CRDF GLOBAL

Seeking a Subject Matter Expert (SME) for the Design and Development of the Research Security Toolkit: Risk Assessment Guide, Program Starter Kit, and Model Template and Workflow Library

[REQ26-0594] REQUEST FOR PROPOSAL

Deadline: August 21, 2026 at 23:59 Eastern Standard Time

Summary:

CRDF Global, in support of the United States Department of State Bureau of Arms Control and Nonproliferation (ACN) Office of Cooperative Threat Reduction (CTR), seeks qualified subject matter expert(s) to design and develop three complementary components of the Research Security Toolkit under a single solicitation: a Research Security Risk Assessment Guide; a Research Security Program Starter Kit; and a Model Template and Workflow Library. All components will be authored in English, designed to be readily translated and localized, and released as freely adaptable resources for the global research security community. CRDF Global may select one or more offerors and may assign complementary roles across selected partners to develop the components.

Scope:

This solicitation covers three tools: (1) the Research Security Risk Assessment Guide, and (2) the Research Security Program Starter Kit and (3) Model Template and Workflow Library, which are to be developed together as one coherent, cross-referenced tool. Experts are welcome to apply to develop one, multiple, or all three tools. A proposal may address part or all of the scope, provided it fully covers at least one complete tool. Respondents are also expected to provide their own design for tools outlined in the scope, while examples are provided, as well as details on potential inclusions, ultimately your expertise is being solicited to design and develop these tools.

Research Security Risk Assessment Guide. The selected contractor will develop an actionable, facilitated guide that helps an office identify, rate, and respond to research security risks. The methodology should be grounded primarily in risk assessment approaches currently in practice at universities and research institutions, drawing on existing academic risk review frameworks such as the NC State University Research Security Risk Matrix, Texas A&M Conflict-of-Interest Review process, Stanford University's Information Security Plans, and other academic system risk review and assessment methodologies to ensure tailoring to an academic environment. Utilizing government and public sector risk review tools such as the National Science Foundation's FRAME tool, the Department of War's Decision Matrix, and the Government of the Netherlands' Quickscan tool as reference points rather than as the primary basis. CRDF Global's preference is a facilitated guide: a resource that walks an office through a structured risk assessment process without being prescriptive, and that supports adaptation to local law, institutional type, and regional context. The specific format and composition are open, and recommending both is part of what is being solicited. The guide will be usable by lower-capacity institutions with minimal training and limited specialist staff, as well as by institutions with mature research security programs, and will produce a clear, documentable output, at minimum a risk rating, the rationale for that rating, and recommended controls or next steps, structured so that it can be documented, recorded, and audited.

Program Starter Kit and Template and Workflow Library. The selected contractor will develop two complementary resources that help research security programs worldwide establish and operate a research security program. The Starter Kit will provide foundational education and step-by-step guidance for standing up a program from a low or nonexistent baseline, covering governance, roles and responsibilities, core policies, foundational processes, and common scenarios, and will be accessible to non-specialist audiences. The Model Template and Workflow Library will provide a curated set of adaptable models and the workflows that place them in context, which could include Technology Control Plans (TCPs), collaboration-

risk review templates, risk management plans, model non-disclosure agreements, information security plans, due diligence processes and checklists, and any similar foundational and advanced research security artifact. The Starter Kit will direct users to the corresponding templates and workflows in the Library at each relevant step, and the Library's templates will, where relevant, accommodate outputs of, and feed into, the toolkit's risk assessment guide and case management tool. The specific formats of the Starter Kit and Library are open and respondents are encouraged to propose recommended formats, inclusions, or other artifacts not outlined within this solicitation.

All components are designed to read and function as part of one coherent toolkit. Formats are open to proposal, oriented toward accessible, self-guided use, and every component will be modular so that regions and institutions can tailor it, adaptable to different regional, legal, and institutional contexts, and authored to be translation-ready. CRDF Global will arrange translation of finalized materials separately; the contractor is not responsible for translation but will design all deliverables to be translated and localized without redesign.

Period of Performance:

Agreement Execution Date through December 31, 2026.

