Digital Frontiers

Request for Proposals (RFP)

No. 2023-05

ProICT: Development of CARICOM Cyber Resilience Strategy

Issue Date: March 30, 2023

WARNING: Prospective Offerors who have received this document from a source other than the DigitalFrontiers@dai.com email address, should immediately contact DigitalFrontiers@dai.com and provide their name and email address in order that amendments to the RFP or other communications can be sent directly to them. Any prospective Offeror who fails to contact DigitalFrontiers@dai.com assumes complete responsibility in the event that they do not receive communications prior to the closing date. Any amendments to this solicitation, questions and answers, or other communications will be issued from DigitalFrontiers@dai.com

Table of Contents

Synopsis of the RFP

RFP No.	2023-05
Issue Date	March 30, 2023
Title	ProICT: Development of CARICOM Cyber Resilience Strategy
Issuing Office & Email	Digital Frontiers c/o DAI DigitalFrontiers@dai.com
Deadline for Receipt of Questions	April 06, 2023, 5pm EST, to DigitalFrontiers@dai.com
Deadline for Receipt of Proposals	April 27, 2023, 5pm EST time, to DigitalFrontiers@dai.com
Point of Contact	DigitalFrontiers@dai.com
Anticipated Award Type	For individuals: Independent Consultant Agreement For companies: Time and Materials or Cost Reimbursable contract
Basis for Award	An award will be made based on the **Trade Off Method**. The award will be issued to the responsible and reasonable offeror who provides the best value to DAI and its client using a combination of technical and cost/price factors.

1. Introduction and Purpose

1.1 Purpose

DAI, the implementer of the USAID-funded Digital Frontiers program, invites qualified offerors to submit proposals to support the Promoting American Approaches to ICT Policy and Regulation (ProICT) activity, for which DAI is seeking firm, advisor, or team of advisors, to support the Caribbean Community (CARICOM) Secretariat with technical expertise to accelerate the development of a regional Cyber Resilience Strategy. Proposals will be accepted from organizations/firms or from independent consultants.

1.2 Issuing Office

The Issuing Office and Contact Person noted in the above synopsis is the sole point of contact at DAI for purposes of this RFP. Any prospective offeror who fails to register their interest with DigitalFrontiers@dai.com assumes complete responsibility if they do not receive direct communications (amendments, answers to questions, etc.) prior to the closing date.

1.3 Type of Award Anticipated

DAI anticipates awarding a Time and Materials, Cost Reimbursable, or Independent Consultant contract. The contracting mechanism applied is subject to change during negotiations.

A Time and Materials Contract is: An award that allows the acquisition of supplies or services based on direct labor and materials at cost. It has two primary components: Labor (Time) and Non-labor (Materials).

A Cost Reimbursable Contract is: An award where the contractor is reimbursed for actual reasonable, allowable, and allocable costs up to a maximum ceiling value of the contract agreement.

If an individual (or group of individuals) is selected, DAI anticipates awarding Independent Consultant Agreement(s) (ICA). An ICA is an award where the consultant is reimbursed for actual labor and non-labor costs up to a maximum ceiling value of the ICA.

2. General Instructions to Offerors

2.1 General Instructions

"Offeror," "Contractor," and/or "Bidder" means a firm proposing the work under this RFP. "Offer" and/or "Proposal" means the package of documents the firm submits to propose the work.

Offerors wishing to respond to this RFP must submit proposals, in English, in accordance with the following instructions. Offerors are required to review all instructions and specifications contained in this RFP. Failure to do so will be at the Offeror's risk. If the solicitation is amended, then all terms and conditions not modified in the amendment shall remain unchanged.

Issuance of this RFP in no way obligates DAI to award a contract or purchase order. Offerors will not be reimbursed for any costs associated with the preparation or submission of their proposal. DAI shall in no case be responsible for or liable for these costs.

Proposals are due no later than **April 27, 2023 at 5pm EST**, to be submitted via email to **DigitalFrontiers@dai.com**. Please include the RFP number (**2023-05**) in the subject line of the email. Late offers will be rejected except under extraordinary circumstances at DAI's discretion. Technical proposals are limited to **three (3) to five (5) pages.**

The submission to DAI of a proposal in response to this RFP will constitute an offer and indicates the Offeror's agreement to the terms and conditions in this RFP and any attachments hereto. DAI reserves the right not to evaluate a non-responsive or incomplete proposal.

2.2 Proposal Cover Letter

A cover letter shall be included with the proposal on the Offeror's company letterhead with a duly authorized signature using Attachment B as a template for the format. The cover letter shall include the following items:

- The Offeror will certify a validity period of **90 days** for the prices provided.
- Acknowledge the solicitation amendments received.

2.3 Questions Regarding the RFP

Each Offeror is responsible for reading and complying with the terms and conditions of this RFP. Requests for clarification or additional information must be submitted in writing via email to DigitalFrontiers@dai.com by **April 06, 2023 at 5pm EST time**. No questions will be answered by phone. Any verbal information received from a DAI or Digital Frontiers employee or other entity shall not be considered as an official response to any question regarding this RFP. Copies of questions and responses will be distributed via email to all prospective bidders who are on record as having received this RFP after the submission date specified in the Synopsis above.

3. Instructions for the Preparation of Technical Proposals

Technical proposals shall be in a separate attachment from cost proposals and shall be clearly labeled as "VOLUME I: TECHNICAL PROPOSAL". Technical proposals are limited to **three (3) to five (5) pages**, excluding personnel CVs, past performance matrix, and cover letter.

