CRDF GLOBAL

REQUEST FOR PROPOSAL

Deadline: May 22, 2026

Summary:

CRDF Global, in support of the U.S. Department of State's Cooperative Threat Reduction (CTR) CASE Program, is seeking a qualified Subject Matter Expert (SME) or organization with expertise in cybersecurity for cryptocurrency ecosystems, API and cloud security, and North Korean IT worker threats. The Contractor should have experience designing and delivering in-person trainings for cybersecurity/IT audiences in the virtual asset service providers and payment platform industry. Under this engagement, the Contractor will develop and deliver a two-day, in-person training in Lagos, Nigeria for approximately 35 private sector cybersecurity professionals at virtual asset service providers (VASPs) and payment platforms. The training will provide foundational knowledge of cybersecurity in cryptocurrency ecosystems, cybersecurity controls, incident response protocols, and threat intelligence related to North Korean tactics, techniques, and procedures for targeting this industry. Travel to Nigeria for delivery is required.

Scope:

The Contractor will serve as the lead trainer and subject matter expert (SME) and will be responsible for developing and delivering a two-day, in-person training in Nigeria focused on compliance, threat awareness, and cybersecurity best practices for the VASP and payments industry. Additionally, the SME should be able to discuss how DPRK-linked actors exploit cryptocurrency ecosystems via exchange hacks, phishing, malware, and advanced persistent threat behavioral typologies and explain wallet architecture, API and cloud security, vulnerability management, North Korean IT worker threats, and defenses against social engineering and insider threats.

The Contractor will also participate in regular planning and coordination calls with CRDF Global and provide a post-engagement subject matter expert report outlining key observations, lessons learned and recommended next steps. The training will incorporate Nigeria-specific case studies on virtual asset technologies and threats, as well as interactive breakout and practical exercises.

Tasks and Deliverables:

Task 1: Implementation Plan and Training Material Development

The Contractor will work with CRDF Global to identify priority topics to present, create an agenda, and develop training materials for the workshop. The Contractor will develop or modify existing training presentations and provide all leave-behind materials for electronic distribution to participants based on feedback from CRDF Global and CTR.

The training will equip participants with the knowledge and skills to better protect their institutions from North Korean-based cyber threats:

- **The DPRK Crypto Threat: Tactics, Techniques, and Procedures (TTPs) and Global Context**: Overview of DPRK cyber operations targeting crypto ecosystem, common hacking tactics, use of DeFi, mixers, and cross-chain bridges for laundering.
- **Transaction Monitoring & Blockchain Analytics**: Blockchain tracing fundamentals, identifying suspicious patterns, integration of blockchain intelligence tools, and red flags specific to DPRK activity.

- **Cybersecurity Architecture for VAPSs**: secure wallet infrastructure, network segmentation and endpoint security, API security for payment platforms, cloud security considerations.
- **Preventing Exchange & Platform Compromise**: Common vulnerabilities exploited by DPRK hackers, secure software development lifecycle, penetration and threat hunting, privileged access management.
- **Social Engineering & Insider Threat Mitigation:** Spear-phishing campaigns targeting employees, fake job recruitment attacks, insider risks including IT worker threats, security awareness programs.
- **Incident Response & Crisis Management:** Incident response planning for crypto theft, steps after a breach, wallet freezing and coordination with exchanges, blockchain tracking and recovery, coordination with law enforcement, public communication and reputational management.
- **Public–Private Cooperation**: Importance of threat intelligence sharing among VASPs, engagement with Financial Intelligence Units (FIUs), international partners, industry partners.
- **Practical Application**: Case studies and tabletop exercises to reinforce operational response and coordination.

Based on these topic discussions, the Contractor will develop all training materials for the relevant Day 1 and Day 2 sessions. These training materials will include presentation slide decks, a minimum of one breakout exercise, and a minimum of two regional case studies. These training materials will be provided to CRDF Global **no later than June 25, 2026** to allow for CRDF Global and CTR review and approval.

Task 1 Deliverables:

1. Agenda
2. Trainer(s) Bio
3. Training materials:
   a. Presentation slide deck for training sessions, including:
      i. A minimum of two (2) breakout exercises
      ii. A minimum of two (2) regionally focused case studies
4. Pre-post training question to assess participant knowledge gain, using the polling or survey tools.

Task 2: Training Implementation

The Contractor will deploy SME(s) to **Nigeria** to implement and deliver onsite training covering the topics. The training will consist of two full days (8 hours each day): Day 1 and Day 2 training sessions.

Task 3: Communication & Reporting

CRDF Global will provide a template to the Contractor to complete a Final Report, which should be submitted within five business days of training completion. The Contractor will participate in weekly and ad hoc planning calls as needed with CRDF Global to discuss programmatic updates, shifts in project implementation, and recent conversations with the funder. CRDF Global and the Contractor will identify a mutually agreed-upon day and time for all parties to meet if needed. In addition, the Contractor will attend the prep meetings to go over the platform for smooth implementation of the webinar, as needed.

