurement (for example, EDR/XDR, next-generation firewall, vulnerability management, SIEM or centralized logging, MFA and privileged access management, and secure backup), each with a vendor-neutral justification and key functional requirements. The supply of such solutions is not part of this procurement.
- Present the final results to SE «ICC» leadership, with a summary briefing for CRDF Global.

Task Three Deliverables:

- Maturity gap analysis report with current and target profiles against NIST CSF 2.0, CIS Controls v8.1, and ISO/IEC 27001:2022.

- Risk-based, prioritized remediation roadmap, including vendor-neutral recommendations for protective solution categories.
- Consolidated vulnerability register covering all findings from Tasks One and Two (risk rating, affected asset, recommended action, and status), for SE «ICC» to track remediation.
- Final results presentation to SE «ICC» and summary briefing for CRDF Global.

Task Four: Validation Retesting of Remediated Vulnerabilities

Objective: Verify that the vulnerabilities identified in Tasks One and Two have been effectively remediated by SE «ICC». Remediation will be carried out by the internal IT and information security teams of SE «ICC»; the contractor will provide recommendations, advisory support, and retesting.

Example Activities include:

- Provide advisory support to SE «ICC» during remediation, including clarification of findings and recommended fixes, ahead of the retest.
- Agree with SE «ICC» the list of remediated findings to be retested and the retest window, within the approved rules of engagement.
- Retest all critical and high-risk findings, and other findings as agreed with SE «ICC», using the techniques that originally identified them.
- Confirm the status of each retested finding (remediated, partially remediated, or not remediated) with supporting evidence, and identify any new issues introduced by remediation.

Task Four Deliverables:

- Validation retest report with the status of each retested finding and supporting evidence, including the share of critical and high-risk findings confirmed as remediated. Updated vulnerability register and, where needed, updated remediation roadmap priorities.

Task Five: Coordination and Reporting with CRDF Global

Objective: Coordinate with CRDF Global and SE «ICC» throughout the period of performance and document completion of all tasks.

Example Activities include:

- Hold a kickoff meeting with CRDF Global and SE «ICC» within [10] business days of agreement execution and agree the rules of engagement.
- Provide brief progress updates to CRDF Global every two weeks, without disclosing sensitive technical findings, and promptly report any risks to schedule or scope.
- Deliver reports to SE «ICC» in Ukrainian, with executive summaries also provided in English to CRDF Global.
- Prepare a final completion report within seven (7) business days of final acceptance.

Task Five Deliverables:

- Kickoff meeting minutes and approved rules of engagement.
- Bi-weekly progress updates.
- Final completion report with signed acceptance certificates and certificate of data destruction.

Anticipated Performance Schedule:

Milestone	Deliverables	Expected Delivery Date
Kickoff and rules of engagement	Kickoff minutes; confirmed scope; signed rules of engagement	Within 2 weeks of execution
External assessment	Task One report	Within [6] weeks of execution
Internal assessment	Task Two report; detection coverage summary	Within [10] weeks of execution
Gap analysis and roadmap	Task Three report; remediation roadmap; final presentation	Within [14] weeks of execution
Validation retest	Task Four validation retest report; updated vulnerability register	Within [22] weeks of execution
Acceptance and closeout	Signed acceptance certificates; final completion report; certificate of data destruction	Within [6] months of execution

Contractor Requirements:

Organization:

- At least [three (3)] years of experience delivering penetration testing and security assessment services.
- At least [three (3)] comparable engagements for government or critical infrastructure organizations completed in the last three years.
- A documented testing methodology aligned with recognized standards such as NIST SP 800-115, PTES, and the OWASP Web Security Testing Guide.
- Legal ability to perform security testing services in Ukraine, and independence from SE «ICC» as described in the Assessment Conduct, Data Protection, and Compliance Terms.

Key Personnel:

- Lead penetration tester with recognized offensive security certifications (for example, OSCP, OSEP, CREST CRT or CCT, GPEN, or GXPN) and demonstrated experience in Active Directory and internal network testing.
- Web application and API testing specialist with relevant certifications or equivalent documented experience.
- Governance, risk, and compliance lead with demonstrated experience in NIST CSF and CIS Controls assessments (for example, CISSP, CISM, CISA, or ISO/IEC 27001 Lead Auditor).
- All personnel with access to SE «ICC» infrastructure must be citizens of Ukraine, and the team must be able to work on-site in Kyiv and in Ukrainian.

General:

- Willingness to enter a three-party agreement with CRDF Global and SE «ICC».

- Willingness to accommodate reasonable changes or adjustments to delivery as directed by CRDF Global or SE «ICC».
- Demonstrated ability and willingness to incorporate cost-sharing, leverage existing resources, and provide in-kind contributions where possible to maximize project impact and efficiency.

