REQUEST FOR PROPOSAL
No. HPI20260510US
Global Security Project

RFP Release Date:	May 28, 2026
Performance Period:	6 Months to One Year
Proposal Submission Deadline:	June 26, 2026
Question/ Inquiry Submission Deadline:	June 15, 2026
Electronic submission to the attention of:	**Arelys Morazan**
Electronic submission:	**RFP@HEIFER.ORG**
Contact information for inquiries about this RFP:	RFP@HEIFER.ORG **Subject Line: RFP Submission-Global Security Project at Heifer**

I. General Information

Heifer International (HI) was founded on a simple belief: when people have the means to feed themselves, they will not go hungry again. Since 1944, Heifer has helped more than 59.8 million smallholder farming households around the world. We currently operate in 19 countries across Africa, Asia, and the Americas, including the U.S., working with small-scale farmers to achieve living incomes and ensuring that they have adequate food, housing, and other essential resources to lead decent and dignified lives. As a development organization we do not operate in active armed conflict zones, many of our operating environments may present varying levels of security risk related to political instability, social unrest, criminal activity, remote operations, and other contextual security considerations.

Heifer's work advances farmer-centered solutions that foster more productive, inclusive, and sustainable food systems and more resilient rural communities. We work with farming communities to establish strong social capital, provide technical and business training, facilitate new formal market avenues, form strategic partnerships at all levels, leverage third-party investments, and invest in and deploy appropriate and accessible technologies. Heifer's model is locally led, built on close collaboration with communities and key stakeholders to catalyze sustainable, scalable impact.

More information following this link: Home - Heifer International

The terms of reference contains background information, the desired methodology, including objectives, the timeframe for conducting the final evaluation, and a list of deliverables. This document also contains information about the kind of expertise that Heifer seeks in this activity and guidance on how to submit a proposal to conduct the activity.

Heifer anticipates awarding an Independent Contractor Agreement for the Global Security Project at Heifer and make payments based on submission and Heifer's approval of deliverables. The award agreement will include a payment schedule with specific deliverables; all payments require 30 business days processing after approval of deliverables.

II. Purpose

The purpose of this Request for Proposals (RFP) is to identify and engage a qualified consultant, firm, or consortium to support the development of a comprehensive organizational security risk management system for Heifer, a globally distributed organization operating across diverse geographic and operational contexts.

The organization seeks to strengthen its overall security governance, operational resilience, duty of care, crisis preparedness, and risk-informed decision-making capabilities through the development of practical, scalable, and context-sensitive security management systems.

The scope of this assignment is specifically focused on security risks arising from:

- Security-related violence and armed threats
- Kidnapping, detention, and extortion risks
- Social unrest, civil disorder, and political instability
- Organized crime and criminality impacting personnel or operations
- Threats affecting staff safety, movement, facilities, field operations, and partner engagement

This assignment is intended to move beyond the development of isolated policies or compliance-driven procedures. Instead, the organization seeks a partner capable of designing an integrated and functional security management framework that can be operationalized across global, regional, and country level operations.

The selected Consultant/Firm will support the organization in:

- Establishing clear security governance and accountability structures
- Strengthening organizational preparedness and crisis management capacity
- Improving threat identification, security risk analysis, and operational decision-making processes
- Developing scalable operational security standards and mitigation measures
- Enhancing security monitoring, reporting, and information management systems
- Building practical and sustainable organizational security capabilities appropriate for decentralized and networked operating environments

Some regional and country level operations have already developed security-related tools, procedures, assessments, protocols, and operational practices tailored to their local contexts.

As part of the scope of work, the selected Consultant/Firm will be expected to conduct a structured review of existing security-related materials across the organization. They shall assess the applicability, effectiveness, consistency, and scalability of these existing materials and identify gaps, overlaps, inconsistencies, or areas requiring alignment. A key objective of this engagement is to ensure that the global security management framework builds upon and integrates relevant existing practices,

assessments, etc. wherever appropriate, rather than replacing or duplicating effective work already completed across the organization.

We are looking to reduce unnecessary duplication of processes or documentation, harmonize inconsistent approaches where needed and identify areas where additional capability, standardization, or governance is required

The project should result in an adaptable and organization-wide security management that:

- supports safe and sustainable operations,
- strengthens organizational resilience,
- enables informed operational decision-making,
- and improves the organization's ability to anticipate, respond to, and recover from security-related risks and incidents.

