**RFP Issuance Due Date: February 10, 2025 (Issuance Date)**

**Questions Due Date: February 21, 2025, 5 PM EST**

**Proposal Submission Due Date: March 14, 2025, 5 PM EST**

**Anticipated Start Date: May 19, 2025**

# SUBJECT: Request for Proposals (RFP) - Annual IT Risk Assessment and Technical Testing

IIE is seeking proposals from qualified organizations interested in providing the services described in the attached Request for Proposals (RFP).

The purpose of this Request for Proposal ("RFP") is to invite qualified organizations to submit a proposal for providing services to conduct an annual IT Security Risk Assessment and associated Testing outlined more fully in Sections III and IV.

IIE intends to issue a fixed price subcontract to suitable vendors who demonstrate that they have the capacity to deliver quality technical assistance and are the most responsive to the requirements of the RFP.

The remainder of this RFP provides additional information that will allow an offeror to understand the scope of the effort and develop a proposal in the format desired by IIE.

Issuance of this Request for Proposal (RFP) does not constitute an award commitment on the part of the IIE. IIE reserves the right to reject any offer received in response to this request. IIE shall not be liable for any costs incurred by Offeror in the preparation and submission of proposal.

The information presented in this RFP is furnished solely for the purpose of assisting the offeror in making its own evaluation of the Scope of Work and does not purport to be all-inclusive or to contain all the information you may require. This RFP is not an offer by IIE to contract, but rather an attempt to establish a common framework for IIE to evaluate potential suppliers. The offeror should make its own investigations, projections and conclusions to verify independently the information contained in this RFP, and to obtain any additional information that it may require, prior to submitting a proposal.

All questions, comments, requests for clarifications must be sent in writing to jlopez@iie.org no later than the date and time indicated above. Questions will not be entertained after this date.

If substantive questions are received which affect the response to the solicitation or if changes are made to the closing date and time as well as other aspects of the RFP, this solicitation will be amended. Any amendments to this solicitation will be issued and posted on the IIE's procurement opportunities website. The worldwide web address is https://www.iie.org/en/Work-With-Us/Subawards-

Procurements/Solicitations-for-Goods-and-Services. Offerors are encouraged to check this website periodically.

Thank you for your interest and we look forward to your participation.

Sincerely,

Jose M. Lopez
Director, Information Security and Compliance
Institute of International Education, Inc.
1350 I (Eye) ST NW Suite 600
Washington, DC 20006
Email: jlopez@iie.org

# Table of Contents

# Statement of Work (SOW)

## I. Background

IIE has adopted the NIST Cyber Security Framework (CSF) as the keystone by which to build and further mature its Information Security Program. Additionally, IIE has contractual requirements to adhere to the Cybersecurity Maturity Model Certification (CMMC) 2.0 program and NIST 800-171v2. These standards for the organization require annual IT Security Risk Assessment and associated technical testing conducted by a third-party firm on an annual basis.

## II. Objectives

The objectives of the request include the following components:

- Assess the level of maturity of IIE's information security program, with an emphasis on cyber security and the organization's ability to defend against and respond to modern cyber security threats affecting its information assets.
- Technically evaluate IIE's servers and key systems to discover unknown vulnerabilities and/or areas of improvement regarding IT Infrastructure and application security.
- Validate IIE's compliance with CMMC NIST 800-171v2 requirements.

## III. Activities and Tasks

**IIE Information Security Program Assessment:**

- Using the NIST 800-171v2, the firm will evaluate IIE's current IT infrastructure and security landscape to identify any findings from an organizational governance, strategy and process perspective
- Review IIE's information security policies and assess the design of documented controls, processes and technology solutions with respect to NIST 800-171v2, including but not limited to the following areas:
    - Access Control
    - Awareness and Training
    - Audit and Accountability
    - Configuration Management
    - Identification and Authentication
    - Incident Response
    - Maintenance
    - Media Protection
    - Personnel Security
    - Physical Protection
    - Risk Management
    - Security Assessment
    - System and Communications Protection
    - System and Information Integrity

