Request for Proposals

Posting Date: May 1, 2024

Proposal submission deadline: May 10, 2024

Services Sought: Risk Intelligence Support

Parameters

No recipient of this RFP is authorized to approach any carrier, service provider or other outside party for any purpose in connection with this RFP, regardless of any current or prior relationship with IREX. IREX reserves the right to disqualify any proposal for failure to comply with this requirement. Recipients of this RFP are responsible for all expenses associated with proposal preparation and presentation, including travel.

If you have questions regarding this RFP or desire additional information, please contact Margarita Fernandez, VP of Global Operations Management at MFernandez@irex.org. Questions may be submitted at any time up to the proposal due date with a 24–48-hour targeted turnaround time.

Proposals and/or any appendices received after the announced time and date of receipt (Due Date/Time) will not be accepted. IREX reserves the right to request additional information at any time from bidders who have submitted proposals, during the procurement process.

Format

Submittals should be presented in the following manner:

i. Introduction
ii. Responses to Section IV. Proposal Submission Requirements
iii. Appendices
    a. Signature sheet
    b. Schedule of Fees

Written submissions should be kept concise and follow the order under section IV. Proposal Submission Requirements. Answers should be specific to the questions and should be written in clear and concise language. Supplemental materials can be submitted but may not be reviewed or evaluated given time constraints.

Selection and Submission

All proposals should be sent via email to the attention of ***Kurt Parker, Global Security Manager at KParker@irex.org.*** The subject line shall include: "IREX Risk Intelligence Support." The deadline for submission of proposals is **no later than May 10, 2024.** Hard copy proposals will not be accepted. All proposals will become part of the requester's files without obligation.

Organizational Overview

About IREX

The International Research and Exchanges Board ("IREX") is a 501(c)(3) not-for-profit corporation established in 1968. Its headquarters office is located at 1275 K Street, NW, Washington, DC. IREX's mission is to build a more just, prosperous, and inclusive world by empowering youth, cultivating leaders, strengthening institutions, and extending access to quality education and information.

IREX embraces a people-focused approach to development that invests in human potential and the conditions that help people to thrive. We work with partners around the world to promote more just, prosperous, and inclusive societies by engaging and empowering youth, cultivating leaders at all levels of society, strengthening institutions, and expanding access to quality education and information. You can learn more about IREX as an institution by visiting our website: www.irex.org.

Traveling both internationally and domestically is essential to IREX's mission and the implementation of our programs. Our staff is also our most important asset, and creating a reliable, user-friendly travel management program is essential to ensuring our staff and institution's success.

IREX has over 750+ full-time, part-time, and temporary employees. Our employees are in our headquarters and twenty-three (23) country offices in Africa, Asia, Eurasia, Europe, and the Middle East. There are 280+ staff members in our DC office and about 461 staff in our global offices.

Overview of IREX's Current Security Program

IREX's Global Security (GS), Global Operations and Information Technology (IT) units seek to increase their capabilities in identifying, assessing, and mitigating various forms of risk through intelligence and analysis. Global Operations and IT have identified to reliable reporting of threats and risks across the physical, digital/cyber, political, geo-political, legal, financial, and economic risk categories as a critical need for organizational success.

IREX seeks a single provider of comprehensive intelligence and analysis reporting that is capable of monitoring multiple global risk categories and providing predictive insights to how these risks may impact the organization and/or its mission.

IREX's Risk Intelligence Support RFP Objective

IREX is seeking proposals from qualified Risk Intelligence and Assessment Companies as it moves towards modernization of its Risk Mitigation systems and processes, and improvements in operational efficacy and overall efficiency. IREX GS and IT seek an intelligence service provider that can monitor, assess, and report on threats and risks IREX faces around the globe in the areas of cyber, physical, personal, economic, political, and supply chain from both state and non-state actors. Monitoring, reporting, and assessment should be ongoing and continuous and bespoke analytical projects available on an as-needed basis. Communication will occur between both GS and IT, and the vendor.