Technical proposals shall include the following contents:

1. **Technical Approach**
   - Narrative summary of consultant/firm's technical approach to the Scope of Work in Attachment A, proposing a methodology for the implementation of the three (3) overarching tasks and demonstration of offeror's technical capabilities and qualifications to implement the Scope of Work. Required technical capabilities are indicated in the SOW.

2. **Management Approach**
   - Proposed implementation and management approach of SOW activities. If multiple consultants are proposed for one position, Offeror must indicate how the consultants will work together to deliver the SOW.
   - A workplan (in Gantt chart format) that outlines how the consultant / firm will approach and achieve the milestones in the specified timeframe.

3. **Past Performance**
   - Past Performance Matrix per the template in Attachment E. The matrix should include a list of at least three (3) recent projects. The information shall include the legal name and address of the organization for which services were performed, a description of work performed, the duration of the work and the value of the contract, and a current contact phone number of a responsible and knowledgeable representative of the organization. This information may be used for validation of experience or reference checks.

4. **Personnel Qualifications**
   - Narrative summary of consultant(s)' technical capabilities, demonstrating that the Offeror is qualified to implement the SOW for the desired position(s).
   - CV(s) of key named personnel that demonstrate relevant qualifications for the SOW. Required qualifications for each position are indicated in the SOW.

3.1 Services Specified

For this RFP, DAI is in need of the services described in Attachment A.

3.2 Technical Evaluation Criteria

All proposals that meet the proposal requirements will be reviewed by the review panel. The proposals will be evaluated according to the evaluation criteria set forth below. To the extent necessary (if an award is not made based on initial proposals), negotiations may be conducted with each applicant whose application, after discussion and negotiation, has a reasonable chance of being selected for the award. **Award will be made to responsible Offerors whose proposals offer the best value**.

Awards will be made based on the ranking of proposals by the review panel according to the evaluation criteria and scoring system identified below:

Evaluation Criteria	Evaluation Sub-criteria	Maximum Points
Technical Approach	1. Technical approach is responsive to the specific needs of each of the three (3) identified activities and related to them tasks and deliverables. 2. Proposed approach demonstrates understanding and ability to provide necessary support identified in the SoW. 3. Proposed deliverables respect the minimum technical specifications as specified in the SoW.	10 points
Management Approach	1. Management plan details an efficient and comprehensive oversight plan that ensures quality control and responsiveness to client needs. 2. A workplan that demonstrates how the consultant(s)/firm will approach and achieve the work in the required timeframe. 3. Narrative summary of Offeror's technical capabilities and proposed management plan demonstrate the ability to coordinate USG and DAI efforts while completing the scope of work.	6 points
Past Performance	1. At least 3 past relevant project examples in past performance matrix demonstrating capabilities to deliver services requested by the SOW;	12 points
Personnel Qualifications	1. Narrative summary of consultant(s)' technical capabilities demonstrating the ability to complete the scope of work. This summary includes a management plan with named personnel within the 3-5-page limit. 2. CVs of key named personnel that include relevant qualifications for selected position(s) the SOW. Proposed personnel demonstrate at least 5 years of experience working on policy issues in the telecommunications and ICT sector, and relevant experience in telecommunications policy development and implementation; direct work experience in cybersecurity policy and management is highly preferable. 3. Experience working in the CARICOM region strongly preferred; 4. Advanced degree in economics, business, law, engineering, computer science, public policy, cybersecurity, or related field 5. Proposed personnel possess excellent written and oral communication skills in English.	12 points
	Total Points	40 points

4. Instructions for the Preparation of Cost Proposals

4.1 Cost Proposals

Cost proposals shall be in a separate attachment from technical proposals and shall be clearly labeled as "VOLUME II: COST PROPOSAL".

Per 2 CFR 700.13, for-profit Offerors must exclude profit from cost proposals. Offerors should use their previous experience and knowledge to inform a cost proposal that reflecting unit prices reasonable for the local market. The

final number and type of events will be determined during the convening design phase of the scope of work. A variety of convenings (sizes, lengths, and virtual and in-person) should be included in costs.

Provided in Attachment C is a template for the cost proposal. Offerors shall complete the template including as much detailed information as possible. The Contractor is responsible for all applicable taxes and fees, as prescribed under the applicable laws for income, compensation, permits, licenses, and other taxes and fees due as required.

4.2 Budget Narrative

The budget must have an accompanying budget narrative and justification that provides in detail the estimated costs for implementation of the SOW in Attachment A. The combination of the cost data and narrative must be sufficient to allow a determination of whether the costs estimated are reasonable. A budget narrative template is included in Attachment C.

5. Basis of Award

5.1 Best Value Determination

DAI will review all proposals, and make an award based on the technical and cost evaluation criteria stated above and select the offeror whose proposal provides the best value to DAI. DAI may also exclude an offer from consideration if it determines that an Offeror is "not responsible", i.e., that it does not have the management and financial capabilities required to perform the work required.

Evaluation points will not be awarded for cost. Cost will primarily be evaluated for realism and reasonableness. DAI may award to a higher priced offeror if a determination is made that the higher technical evaluation of that offeror merits the additional cost/price.