Task 3 Deliverables:

1. Subject Matter Expert Report: including outcomes, lessons learned, and recommendations, to be submitted no later than five business days after the last day of the training

Travel:

Contractor is responsible for booking and managing all their travels, required to perform services under this Agreement. All travel must comply with applicable U.S. federal travel requirements, including the Fly America Act where applicable. Contractor must obtain prior written approval of travel itineraries from the Company to confirm compliance. Travel costs that are not approved in advance or that fail to meet applicable compliance requirements will not be reimbursed

Contractor Expertise, Technical, and Experience Requirements:

- Demonstrated expertise in cybersecurity specific to cryptocurrency and virtual asset ecosystems, including hot and cold wallet strategy, network segmentation and endpoint security, API and cloud security for payment platforms, privileged access management, social engineering, and ransomware, among other topics.
- In-depth knowledge of insider threat management and mitigation, including collusion risks, monitoring controls, and North Korean IT worker schemes.
- Proven hands-on capability with professional blockchain analytics and investigation workflows, including real-time transaction monitoring, wallet screening, risk scoring, case management, evidentiary reporting, and support to asset freezing, seizure, and forfeiture processes.
- Experience delivering practitioner-level, in-person training to cybersecurity professionals in the DeFi, payments, VASP industry, with the ability to develop structured curricula, case studies, simulations, and practical exercises.
- Demonstrated track record of supporting public-private sector cooperation and information sharing.
- Prior experience implementing U.S. Government or internationally funded capacity-building programs, preferably in Nigeria or West Africa.
- Availability of certified and experienced instructors with recognized professional credentials in or cybersecurity
- Capability and willingness to travel to Nigeria and deliver the full two-day training in person; familiarity with Nigerian VASP and cultural context is a strong asset given the local context and participant profile.

Proposal Requirements:

- Statement of Interest and Technical Capabilities
- Cost proposal
- CV(s)
- List of recent experience in the RFP Subject Matter area and applicable references/past performance
- Any Small or Disadvantaged Business Designations (Veteran Owned, HUB Zone, Women Owned, Disadvantaged Businesses)
- NAICS Codes: 541620 Environmental Consulting Services- Small Business Threshold $15 million, 541690 Other Scientific and Technical Consulting Services – $15 million

Timetable:

May 18: RFP Questions due
May 19: RFP Questions & Answers released
May 22: RFP submissions due
May 26: Contract start date

Contractor Selection Criteria:

CRDF Global will select the contractor that provides the best value in terms of overall price and experience. The contractor should have proven experience working in cybersecurity within the cryptocurrency industry.

CRDF Global prioritizes a safe and collaborative work environment in which diversity, equity, and inclusion is championed and discussed. CRDF Global provides equal employment opportunities to all qualified individuals without regard to age, race, color, religion, sex, sexual orientation, and gender identity, national origin, protected veteran, or disabled status. We are dedicated to creating and maintaining a respectful work environment that is safe, engaging, and comfortable for all. CRDF Global pledges to prioritize sponsorship of diverse events and panels of experts whenever possible.

Selection Criteria and Evaluation Methods

Evaluation Factors

1. Technical Approach
2. Key Personnel and Qualifications
3. Management Approach
4. Price/Cost
5. Small Business Utilization (if applicable):
6. Risk Management

Evaluation Methods

7. Best Trade-Off Value

Evaluation Scoring Methodology:

Proposals will be evaluated based on the following scoring system:

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

Basis for Award:

The award will be made to the offeror whose proposal is determined to be the best value to CRDF Global and the U.S. Department of State, considering both technical merit and cost. Proposals will be evaluated based on the contractor's demonstrated expertise in cryptocurrency and virtual asset cybersecurity, DPRK-linked actors exploit cryptocurrency ecosystems via exchange hacks, phishing, malware, and advanced persistent threat behavioral typologies and explain wallet architecture, API and cloud security, vulnerability management, North Korean IT worker threats, and defenses against social engineering and insider threats for private sector stakeholders; the qualifications and experience of proposed subject matter experts and trainers; the quality and relevance of the proposed training approach and materials; and the contractor's ability to deliver the training in Nigeria, including logistical readiness and language capability. Cost reasonableness and overall value for money will be assessed in relation to the technical quality and experience offered. The contract will be awarded to the offeror that provides the best overall combination of technical capability, relevant experience, and price.

Submission:

Proposals should be submitted to procurement@crdfglobal.org, and gkelly@crdfglobal.org, no later than *5:00 PM EST time on May 19, 2026*. Proposals should be submitted as electronic documents in PDF, Word or Excel format.

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; Kyiv, Ukraine; and Amman, Jordan, 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.

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 are discussed, championed, and supported. We acknowledge and honor the fundamental value and dignity of all individuals. We pledge ourselves to create 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, 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 conditions 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 is 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.