**Technical Security Testing**

- Firm will assess IIE's alignment with technical safeguards within NIST 800-171 on IT Infrastructure and specific high-risk applications (Details provided after NDAs are signed)
- Infrastructure Security Assessment
    - Review IIE's network infrastructure (Routers, Firewalls, Wireless access points) against industry-accepted hardening standards to identify opportunities to improve secure configuration.
    - Review IIE's server and end-point infrastructure against industry-accepted hardening standards.
    - Review IIE's cloud infrastructure against industry-accepted hardening standards.
- Penetration testing assessments:
    - Identify security vulnerabilities in critical systems. (Approximately 25 web-facing applications)
    - Identify security vulnerabilities involving IIE's application interfaces. (Approximately 6 interfaces)
- Application Programming Interface (API) testing

The following communications tasks are associated with this request:

- Firm to hold a formal "kick-off" meeting to formally confer with IIE on scope of IT risk assessment and technical testing and discuss expected timeline for completion
- Firm to conduct initial discovery interviews with relevant IIE Tech stakeholders
- Firm to hold weekly progress report meetings with relevant IIE Tech Team Members

## IV. Deliverables

- **Comprehensive Risk Assessment Portfolio** that contains the following deliverables:
    - **Executive Summary** - The overview package will include an Executive Summary outlining the scope of the project and any critical risks identified. The Executive Summary may also provide organizational and strategic security recommendations based on findings.
    - **IT Security Risk Assessment Report** with recommendations based on findings of the objectives outlined and benchmarks to the NIST 800-171v2 maturity model for year-over-year comparison. Security Assessment Report identifying items for a Plan of Action and Milestones (POA&M), provide a SP 800-171 DoD Assessment score.
    - **Penetration Testing Reports** with suggested remediations
    - **CMMC Supplier Performance Risk System (SPRS) score** for audits conducted
- **Project Communication** - During the term of the Assignment, the vendor will provide regular updates on open tasks, requests, and efforts required to complete the engagement.
    - Kick-off Meeting slide deck
    - Weekly Progress Report briefs

## V. Duration and Location

Duration:

Vendor should endeavor to begin work the week of May 19, 2025; all work must be tracked to closure (deliverables closed out and invoiced by IIE) before July 31, 2025.

Location:

Given IIE's cloud-hosted infrastructure, all work can be performed virtually.

## VI. DoD Accredited Auditor

Preferences to  firms that are accredited CMMC Third Party Assessment Organizations (C3PAOs)

# Submission Information

## VII. Submission Information

This section contains general and specific requirements for submitting the technical and cost proposals. Please ensure completed forms, along with a copy of your legal registration, are included with the technical proposal otherwise your proposal will be rejected.

1. This RFP is issued as a public notice to ensure that all interested, qualified and eligible organizations legally registered for business in the United States have a fair opportunity to submit proposals. Qualified international firms should have local and/or international experts available to provide these services.

2. The Offeror is requested to submit a proposal directly responsive to the terms, conditions and clauses of this RFP. The overall proposal shall consist of two (2) physically separated parts: Technical Proposal and Cost Proposal.

   Alternative proposals will not be considered. Proposals not conforming to this solicitation may be categorized as unacceptable and eliminated from further consideration.

   Offerors can submit one proposal. If an Offeror participates in more than one proposal, all proposals involving the Offeror will be rejected.

3. Proposals shall be written in English. Cost proposals shall be presented in USD.

4. Proposals must remain valid for a minimum of **120 (one hundred twenty) days**. The Offeror may submit its proposal by the following means:

   Electronically – Internet email with up to two (2) attachments per email compatible with MS WORD, Excel and Adobe Acrobat in a MS Windows environment to: jlopez@iie.org.

5. The person signing the Offeror's proposal must have the authority to commit the Offeror to all the provisions of the Offeror's proposal.

6. The Offeror should submit its best proposal initially as IIE intends to evaluate proposals and make an award without discussions. However, IIE reserves the right to conduct discussions should IIE deem it necessary.

7. Proposals must be clearly and concisely written and must describe and define the Offeror's understanding and compliance with the requirements contained in the STATEMENT OF WORK. All pages must be sequentially numbered and identified with the name of the Offeror and the RFP number.

**PART A: TECHNICAL PROPOSAL**

The technical proposal shall be straightforward and concise, outlining in sequence, how the Offeror intends to carry out the technical requirements under each main activity. No contractual price information is to be included in the Offeror's implementation work plan in order that it will be evaluated strictly on its technical merit.