The organization expects the engagement to incorporate international best practices in security risk management while remaining operationally realistic, resource-conscious, and appropriate to the organization's mission, structure, and operating model.

a) Specific Objectives:

1: Security Risk Assessment & Threat Analysis

Establish a standardized organizational approach for identifying, analyzing, prioritizing, and monitoring security threats, vulnerabilities, and operational security risks across all areas of operation.

2 — Security Governance & Operational Decision-Making

Establish clear governance structures, accountability mechanisms, escalation pathways, and operational decision-making processes for security risk management across all levels of the organization.

3 — Incident, Crisis & Emergency Management

Strengthen the organization's preparedness and response capacity for security incidents, emergencies, and crises affecting personnel, operations, partners, or assets.

4 — Operational Security Controls & Mitigation

Establish practical operational security standards, mitigation measures, and protective systems that reduce organizational exposure and support safe program implementation.

5 — Security Intelligence, Monitoring & Reporting Systems

Improve the organization's ability to collect, validate, analyze, and communicate security-related information to support informed operational and strategic decision-making.

6 — Organizational Preparedness & Security Capacity

Strengthen security awareness, preparedness, and operational capability through training, guidance, and capacity-building systems.

b) Scope of work

The consultant will lead the development of organizational security frameworks, methodologies, tools, and recommendations, informed by consultation with relevant stakeholders across global, regional, and country operations to ensure practicality, contextual applicability, and organizational adoption

1 — Security Risk Assessment & Threat Analysis
The Consultant/Firm will:

- Conduct an organizational security risk and vulnerability assessment
- Identify major operational, geographic, personnel, and program-related security threats
- Develop security risk mapping methodologies that are global, but application can be contextualized by country
- Design organizational security risk assessment tools and templates
- Develop standardized security risk scoring and prioritization methodologies
- Define organizational security risk tolerance and escalation thresholds
- Assess security exposure related to travel, remote operations, partnerships, facilities, events, and field activities
- Develop systems for ongoing security threat monitoring and strategic security risk reporting
- Provide recommendations for leadership-level security risk visibility and reporting

2 — Security Governance & Operational Decision-Making in matters of security
The Consultant/Firm will:

- Define multi-level organizational security governance models and reporting lines at global/regional/country levels
- Clarify security roles and responsibilities across HQ, regional, and country levels
- Develop operational decision-making frameworks for varying security risk levels
- Establish escalation pathways and security incident notification protocols
- Develop operational security thresholds for movement restrictions, program opening, continuation, suspension, or closure
- Create risk-informed approval and accountability mechanisms
- Recommend security governance oversight and coordination structures

3 — Incident, Crisis & Emergency Management
The Consultant/Firm will:

- Develop organizational incident and crisis management frameworks
- Establish emergency response procedures and escalation systems
- Define crisis coordination structures and leadership responsibilities
- Develop serious incident response guidance, including:
    - medical emergencies,
    - kidnappings,
    - civil unrest,
    - political instability,
    - and operational disruptions
- Develop crisis communications protocols, including backup communication procedures

- Establish incident reporting and tracking procedures
- Develop medical evacuation and trauma response guidance
- Recommend preparedness and contingency planning measures

4 — Operational Security Controls & Mitigation Measures

The Consultant/Firm will:

- Develop minimum operational security standards
- Assess travel, movement, transport, and field operation security risks
- Develop journey management and travel safety procedures
- Develop security mitigation and protective measures appropriate to varying risk environments
- Assess remote operations and decentralized implementation security risks (if applicable)
- Develop security guidance related to:
    - transport safety,
    - communications,
    - Cyber-related vulnerabilities that directly affect personnel safety, duty of care, or security incident management
    - events,
    - field activities,
    - and partner engagement
- Recommend practical and scalable operational safeguards
- Support integration of community acceptance and contextual mitigation approaches where appropriate

5 — Security Intelligence, Monitoring & Reporting Systems

The Consultant/Firm will:

