CRDF GLOBAL
REQUEST FOR PROPOSAL (RFP)

DPRK, Russia, and Iran Sanctions Evasion Experts - Organizational

Submission Deadline: 5:00 PM EDT |November 6, 2026

Summary:

CRDF Global organizes a wide variety of programs focused on **maritime sanctions evasion, cryptocurrency, North Korean IT worker schemes, cybersecurity, and counterproliferation finance (CPF)**, including online training modules, multilingual presentations, and educational discussions for global audiences. Areas of programming and expertise include, but are not limited to:

- Workshops to train port authorities to enforce UNSCR (United Nations Security Council Resolution) sanctions on the DPRK and/or Iran, and U.S., Canadian, and EU sanctions on Russia.
- Maritime sanctions-evasion prevention topics such as ultimate beneficial ownership, shadow fleets, ship-to-ship transfers, fraudulent flagging, vessel and port maintenance and inspection, and compliance measures for shipbrokers and chartering services to prevent engagement in activities linked to the DPRK, Russia, and/or Iran.
- Financial institutions' and banks' responsibilities for complying with UNSCR sanctions, including building effective sanctions-compliance frameworks, taking preventive measures to manage risks related to illicit financial activities or procurement networks involving the DPRK, Russia, and/or Iran, and conducting effective enhanced due diligence.
- Counterproliferation finance through fiat and/or virtual currencies, such as blockchain investigations and analysis and money laundering tactics and obfuscation techniques related to the DPRK, Russia, and Iran.
- Expertise in DPRK, Russian, and/or Iranian offensive cyber operations against financial institutions, cryptocurrency exchanges, universities, and research centers; cyber hygiene for nontechnical audiences; cyber incident response; cyber threat hunting; cyberthreat tactics, techniques, and procedures; cybersecurity strategy development and enterprise-wide cybersecurity; and cybersecurity tabletop or interactive exercise development.
- Create country-specific presentations and training regarding sanctions enforcement, counterproliferation finance, theft of sensitive intellectual property, or cyber operations.
- We expect any materials developed on the above topics to be high quality and presentable to an audience of professionals in the public and private sectors.

As such, CRDF Global requires on-going, flexible, and lasting partnerships with experts in the field.

If you are seeking to apply as an *individual* rather than as an organization, please see the separate **REQUEST FOR PROPOSAL: Sanctions Expertise – Individuals.**

Scope & Tasks:

Types of Engagement Support (include but are not limited to the following):

- Development and delivery of presentations, case studies, exercises, and technical material
- Facilitating and/or contributing to technical discussions
- Implementing workshops and trainings worldwide
- Providing consultative services
- Conducting open-source research

RFP Subject Matter Expertise: Maritime sanctions evasion; UNSCR, U.S., and European sanctions concerning the DPRK, Russia, and/or Iran; illegal ship-to-ship transfers; regulations and due-diligence requirements for shipbrokers and chartering services; UNSCR sanctions compliance for financial institutions and cryptocurrency exchanges; anti-money laundering related to the DPRK, Russia, and/or Iran; blockchain investigations and analysis; forced North Korean labor overseas; cyberattacks by DPRK, Russian, and Iranian actors against financial institutions; and cyberattack investigation and attribution.

The selected Subject Matter Expert(s) (hereafter, "SME(s)") would be expected to provide contracted services such as, but not limited to:

a) Building, tailoring, and delivering curricula and interactive exercises for private- and public-sector audiences worldwide, both in person and online through live webinars, e-courses, and other asynchronous training methods.
b) Researching and providing detailed reports on the DPRK, Russia, and/or Iran's sanctions evasion tactics and methods to circumvent laws and regulations.
c) Developing tools and/or documents for relevant staff at targeted institutions related to strengthening their capacity to prepare for and identify DPRK, Russian and/or Iranian sanctions evasions tactics.
d) Communicating and collaborating with CRDF Global to develop and deliver related trainings around the world.
e) Offering outreach assistance, such as leveraging SME networks and contacts to assist CRDF Global with participant recruitment and selection for global trainings.
f) Leading training implementation, including delivering curriculum developed, answering questions from participants, and providing follow-up guidance as requested by participants.
g) Assistance with developing daily readouts during events, e.g., providing short summaries and key points of each presentation and discussion.
h) Delivery of an After-Action Report that summarizes observations, successes, lessons learned, and recommendations for future programming on the relevant topic
i) Providing reporting, such as financial reports, with all relevant documentation (e.g., receipts, invoices, travel documentation, etc.), weekly and/or ad-hoc check-ins by phone or video conference during project planning and implementation, and final project reports including recommendations for next steps.
j) Attending and participating in regular meetings with CRDF Global staff, funder, and other parties as necessary to coordinate successful implementations. Also attending lessons learned calls to discuss how to improve future engagements.