The implementation work plan shall be limited to five (5) five pages in total. **Pages in excess of 5 pages will not be read or evaluated.**

Detailed information should be presented only when required by specific RFP instructions. Items such as graphs, charts and tables may be used as appropriate but will be considered part of the page limitation. Key personnel resumes, bio-data sheets, references and dividers are not included in the page limitation. No material may be incorporated in the proposal by reference, attachment, appendix, etc. to circumvent the page limitation.

1. **Organizational Information:**
    - Organization's legal name
    - Contact name and position or title
    - Organization's E-mail address, physical address and telephone number
    - Copy of legal registration for business (United States)
    - Proof of CMMC Third Party Assessment Organizations (C3PAOs) accreditation

2. **Technical Approach:** In a narrative – not to exceed four (2) pages – the Offeror will demonstrate its understanding, ability and overall approach to performing the requirements described in the Scope of Work, Activities & Tasks and Deliverables.

3. **Capability Statement:** A narrative – not to exceed two (2) pages – that explains the Firm's capability to perform the scope of work, activities & tasks and deliverables. The Offeror will demonstrate it has industry-recognized IT certifications and organizationally compliant systems and procedures (e.g., technical tools), effective project management, equipment and personnel knowledge in place to successfully comply with the contract requirements and to accomplish the expected results. It will demonstrate it has the **in-house resources** to provide the required services – no subcontracting will be accepted. A description of relevant personnel training and qualifications, including CVs for key individuals, where applicable. CVs are not included in the 3-page length limit.

4. **Past Performance:** Not to exceed two (2) pages, the Offeror will submit a list of current and past similar work and assignments completed in the past five years that were similar in size, scope and complexity – preferably in areas listed in the SOW.

5. **References:** References from a minimum of two (2) clients worked with in the past two years on activities similar to this scope of work. Include the contact information: company or organization, name, phone number and email.

6. **Personnel/Staffing:** Not to exceed two (2) pages, the Offeror will identify, in summary format of 2-3 sentences, the names, anticipated positions of the key team leaders and essential personnel proposed to perform the requirements of this scope of work, activities & tasks and deliverables. The narrative will include the percentage of staff time of principals and managers

on this activity. CVs (not to exceed two (2) pages) that clearly describe education, experience and professional credentials and biodata forms will be completed and attached for the proposed personnel. These pages do not count toward the page limitation for this section.

**PART B: COST PROPOSAL**

The Offeror will propose costs it believes are **realistic** and **reasonable** for the work in accordance with the Offeror's technical approach. The Offeror shall provide a complete budget based on cost elements described below.

The detailed cost proposal will include the following:

a. Proposed staff, rates and number of days needed to accomplish the work
b. Transportation and logistics costs
c. Related materials and supplies

Provide in the Budget Narrative section**,** a concise description and justification for each line item cost. Be sure to include data and/or methodologies to support cost estimates.

The Budget Narrative shall be presented in such a way as to be easily referenced from the budget and should provide sufficient information so that IIE may review the proposed budget for reasonableness.

All projected costs must be in accordance with the organization's standard practices and policies.

Offers including budget information determined to be unreasonable, incomplete and/or unnecessary for the completion of the proposed project or based on a methodology that is not adequately supported may be deemed unacceptable.

**Guidelines:**

1. Cost proposals from Offerors shall be presented in USD.
2. Offer must be inclusive of any applicable taxes such as sales tax.
3. If the Offeror proposes a fringe benefit rate on salaries, it must be supported by an established written policy. Please provide a detailed explanation in the budget narrative.
4. For employee salaries – List employee name (when identified), functional position and duration of assignment (in terms of person days) and daily rate. The daily rate is derived by dividing base annual salary exclusive of fringe benefits, incentives, bonuses, overtime, allowances and differentials by 260 days.
5. Travel and transportation – Provide the number of trips, origin and destination of trips, estimated airfares and other costs such as taxi fees.
6. Per diem – Offerors will budget per diem associated with travel and transportation in accordance with their established written policy that shall not exceed the rates established by General Services Administration (GSA) for domestic travel within United States, and the Department of State for travel outside United States.
7. Other direct costs – Itemize and provide complete details of other direct costs including unit prices that may be incurred.

## VIII. Evaluation Criteria

IIE will select the offeror whose proposal represents the best overall value to IIE in terms of the selection criteria specified below. Offerors who do not follow the instructions in this RFP may be disqualified from consideration.

Offers must first meet the mandatory requirements before their technical and cost proposals will be reviewed. Those bids not meeting the mandatory requirements will be automatically rejected.