Ownership, Use, and Licensing of Materials:

Ownership of work product. All guides, templates, workflows, training materials, and other materials produced under the resulting agreement are the exclusive property of CRDF Global and/or the funding agency. The successful offeror assigns to CRDF Global all right, title, and interest, including all intellectual property rights, in the deliverables, sufficient to allow CRDF Global to freely release, adapt, translate, and redistribute the toolkit components to the global research security community as described in the Scope.

1. **Third-party and licensed content.** Any third-party frameworks, templates, or content referenced, adapted, or incorporated (for example, existing academic risk matrices, government tools, or model agreements) must be disclosed, and used only under licenses or permissions compatible with CRDF Global's intended free, adaptable release of the toolkit. Content that cannot be freely redistributed or adapted on an open, non-proprietary basis may not be incorporated without CRDF Global's prior written approval.
2. **Confidentiality of pilot and institutional data.** Any institutional information, feedback, or data the contractor accesses or collects in the course of piloting, testing, or validating the Guide, Starter Kit, or Library shall be treated as confidential, used solely to perform the resulting agreement, and not retained, copied, or disclosed beyond what is necessary for that purpose.

Task One: Research Security Risk Assessment Guide

Objective: Develop an actionable, facilitated risk assessment **guide**, grounded primarily in risk assessment methods currently used at universities and research institutions, suited to institutions of any capacity level, and finalize it for release within the Research Security Toolkit. Provide user instructions for implementation of the guide, and framework via recorded trainings, user guides, or other instructional methods.

Example Activities include:

- Coordinate with CRDF Global to define the guide’s objectives, intended users, and success criteria.
- Review risk assessment practices currently in use at universities and research institutions and synthesize it alongside existing frameworks (such as NSF's FRAME tool, the Department of War's Decision Matrix, and the Government of the Netherlands' Quickscan tool) used as reference points, to identify the core elements suitable for the guide.

- Recommend and justify the guide's format, consistent with the facilitated, non-prescriptive, and adaptable design intent described in the Scope, and confirm it with CRDF Global before full development.
- Develop the guide using plain language, clear step-by-step guidance, and minimal jargon; build it to be modular and adaptable across regional, legal, and institutional contexts; and design its output to produce, at minimum, a risk rating, the rationale, and recommended controls or next steps, structured to ensure consistency, repeatability, and standardization.
- Develop supporting facilitation materials, such as a short user or facilitator guide, a recorded training module on tool use, and at least one worked example.
- Pilot the guide with a small set of representative institutions spanning different capacity levels, collect structured feedback on usability and output quality, and revise the guide to resolve identified issues prior to finalization.
- Incorporate CRDF Global and pilot or expert feedback, document sources and adaptations with attributions, and finalize the guide in editable source formats.

Potential inclusions (illustrative and non-exhaustive; the selected expert is expected to recommend the final composition):

- A simple method for distinguishing serious risks from minor, low-priority ones.
- A short questionnaire covering the top risk areas, such as data security, foreign funding, foreign affiliations, dual-use research, and talent programs.
- An accessible low-, medium-, and high-risk rating scale.
- Sample cases showing how to apply the guide.
- Guidance on when a quick check is sufficient versus when to escalate for deeper review.
- A condensed one-page quick-check version for smaller offices.

Task 1 Deliverables:

- Format recommendation and rationale, with a mapping to the source frameworks the guide draws upon, delivered with the prototype.
- Prototype (end of September), iteration incorporating feedback (end of October), and final guide with user or facilitator guide, recorded training module, worked example, and source documentation (end of November).
- Pilot validation summary documenting the institutions or reviewers consulted, the issues identified, and how feedback was incorporated prior to finalization.

Task Two: Research Security Program Starter Kit

Objective: Develop a Starter Kit that provides foundational education and step-by-step guidance for standing up a research security program from a low or nonexistent baseline, accessible to non-specialist audiences.

Example Activities include:

- Coordinate with CRDF Global to define the Kit's objectives, intended users, and scope, and recommend and justify the format.
- Develop or source foundational, non-technical education on core research security concepts and why they matter.
- Develop step-by-step guidance covering governance, roles and responsibilities, core policies, foundational processes, and common scenarios a new program will encounter.
- Build in cross-references that direct users to the corresponding templates and workflows in the Library (Task Three) at each relevant step.
- Design the Kit to be usable by lower-capacity institutions, adaptable across contexts, and translation-ready.
- Pilot the Starter Kit with a small set of representative institutions across capacity levels and incorporate structured feedback before finalizing.