Contract for Services:

Following selection, CRDF Global will negotiate a General Services Contract (hereafter "GSC") with the selected SME(s).

While the GSC is not a guarantee of any work, the selected SME(s) on a GSC can be engaged by CRDF Global staff with an abbreviated selection process. This allows CRDF Global to potentially leverage the partnership with the SME for strategic initiatives, proposal submissions, and programmatic responses to urgent timelines.

The GSC will be structured to allow CRDF Global Agreement Officers to issue task orders to the SME(s) upon successful negotiation of the task order scope and budget.

The term of the GSC can be negotiated following selection but is generally expected to be 3 years with an option to extend for up to 2 years.

The GSC would seek to negotiate and lock in elements of pricing and cost that are agreeable to both parties.

Selection Requirements and Criteria:

Selection will be based on CRDF Global's evaluation of the SME's ability to meet any or multiple of the following requirements as well as factors such as competitive pricing, quality of proposal, past performance, and other intangible factors. While CRDF Global does not expect any SME to meet every single requirement listed, the proposal must clearly speak to the requirements that the SME does meet.

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.

<u>Evaluation Factors</u>

1. Qualifications (40%)
    a. The organizational applicant's credentials and the qualifications of its proposed personnel in the relevant technical areas across industry, the public sector, and/or academia. Consideration will be given to the length, breadth, and depth of relevant experience and capabilities.
2. Past Performance (30%)
    a. The organizational applicant's experience with similar activities will be evaluated based on the resumes or CVs of proposed key personnel, the statement of interest and technical capabilities, and any relevant past-performance information provided.
3. Price/Cost (30%)
    a. Price will be evaluated for reasonableness, fairness, and alignment with the proposed scope of work. The project seeks a balance between competitive pricing and technical merit.

<u>Evaluation Methods:</u>

- 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 experience, qualifications, 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. CRDF Global 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 based on the following scoring system:

- Excellent (5): Exceeds all requirements and offers superior benefits.
- Good (4): Meets all requirements with some additional value.
- Acceptable (3): Meets all minimum requirements.
- Marginal (2): Meets some requirements but has deficiencies.
- Unacceptable (1): Fails to meet requirements.

General Requirements

- Has experience developing standard operating procedures (SOPs) and training plans.
- Has proven experience developing global networks within CPF, cyber sanctions evasion, maritime sanctions evasion, and related critical infrastructure institutions, particularly with members of the UNPOE.
- Has experience delivering trainings to audiences with live interpretation.
- Has experience delivering trainings in-person and online to relevant levels of customs officials, financial professionals, and cybersecurity professionals.
- Has a global network of port authorities, customs officials, financial professionals, and cybersecurity professionals who understand US, EU, and UNSCR sanctions related to the DPRK, Russia, and/or Iran.
- Has experience working in / with port authorities, customs officials, financial institutions / cryptocurrency exchanges, law enforcement, and cybersecurity organizations around the world.
- Has demonstrated expertise and experience working in maritime sanctions enforcement, cybersecurity, cryptocurrency, or illicit financial flows to the DPRK, Russia, and/or Iran and has access to a deep pool of experts.
- Has experience working with the U.S., Canadian, and other partner governments or has substantive knowledge of government objectives regarding maritime sanctions enforcement and counterproliferation programming.
- Has experience working with governments and the private sector around the world.