Scope of Services

Global Security

The applicant should be capable of providing a full spectrum of analytical and assessment services pertaining to risk and threats to IREX. These services should be inclusive of cultural, political, and socio-economic contextual considerations, and compiled and curated by trained intelligence and security experts with global insight and international experience. The desired end state of services provided is a comprehensive multidimensional picture of safety, security, and risk considerations in countries and regions across the globe as presented by both state and non-state actors. The applicant should be able to provide, at a minimum, the following specific services:

1. Reporting of economic conditions and changing trends, and evaluation of risk of economic destabilization
2. Assessments of a country's general supply chain stability and risk, especially as it relates to food, fuel, medical care, and other critical infrastructure and commodities,
3. Assessment and evaluation of political risk vectors related to targeting persons or organizations based on political affiliation, religious beliefs, sexual orientation, ethnic origin, and other personal or organizational attributes. This may include, but not be limited to, new laws, use of administrative/bureaucratic powers and authorities, shifts regarding respect for and protection of civil and human rights, etc.
4. Real time threat reporting and continuous monitoring.
5. Assessment on safe freedom of movement throughout the country for indigenous citizens and expatriates.
6. Political analysis of changing political trends from governments or parties/affiliations within the government, as well as political movements that may present risk vectors to a nation's stability.
7. Election monitoring, analysis, and commentary
8. Analysis/evaluation of how favorable the U.S./Western allies are viewed by the government, political parties, and leaders,
9. Bespoke topical analysis on request,
10. A dashboard or application providing client accessible information, analysis, and research system or dashboard for access to information and analysis provided by vendor,
11. Ability of end user to specify type and frequency of security alerts generated and delivered by the platform,

12. Regular briefings between vendor and client (IREX) at an interval to be negotiated, but no less frequently than monthly, where the vendor will provide a summary of notable and critical developments being observed and assessed around the globe.
13. Identification and analysis of cyber threats relevant to IREX's industry and operations.
14. Provision of timely and actionable information concerning cyber threat actors (Storm, APT 23, APT41, etc..), cyber-threat vectors (malware, phishing, ransomware, and others), and Indicators of Compromise (IOCs) -- including but not limited to IP addresses, domain names, file hashes, and URLs.
15. Working closely with IREX's internal information security team through timely communication to guarantee "Just in time" threat information about zero day and time-sensitive threats.
16. Integration with IREX's Microsoft Sentinel SIEM and Microsoft Defender for Endpoint (MDE) threat detection tools and management tools.
17. Access to a user-friendly cyber-threat intelligence platform or portal for easy consumption and analysis of threat data.
18. Offer customizable cyber threat reports and alerts based on IREX's threat and risk profile.
19. Offer country and region level cybersecurity reports including Internet Freedom profiles, cyber drafts/legislation in progress, summary of data privacy regulations, summary of relevant laws regarding encryption and VPN use, and summary of available telcos; mobile phone providers; and Internet Service Provider.
20. Platform supports modern authentication methods including Single Sign On integrations with Microsoft Identity (M365).

Proposal Submission Requirements

In response to this RFP, please provide the following information:

1. Introductory letter containing the following:
    a. Company's values, mission, and customer service approach and how they relate to your performance.
    b. Description of experience serving mid-size international organizations and businesses with a wide geographic footprint, stretched over numerous time zones.
    c. Description of experience providing services requested.
    d. Descriptions of typical experience and expertise of employees which would be assigned to this contract.
    e. Four references (at least two references should be from international organizations) who can attest to the firm's knowledge, quality of work, timeliness, diligence, flexibility in providing services requested.

2. Based on IREX's size and split of domestic and international operations, advise your ability to assess outlined risks across a global footprint and your staff's experience monitoring and assessing global risks.
3. Based on IREX's standing as an implementor of programs for the USG, your ability to assess political risk presented by both state and non-state actors in various regions.
4. A demonstration of the client facing information dashboard providing 24hr access to current available information.
5. Summarize and provide examples of client briefings and reports representative of both periodic reporting and bespoke/on demand analysis.

6. Describe methods of assessing changes to a country/region's risk categories:
    a. Political
    b. Social
    c. Economic
    d. Terrorism/violence/unrest
    e. Cyber
    f. Supply Chain
    g. Foreign influence

7. A brief description of customer service performance metrics including:
    a. Average length of time for incident reporting.
    b. Average length of time to generate an analytical report upon request.
    c. Capability and expertise in assessing risk on a global scale.

