Request for Proposals

Global Security Advisory Services

Issue Date:	**November 19, 2021**
Closing Date for Proposals:	**December 13, 2021**
Closing Time:	**12:00 p.m. Eastern Standard Time (Washington, D.C.)**
Offer Reference Number:	**GLOBAL SECURITY ADVISORY SERVICES RFP-001-2021**

1. Disclaimer

The information contained in this request for proposals (hereinafter referred to as RFP) document is provided to the Offeror(s) by the International Executive Service Corps (IESC).

IESC plans to award one contract as the result of this RFP.

The purpose of this RFP document is to provide Offeror(s) with information to assist them in the preparation of their proposal/s for the services that IESC seeks to source. This RFP document does not claim to contain all the information each Offeror may require. Each Offeror should conduct their own assessment and should check the accuracy, reliability, and completeness of the information in this RFP document, and where necessary obtain independent advice from appropriate sources.

IESC may cancel this RFP and is under no obligation to make an award as a result of this RFP, although IESC fully anticipates doing so. Activities are anticipated to begin in January 2022.

Note that IESC determines proposal notification, award, and start dates, and they are subject to change at IESC's discretion. Any activities under a final agreement are subject to and will be carried out in accordance with the regulations promulgated by IESC under 2 CFR 200 and any other subsequently published rule or regulation governing the program.

IESC may, at its own discretion, but without being under any obligation to do so, update, amend, or supplement the information in this RFP document.

IESC may elect to interview final Offerors in the competitive range.

Interested offerors are responsible for all costs associated with preparation and submission of proposals and will not be reimbursed by IESC.

Any contract resulting from this RFP will be a Time and Materials contract with three base years and up to two option years.

2. Background

IESC is a leading U.S. nonprofit organization that fosters private sector development in the economically developing world. Since 1964, we have delivered lasting solutions that have resulted in more than 1.5 million jobs in 137 countries. We partner with businesses, cooperatives, entrepreneurs, jobseekers, and governments to sustainably build capacity, create jobs, and grow enterprises, sharing proven skills and experience that improve the lives of individuals, families, and communities around the world. Our major funders today are the U.S. Agency for International Development (USAID) and the U.S. Department of Agriculture (USDA), among others. IESC desires to receive proposals from companies (Offerors) to provide strategic and operational support for overall security and risk management for IESC and its offices globally on a part-time basis.

IESC is currently implementing international economic development programs in eight countries, with additional country offices anticipated. IESC programs are primarily under Cooperative Agreements and Contracts with the US Agency for International Development, the U.S. Department of Agriculture, the European Union and the Swiss Development Corporation.

In the past decade, IESC has been operating in high-risk environments and has seen increased risk in lower risk countries with smaller program offices. As a result, IESC has instituted a revised and broader approach to security, requiring a part-time Security Advisor to provide services supported by the additional training and support services a security-focused company offers.

IESC has a commitment to provide duty of care to its staff members. The Offeror and the Security Advisor will ensure that a measured, consistent, but flexible approach to security is applied in their approach to IESC services.

3. Period of Performance

The anticipated period of performance, should the Offeror be selected, will be January 2021 until December 2023 as three base years, with two additional option years to be reviewed annually by agreement of both parties.

4. Scope Statement

The Offeror will provide a mix of organizational capacity building security services and a technical management approach for day-to-day security operations. The Offeror will hire,

guide and support a dedicated Security Advisor for IESC as well as provide additional ad hoc services as needed.

The Security Advisor will provide remote-based security services, with time in the IESC home office as needed. The Security Advisor will serve as a resource to the IESC Executive Security Management Team and home office staff members, with primary support provided to travelers and field office staff members.

The Security Advisor will ensure compliance with IESC organizational Security Policies and Procedures, ensure compliance with security requirements of the funders of IESC programs and the host country governments where those programs are based, develop training plans and create additional tools for IESC home and field offices. The Security Advisor will work with the home office Security Focal Point (SFP) and the SFPs in each overseas office to implement security related activities. This role will ensure consistency with new hire orientations, traveler training, traveler tracking and support for new business proposals and new business travel.