The mandatory requirements are:

| | MANDATORY REQUIREMENTS | MEETS REQUIREMENT |
|---|---|---|
| 1. | Legally registered to do business in United States – Offeror shall provide a copy of its registration document with the technical proposal.<br>Also offeror will provide the Unique Entity Identifier (UEI) if available. | YES/NO |
| 3. | Pass IIE's Responsibility Determination. IIE will check to make sure that final offer is not listed under terrorism list of U.S. Treasury Department, United Nations and that it is not listed as an excluded party under the System for Award Management www.sam.gov | YES/NO |
| 4. | The detailed cost proposal follows the prescribed format. | YES/NO |

The technical evaluation will be based on the following weighted categories:

| **Criteria Technical Proposal (implementation work plan) 70%** | **Percentage 70%** |
|---|---|
| Experience and qualifications of the IT firm | 20% |
| Experience and qualifications of proposed personnel | 20% |
| Implementation work plan | 20% |
| Past performance | 10% |
| **Cost Price Proposal Criteria 30%** | **Percentage 30%** |
| Cost data will be evaluated based on cost reasonableness, allowability and realism based on the following considerations:<br>- Are proposed costs realistic for the work to be performed under the award?<br>- Do the costs reflect a clear understanding of the work requirements?<br>- Are the costs consistent with the various elements of the Offeror's technical proposal?<br>An all-inclusive day rate for each team member (professional and administrative) | 30% |

## IX. General Terms and Conditions

1. Any proposal received in response to this solicitation will be reviewed **strictly** as submitted and in accordance with Section VII, Evaluation Criteria.

2. EXECUTIVE ORDER 13224 ON TERRORIST FINANCING

   Offerors are informed that IIE complies with U.S. Sanctions and Embargo Laws and Regulations including Executive Order 13224 on Terrorist Financing, which effectively prohibit transactions with persons or entities that commit, threaten to commit or support terrorism. Any person or entity that participates in this bidding process, either as a prime or sub to the prime, must certify as part of the bid that he or it is not on the U.S. Department of Treasury Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) List and is eligible to participate. IIE shall disqualify any bid received from a person or entity that is found to be on the List or otherwise ineligible.

   Firms or individuals that have an active exclusion on the System for Award Management (www.sam.gov) shall not be eligible for financing and shall not be used to provide any commodities or services contemplated by this RFP.

3. TERMS AND CONDITIONS

   Offerors are responsible for review of the terms and conditions described.

4. CONTRACT MECHANISM

   IIE is anticipated to award a fixed price subcontract to the Offeror whose proposal will be evaluated based on the evaluation criteria described previously. Based on the merits of the offers received, IIE reserves the right to award more than one subcontract.

5. WITHDRAWALS OF PROPOSALS

   Offerors may withdraw proposals by written notice via email received at any time before award. Proposals may be withdrawn in person by a vendor or his/her authorized representative if the representative's identity is made known and if the representative signs a receipt for the proposal before award.

6. RIGHT TO SELECT/REJECT

   IIE reserves the right to select and negotiate with those firms it determines, in its sole discretion, to be qualified for competitive proposals and to terminate negotiations without incurring any liability. IIE also reserves the right to reject any or all proposals received without explanation.

7. DUE DILIGENCE PROCESS

   Any selected firm may be required to complete a Financial Pre-Award Risk Assessment in order for IIE to ascertain that the organization has the capacity to perform successfully under the terms and conditions of the proposed award. As part of the Pre-Award Risk Assessment process, the firm will also be

requested to submit a financial audit report from the previous fiscal year. In addition, payroll records and other financial information may be requested to support budgeted costs.

8. CLIENT PRIOR APPROVAL

   Based on the amount of the final award and the type of contractual mechanism, the selected Offeror may be subject to funding agency approval before a subcontract can be awarded. Therefore, organizations are reminded that there may be delays for this process to be completed. In addition, should such approval not be given, this subcontract cannot be awarded.

9. DISCLAIMER

   This RFP represents only a definition of requirements. It is merely an invitation for submission of proposals and does not legally obligate IIE to accept any of the submitted proposals in whole or in part, nor is IIE obligated to select the lowest priced proposal. IIE reserves the right to negotiate with any or all firms, but with respect to price, costs and/or scope of services. IIE has no contractual obligations with any firms based upon issuance of this RFP. It is not an offer to contact. Only the execution of a written contract shall obligate IIE in accordance with the terms and conditions contained in such contract.