DAI may award to an Offeror without discussions. Therefore, the initial offer **must contain the Offeror's best price and technical terms.**

5.2 Responsibility Determination

DAI will not enter into any type of agreement with an Offeror prior to ensuring the Offeror's responsibility. When assessing an Offeror's responsibility, the following factors are taken into consideration:

1. Evidence of a UEI number, CAGE/NCAGE code, and SAM.gov registration (explained below and instructions contained in Attachment D).
2. The source, origin and nationality of the products or services are not from a Prohibited Country (explained below).
3. Offeror has adequate financial resources to finance and perform the work or deliver goods or the ability to obtain financial resources without receiving advance funds from DAI.
4. Ability to comply with required or proposed delivery or performance schedules.
5. A satisfactory past performance record.
6. A satisfactory record of integrity and business ethics.
7. Offeror has the necessary organization, experience, accounting and operational controls and technical skills.
8. Is qualified and eligible to perform work under applicable laws and regulations.

6. Inspection & Acceptance

The designated DAI Project Manager will inspect from time to time the services being performed to determine whether the activities are being performed in a satisfactory manner, and that all equipment or supplies are of acceptable quality and standards. The contractor shall be responsible for any countermeasures or corrective action, within the scope of this RFP, which may be required by the DAI Project Director as a result of such inspection.

7. Compliance with Terms and Conditions

7.1 General Terms and Conditions

Offerors agree to comply with the general terms and conditions for an award resulting from this RFP. The selected Offeror shall comply with all Representations and Certifications of Compliance listed in Attachment F.

7.2 Prohibited Technology

Offerors MUST NOT provide any goods and/or services that utilize telecommunications and video surveillance products from the following companies: Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company, or any subsidiary or affiliate thereof, in compliance with 2 CFR 200.216.

7.3 Source and Nationality

DAI must verify the source and nationality of goods and services and ensure (to the fullest extent possible) that DAI does not procure any goods or services from prohibited countries listed by the Office of Foreign Assets Control (OFAC) as sanctioned countries. OFAC sanctioned countries may be searched within the System for Award Management (SAM) at www.SAM.gov. The current list of countries under comprehensive sanctions include: Cuba, Iran, North Korea, Sudan, and Syria. Goods may not transit through or be assembled in comprehensive sanctioned origin or nationality countries nor can the vendor be owned or controlled by a prohibited country. DAI is prohibited from facilitating any transaction by a third party if that transaction would be prohibited if performed by DAI.

By submitting a proposal in response to this RFP, Offerors confirm that they are not violating the Source and Nationality requirements of the goods or services being offered and that the goods and services comply with the exclusions for prohibited countries outlined above.

Under the authorized geographic code for its agreement DAI may only procure goods and services from the following countries. DAI has the option to seek a waiver to these requirements if selected Offeror is registered in a country outside of Geographic Code 937.

Geographic Code 937: Goods and services from the United States, the cooperating country, and "Developing Countries" other than "Advanced Developing Countries: excluding prohibited countries. A list of the "Developing Countries" as well as "Advanced Developing Countries" can be found at: *http://www.usaid.gov/policy/ads/300/310maa.pdf* and *http://www.usaid.gov/policy/ads/300/310mab.pdf* respectively.

7.4 US Government Registrations

There is a **mandatory** requirement for your organization to provide evidence of the following registrations to DAI prior to being awarded an agreement. Without registering in the required databases, DAI cannot deem an Offeror "responsible" to conduct business with and therefore, DAI will not enter into a contract or monetary agreement with any organization. The determination of a successful offeror/applicant resulting from this RFP is contingent upon the winner providing a UEI number, CAGE/NCAGE Code, and evidence of SAM.gov registration to DAI. Offerors who fail to provide these will not receive an award and DAI will select an alternate Offeror.

- Offerors need to obtain the following before award of an agreement:
  - UEI Number
  - Registration with SAM
  - CAGE/NCAGE

For detailed information on registration in the above USG databases, see Attachment D - Instructions for Obtaining CAGE/NCAGE Code, SAM Registration, and UEI Number.

Restricted/Sanctioned Groups or Individuals

U.S. Executive Orders and U.S. law prohibit transactions with, and the provisions of resources and support to, individuals and organizations associated with terrorism. These requirements apply to Vendor/Subcontractor. No material support or resources may be provided to individuals or entities that appear on the following lists[1]:

a. Office of Foreign Assets Control (OFAC) (Department of Treasury) Sanctions List: https://sanctionssearch.ofac.treas.gov/

b. OFAC's List of Specially Designated Nationals (SDN) and Blocked Persons, and the database formerly known as EPLS, now searchable at www.sam.gov

c. Consolidated United Nations Security Council Sanctions List, available at https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

The term "material support" includes "any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, and transportation, except medicine or religious materials."
Please note that the following are included in the list of sanctioned entities:

- Fuerzas Armadas Revolucionarias de Colombia (FARC)
- FARC Communes/Political Party
- The National Liberation Army (ELN) (Colombia and Venezuela)
- Shining Path (SL) (Peru)

Further information is available at:
https://www.state.gov/j/ct/rls/other/des/122570.htm
https://www.treasury.gov/resource-center/sanctions/Programs/Documents/terror.pdf

7.5 Fly America Act

The contractor must comply with Fly America Act restrictions for all international travel under this award. See Attachment G for the mandatory standard provision regarding international air travel.