The Security Advisor will also provide security direction including policy, plans and guidelines to Chiefs of Party and to the IESC home office. Each IESC field office has a security focal point, to serve as the local office liaison for the security advisor. The primary responsibilities are to ensure the safety of all IESC staff and travelers, to advise on the IESC selection of and relationship with or security providers, to ensure compliance with U.S. government and host country security regulations and requirements, related to safety and security, and to advise IESC project staff and home office management on security issues in country. The Security Advisor will ensure that security-related operating procedures and the services delivered by overseas security providers are consistent with program implementation and IESC security needs and requirements.

IESC reserves the right to replace the Security Advisor at any time for documented poor performance. If a replacement is required, the Offeror will propose replacement candidates within 10 working days.

5. Statement Of Work

5.1. Schedule of Authorities

The Security Advisor will report to IESC's Vice President, Operations. The role of the Security Advisor is to offer a combination of technical advisory services as well as support organizational capacity building for day-to-day security operations across the company. The Security Advisor will provide IESC's senior leaders with both strategic and technical security advice, counsel and recommendations regarding programmatic security risks, training requirements and security performance.

5.2. Activities

The Security Advisor provides expert advice to support the execution of IESC's Security Policies and Procedures. The Security Advisor will create security related tools, work products and templates for use by the IESC's home and field offices to assist the compliance effort.

A. General Security Advisor Task Overview

The Offeror will provide corporate security advisory services to IESC through the provision of a part-time, off-site, Security Advisor. The Security Advisor may be required to attend meetings at the IESC offices on an as needed basis.

The Security Advisor will provide strategic management planning and support to IESC's security activities through the provision of tools and training to staff, and by providing support for new business efforts. All activities will be consistent and compliant with IESC's Security Policies and Procedures.

The Security Advisor will check the designated IESC email inbox, at a minimum, on a daily basis, Monday through Friday, and be available for emergency security requests via mobile or other messaging services outside of those hours.

The Offeror is responsible for providing Security Advisory coverage on an on-going and as needed basis. In the event of the Security Advisor's scheduled or unscheduled leave, the Offeror will provide the services of another qualified consultant to fill in such gaps, as approved by IESC. Further, the Offeror will work with IESC to develop a contingency plan to address both scheduled and unscheduled gaps in service.

B. Organizational Security Advisory Services

In support of IESC's organizational security requirements the Security Advisor will:

- Provide safety and security guidance to IESC Senior Management as needed.
- Adhere to and provide input and guidance on reviews of IESC's Safety and Security Policies and Procedures and be responsible for identifying vulnerabilities and the corresponding mitigation solution options through the testing and use of policies and procedures in the period leading up to the review.
- Provide technical advice for the development of security related Requests for Proposals (RFPs) or Request for Applications (RFAs), generally related to local providers in the countries where we work. Serve on Selection Committees of potential security suppliers, as required.

- Provide technical support to US Home and Field Offices for on-going implementation of Security Requirements. This includes providing on-going monitoring, risk assessments, strategy, planning, recommendations, implementation, reports, and remote incident control.

- Provide safe, timely and appropriate response to any emergencies in coordination with heads of overseas program offices and home office management. Coordinate with local suppliers and service providers in the event of medical emergencies. Track emergency communications. Provide as needed advisory support related to IESC management of medevac assistance providers.

- Coordinate an integrated staff and traveler tracking system, to monitor the location of international travelers and project staff members while on in-country travel. IESC currently requires all travelers to purchase tickets through the IESC travel management company partner, for tracking of flights, as well as a What's App system for traveler check in. IESC may consider other proposed tracking systems.

- Coordinate and develop, review or update safety and security management tracking systems, templates, and management tools.

- Manage information and inputs on the safety and security page of the IESC Global SharePoint site (templates, guidelines, procedures, etc.).

- Maintain a tracking dashboard to ensure organizational safety and security targets are met for training, compliance checks on safety and security manuals, and traveler briefs.

- Provide security and health assessments of countries to assist in decision making related to staff travel. Develop pre-departure briefs for all staff, consultants and volunteers traveling internationally on behalf of IESC to field offices. Review and provide guidance as needed for IESC sub-recipient travel.

C. Training

In support of IESC's requirements for training the Security Advisor will:

- Conduct an annual assessment of IESC's staff security training needs in the home and field offices and propose an appropriate training curriculum and conduct training directly or propose potential local training providers as appropriate and with IESC approval.

- Develop training materials and provide training for staff on the IESC Safety and Security Policies as required.