- Assess existing Heifer security information management tools, processes and reporting mechanisms and identify gaps, overlaps, and opportunities for integration across the organization
- Develop threat monitoring and intelligence methodologies
- Recommend tools and platforms for security monitoring and reporting
- Develop reporting templates, dashboards, and briefing mechanisms
- Establish standards for validating and verifying security-related information
- Develop security guidance related to:
    - open-source intelligence,
    - social media monitoring,
    - misinformation/disinformation verification,
    - and AI-generated information assessment
- Recommend centralized and decentralized security information-sharing mechanisms
- Support development of strategic security risk reporting systems

6 — Organizational Preparedness & Security Capacity

The Consultant/Firm will:

- Develop risk-based security training frameworks
- Assess organizational preparedness and staff security awareness needs

- Recommend security training requirements by operational risk level
- Develop security onboarding and security briefing guidance
- Provide recommendations for hostile environment awareness training (HEAT) and specialized training needs as needed
- Develop security preparedness exercises and simulation recommendations
- Support security capacity-building approaches for leadership and staff
- Recommend systems for sustaining organizational security awareness and operational readiness

c) Deliverables:

Deliverable	Description
Inception Report and Workplan	A document outlining the consultant's understanding of the assignment, proposed methodology, implementation approach, stakeholder engagement process, timeline, milestones, assumptions, and project management structure.
Organizational Security Risk Assessment	A comprehensive assessment of the organization's current security environment, including operational security risks, security gaps, organizational security exposure, and existing security risk management practices across global operations.
Security Threat & Vulnerability Analysis	An analysis identifying priority threats, contextual security risks, operational vulnerabilities, and exposure factors affecting safety and security of personnel, programs, partners, travel, facilities, and field operations, specific for each Heifer country program.
Global Security Risk Management Framework	A comprehensive security risk framework establishing the organization's overall approach, principles, systems, standards, and processes for managing security risks across all operational contexts.
Security Governance Framework	A framework defining security governance structures, reporting lines, authority levels, accountability mechanisms, oversight responsibilities, and coordination processes across Heifer International's global network, including regional, and country operations.
Operational Security Decision-Making & Escalation Framework	A structured framework outlining operational decision thresholds, escalation pathways, approval processes, movement restrictions, evacuation triggers, and procedures for operational continuation, suspension, or closure.
Security Incident & Crisis Management Framework	A framework outlining organizational procedures and coordination structures for responding to security incidents, emergencies, and crises, including escalation workflows, crisis

Deliverable	Description
	communications, serious incident response, and emergency coordination mechanisms.
Operational Security Standards & Mitigation Guidance	A set of minimum operational security standards and practical mitigation measures designed to reduce organizational exposure and strengthen personnel safety across varying operational environments.
Travel & Journey Management Procedures	Procedures and guidance related to staff travel, field movement, transport safety, journey management, remote operations, and travel risk mitigation measures.
Medical & Emergency Response Guidance	Guidance related to medical emergency preparedness, trauma response, medical evacuation planning, first aid standards, emergency coordination procedures, and access to medical support services.
Security Intelligence & Reporting Recommendations	Recommendations for security monitoring systems, threat intelligence methodologies, reporting structures, information-sharing mechanisms, and tools to support operational and strategic security decision-making.
Security Risk Monitoring & Reporting Templates	Standardized templates and tools for country security risk summaries, incident reporting, threat monitoring, operational security risk tracking, leadership briefings, and organization-wide security risk visibility.
Security Training & Preparedness Framework	A framework outlining organizational security training requirements, staff awareness systems, onboarding procedures, preparedness measures, hostile environment awareness recommendations, and ongoing capacity-building needs.
Implementation Roadmap & Prioritized Action Plan	A phased implementation plan outlining recommended sequencing, timelines, priorities, piloting/testing, resourcing considerations, and organizational adoption strategies for implementing the security framework and associated security management systems.
Final Report and Executive Presentation	A consolidated final report summarizing key findings, recommendations, frameworks, tools, implementation priorities, and strategic considerations, accompanied by an executive-level presentation for leadership and governance stakeholders.