Potential inclusions (illustrative and non-exhaustive; the selected expert is expected to recommend the final composition):

- A quick self-assessment questionnaire for an institution to gauge where it currently stands and to measure progress over time.
- A sample mandate and job description for a Research Security Officer or lead. In CRDF Global's survey, the presence of a designated lead or office was the strongest predictor of program success.
- A model policy or standard operating procedure that an institution can adopt and edit.
- Governance model options describing a few ways to structure the function, from a coordinated research, legal, and commercial model to a simpler single-lead model, so institutions can choose what fits their size.
- An implementation roadmap sequencing what to do first, second, and third when standing up the function.
- Tiered review thresholds distinguishing situations that need a quick check from those that warrant a deeper review.
- A basic self-audit checklist for periodic review, since most surveyed institutions have no regular way to check their own decisions.
- A curated list of existing free training modules, from NSF and others, to point staff to rather than building new training.

Task 2 Deliverables:

- Prototype: first working version of the Starter Kit, with format rationale (end of September).
- Iteration: revised version incorporating CRDF Global and pilot or expert feedback (end of October).
- Pilot validation summary documenting the institutions or reviewers consulted and how their feedback was incorporated.

Task Three: Model Template and Workflow Library

Objective: Develop a curated library of adaptable model templates and the workflows that place them in context, editable and annotated for tailoring to institutional, regional, and legal context. Provide user instructions for implementation of the templates, and workflows via recorded trainings, user guides, or other instructional methods.

Example Activities include:

- Develop and/or source the model templates and workflows that make up the Library (see potential inclusions below), and propose additional templates, processes, or workflows to be included.
- Develop workflows showing how each template fits into a research security process.
- Annotate each template for tailoring to institutional, regional, and legal context, and design each to be adaptable and translation-ready.
- Where relevant, design templates to accommodate outputs and inputs to the toolkit's risk assessment guide and case management tool, for example enabling a Technology Control Plan or due diligence checklist to reference a documented risk assessment outcome.
- Recommend appropriate guidance for institutions to review model legal templates, such as non-disclosure agreements, with their own counsel before use.
- Pilot the Library’s templates and workflows with a small set of representative institutions and incorporate feedback before finalizing.

Potential inclusions (illustrative and non-exhaustive; the selected expert is expected to recommend the final composition):

- Technology Control Plan template.
- Collaboration-risk review templates for evaluating a potential foreign university, company, or researcher partnership.
- Model non-disclosure agreements.

- Disclosure and red-flag checklists for screening visiting scholars, funders, and partner organizations.
- A one-page risk matrix for quickly sorting a partnership or project into low, medium, or high risk.
- Conflict-of-interest review templates for disclosing outside relationships, funding, or affiliations, which could be modeled on an existing process such as Texas A&M's.
- Visiting scholar and delegation disclosure templates.
- Gift, grant, and contract disclosure templates for reviewing incoming funding or in-kind support before acceptance.
- A data security translation guide and a decision documentation template.
- Additional items the expert may propose, such as conference screening and foreign travel disclosure templates.

Task 3 Deliverables:

- Prototype: first working version of the Library, including the initial template set and associated workflows (end of September).
- Iteration: revised version incorporating CRDF Global and pilot or expert feedback (end of October).
- Pilot validation summary documenting the institutions or reviewers consulted and how their feedback was incorporated.

Task Four: Integration, Finalization, and Coordination with CRDF Global

Objective: Finalize the Research Security Risk Assessment Guide, Starter Kit, and the Library as one coherent, cross-referenced set, and coordinate with CRDF Global throughout the period of performance.