- Facilitate Crisis Management Drills for the home office on an annual basis. Facilitate Incident Management Drills at the field office level, as identified in the training plan for each office, to test and validate program security policies and procedures for programs operating in moderate, high and extreme threat environments.

D. New Business Security Advisory Services

In support of IESC's new business requirements the Security Advisor will:

- Provide security and health assessments of countries to assist in decision making related to new business staff travel.
- Develop and provide pre-departure briefings for staff engaged in new business and consultants as requested.
- Provide recommendations for IESC staff engaged in for new business proposals related to security, risk management and the health and welfare of proposed staff.
- Draft short write-ups on security and risk management for inclusion in the management section of proposals including providing recommended security services, vendors and arrangements and their associated costs to be included in the budget/cost proposal.
- Develop risk assessments, security plans and other documents required in new business efforts, as needed.

E. IESC Office Security Advisory Services

In support of IESC's office security requirements the Security Advisor will:

- Support project field offices in their requirements to complete and/or update Security Risk Assessments (SRAs) for each IESC office.
- Support the IESC home office in Washington, DC to update its safety and security plan on an annual basis.
- Support project field offices in their requirement to develop (new programs) and/or update (on an annual basis) Program Safety and Security Plans (PSSPs) for each IESC office.
- Review security checklist and provide approval from a safety and security perspective for all new program office spaces. Advise on office safety and security supply and equipment purchases.

- For programs in which IESC is a sub-awardee, review and approve the prime implementing organization's security plan, as applicable, and coordinate with the prime's security advisor as needed to ensure safety and security measures for IESC program staff, consultants and volunteers are being implemented appropriately.
- Review journey management plans for in-country travel for medium to high-risk countries.
- Develop pre-departure briefs for all staff, consultants and volunteers traveling internationally on behalf of IESC to field offices. Review and provide guidance as needed for IESC sub-recipient travel.
- Manage information and inputs on the safety and security page of the IESC Global SharePoint site (templates, guidelines, procedures, etc.).
- As required, serve as part of the start-up or close-out team for a field office, which may include travel to the field office.
- Advise on program office communications equipment as needed.

F. Deliverables and Project Documentation

Safety and Security Documents:

Documents produced for the home office or for field-based programs, on an as assigned basis. These may include, but are not limited to: policies and procedures, manuals, pre-departure briefs, safety and security plans, training presentations, checklists, tracking documents, fact sheets/quick guides, assessments, technical writeups for proposals, and updates to safety and security management tools. Work products may be in MS Word, Forms, Excel, PowerPoint or other. Documents are to be saved to the safety and security page of the IESC SharePoint site.

Security Work Plan and Road Map. The Security Road Map contains specific activities and deliverables to which both the contracted Offeror and IESC will agree. The status of the Roadmap will be reviewed with IESC on a quarterly basis and updated quarterly to reflect an updated forecast. The format of the roadmap to be agreed upon with IESC and the contracted Offeror at the beginning of the contract.

6. Contract Type

The contract is anticipated to be a Time and Materials contract and based on achievement of assigned tasks and key deliverables to be paid monthly based on timesheets.

7. Instructions to Offerors

7.1. Submission

1) Offers received after the closing date may not be considered.
2) Offers must be in U.S. Dollars.
3) Technical and cost proposals must be submitted as two separate documents. Cost information must not be included in the technical proposal.
4) All quotations must be valid for 90 days.

Offerors must submit their proposals by the closing date and time, as listed on page one, to the following: **Valentine Henry de Frahan, Program and Operations Associate, GlobalAwards@iesc.org**.

7.2. Clarification and Amendments

Offerors may request clarifications via email to **Valentine Henry de Frahan, Program and Operations Associate, GlobalAwards@iesc.org** no later than **5:00 p.m., Washington DC Eastern Standard Time, on Wednesday, December 1, 2021**. IESC will provide answers to these questions and requests for clarification asked by all Offerors simultaneously via email and posted on the IESC website with the RFP before the close of business on/or before **Friday, December 3, 2021**. IESC may not answer questions before the proposal submission deadline outside of the allotted response period for clarifications. No questions will be answered over the phone or in person.

