CRDF GLOBAL
REQUEST FOR PROPOSAL
Deadline: ***June 26, 2026***

Summary:
The Emerging Technology program at CRDF Global is committed to protecting and defending advanced research, data, and technology from exploitation, theft, and IP infringement by adversarial actors. To support this effort CRDF Global, on behalf of the United States Department of State Office of Cooperative Threat Reduction (CTR), is seeking experts to design, develop, and deliver two (2) distinct multilateral workshops in Thessaloniki, Greece for research, administrative, compliance, legal, and operational professionals from academic institutions, research organizations, and private-sector companies in Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Greece, Kosovo, Montenegro, North Macedonia, Romania, Serbia, Slovenia, and Türkiye who are engaged in or support work involving sensitive or dual-use technologies such as but not limited to AI, quantum computing, space technologies, and semiconductors.

Scope of Work:
On behalf of the United States Department of State, Bureau of Arms Control and Nonproliferation, Office of Cooperative Threat Reduction (ACN/CTR), CRDF Global is seeking Subject Matter Experts (SMEs) to design and deliver two (2) two-day workshops in Thessaloniki, Greece for professionals from academic institutions, research organizations, and small and medium-sized enterprises in Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Greece, Kosovo, Montenegro, North Macedonia, Romania, Serbia, Slovenia, and Türkiye.

The selected SME(s) will develop tailored curricula and materials and deliver applied training that strengthens institutional capacity to protect sensitive and dual-use technologies across research environments and supporting supply chains. CRDF Global will provide a 1–2-page briefing developed in coordination with regional experts that identify priority topics and vulnerabilities per country that will support workshop customization and ensure relevance to participating countries and institutional environments. Tailored primarily to institutional stakeholders, including researchers, university administrators, compliance personnel, research management professionals, and operational staff, the workshops will address risks associated with research collaboration, technology development, procurement, commercialization pathways, and supply chain engagement while emphasizing practical mitigation measures applicable to universities, laboratories, and industry settings. The workshops should reflect the current maturity level of research security awareness across the region by incorporating foundational lectures and case-study presentations during initial sessions, followed by more interactive and applied exercises focused on institutional implementation, policy development, and risk mitigation at both national and regional levels across the Balkans research and innovation ecosystem.

The two workshops will address complementary aspects of safeguarding innovation. One will focus on research security within collaborative dual-use sensitive research and development environments, including governance, partner evaluation, and protection of intellectual assets. The second will focus on supply chain security, including procurement integrity, vendor due diligence, and management of materials, equipment, and services that support advanced technology work. Preparatory research conducted by the SME(s) must directly inform material development, case studies, and exercises used in each workshop to ensure regional relevance and applicability to both academic and industry participants.

The workshops will emphasize facilitated discussions, scenario-based exercises, and action-oriented planning sessions designed to help participants apply concepts within their own institutional and operational contexts.

The workshops are intended to:

- Increase institutional and researcher awareness of research security principles, dual-use technology risks, and vulnerabilities associated with international collaboration and advanced technology ecosystems.
- Strengthen institutional governance, transparency, and accountability mechanisms related to governing international partnerships, funding sources, and collaborative research activities by establishing clear oversight structures, robust due diligence practices, and regular compliance reviews..
- Develop practical institutional tools and processes for universities, laboratories, and SMEs, including collaborator vetting procedures, risk assessment methodologies, and information-sharing mechanisms.

- Provide participants with real-world case studies and examples of research security incidents, supply chain vulnerabilities, and technology transfer concerns to support applied learning and institutional preparedness.

Across both workshops, the SME(s) will ensure that preparatory analysis, instructional content, and implementation resources are clearly aligned to the thematic focus of each engagement and tailored to the operational roles of participants. The SME will produce background materials, training content, and leave-behind resources, including templates, checklists, and guidance documents, and deliver two in-person trainings incorporating lectures, facilitated discussion, and applied exercises. The SME(s) will coordinate regularly with CRDF Global to ensure alignment with program objectives and regional context.

Period of Performance: July 2026 - December 2026

Task One: Agenda and Materials Development
The SME will design and develop two distinct workshop curricula: (1) Research Security and (2) Supply Chain Security. Workshop materials should include foundational instructional content introducing core research security and supply chain security concepts for audiences with limited prior exposure, followed by progressively more applied, scenario-based, and interactive modules focused on institutional implementation, governance practices, and risk mitigation strategies.