Example Activities include:

- Verify and finalize the cross-referencing between the Starter Kit and the Library so the two function as separate but mutually supportive aspects of the full toolkit.
- Ensure consistent look, structure, and terminology across the workstreams, and finalize both deliverables in editable source formats, with sources and attributions documented.
- Participate in coordination calls with CRDF Global and, as relevant, the funder and other experts contributing to the toolkit, and provide regular progress updates across all components.
- Provide a brief After Action Report of the work, including any lessons learned and recommendations for future toolkit development.
- Develop a maintenance and update guide enabling CRDF Global staff to independently revise, adapt, and extend the Starter Kit and Library after project completion, and conduct at least one dedicated knowledge-transfer session with CRDF Global staff distinct from the general coordination calls.

Task 4 Deliverables:

- Final version of the Starter Kit and the Library, delivered together as two separate but mutually supportive tools (end of November).
- Up to 10 one-hour virtual calls with CRDF Global, the funder, and/or other members of the toolkit team.
- Maintenance and update guide, and at least one dedicated knowledge-transfer session with CRDF Global staff, delivered alongside the final materials.
- After Action Report, delivered within 7 business days of final delivery.

Anticipated Performance Schedule:

Task	Deliverables	Expected Delivery Date
1	Research Security Risk Assessment Guide (prototype end of September; iteration end of October; final end of November)	September - November 2026
2	Research Security Program Starter Kit (prototype end of September; iteration end of October; final end of November)	September - October 2026

Task	Deliverables	Expected Delivery Date
3	Model Template and Workflow Library (prototype end of September; iteration end of October; final end of November)	September - October 2026
4	Integration, Finalization, and Coordination with CRDF Global	Throughout Period of Performance

Contractor Requirements:

- Demonstrated expertise in research security, research integrity, research security policy, compliance, or program management, or a closely related field.
- Familiarity with how universities and research institutions currently conduct research security risk assessments, and with existing frameworks and benchmarks (e.g., NSF FRAME, NSPM-33, NIST, the Australian University Foreign Interference Taskforce, and the UK Trusted Research guidelines), and the ability to adapt them for a global audience.
- Experience with export control and Technology Control Plans, and familiarity with model agreements such as non-disclosure agreements and with due diligence practice.
- Experience with research security governance, including screening and due diligence, funding and investment screening, technology transfer risk, and related considerations in academic research environments.
    - Preference for experience leading or working within an academic research security environment. To include experience developing internal tools, workflows, SOPs, templates, and other relevant research security artifacts.
- Demonstrated ability to translate technical or specialist content into plain-language, practitioner-facing tools and guidance for users with varying levels of experience.
- Instructional design or facilitation experience, and ideally international capacity-building experience relevant to a global audience.
- Ability and willingness to participate as part of a team of experts contributing to the Research Security Toolkit.
- Willingness to accommodate reasonable changes or adjustments to content or delivery as directed by CRDF Global or the funder.
- 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:

Offerors may propose to build one, two, or all three tools. A proposal that addresses a single tool should complete the technical approach and cost proposal only for the tasks and deliverables associated with that tool, including only the corresponding rows of the cost table below.

Each proposal must include:

- **Proposed Technical Approach and Project Team**
    - Detailed description of the services offered in correlation with the RFP scope and tasks, including your vision for the completed components and individual deliverables. Specificity is greatly encouraged.
    - Technical approach, including CVs and/or bios for the proposed expert or expert team.
    - The technical approach must clearly outline, as applicable to the tool(s) proposed: the recommended format for each proposed component and the rationale; the methodology for developing a risk assessment guide
    - grounded in methods currently used at universities, with a standardized, repeatable, and consistent output; the approach to developing accessible Starter Kit guidance and

adaptable Library templates and workflows for institutions of varying capacity; the approach to cross-referencing the Starter Kit and Library into one coherent set; and the approach to modularity, localization, and translation-readiness.
    - List of recent, relevant experience, including developing research security tools, guidance, program frameworks, or model templates, adapting frameworks for practitioner use, and capacity-building work with institutions of varying maturity. Applicable references and past performance should be clearly included.
- **10-page limit excluding CVs and cost proposals**
- **Cost Proposal in USD**
    - **NOTE:** Applicants are required to submit their cost proposal using the provided budget template or a template following the same structure. Applicants may add additional rows or subcategories as needed to include 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.