7.3. Cover Page and Markings

In addition to the required proposal documents listed in sections 10 and 11 below, please include a cover page with your submission for the technical and the cost proposals (separate cover pages). The cover page should be on company letterhead and should contain the following information:

1) Project or Title (from the front page of this RFP document)
2) Offer Reference Number (from the front page of this RFP document)
3) Company Name
4) Company Address
5) Name of Company's authorized representative
6) Contact person if different than Company's representative
7) Telephone #, Cellular/Mobile Phone #, Email address
8) Duration of Validity of proposal
9) Payment terms
10) DUNS # (Applies to companies, not to individuals)

11) Total Proposed Price (***cover page of cost proposal only, no cost to be included in technical***)
12) Signature, date, and time

8. Eligibility Requirements

Offeror may be required to present a business license and must have experience in conflict countries. Offerors must demonstrate knowledge of the rules and regulations governing U.S. Government awards. Offerors may need to obtain a DUNS number and an eligibility notice prior to receiving any award. Candidates for the Security Advisor position must be able to travel with short-term notice for periods of up to two months.

9. Basis for Award

IESC anticipates that the award will be based on best-value principles. Accordingly, the award will be made to the technically acceptable Offerors whose proposals provide the greatest overall value to IESC and its program, price, and other factors considered. The winning proposal must conform to all solicitation requirements.

To determine best value, proposals will be evaluated on the criteria below. The number of points assigned, totaling 100 points, indicates the relative importance of each individual criterion. Offerors should note that these criteria serve to: (a) identify the significant factors that Offerors should address in their proposals; and, (b) set the standard against which all proposals will be evaluated.

IESC will conduct interviews for Offerors selected as finalists. The final evaluation for each Offeror will be based on a review of both the written submission and oral interview.

10. Technical Proposal Evaluation

Please read carefully, the following are instructions for preparing proposals. Proposals must be organized into sections corresponding to the sections presented in **10.1 Technical Evaluation Criteria** and numbered accordingly. Please stay within the page limits given below. Only include the requested information and avoid submitting extra content. Any pages exceeding the page limitation for each section of the proposal may not be evaluated.

Proposals will be written in English with each page numbered consecutively. Cover pages, dividers, and tables of contents are not subject to the page limit.

10.1. Technical Evaluation Criteria

Proposals will be evaluated according to the following criteria. Points will also reflect the overall presentation of the proposal, which should be clear, complete, well organized, and well written. Most importantly, proposals should address all the requirements listed in this RFP.

[1] Organizational Capacity and Technical Approach: 4-page limit; possible points 40

Proposals will be scored on the effectiveness of the proposal to meet the responsibilities outlined in **Section 5.2 Activities**.

Offerors will describe their organizational capacity and the structure and management of their organization. Offerors must provide a list of security services they provide and describe how they would approach similar engagements and address the needs of IESC.

Offerors must demonstrate a knowledge and understanding of the international development security environment. Offerors will describe how they anticipate the Security Advisor will advise IESC management in the home and field offices. Offerors will address their experience providing part-time security advisory services to international development organizations and their approach to implementing the items listed in the Statement of Work for:

1) IESC overall organizational security
2) IESC Travel
3) Training
4) IESC new business
5) IESC field offices
6) IESC new business

[2] Offeror's past performance and references: 3-page limit (not including samples of previous work, which may be attachments and/or references); possible points 20

The proposal must provide a detailed account of the Offeror's record in implementing similar activities to those outlined in the tasks and activities. The technical proposal will include a summary of past performance providing security advisory services for international development organizations. Offerors should provide experience in relation to the scope of work in general, and specifically include experience in providing technical advisors for international development organizations.

The proposal should include sufficient information to demonstrate the Offeror's performance for the above tasks and activities and include how the overall approach, including problem solving, is based on extensive prior experience.

Offerors should provide a minimum of three (3) references for on-going contracts or contracts that have a closing date of no later than six months prior to the release date of this RFP. The section should include a brief description of the Security Advisory services provided. References must include contact information. The list of references, with contact information and years for which service was provided, is to be included separately as an attachment.

[3] Offeror's Personnel Experience and Capacities: 3-page limit (not including resumes or CVs, which are attachments); possible points 40

Security Advisors: The technical proposal will include a staffing section and include the CVs of a minimum of two proposed Security Advisors. The staffing section should detail the number of years of relevant experience for each candidate in providing security advisory services for organizations in the international development field and describe their experience managing or providing security/risk management operations for civilian contractors or organizations in these countries under USAID, USDA and other U.S. Government-funded programs, as related to the IESC scope of work.