8. Procurement Ethics

Neither payment nor preference shall be made by either the Offeror, or by any DAI staff, in an attempt to affect the results of the award. DAI treats all reports of possible fraud/abuse very seriously. Acts of fraud or corruption will not be tolerated, and DAI employees and/or contractors/subgrantees/vendors who engage in such activities will face serious consequences. Any such practice constitutes an unethical, illegal, and corrupt practice and either the Offeror or the DAI staff may report violations to DAI's Ethics Hotline at +1-503-597-4328, Ethics@dai.com, or www.dai.ethicspoint.com. DAI ensures anonymity and an unbiased, serious review and treatment of the information provided. Such practice may result in the cancellation of the procurement and disqualification of the Offeror's participation in this, and future, procurements. Violators will be reported to USAID, and as a result, may be reported to the U.S. Department of Justice to be included in a Restricted Parties list, preventing them from participating in future U.S. Government business.

Offerors must provide full, accurate and complete information in response to this solicitation. The penalty for materially false responses is prescribed in Section 1001 of Title 18 of the United States Code.

In addition, DAI takes the payment of USAID funds to pay Terrorists, or groups supporting Terrorists, or other parties in exchange for protection very seriously. Should the Terrorist, groups or other parties attempt to extort/demand payment from your organization you are asked to immediately report the incident to DAI's Ethics and Compliance Anonymous Hotline at the contacts described in this clause.

By submitting an offeror, offerors certify that they have not/will not attempt to bribe or make any payments to DAI employees in return for preference, nor have any payments with Terrorists, or groups supporting Terrorists, been attempted.

9. Attachments

9.1 Attachment A: Scope of Work for Services

ProICT: Development of CARICOM Cyber Resilience Strategy

Digital Frontiers implements USAID's Promoting American Approaches to ICT Policy and Regulation (ProICT) program activity. As part of the Digital Connectivity and Cybersecurity Partnership (DCCP), ProICT is designed to fund intensive, dedicated policy engagements to help countries adopt American models of telecommunications, internet, and ICT regulation, including promoting:

- Open, interoperable, reliable, and secure internet and communications networks;
- Multi-stakeholder models of internet governance;
- Pro-competitive and pro-investment spectrum, telecommunications infrastructure, and regulatory policies;
- Effective approaches to advancing cybersecurity frameworks, supply chain policies, and regulation of communications networks.

ProICT is implemented in coordination with the USAID Technology Division in the Bureau for Development, Democracy, and Innovation (DDI). ProICT can implement activities together with the Department of State, USAID Missions, and other USG agencies.

By issuing this Scope of Work, ProICT is seeking a firm, an advisor, or team of advisors to support the Caribbean Community (CARICOM) Secretariat with technical expertise to accelerate the development of a regional Cyber Resilience Strategy.

1. BACKGROUND

The Regional Context

Over the last decade, digitalization has grown exponentially worldwide, facilitating exchange of services, commerce, and information. Despite the numerous benefits that accompany this process, there are inherent risks, including an increased risk of disruptive cyberattacks, increased cybercrime, and malicious surveillance. Cybersecurity vulnerabilities represent significant threats to governments, businesses, organizations, and individuals, and carry significant legal, financial, and reputational risks. Among other dangers, cyberattacks can reveal personally identifiable information or disrupt critical services upon which societies depend.

Recent years have seen a significant surge in cyberattacks on both public and private institutions throughout the Caribbean and Latin America. For example, in 2016, hackers were able to penetrate the Bahamas Corporate Registry and unlawfully publish 1.3 million files containing data on over 175,000 Bahamian companies, trusts, and foundations. It is likely that a significant number of cyberattacks are not reported by targeted institutions because of perceived reputational damage or even a lack of capacity to either detect or to fully understand the nature and extent of the attacks themselves.

Although CARICOM countries generally recognize the import of these dangers, too few have yet developed comprehensive strategies, laws and regulations as a form of response. At present, Trinidad and Tobago and Jamaica are outliers as the only countries in the region with cybercrime legislation and cybersecurity strategies in place, while the Bahamas, Barbados, Saint Lucia, Dominica, Haiti, and Suriname are currently in the process of developing national cybersecurity strategies.

Even as the formulation, adoption, and implementation of these national strategies proceeds at a deliberate pace, capacity issues present a significant challenge; the region grapples with a lack of ICT skills and both the human and organizational capacity needed to implement these strategies with a reasonable degree of effectiveness.

Regional Response

In order to develop a regional approach to address these challenges, a number of regional stakeholders have been working together to establish a commitment to action. Examples include:

- In 2016, CARICOM Implementation Agency for Crime and Security (IMPACS), spearheaded the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) in partnership with the Caribbean Telecommunications Union (CTU), the Commonwealth Secretariat, and the Organization of American States Inter-American Committee against Terrorism (OAS/CICTE)[1]. This Action Plan includes five key areas of interventions: (1) increasing public awareness (cyber hygiene); (2) developing long-term cyber capacity; (3) investing in critical infrastructure and setting technical standards; (4) creating a legal environment that can prosecute cybercrime; and (5) enabling regional and international coordination for knowledge sharing around incident response, cybercrime investigation, and capacity building;
- CARICOM Secretariat has a mandate to play a lead role in establishing a *Single ICT Space*, with the goal of providing the ICT-enabled foundation for enhancing both CARICOM's functional cooperation and fulfilling the social, cultural, and economic imperatives of the region. In general, the Space will be characterized by: (1) Regionally harmonized ICT policy, legal and regulatory regimes; (2) Robust national and regional broadband infrastructure; (3) Common frameworks for Governments, ICT service providers and consumers; and (4) Effective, secure technology and management systems. Importantly, cybersecurity is one of the pillars of the CARICOM Single ICT Space;