The Consultant/Firm shall ensure that all recommendations and deliverables:

- Are practical, scalable, and appropriate for the diverse geographic, operational, and security environments in which the organization operates
- Reflect international security management best practices
- Support organizational duty of care obligations
- Are scalable across varying country contexts and security risk levels
- Are practical, implementable, and resource-conscious
- Incorporate considerations related to inclusion, accessibility, and local operational realities
- Strengthen organizational resilience and continuity

Methodology Expectations

The Consultant/Firm is expected to use a collaborative and participatory approach that may include:

- Stakeholder interviews
- Workshops and consultations
- Document and policy reviews
- Organizational assessments
- Comparative benchmarking
- Security Risk analysis methodologies
- Validation sessions with country teams

The proposed methodology should clearly describe:

- Approach
- Phasing and implementation sequencing
- Stakeholder engagement
- Deliverable development process
- Pilot testing, validation, and refinement approach
- Quality assurance mechanisms
- Assumptions and dependencies

d) Relationship and Responsibilities

The vendor will keep Heifer informed of their progress. During the project, the vendor may seek and receive additional advice or guidance if needed.

Reporting & Coordination

The Consultant/Firm will be expected to:

- Participate in regular coordination meetings
- Provide periodic progress updates
- Facilitate stakeholder consultations
- Present draft findings and recommendations
- Incorporate organizational feedback into final deliverables

The organization expects a collaborative process that supports long-term organizational adoption and operationalization of the resulting security systems.

III. Required Expertise and Qualifications

The organization seeks proposals from qualified consultants, firms, or consortiums with demonstrated expertise in organizational security risk management, crisis preparedness, and operational security systems for international NGOs.

The selected Consultant/Firm should demonstrate a combination of strategic, operational, and technical expertise relevant to the scope of the assignment.

Required Organizational Expertise

The Consultant/Firm should demonstrate:

- Proven experience designing and implementing organizational security risk management systems for international organizations, particularly INGOs.
- Demonstrated experience supporting organizations operating in complex, fragile, high-risk, or politically sensitive environments
- Experience developing:
    - security governance frameworks,
    - crisis management systems,
    - operational security standards,
    - threat analysis methodologies,
    - and duty of care systems
- Strong understanding of international security management standards and best practices
- Demonstrated ability to operationalize security frameworks beyond policy development into practical implementation systems
- Experience facilitating multi-stakeholder consultations, workshops, and organizational change processes
- Experience working across multiple geographic regions and cultural contexts
- Capacity to provide practical, scalable, and resource-conscious recommendations appropriate for varying operational environments

Required Technical Expertise-The proposed team should collectively demonstrate expertise in the following areas:

Security Risk Management

- Organizational security risk assessment
- Threat and vulnerability analysis
- Security risk matrix and risk scoring methodologies
- Operational security risk management systems
- Security governance and accountability structures

Crisis & Incident Management

- Crisis management systems and coordination structures
- Serious incident response
- Emergency preparedness and response
- Evacuation planning and operational continuity
- Crisis communications and escalation systems

Operational Security

- Travel security and journey management
- Field and remote operations security
- Protective measures and mitigation planning
- Partner and third-party security risk management
- Safety protocols and operational standards

Security Intelligence & Information Management

- Threat monitoring and intelligence methodologies
- Security reporting systems
- Open-source intelligence (OSINT)
- Information verification and validation
- Misinformation/disinformation security risk management

Organizational Security Capacity & Preparedness

- Security training frameworks
- Hostile environment awareness approaches
- Staff preparedness and awareness systems
- Organizational readiness exercises and simulations
- Change management and organizational adoption

Duty of Care & Human-Centered Security

- Duty of care systems and obligations
- Trauma-informed approaches
- Medical emergency preparedness
- Staff well-being considerations in insecure environments

Minimum Qualifications- Key personnel should demonstrate:

- Relevant academic and/or professional qualifications
- Significant professional experience in security management or related fields
- Experience working internationally and across diverse operational contexts
- Strong analytical, facilitation, and communication skills
- Ability to work collaboratively with leadership, operational teams, and local stakeholders

Professional certifications in security management, crisis management, humanitarian security, risk management, or related fields are desirable.