Using the briefing provided by regional experts, each curriculum must reflect findings and clearly align content, case studies, and exercises to the specific risk domain identified in the briefing. Materials shall provide practical guidance applicable to academic institutions, research organizations, and industry. Materials should incorporate practical tools and leave-behind resources such as collaborator vetting guidance, institutional risk assessment templates/frameworks, due diligence checklists, information-sharing mechanisms, and policy development resources that participants can adapt and implement within their own organizations. CRDF Global and ACN/CTR will review draft materials, and feedback shall be incorporated into final versions.

Task 2 Deliverables:

1. Two draft workshop agendas aligned to research security and supply chain focus areas.
2. Final workshop agendas with ACN/CTR and CRDF Global feedback incorporated.
3. Draft training materials and leave-behind resources (templates, checklists, and guidance materials).
4. Final training materials and leave-behind resources (templates, checklists, and guidance materials) with feedback incorporated.
5. Draft pre- and post-training assessments to measure knowledge gain and other indicators of success as directed by CRDF Global and/or ACN/CTR.
6. Final pre- and post-training assessments with ACN/CTR and CRDF Global feedback incorporated.

Task Two: Workshop Delivery
The SME will deliver two (2), two-day in-person multilateral workshops, back-to-back, in Thessaloniki, Greece, applying the curricula and materials developed under Task Two. Each workshop shall be delivered in alignment with its respective focus area, Research Security and Supply Chain Security, and will emphasize practical application through facilitated discussion, and applied exercises tailored to participant roles across academia, research organizations, and industry.

Workshop delivery should balance traditional lecture-based instruction and case-study presentations during initial sessions with facilitated discussions, collaborative analysis, and applied institutional exercises during later sessions to support practical understanding and implementation. The workshops should incorporate examples and case studies demonstrating real-world research security concerns, including risks associated with inappropriate technology transfer, foreign malign influence, procurement vulnerabilities, and challenges related to international academic and research collaboration.

Task 3 Deliverables:

1. Brief daily readout following the completion of each workshop day using a CRDF-Global provided template.

Task Three: Communication and Reporting with CRDF Global
The SME will coordinate regularly with CRDF Global and ACN/CTR to ensure alignment throughout project execution and will provide reporting on project activities, outcomes, and recommendations.

Task 4 Deliverables:

1. Regular virtual coordination engagements with CRDF Global, ACN/CTR, and/or other members of the project and expert team.
2. An After-Action Report that includes:
    a. An overall assessment of the project, including successes and lessons learned.
    b. Key observations resulting from workshop engagement and regional discussions.
    c. Recommendations for next steps and future work on this topic.

Tentative Schedule of Performance:

Task	Deliverables	Expected Delivery Date
1	Agenda and Materials Development	July-September 2026
2	Workshop Delivery	Early November 2026
3	Communication and Reporting with CRDF Global	July – December 2026

Contractor Requirements:

- Demonstrated ability and willingness to incorporate cost-sharing, leverage existing resources, and provide in-kind contributions (e.g., staff time, materials, tools, or institutional support) to maximize project impact and efficiency.
- Ability/willingness to participate as part of a team of experts contributing to development and delivery of project activities and materials.
- Willingness to accommodate reasonable changes or adjustments to content or delivery as directed by CRDF Global or ACN/CTR.
- Demonstrated experience designing, developing, and delivering university, research institution, and/or innovation-sector stakeholder trainings, facilitated discussions, or institutional capacity-building engagements in one or more of the following areas:
    - Research security and protection of sensitive or dual-use technologies.
    - Risk management in international research collaboration and development partnerships.
    - Due diligence, compliance, or vetting practices applicable to research institutions and small and medium-sized enterprises.
    - Supply chain security, procurement risk management, or vendor evaluation in advanced technology environments.
    - Development of practical guidance, training curricula, or implementation tools for institutional or industry use.
- Demonstrated ability to translate complex research security or supply chain risk concepts into participant-centered, interactive training curricula utilizing case studies, scenario-based learning, facilitated discussion, practical exercises, and implementation-focused tools appropriate for audiences with limited prior exposure to these topics.
- Experience in developing practical implementation resources, including policy guidance, risk assessment frameworks, due diligence tools, or institutional governance materials.
- Experience working with university, research, innovation, or public-sector stakeholders in Central Europe, Balkans and Southeast Europe, and Türkiye Region, including familiarity with regional institutional, governance, and geopolitical dynamics, is strongly preferred.