In 2019, the CARICOM Council on Trade and Economic Development (COTED) agreed that the region should develop a Cyber Resilience Strategy 2030 (CRS 2030)[2]. Required elements of CRS 2030 include:

- Cooperation. For cybersecurity initiatives to be successful, it is essential that there is formal and sustained cooperation and partnership between all related international and regional public sector cybersecurity stakeholders, as well as private sector, civil society, the Internet technical community, academia, and others.
- Information-sharing. There is a dearth of statistics on cybercrime in the CARICOM region. If the region is to successfully counter and prevent cybercrime, relevant agencies will require mandate and resources to collect, share and analyze data on cybercrimes – both at the national and regional level.
- Collaborative development of cybersecurity policy and implementation. No single existing ministry can claim a comprehensive understanding and sufficiently wide authority to manage all facets of cybersecurity. Thus, coordination among all the relevant bodies is essential;
- Capacity building and awareness. Given the vital role of ICT to each Member State and with the ever-present 'build out' of digital assets across government and the added requirement to assure citizens of protection in the cyber world. Also the need to determine the personnel needs of the sector;
- Clear lines of authority and accountability. Defined roles and responsibilities of Ministries of Security and ICT in national and regional coordinating mechanisms (e.g. Regional steering Committee or working group);
- Formation of National CIRTS / CERTS with a view towards developing a CIRT/CERT with overarching regional purview.

The objective of the *ProICT CARICOM Cybersecurity Resilience Support Activity* will be to inform and accelerate the development of a CARICOM Cyber Resilience Strategy 2030 through a series of critical analyses, stakeholder coordination exercises, and the development of a Draft Strategy document.

---

[1] CARICOM Cyber Security and Cybercrime Action Plan

[2] Cyber resilience is the ability to prepare for, respond to, and recover from cyberattacks. It helps an organization protect against cyber risks, defend against, and limit the severity of attacks, and ensure its continued survival despite an attack. Several experts recommend a five-pillar model for building a cyber resilience strategy: prepare, protect, detect, respond, and recover.

2. Activities, Tasks, and Deliverables

Activity 1: Orientation/Work Plan Development/Inception Report

- Consultant(s) will:
    - Meet with relevant contacts from the CARICOM Secretariat to receive background briefing and agree on work plan.
    - Conduct regional coordination stakeholder mapping and outreach:
        - Includes identification and engagement of National Cyber Points of Contact, Regional Cyber Committee members, and other relevant stakeholders that would be critical partners necessary to ensuring the proper uptake and implementation of a regional approach to cybersecurity resilience[3];
- **Deliverable:** Inception Report detailing key background information, proposed revisions to approach, and updated work plan with regional stakeholder map and outreach tracker

Activity 2: Analysis of cyber resiliency landscape in CARICOM region

- Consultant(s) will draft and deliver analysis/analyses (based on desk research and key informant interviews, as appropriate) detailing:
    - *Legal and Regulatory Overview:* Assessment of existing legal and regulatory frameworks among CARICOM members states to identify critical barriers, challenges, and other relevant factors influencing the development and implementation of the Cyber Resilience Strategy 2030;
    - *Regional Cybersecurity Human Capacity and Workforce Development Overview:* Assessment of the cybersecurity talent pool in the CARICOM region. Analysis will include regional benchmarking and will propose recommended interventions for improving the quantity and quality of cybersecurity-focused professionals. Recommendations will include perspectives on how to best facilitate the development of robust cybersecurity curricula and workforce training opportunities with higher education and vocational training institutes (e.g., internship programs with government CSIRTs, relevant ministries, local security forces, CARICOM IMPACS, and private sector organizations that can hire and retain this talent).
    - *Cybersecurity Market Overview:* Estimation of the current and projected market for cybersecurity services, to include priority areas for strategy/policy intervention to accelerate market growth;
- **Deliverable:** Analytical report with overviews of legal and regulatory cybersecurity frameworks, cybersecurity human capacity and workforce development, and cybersecurity market as described above.

Activity 3: Develop a draft Cyber Resilience Strategy 2030 document

- Based on prior analysis, the consultants will deliver a draft *Cyber Resilience Strategy 2030* document to be presented to the CARICOM Secretariat.
- Draft strategy will include:
    - A regional cybersecurity **governance model** to enhance cooperation and collaboration
    - Assessment of the **cybersecurity threat information sharing** space (both formal and informal) and effectiveness of CSIRTS/CERTs, if they exist;[4]
    - **Overview of emerging technologies** to help CARICOM stakeholders to better understand how emerging technologies like AI, IoT, and quantum computing might impact assessments of the future threat landscape;

[3] This would include points of contact from key stakeholders (i.e., CARICOM Secretariat, IMPACS, CPSO, and at least three member states) to participate in the CARICOM Cybersecurity Working Group

[4] Assessment could include administration of a survey to relevant stakeholders to assess the cybersecurity threat information sharing space and determine the effectiveness of CERT/CSIRTs

- Scan/mapping of existing national cybersecurity strategies of CARICOM Member States and other commonwealth Small Island Developing States, with similar market / population size, legislative foundation, and cyber maturity level;
- A detailed overview of **human resource, capacity-building, and technical assistance requirements** for strategy implementation among key stakeholder groups;
- A **framework for engaging national and regional Cyber Points of Contact**, the IMPACS 11th EDF Regional Cyber Committee, and other relevant stakeholders to establish and/or affirm roles and responsibilities and to ensure uptake of the Strategy 2030 plan and related implementation support;
- Recommendations on **priority actions to be undertaken** by CARICOM region and Member States to identify, share information, track and mitigate cyber incidents;
- Recommendations for the **design and implementation of an online space** to help CARICOM Member States to privately report/track cyber incidents.