Desired Competencies

The organization will value teams that demonstrate:

- Strategic thinking combined with operational practicality
- Strong contextual judgment and risk analysis capability
- Experience balancing security with operational enablement
- Cultural sensitivity and collaborative engagement approaches
- Ability to develop realistic and implementable systems
- Strong communication and stakeholder facilitation skills
- Adaptability and problem-solving in complex environments

Language Requirements
The Consultant/Firm should demonstrate strong written and verbal communication skills in English. Additional language capabilities relevant to the organization's operational regions may be considered an asset.

References and Past Performance
Consultant/Firm should provide:

- Examples of similar assignments completed
- Relevant client references
- Sample deliverables or case studies where appropriate
- Evidence of successful implementation support for comparable organizations

Preference may be given to Consultant/Firm with demonstrated experience implementing organization-wide security management systems rather than solely producing policy documentation.

IV. Proposal submission requirements:

Interested Consultant/Firm are invited to submit a complete proposal that clearly demonstrates their understanding of the assignment, technical capability, operational experience, and ability to deliver a comprehensive organizational security risk management system aligned with the requirements outlined in this RFP. Proposals should be clear, concise, and sufficiently detailed to allow for a thorough evaluation.

1. Technical Proposal
The Technical Proposal should include the following components:
A. Cover Letter

- Name of the firm/Consultant/Firm
- Primary contact information
- Statement of interest in the assignment
- Confirmation of availability for the proposed timeline
- Confirmation of ability to comply with the requirements of the RFP

B. Organizational Profile and Relevant Experience
A summary describing:

- The organization/firm and areas of specialization
- Relevant experience delivering comparable assignments
- Experience working with INGOs or Global Organizations
- Experience operating in complex or high-risk environments
- Relevant regional or global operational experience
- Preferred capability to operate effectively across the 19 countries in which Heifer maintains operations.

The proposal should include examples of similar projects completed, including:

- Client/organization name
- Scope of assignment
- Geographic coverage
- Services provided
- Project outcomes or results

C. Understanding of the Assignment

A narrative demonstrating:

- Understanding of the organization's needs and operating context
- Understanding of the project objectives and expected outcomes
- Key security risks, considerations, and implementation challenges

D. Technical Approach and Methodology

A detailed description of the proposed methodology, including:

- Overall project approach
- Proposed phases and workstreams
- Assessment methodologies
- Stakeholder engagement approach
- Consultation and facilitation methods
- Security risk analysis methodologies
- Approach to framework development
- Quality assurance measures
- Organizational adoption and implementation considerations

The methodology should clearly explain how the Consultant/Firm will support the development of:

- practical,
- scalable,
- and operationally realistic security systems.

E. Workplan and Timeline

A proposed workplan that includes:

- Project phases
- Major activities
- Deliverables
- Estimated timelines
- Key milestones
- Dependencies and assumptions

The Consultant/Firm should clearly indicate the estimated level of effort required for the assignment.

F. Team Composition and Key Personnel

The proposal should include:

- Proposed team structure
- Roles and responsibilities of team members
- Short biographies/CVs of key personnel
- Relevant technical and operational expertise
- Availability of proposed personnel

The proposal should identify the Team Lead and primary point of contact.

G. Relevant Experience of Key Personnel

The proposal should highlight:

- Security risk management experience
- Crisis and incident management expertise
- Experience in INGO
- Experience in global operational environments

Professional certifications and language capabilities should also be included where relevant.

H. References

Provide at least:

- Three (3) professional references from comparable assignments

References should include:

- Organization name
- Contact person
- Title/role
- Email address and phone number
- Brief description of the assignment

2. Financial Proposal

The Financial Proposal should be submitted separately from the Technical Proposal and should include:

A. Detailed Budget

A detailed budget breakdown including:

- Professional fees/daily rates
- Estimated level of effort
- Administrative or operational costs
- Workshop/facilitation costs (if applicable)
- Taxes and other applicable charges

B. Budget Narrative

A brief explanation describing:

- Budget assumptions
- Basis for cost estimates
- Staffing assumptions
- Any exclusions or dependencies

3. Required Supporting Documentation

Consultant/Firm may also be required to submit:

- Company registration documents
- Proof of insurance coverage
- Organizational policies related to safeguarding, confidentiality, and ethics
- Conflict of interest disclosure
- Data protection and confidentiality procedures
- Relevant certifications or licenses

4. Submission Format

Proposals should:

- Be submitted electronically
- Be written in English
- Clearly separate the Technical and Financial Proposals
- Include all requested documentation
- Follow the structure outlined in this RFP

Late submissions may not be considered.