Proposal Requirements:
Each proposal must include:

- **Statement of Interest and Technical Capabilities**
    - Detailed description of services offered in correlation with the RFP scope and tasks. Your vision for the completed scope and individual deliverables.

  - Technical approach, including CVs and/or bios for the proposed team who can travel to Greece in November for implementation of both workshops.
  - Description of the approach to curriculum and agenda development, including (a) the methodology that will be used to ensure the engagements remain interactive, case-based, and outcome-oriented including approaches to participant engagement, facilitated discussion, scenario exercises, and practical implementation plannings; and (b) how content will be tailored to participants with varying levels of prior familiarity with research security, supply chain resilience, or institutional risk management concepts.
  - List of recent experience in designing, developing, and delivering customized research security training; supporting institutional governance, due diligence, compliance, or supply chain resilience efforts; working with university or research institution engagement in research security, due diligence, institutional governance, compliance, or supply chain resilience; and work in Central, Eastern, or Southeast Europe (preferred).
- Sample agenda, training materials, facilitation approach, or implementation tools from comparable prior engagements (sanitized/redacted versions acceptable).
- 10-page limit excluding CVs and cost proposals.
- **Cost Proposal in USD**
  - NOTE: Applicants are required to submit their cost proposal using the budget template provided below. Applicants may add additional rows or sub-categories as needed to include travel costs, cost-sharing, leveraged resources, in-kind contributions, or any other items required to fully represent their technical and cost approach. All additions should be clearly labeled.
  - **Travel Cost Proposal:** If travel is required under the proposed Scope of Work, the Applicant must include a detailed travel budget that reflects the nature of the proposed technical approach and implementation plan. Travel costs must be reasonable, necessary, and directly allocable to the performance of the project. The travel budget must, at a minimum, include: number of travelers, origin and destination, estimated airfare (economy/coach class only unless otherwise justified), lodging costs, meals & incidental expenses (M&IE), ground transportation, any visa or required travel documentation costs.
    - All proposed travel costs must be prepared in accordance with applicable Federal Travel Regulations (FTR) and U.S. General Services Administration (GSA) per diem rates, as applicable to the travel location. Lodging and M&IE rates shall not exceed the allowable federal per diem rates unless specifically justified and approved in writing.
    - In addition, all air travel funded under this award must comply with the Fly America Act (49 U.S.C. § 40118). Applicants must budget for U.S. flag air carriers unless a documented exception applies under the Fly America Act or applicable Open Skies Agreement.
    - Failure to provide a detailed and compliant travel budget may result in the cost proposal being deemed non-responsive.
- 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

Task / Deliverable	Proposed Number of Hours	Hourly Rate (USD)	Total (USD)
(Task 1) Program Design and Agenda Development			

(Task 2) Development of Program Materials			
(Task 3) Program Delivery			
(Task 4) Communication and Reporting with CRDF Global			
Travel Expenses (include detailed travel budget in separate table)			
	Total (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/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 will select the contractor who provides the best value in terms of overall price and experience.

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, innovation, 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. CRDF Global also reserves the right to select multiple proposals and/or SMEs and combine or assign complementary roles among selected offerors to achieve the best overall technical approach and value in support of the activity.

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

Evaluation Criteria	Weight (%)	Subfactors
1. Technical Approach	60%	- Understanding of the requirements - Feasibility of the approach - Alignment with project goals
2. Price/Cost	15%	- Overall cost compared to market rates - Cost realism - Price structure -In-kind contributions or cost-share offered
3. Key Personnel and Qualifications	15%	- Relevant experience of personnel - Availability and commitment to the project
4. Past Performance	10%	- Relevance of past projects - Performance ratings or assessments

Procurement Timetable:
This procurement process is intended to follow the timeline below:

Activity	Date
1. Request for Proposal (RFP) Issued	June 5, 2026

2. Deadline for Questions & Inquiries	June 12.2026
3. RFP Questions & Answers Released	June 19, 2026
4. Proposal Submission Deadline	June 26, 2026, 17:00 PM Eastern Standard Time
5. Anticipated Contract Issuance	July 10-24, 2026

Submission:
Proposals should be submitted to procurement@crdfglobal.org & akelkar@crdfglobal.org, no later than ***17:00 Eastern Standard Time June 26th, 2026***. Proposals should be submitted as electronic documents in **PDF, Word or Excel format** and **please add "RFP Response – Balkans Research and Supply Chain Security" to the subject line.**

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 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.