Maritime

- Demonstrated expertise in the evolving maritime sanctions evasion strategies employed by Russia, Iran, and the DPRK, including the use of shadow fleets, front companies, complex ownership structures, fraudulent vessel registration practices, and third-country intermediaries to facilitate sanctioned trade and financial activity.
- Experience conducting maritime investigations using vessel-tracking data, Automatic Identification System (AIS) analysis, beneficial ownership research, trade documentation review, port-call analysis, and commercial shipping intelligence tools to identify deceptive shipping practices and sanctions violations.
- Expertise identifying indicators of sanctions evasion, including ship-to-ship transfers, AIS manipulation or disablement, falsified cargo and customs documentation, transshipment through third countries, vessel identity changes, flag hopping, and efforts to obscure beneficial ownership.
- Experience supporting collaboration among maritime authorities, customs agencies, financial institutions, insurers, commodity traders, flag registries, shipping companies, and law enforcement organizations to investigate, report, and disrupt sanctions-evasion networks operating across global supply chains.
- Has expertise assessing, deploying, and leveraging maritime domain awareness (MDA) tools.

Cybersecurity

- Demonstrated expertise designing and implementing cybersecurity frameworks for cryptocurrency exchanges, VASPs, fintech firms, and financial institutions, including governance, risk assessments, security controls, incident response planning, and operational resilience measures.
- Deep knowledge of cyber threats posed by North Korean, Russian, and Iranian actors, including spear-phishing campaigns, credential theft, malware deployment, insider threats, social engineering, and attacks targeting virtual asset platforms, financial institutions, and government networks.
- Experience developing and implementing security protocols for digital asset environments, including wallet security, transaction-signing procedures, access management, multi-factor authentication, custody solutions, blockchain monitoring technologies, and controls designed to prevent theft, fraud, and unauthorized transactions.
- Expertise in leveraging cyber threat intelligence, network monitoring, threat hunting, and incident response methodologies to identify, investigate, contain, and mitigate cyber intrusions affecting cryptocurrency businesses and other high-risk sectors. Experience translating threat intelligence into actionable defensive measures is strongly preferred.
- Experience training government agencies, financial institutions, VASPs, and private-sector organizations on cyber hygiene, threat awareness, information sharing mechanisms, and coordinated responses to nation-state cyber threats targeting digital finance and critical infrastructure sectors.

Counter Proliferation Finance (CPF)

- Has demonstrated expertise and experience working in counterproliferation finance, anti-money laundering, counterterrorism financing, and sanctions compliance. Expertise in these areas must include developing case studies on sanctions evasion activities and interactive exercises relevant for a financial sector and compliance-related audience.
- Is knowledgeable of DPRK, Iran, and other sanctions evasion-related activities and how to combat such activities through strengthening counterproliferation finance, anti-money laundering, counterterrorism financing, and sanctions compliance.
- Has knowledge on fiat or cryptocurrency money laundering and obfuscation techniques, including transaction screening and monitoring, suspicious activity reporting, and identifying “red flags” associated with each of the aforementioned threat actors.
- Has background in anti-money laundering, financial intelligence analysis, or related area and holds related certifications (CAMS, CSS).

Cryptocurrency Compliance

- Demonstrated expertise in implementing and advising on virtual asset sanctions compliance programs, including the Office of Foreign Assets Compliance (OFAC), UN Security Council sanctions, FATF Recommendation 15, the Travel Rule, transaction monitoring, sanctions screening, and risk-based compliance frameworks for virtual asset service providers (VASPs), financial institutions, and regulators.

- Deep knowledge of nation-state sanctions evasion methods involving digital assets, including DPRK cryptocurrency thefts and laundering networks, Iranian shadow banking and crypto-financing schemes, and Russian sanctions-evasion facilitators, exchanges, payment networks, and illicit financial intermediaries. Expertise should include real-world case studies and recent enforcement actions.
- Practical experience conducting blockchain-based investigations, tracing illicit funds across multiple blockchains, identifying wallet clusters, analyzing mixers, cross-chain swaps, OTC brokers, DeFi protocols, and supporting asset-freezing, seizure, or enforcement actions through blockchain intelligence tools and open-source techniques.
- Subject expertise on how sanctioned states and their proxies use virtual assets, cybercrime, front companies, shell entities, shadow banking systems, money brokers, and trade-based mechanisms to support weapons programs, military procurement, and illicit revenue generation.
- Experience delivering advanced training to regulators, financial intelligence units (FIUs), law enforcement, customs authorities, intelligence services, financial institutions, and VASPs. SMEs should be capable of developing tabletop exercises, investigations workshops, compliance simulations, and actionable guidance tailored to operational audiences.
- Expertise in DPRK, Russian, and Iranian cyber-enabled financial crime, including exchange compromises, spear-phishing, insider threats, ransomware, crypto theft, and defensive measures for digital asset service providers.