5. Submission Instructions

Proposals should be submitted electronically to: **rfp@heifer.org**

Subject Line: **"Company Name –Global Security Project"**

Submission Deadline: **Close of Business June 26th**
Questions regarding the RFP may be submitted to: **RFP@heifer.org**
Responses to questions may be shared with all participating Consultant/Firm.

6. Additional Conditions
The organization reserves the right to:

- Request clarifications or additional information
- Conduct interviews or presentations with shortlisted Consultant/Firm
- Request revised proposals
- Negotiate scope, methodology, staffing, or budget
- Reject any or all proposals
- Cancel or modify the RFP process at any stage

Submission of a proposal does not guarantee selection or award of contract.

7. Confidentiality
All information shared as part of this RFP process should be treated as confidential and used solely for the purpose of preparing the proposal.
Consultant/Firm are expected to maintain appropriate confidentiality and data protection standards throughout the procurement process and any subsequent engagement.

V. Selection Criteria

Submitted proposals must clearly demonstrate alignment with the SOW outlined above with appropriate level of details. An agreement will be signed with the Consultant/Firm whose proposal follows the instructions in this RFP. Proposals will be evaluated according to the following criteria:

Proposal evaluation focus	**Percentage**
Technical approach, methodology, and implementation strategy	25%
Team expertise and operational security competencies	25%
Relevance and capability/skill to implement/manage the assignment	20%
Change management, training, and stakeholder engagement approach	10%
Information integrity, ethics, confidentiality, and risk governance	10%
Affordability and value for money	10%
Total	100%

The selection committee will evaluate the technical proposal based upon the criteria listed above and the financial proposal will evaluate the reasonableness of costs and cost-effectiveness in the budget.

VI. Award Process and Contract Mechanism

No.	**Activity**	**Due date**
1	Proposal reception	June 26
2	Selection Committee review	July 6-17
3	Notification of Selection	July 20
4	Agreement negotiation	July 21-24
5	Signing Agreement	Aug 7

Heifer will issue an Independent Contractor Agreement. Once an award is issued, it will include payment schedule with deliverables specified above.

VII. Limitations

This RFP does not represent a commitment to award a contract, to pay any costs incurred in the preparation of a response to this RFP, or to procure or to contract for services or supplies. Heifer reserves the right to fund any or none of the applications submitted and reserves the right to accept or reject in its entirety and absolute discretion any proposal received as a result of the RFP. Intellectual Property

VIII. Contracting Terms and Agreement Requirements

The selected consultant or firm will be engaged under the organization's standard Independent Contractor Agreement.
A template of the Independent Contractor Agreement is included in the RFP package for reference and review by prospective bidders. Submission of a proposal indicates acknowledgement of the organization's intended contractual framework, subject to final negotiation and execution.

IX. Applicable Regulations

Consultant/Firm must be legally registered to operate within Latin America, Africa, Asia and the US, and comply with local applicable legislation, including but not limited to labor law, financial requirements, taxes, etc.

Consultant/Firm will also be required to comply with all applicable international, national, and organizational regulations, standards, and policies relevant to security risk management, duty of care, data protection, safeguarding, and operational compliance for this assignment. This may include, but is not limited to:

- International humanitarian and human rights principles where applicable
- Duty of Care obligations and occupational health and safety standards
- Applicable national security, labor, and operational regulations in countries of implementation
- Data protection and privacy regulations, including GDPR or equivalent standards where applicable
- Confidentiality and secure information handling requirements
- Safeguarding and protection policies, including prevention of sexual exploitation, abuse, and harassment (PSEAH)
- Ethical standards for security risk management and intelligence gathering
- Anti-corruption, anti-bribery, and fraud prevention regulations
- Relevant NGO, INGO, or donor compliance requirements applicable to the organization's operations
- International best practices and recognized standards in security risk management and crisis management

Consultant/Firm should demonstrate their ability to operate in compliance with these standards and describe the internal policies, protocols, and safeguards they maintain to ensure ethical, lawful, and secure implementation of the assignment.