A separate, complete budget table must be submitted for each component the bidder is proposing on. Do not combine tasks from different components into a single table.

Only submit the budget table(s) that correspond to the component(s) you are proposing on. Do not submit blank tables for components you are not bidding on.

Budget Table 1 — Research Security Risk Assessment Guide

Submit only if proposing on this component.

Task / Deliverable	**Number of People**	**Level of Effort (LOE)**	**Hourly Rate (USD)**	**Total (USD)**
Research Security Risk Assessment Guide				
Integration, Finalization, and Coordination				
Subtotal (USD)				

Budget Table 2 — Research Security Program Starter Kit

Submit only if proposing on this component.

Task / Deliverable	**Number of People**	**Level of Effort (LOE)**	**Hourly Rate (USD)**	**Total (USD)**
Research Security Program Starter Kit				
Integration, Finalization, and Coordination				
Subtotal (USD)				

Budget Table 3 — Model Template and Workflow Library

Submit only if proposing on this component.

Task / Deliverable	**Number of People**	**Level of Effort (LOE)**	**Hourly Rate (USD)**	**Total (USD)**
Model Template and Workflow Library				
Integration, Finalization, and Coordination				
Subtotal (USD)				

Grand Total

For bidders proposing on multiple components, provide the sum of all submitted table subtotals below.

Task / Deliverable	Number of People	Level of Effort (LOE)	Hourly Rate (USD)	Total (USD)
Task One: Research Security Risk Assessment Guide				
Task Two: Research Security Program Starter Kit				
Task Three: Model Template and Workflow Library				
Task Four: Integration, Finalization, and Coordination				
Grand 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 technical 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 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 below.

Evaluation Criteria	Weight (%)	Subfactors
1. Technical Approach	60%	Understanding of the requirements; feasibility of the approach; alignment with project goals; proposed development timeline and justification for timeline
2. Past Performance / Qualifications	30%	Relevance of past projects; performance ratings or assessments; relevant experience of personnel; demonstration of expertise; availability and commitment to the project
3. Price / Cost	10%	Overall cost compared to market rates; cost realism; price structure; cost share

Timetable:

The procurement process is intended to follow the timeline below.

Activity	Date
Request for Proposal (RFP) Issued	August 3, 2026
Deadline for Questions and Answers	August 12, 2026
RFP Questions and Answers Released	August 13, 2026
Proposal Submission Deadline	August 21, 2026
Anticipated Contract Issuance	By September 30,2026

Questions and Answers:

Interested parties may submit questions regarding this RFP to Josh Carpenter (jcarpenter@crdfglobal.org) and Salman Al-Darbisi (saldarbisi@crdfglobal.org). Questions will be accepted through 11:59 PM Eastern Standard Time on August 12, 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 Josh Carpenter (jcarpenter@crdfglobal.org) and Salman Al-Darbisi (saldarbisi@crdfglobal.org), no later than **23:59 Eastern Standard Time on August 21, 2026**. Proposals should be submitted as electronic documents in PDF, Word, PowerPoint, 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 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.

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 opportunity to all qualified individuals and does not discriminate on the basis of age, race, color, religion, sex, sexual orientation, gender identity, national origin, protected veteran status, or disability. CRDF Global is committed to fostering a professional and collaborative environment grounded in mutual respect, fairness, and open dialogue. We recognize the inherent dignity and value of all individuals and strive to maintain a workplace and program environment that respects a wide range of backgrounds, traditions, 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.

Ownership of Deliverables; Intellectual Property. All deliverables, materials, and work product developed under any resulting Agreement, including the Research Security Risk Assessment Guide, Program Starter Kit, and Model Template and Workflow Library and all associated source files, shall be owned by CRDF Global and made available for release as freely adaptable resources for the global research security community, consistent with the funding source's requirements. Where a proposal's approach or deliverables incorporate or adapt pre-existing third-party materials, frameworks, or templates, the offeror shall identify such materials, provide appropriate attribution, and confirm that the offeror has the necessary rights to permit CRDF Global's intended use, adaptation, translation, and redistribution of the deliverables. Offerors should describe their proposed approach to ownership, licensing, and attribution as part of their technical proposal.

.