10. REQUEST FOR PROPOSAL FIRM GUARANTEE

    All information submitted in connection with this RFP will be valid for 120 (one hundred twenty) days from the RFP due date. This includes, but is not limited to, cost, pricing, terms and conditions, service levels and all other information. If your firm is awarded the contract, all information in the RFP and negotiation process is contractually binding.

11. OFFER VERIFICATION

    IIE may contact Offerors to confirm contact person, address, bid amount and that the bid was submitted for this solicitation.

12. FALSE STATEMENTS IN OFFER

    Offerors must provide full, accurate and complete information as required by this solicitation and its attachments.

13. CONFLICT OF INTEREST

    Offerors must provide disclosure of any past, present or future relationships with any parties associated with the issuance, review or management of this solicitation and anticipated award in or outside of the country of performance.

    Failure to provide full and open disclosure may result in IIE having to reevaluate selection of a potential vendor.

14. RESERVED RIGHTS

    All RFP responses become the property of IIE, and IIE reserves the right in its sole discretion to:

    - Disqualify any offer based on Offeror failure to follow solicitation instructions.

- Waive any deviations by vendors from the requirements of this solicitation that in IIE's opinion are considered not to be material defects requiring rejection or disqualification, or where such a waiver will promote increased competition.
- Extend the time for submission of all RFP responses after notification to all vendors.
- Terminate or modify the RFP process at any time and reissue the RFP to whomever IIE deems appropriate.
- Issue an award based on the initial evaluation of Offerors without discussion.
- Award only part of the activities in the solicitation or issue multiple awards based on solicitation activities.
- Not compensate Offerors for preparation of their response to this RFP.
- Not guarantee that IIE will award a subcontract based upon the issuing of this RFP.
- Award a subcontract to more than one Offeror for specific parts of the activities in the RFP.
- The successful Offeror will be obligated to enter into an agreement containing the same or substantially similar terms and conditions found at https://www.iie.org/Work-With-Us/Subawards-Procurements/Solicitations-for-Goods-and-Services. The IIE terms and conditions may be changed, added to, deleted or modified by IIE prior to awarding the agreement. Other terms and conditions may be negotiated between IIE and the successful Offeror, at IIE's discretion. State Universities and Agencies should not expect or ask IIE to modify its Terms and Conditions to incorporate any State Regulations or Statutes.
- Payment terms for the award shall be approximately net thirty (30) days after satisfactory completion of each deliverable or milestone agreed upon and established in the resulting agreement. Payment shall be made by the Institute of International Education ("IIE") via check or electronic funds transfer/bank wire. The final payment terms in the contract will control, not this RFP. No advance payments will be provided.
- Annual Renewal: Selection(s) may be renewed annually, at IIE's sole discretion, for up to five years before re-competition. IIE reserves the right to exercise any one of the following options:
    - Accept the updated proposal if changes are reasonable and within the scope of the original selection;
    - Negotiate any updates/changes; or,
    - Decide not to renew

# Attachment A - Additional Requirements

**Third-Party IT Risk Management Process (TPRM)**

An **IT Security Questionnaire** is required prior to signing a contract if the vendor will process IIE proprietary data or Personal Data according to GDPR's definition on behalf of IIE or connect to IIE's network.

- Vendors who can furnish evidence of an **ISO 27001 Certification** are asked to attach such documentation and to provide their up-to-date **System and Organization Controls (SOC) 2 Type 2 Attestation**.

- Vendors who cannot furnish IIE with ISO 27001 Certification evidence will be asked to provide a **SOC 2 Type 2 attestation** and complete a **security assessment that is mapped to the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF)**. NIST is a guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. The NIST CSF consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's cybersecurity risk management.

- If your organization does not wish to complete this request using the automated OneTrust platform, please visit the "Welcome" screen of the IT Security Questionnaire (using the emailed link from OneTrust) and click "*Complete Offline Using Excel*" to download the **Excel** version of the NIST CSF assessment. Please make sure to upload the completed file to OneTrust using the same path and **Submit**.

**Prohibition on certain telecommunications and video surveillance services or equipment**

IIE cannot enter into a contract to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. As described in Public Law 115-232, section 889, covered telecommunications equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

Covered equipment and services must not be part of your offer to IIE.