- **Deliverable:** Draft *Cyber Resilience Strategy 2030* document and draft PowerPoint presentation summarizing the draft *Cyber Resilience Strategy 2030*.

3. Reports

In addition to the written deliverables set forth in Section 3, the consultant(s) will provide project status and updates via:

- Bi-weekly Check Ins: Consultant(s) will participate in a bi-weekly check in to provide an update on their progress, indicating objectives, outcomes, and recommended changes (if any) to the work plan.
- Monthly Reports: Consultant(s) will prepare monthly reports to document and share progress against the areas described above. Monthly reports should include a summary of activities completed, challenges incurred, and suggested changes (if any) to the work plan.
- Final Report: Consultant(s) will prepare a report that summarizes the entire consultancy, with recommendations and other components of the assignment. The report shall contain an executive summary, main body, recommendations, and appropriate attachments (e.g., work plan, list of contacts made, recommended additional contacts, topical reports, and any additional information the consultant believes will add value to the consultancy).

4. Minimum Technical Specifications

- Work Plan: Once work commences, within the first month, the consultant(s) will be asked to submit an updated work plan based on the version submitted during the technical review process which reflects input from initial consultations with relevant USG agencies and project stakeholders. This updated work plan will discuss preliminary findings and/or process impacts and describe how the consultant(s) expects to identify key informants, sources of information, and stakeholders. Additionally, the work plan will include an updated timeline for completion of activities and illustrative performance benchmarks.
- Period of Performance: Initiation in April 2023; **approximately 9 months in duration.**
- Location of Effort: Flexible, with ability to deploy to Georgetown, Guyana on an intermittent basis.
  NOTE: *No travel will be scheduled without first considering global COVID-19 pandemic guidelines and restrictions.*
- Level of Effort: estimated **150 business days.**
- Minimum qualifications for consultant(s):
  - Relevant experience in telecommunications policy development and implementation; direct work experience in cybersecurity policy and management is highly preferable;
  - Ability to travel to CARICOM region member countries required
  - Experience working in the CARICOM region strongly preferred
  - Advanced degree in economics, business, law, engineering, computer science, public policy, cybersecurity, or related field;
  - A minimum of 5 years' experience working on policy issues in the telecommunications and ICT sector.

5. Coordination

Given the complexity of the operating environment, the interdependence of the elements of this activity, and the range of stakeholders engaged on this topic, the consultant(s) will coordinate efforts under a supervisory structure as designated by the USG and DAI. USAID will assign a Project Manager who will collaborate with DAI to coordinate the overall management of the Project in close collaboration with the project Focal Point(s) indicated by the CARICOM Secretariat. If the consultant is composed of a team, a primary point of contact will be assigned. The Focal Point from the CARICOM Secretariat, the USAID-assigned Project Manager, and the consultant contact will work together to prepare Progress Reports (detailed above). Moreover, all consultant experts will coordinate efforts with the following parties:

- One of more points of contact at USAID/Eastern and Southern Caribbean;
- The USAID Innovation, Technology, and Research (ITR) Hub's Digital Inclusion team;
- With and through the ProICT Advisory Council and other USG interagency partners;
- With and through the DAI Digital Frontiers DCCP Project Director Komal Bazaz Smith and/or her designated representatives in the US and/or in-country;
- CARICOM Secretariat and regional organizations and entities.

To ensure that the project remains in line with this interagency coordination process, the consultant will participate in bi-weekly check ins and file monthly reports on progress, activities, actions, and results with DAI Digital Frontiers Project, who will circulate to the ProICT Advisory Council.

At the start of the engagement, USAID and the Department of State will host an orientation briefing with the consultant(s) to coordinate on all relevant issues and policy considerations related to this Scope of Work with all relevant U.S. government agencies and parties.

9.2 Attachment B: Proposal Cover Letter

[On Firm's Letterhead]

<Insert date>

TO: Click here to enter text.

DAI Global, LLC

We, the undersigned, provide the attached proposal in accordance with RFP- 2023-05-Click here to enter text.-Click here to enter text. issued on Click here to enter text. Our attached proposal is for the total price of <Sum in Words ($0.00 Sum in Figures) >.

I certify a validity period of 90 days for the prices provided in the attached Cost Proposal. Our proposal shall be binding upon us subject to the modifications resulting from any discussions.
Offeror shall verify here the items specified in this RFP document.

We understand that DAI is not bound to accept any proposal it receives.

Yours sincerely,

Authorized Signature:
Name and Title of Signatory: Click here to enter text.
Name of Firm: Click here to enter text.
Address: Click here to enter text.
Telephone: Click here to enter text.
Email: Click here to enter text.