DPRK IT Worker Schemes

- Demonstrated expertise in DPRK remote IT worker operations, including fraudulent identity creation, employment procurement techniques, revenue-generation models, use of overseas facilitators, and the connection between IT worker activity, sanctions evasion, and weapons proliferation financing.
- Experience helping organizations identify and mitigate DPRK IT worker risks through enhanced hiring practices, identity verification, contractor screening, onboarding controls, insider-threat detection, and risk-management frameworks for technology companies, staffing firms, financial institutions, and virtual asset businesses.
- Practical expertise investigating cyber-enabled threats associated with DPRK personnel, including unauthorized access, credential abuse, data exfiltration, malicious code insertion, spear-phishing, and other insider-risk indicators. Experience developing mitigation measures and incident-response procedures is strongly preferred.
- Knowledge of U.S., UN, and international sanctions authorities related to DPRK revenue-generation activities, including mechanisms for reporting suspicious activity, information sharing, blockchain and financial investigations, and coordination among law enforcement, regulators, financial institutions, VASPs, and private-sector employers.

Proposal Requirements:

Proposal submission must be in English. Non-English proposal submissions will be disqualified.

Each proposal must include:

1. Statement of Interest and Technical Capabilities
    - Detailed description of the services offered in correlation with the RFP Subject Matter Expertise detailed under **Scope and Tasks** as well as the relevant Requirements met detailed under **Selection Requirements and Criteria**
    - List of recent experiences working with the U.S. and Canadian Governments and/or CRDF Global programming
    - CVs (no more than 2 pages each) of key contact(s)/project lead(s)/trainers
    - If applicable, examples of past content development in subjects related to the RFP subject matter expertise
2. Cost proposal
        - Description of pricing and cost factors (e.g., hourly rates and fixed-price amounts for standard services) that the SME would be willing to discount and negotiate under the GSC.
3. Completion & online submission of CRDF Global's Contractor Data Form
    - Within the form **Massoud Ahmad** must be selected as the Procurement Representative.
4. *[Required for U.S.-based orgs only]:*
    - Any Small or Disadvantaged Business Designations (Veteran Owned, HUB Zone, Women-owned, Disadvantaged Businesses)

RFP Timetable:

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

Friday, October 2, 2026:	RFP Posted & Live
Thursday, October 8, 2026:	RFP Questions Due
Monday, October 12, 2026:	RFP Questions & Answers Released
5:00 PM EDT; Friday, November 6, 2026:	RFP Submissions Due
Week of November 19, 2026:	Selected SME(s) Notified

Proposal Submission:

Proposals must be submitted electronically in PDF or Word format, with the cost proposal provided in Excel format. Proposals must be emailed to Massoud Ahmad (mahmad@crdfglobal.org), Shakeela Amaj (samaj@crdfglobal.org), and Greg Kelly (gkelly@crdfglobal.org) no later than **5:00 PM EDT | November 6, 2026**.

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_Sanctions Evasion SME

Background:

CRDF Global is an independent nonprofit that advances U.S. national security by mitigating threats and expanding opportunities through technology, innovation, and collaboration. Founded in 1995, the organization has implemented some of the most critical foreign assistance initiatives of the past three decades and today works across threat reduction, cybersecurity, global health, stabilization, and emerging technology security. Operating in approximately 80 countries, CRDF Global partners with governments, institutions, and technical experts to strengthen resilience, counter illicit networks, and address transnational challenges that undermine global security. With a workforce of approximately 150 and offices in the United States, Jordan, Poland, Ukraine, the Philippines, Kazakhstan, and beyond, CRDF Global combines global reach with trusted local partnerships to deliver sustainable, impact-driven security solutions.
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.

No Obligation. This RFP does not bind or obligate CRDF Global in any way. CRDF Global makes no express or implied representation that it will accept or approve, in whole or in part, any proposal submitted in response to this RFP. CRDF Global may award all, part, or none of the work described in this RFP at its sole discretion.

Proposal Validity. Following the proposal submission deadline, the pricing and other terms included in a proposal shall remain valid and available for negotiation until execution of a GSC, unless otherwise agreed in writing by CRDF Global and the supplier.

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.