Proposal Requirements:
Each proposal must include:

Proposed Technical Approach and Project Team

- Methodology for each task, including tools, testing techniques, safeguards for production availability, and the approach to the NIST CSF 2.0 and CIS Controls v8.1 assessment.
- Outline of the proposed rules of engagement and of the data handling plan for findings, evidence, and personal data.
- CVs and certifications for all key personnel, with each person's role, level of effort, and citizenship.
- List of recent, relevant experience with at least [three (3)] references, with past performance clearly included.
- **15-page limit, excluding CVs, sample report, and cost proposal**

Written Acceptance of Terms and Conflict of Interest Disclosure

- Written acknowledgment and acceptance of the Assessment Conduct, Data Protection, and Compliance Terms and of the three-party agreement structure; disclosure of any relationship with SE «ICC»; and a self-certification that the offeror is not excluded from U.S. federal awards and complies with the Section 889, Kaspersky, and sanctions requirements. A proposal that does not accept these terms may be found non-responsive.

Cost Proposal in USD

- **NOTE:** Offerors are required to submit a firm fixed price for each task using the format below or a template following the same structure, supported by the number of people, level of effort, and daily rate. Prices must be quoted in U.S. dollars exclusive of VAT (see the tax exemption provision above) and valid for at least [90] days from the submission deadline. Travel and other direct costs must be listed separately. Prices must include all testing tool licenses; SE «ICC» will not procure or license any tools. Offerors may add rows to show cost-sharing, leveraged resources, or in-kind contributions; all additions should be clearly labeled.

Cost proposal as formatted below:

Table A – Price Summary by Task

Task	**Firm Fixed Price (USD)**
Task One: External Perimeter Assessment, including Web Application and API Security	
Task Two: Internal Perimeter Assessment	
Task Three: Maturity Gap Analysis and Risk-Based Remediation Roadmap	
Task Four: Validation Retesting of Remediated Vulnerabilities	
Task Five: Coordination and Reporting	

Task	Firm Fixed Price (USD)
Total (USD), core scope	

Table B – Level of Effort and Daily Rates by Key Personnel

This is an example only; offerors may amend it as needed.

Key Personnel / Role (name)	Daily Rate (USD)	Days Task 1	Days Task 2	Days Task 3	Days Task 4	Total Days	Total (USD)
Project lead / manager							
Lead penetration tester							
Web application and API testing specialist							
Governance, risk, and compliance lead							
Other personnel (specify)							
Total labor (USD)							

Contractor Selection Criteria:
Scoring will be based on CRDF Global's evaluation of the contractor's ability to meet CRDF Global's key requirements. That includes competitive pricing, quality of proposal, past performance, and credentials and experience of key personnel. CRDF Global reserves the right to accept or reject any and all proposals and to negotiate terms of any subsequent agreements at its own discretion. CRDF Global will select the contractor who provides the best value in terms of overall price and technical experience. Independence from SE «ICC», eligibility, and acceptance of the Assessment Conduct, Data Protection, and Compliance Terms are conditions of award rather than scored trade-offs.

Best Value Trade-Off:
Successful proposals will be selected based on both technical and price factors, weighing them to determine which offer represents the best value. Technical factors, such as methodology, qualifications of key personnel, and past performance, may be more heavily weighted than price. CRDF Global reserves the right to select a higher-priced proposal if it offers superior technical benefits or overall value, and retains full discretion to contract for all, some, or none of the activities included in any proposal submitted under this RFP.

Evaluation Scoring Methodology:
Proposals will be evaluated on a 100-point scale. Scoring will be based on alignment with the stated objectives, soundness and safety of the proposed methodology, and the realism of the scope, weighted according to the criteria identified below.

Evaluation Criteria	Weight (%)	Subfactors
1. Technical Approach and Methodology	[50%]	Understanding of the requirements; depth and safety of testing methodology; quality of the maturity assessment approach; quality of sample report; data handling plan
2. Past Performance / Qualifications	[20%]	Relevant engagements with government or critical infrastructure clients; certifications and experience of key personnel; references
3. Price / Cost	[30%]	Overall cost compared to market rates; cost realism; level of effort proposed; cost share

Timetable:
The procurement process is intended to follow the timeline below.

Activity	Date
Request for Proposal (RFP) Issued	October 20, 2026
Deadline for Questions and Answers	October 27, 2026
RFP Questions and Answers Released	October 29, 2026
Proposal Submission Deadline	November 05, 2026
Anticipated Contract Issuance	By November 30, 2026

Questions and Answers:

Interested parties may submit questions regarding this RFP to Yana Zarakhovska yzarakhovska@crdfglobal.org . Questions will be accepted through 23:59 Eastern Time on October 27, 2026 and will be addressed as received. Following the close of the Q&A period, a consolidated Q&A document containing questions received and the corresponding responses will be posted alongside the RFP on the CRDF Global website.

Submission:
Proposals should be submitted to Yana Zarakhovska, yzarakhovska@crdfglobal.org , no later than **23:59 Eastern Time on November 05, 2026**. Proposals should be submitted as electronic documents in PDF, Word, or Excel format. Email subject REQ26-0909_Title of RFP

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 ast 30 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 status, or disability. We are committed to fostering a respectful, collaborative, and supportive work environment where all individuals can contribute and thrive. We recognize and uphold the inherent value and dignity of every person, and we strive to maintain a workplace that honors a wide range of backgrounds, perspectives, 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, 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 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.