9.3 Attachment C: Budget and Budget Narrative Template

	Name	Rate	LOE/Units	Unit Type	Cost
I. Salaries and Wages					
Person 1	TBD	$0.00	0		$0
Person 2	TBD	$0.00	0		$0
Person 3	TBD	$0.00	0		$0
Total Salaries and Wages			0		$0
II. Indirect Costs on Labor					
Fringe (full-time employees)					$0
Overhead on Labor					$0
Total Indirect Costs on Labor					$0
III. Other Direct Costs					
1. Project Management Expenses					
Communications		$0.00	0		$0
Other (DESCRIBE)		$0.00	0		$0
Total Other Direct Costs					$0
Total Program Expenses					$0
Indirect Costs on All Costs			0		$0
Grand Total					$0

Budget Narrative Template

The following narrative follows the format of the budget. *Firm Name* has priced its proposal on a: (specify) Cost Reimbursable or Time and Materials (T&M) basis.

Salaries and Wages

For our labor cost estimates, we have used the daily rates for personnel, as supported by actual salaries and/or prevailing labor rates (please explain and provide justification or backup for rates).

- Name, Title proposed for a total of XX days at a daily rate of $XXX.

- Name, Title proposed for a total of XX days at a daily rate of $XXX.
- Name, Title proposed for a total of XX days at a daily rate of $XXX.
- Name, Title proposed for a total of XX days at a daily rate of $XXX.

Level of Effort (LoE) allocations should be accompanied with brief technical justifications describing each position's roles and responsibilities (and requisite LoE) for each of the Tasks outlined in Attachment A.

Other Direct Costs

This category includes basic support costs for the project such as XXXX (Explain and provide backup for costs). Included within this cost category are all costs necessary for the successful operation of this activity.

Offerors should use their previous experience and knowledge to recommend the number of convenings within the budget. A variety of convenings (sizes, lengths, and virtual verse in-person) should be included in costs.

Indirect Costs on All Costs

All indirect costs must be in accordance with the Firm's policies (explain and provide justification). Per 2 CFR 700.13, for-profit Offerors must exclude profit from cost proposals.

9.4 Attachment D: Instructions for Obtaining a CAGE/NCAGE Code, SAM Registration, and UEI Number

Background: Summary of Current U.S. Government Requirements

There are mandatory requirements for Contractors to obtain the following items/registration before a contract of any kind can be awarded. Without registering in the required databases, DAI cannot deem an Offeror to be "responsible" to conduct business with and therefore, DAI will not enter into an agreement with any such organization. The award of a contract resulting from this RFP is contingent upon the winner providing a UEI, a CAGE/NCAGE code, and proof of registration in the SAM.gov system. Organizations who fail to provide these will not receive an agreement and DAI will select an alternate Offeror.

CAGE/NCAGE Code

The Commercial and Government Entity (CAGE) Code was established by the US. The NATO Codification System developed the NATO Commercial and Government Entity (NCAGE) Code. When a business/organization is assigned a CAGE/NCAGE, they are in fact the same type/structure of code but identifies which nation or if the NATO Support Agency assigned the CAGE/NCAGE. You must have a CAGE/NCAGE code before registering in SAM.

- o Link to the CAGE/NCAGE Code request:

  https://eportal.nspa.nato.int/AC135Public/scage/CageList.aspx

- o Link to CAGE/NCAGE code request instructions:

  https://eportal.nspa.nato.int/AC135Public/Docs/US%20Instructions%20for%20NSPA%2 0NCAGE.pdf

System for Award Management (SAM) Registration

You must have an active registration with www.SAM.gov to do business with the Federal Government. To register in SAM, at a minimum, you will need the following information:

- o U.S. Registrants:

  1) Your Legal Business Name and Physical Address

  2) Your Taxpayer Identification Number (TIN) and Taxpayer Name associated with your TIN; Review your tax documents from the IRS (such as a 1099 or W-2 form) to find your Taxpayer Name

  3) Your bank's routing number, your bank account number, and your bank account type, i.e. checking or savings, to set up Electronic Funds Transfer (EFT)

- o International Registrants:

  1) Your NATO Commercial and Government Entity (NCAGE) Code

Follow this link to create a Sam.gov user account and register your organization:

https://sam.gov/content/entityregistration

Unique Entity ID (UEI)

Effective April 4, 2022, the federal government transition away from the DUNS Number to the Unique Entity ID (SAM), or 'UEI', for entity identification of federal awards government-wide. Entity identification in federal awards (grants, loans, contracts, etc.) means a unique set of numbers and letters used to identify every entity seeking to do business with the federal government. Each awardee will be required to obtain a Unique Entity ID (UEID) via sam.gov. Below are some helpful tips on how an organization can obtain the UEID.

1. Obtaining a UEID and registering as an entity are two different processes. Obtaining a UEID is quicker and requires a less intensive validation process. A NCAGE code is not needed for entity validation and to get a UEID, but it is needed for full registration in SAM.

2. For new entities:
a. Prior to starting entity validation process, an entity should be prepared with documents that:
i. shows the entity's legal business name and physical address in the same document and is less than 5 years old;
ii. shows the legal business name and start year in the same document, and;
iii. shows legal business name and US state of Incorporation (for US entities) or National Identifier (for non-US entities). If any documents are in a language other than English, they must be accompanied by certified translations (see the link below for more details).
b. This GSA guide has detail on documentation requirements. It includes a downloadable document outlining what type of documentation is acceptable, general guidelines, and guidance on translations.
c. Additionally there is a general FAQ also maintained by GSA.