The proposal should identify and include the CV of the Offeror's client contact who will oversee the contract with IESC and who will manage the Security Advisor. The section should describe the Offeror's client contact's experience in providing client services to organizations with primarily USAID or USDA-funded programs and budgets, and in invoicing and maintaining timesheets and other backup documentation.

CVs should be included as attachments and do not count within the page limitations of this section.

This section will be evaluated on the extent to which the Offeror's personnel have experience with providing the required security advisory services at the organizational level as well as in overseas field environments, including conflict and post-conflict environments.

For technical and budgeting assumptions, minimum qualifications, for the Security Advisor position, are provided below:

Security Advisor:

- Bachelor's Degree, or equivalent level of education and training, is required.

- Sound knowledge of risk management, security, contingency planning, and crisis management in the international development context.
- Over five years of experience in public and private sector security and risk management for development assistance programs at all levels of operation, from overall security programming and coordination to field program and protection services.
- Over five years of experience developing security plans and standard operating procedures for development programs in the challenging security environments for wide ranging and complex project operations requiring flexibility, adaptation to local operating environments, and close coordination with program technical staff.
- At least five years of experience in emergency response, extraction, securing locations, and coordinating critical actions with senior program management in response to incidents.
- Demonstrated success in working closely with the clients to facilitate program success while maintaining the safety of staff and accomplishing project objectives.
- Experience in advising clients on security management as well as on physical security improvements, equipment, and cost effectiveness measures.
- Experience working and traveling in moderate and high-risk countries with limited infrastructure.
- Experience providing travel advisory services, including related to COVID-19.
- Ability to travel on short notice, if needed, but rarely anticipated.
- Excellent oral and written communication skills in English (An additional language will be an advantage).
- Advisor must be available to be on call for 24/7 emergencies.

11. Cost Proposal Evaluation

The Offeror will submit a separate cost proposal. Offerors should present a cost proposal with detailed budget notes to demonstrate and explain how costs were developed or estimated. The budget narratives should be in a separate document and detail how the cost was obtained and why the unit cost represents a reasonable cost. In preparing cost estimates, the following assumptions may be used:

- The Security Advisor will be budgeted on a fixed daily rate basis, based on an 8-hour day. The fixed daily rate contains the base salary burdened with fringe benefits, indirect and/or overhead costs, and profit, if any. A breakdown of costs is not required for the proposal submission, however, may be requested.
- The multiplier used to calculate the burdened rate must be provided.
- Travel to overseas location, if needed, will be reimbursed at cost, without markup, and must comply with IESC Travel Policies to meet the US Government and other

donor rules and regulations. Only economy class tickets, complying with Fly America will be reimbursed.

The cost criteria will be evaluated separately and will consider factors including cost effectiveness, cost control and cost realism. While IESC believes in cost savings, budgets should be realistic and value for the services should be clearly demonstrated. A proposal with the lowest estimated cost will not necessarily win the bid.

All proposed costs must be in accordance with the U.S. Government Cost Principles under 2 CFR 200 Subpart E or FAR Part 31, as applicable.

12. Discrepancies

Please read the instructions carefully before submitting your proposal. Any discrepancy in following the instructions or RFP provisions may disqualify your proposal without recourse or an appeal for reconsideration at any stage. However, IESC reserves the right to consider such proposals and waive minor discrepancies, where such a waiver will promote increased competition and best value to IESC.

13. Conflict of Interest Declaration

The following steps outline IESC's contract selection process and should be understood by all Offerors to ensure the transparency of awards and avoid conflict of interest.

1) Request for Proposals (RFPs) are posted on IESC's website. The offer is open to all qualified offerors;
2) Clarifications will be emailed to all offerors submitting questions, as well as posted on IESC's website, simultaneously;
3) Once the proposals are received, an evaluation committee scores them;
4) Cost proposals are evaluated for reasonableness, accuracy, and completeness;
5) The best value proposal is selected based on a combination of the technical score and the cost;
6) No activity can be started until both IESC and the awardee have signed a formal contract; and,
7) IESC policy against fraud and code of business ethics exists throughout the life of the contract and beyond. Even if the contract is closed, if any party is found guilty of fraud, IESC will make a full report to the appropriate Office of Inspector General, which may choose to investigate and prosecute guilty parties to the fullest extent of the law.

Any contracts awarded will be required to comply with all administrative standards and provisions required by any donors funding IESC programs.

-END-