8. Discuss the various integration methods of your product with Microsoft 365, Microsoft Defender for Endpoint, and Microsoft Sentinel product suites. Explain the methods and timing through which IREX can disseminate threat intelligence to its programs, partners, and donors.
9. Detail the licensing structure governing access to the portal for information retrieval and report generation.
10. Elaborate on the update timing for IOC and Zero Day threat intelligence.
11. Provide a concise overview of the cybersecurity threat intelligence available per country and region.
12. Describe the fee framework for analytical reporting, delineating what is encompassed within the annual fee and what is not.
13. Timeline of implementation
14. Please provide a description of your technology and digital security protocols to ensure that IREX information is secure.
15. Describe the approach your company would take to assist us in achieving significant cost control and cost reduction.
16. Please complete the Signature Sheet (Appendix A)
17. Please complete the Schedule of Fees Chart (Appendix B)
18. Please provide a sample budget/fee structure including any one-time setup charges.

Proposal Evaluation Criteria

IREX reserves the right to determine which bidders have met the requirements of this RFP. In addition, IREX may reject, in whole or in part, any and all proposals, waive minor irregularities in proposals, allow a bidder to correct minor irregularities and negotiate with all responsible efforts in any matter deemed necessary to serve the best interest of IREX.

IREX reserves the right to reject any and all proposals when such rejection is in the interest of IREX, to reject the proposal of a bidder who has not met the prerequisites of the bid proposal or who has previously failed to perform properly or complete on time contracts of a similar nature, and to reject the proposal of a bidder who is not, in the sole opinion of IREX, able to perform the contract to the sole satisfaction of IREX.

IREX also reserves the right to waive any informalities and technicalities in the bidding. IREX reserves

the right, however, to award the contract in accordance with its best interest and will not be required to accept the lowest bid.

IREX may, upon its discretion, establish a competitive range of qualified proposals for award consideration. IREX will not conduct discussions or negotiations with contractors who are not within the competitive range and those contractor bids will not be considered for award. IREX will assess all applicants based on, but not limited to, the following criteria:

- **Demonstrated Qualifications and Institutional Capacity**. This may include years in business providing, experience serving accounts of comparable size, complexity, and volume, experience serving government contractors, experience providing backup services to account.

- **Management Plan**. Business practices and organization structure including corporate support, proactive business practices and philosophies to ensure staff are trained, supported and available to meet IREX's needs. Include an overview of the structure of the account management team and how it will be structured (i.e., all HQ based, internationally based, knowledge of after-hours team of the IREX account, etc.)

- **Personnel and Staffing**: Qualifications and experience of key personnel.

- **Understanding of Scope of Services.** Innovations in providing services through the Risk Intelligence Company's staffing approach, technology usage and customer service approach. Approach to achieving successful day-to- day operations. Flexibility in meeting service needs and ability of business model to re- focus and adjust work processes as needed. Include details of licensing model and level of enterprise access to the tools/dashboard.

- **Past Performance and Related Experience**. Quality and positive feedback from references including ability to: perform scope of services specified, ability to meet schedules and needs of

Summary of Key Dates

Request for Proposal is posted	**May 1,2024**
Proposal Submission Deadline, by 5:00 PM ET	**May 10, 2024**
Contractor Selection and Notification	**May 15, 2024**
Anticipated Service Start Soft Date (*Transition period*) Anticipated Service Start Date (*Estimated*)	**June 1, 2024**

Qualified bidders will be alerted to any schedule changes.

Appendix A: Signature Sheet

My signature certifies that the proposal as submitted complies with all Terms and Conditions as set forth in the RFP.

To receive consideration for award, this signature sheet must be included as part of your response. Complete Legal Name of Firm: _____

Address: _____

_____

Federal Tax ID Number: _____

Signature of Authorized Representative: _____

Type Name and Title: _____

Primary contact person for questions and concerns relative to this project:

Contact Name and Title: _____

Phone: (_____) Fax: (_____
Email: _____