3. If, after entering the required information, an entity receives a validation error message and/or is not a match with any of the returned potential matches, the entity should create an incident. There are two new, useful videos that GSA has recently published to help explain this process. These are different than the brief overview video that has been previously shared, so projects and partners are encouraged to watch:

a. This video provides a detailed, step-by-step walk through of the entity validation process. Be advised the scenario it addresses is for an existing entity that has to update some information (rather than a new entity, which is the case for most of our partners), but the steps are the same: https://www.youtube.com/watch?v=ZKc9UfxtOIA (the "create incident portion" runs from 27:58 to 35:05).

b. This video provides guidance on how to manage the validation ticket once it has been submitted: https://www.youtube.com/watch?v=a3nPZvnPpE0 (the "managing your validation ticket" portion runs from 17:34 to 28:55).

4. Entities need to regularly check their email – including spam folders – after they have submitted the incident report for emails from fsdsupport@gsa.gov. They should be able to look up the status either by logging into their user account on SAM.gov (go to the "Workspace" view and click the "View" button under the Incident Report Number) or in fsd.gov (directions on how to do this can be found here). Entities can communicate with an EVS (Entity Validation System) agent in FSD.gov or by responding to the email. If the entity is unable to generate an incident report for some reason (this was a problem we saw this past week), the entity can also go to FSD.gov and start a chat with an agent by clicking on the "live chat" button in the lower right-hand corner. Agents are available from 8AM to 8PM EST.

5. Once they are contacted by the EVS agent, the entity will have 5 days to respond, or the incident report will be automatically closed and they will have to start again. If the entity needs more time, they should respond to the EVS agent and communicate this. If the ticket is closed, when the entity starts a new one they should include the original ticket number in the Comments Section.

6. Requested documents need to be uploaded at sam.gov, not at fsd.gov.

7. Once the FSD agent has confirmed the entity has been validated, the entity is not done! It will need to go back to SAM.gov to enter its information again and select the current, correct entity info. This step must be done in order to generate the UEID.

9.5 Attachment E: Past Performance Table Template

Include projects that best illustrate your work experience relevant to this RFP, sorted by decreasing order of completion date.

Projects should have been undertaken in the past three years. Projects undertaken in the past six years may be taken into consideration at the discretion of the evaluation committee.

#	Project Title	Description of Activities	Reference(s) Name, email and/or phone	Client Name and Address	Cost in US$	Start-End Dates	Problem(s) Encountered and Resolutions
1							
2							
3							
4							
5							

9.6 Attachment F: Representations and Certifications of Compliance

1. Federal Excluded Parties List - The Bidder Select is not presently debarred, suspended, or determined ineligible for an award of a contract by any Federal agency.

2. Executive Compensation Certification- FAR 52.204-10 requires DAI, as prime contractor of U.S. federal government contracts, to report compensation levels of the five most highly compensated subcontractor executives to the Federal Funding Accountability and Transparency Act Sub-Award Report System (FSRS)

3. Executive Order on Terrorism Financing- The Contractor is reminded that U.S. Executive Orders and U.S. law prohibits transactions with, and the provision of resources and support to, individuals and organizations associated with terrorism. It is the legal responsibility of the Contractor/Recipient to ensure compliance with these Executive Orders and laws. Recipients may not engage with, or provide resources or support to, individuals and organizations associated with terrorism. No support or resources may be provided to individuals or entities that appear on the Specially Designated Nationals and Blocked persons List maintained by the US Treasury (online at www.SAM.gov) or the United Nations Security Designation List (online at: http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml). This provision must be included in all subcontracts/sub awards issued under this Contract.

4. Trafficking of Persons – The Contractor may not traffic in persons (as defined in the Protocol to Prevent, Suppress, and Punish Trafficking of persons, especially Women and Children, supplementing the UN Convention against Transnational Organized Crime), procure commercial sex, and use forced labor during the period of this award.

5. Certification and Disclosure Regarding Payment to Influence Certain Federal Transactions – The Bidder certifies that it currently is and will remain in compliance with FAR 52.203-11, Certification and Disclosure Regarding Payment to Influence Certain Federal Transactions.

6. Organizational Conflict of Interest – The Bidder certifies that will comply FAR Part 9.5, Organizational Conflict of Interest. The Bidder certifies that is not aware of any information bearing on the existence of any potential organizational conflict of interest. The Bidder further certifies that if the Bidder becomes aware of information bearing on whether a potential conflict may exist, that Bidder shall immediately provide DAII with a disclosure statement describing this information.

7. Business Size and Classification(s) – The Bidder certifies that is has accurately and completely identified its business size and classification(s) herein in accordance with the definitions and requirements set forth in FAR Part 19, Small Business Programs.

8. Prohibition of Segregated Facilities - The Bidder certifies that it is compliant with FAR 52.222-21, Prohibition of Segregated Facilities.

9. Equal Opportunity – The Bidder certifies that it does not discriminate against any employee or applicant for employment because of age, sex, religion, handicap, race, creed, color or national origin.

10. Labor Laws – The Bidder certifies that it is in compliance with all labor laws..

11. Federal Acquisition Regulation (FAR) – The Bidder certifies that it is familiar with the Federal Acquisition Regulation (FAR) and is in not in violation of any certifications required in the applicable clauses of the FAR, including but not limited to certifications regarding lobbying, kickbacks, equal employment opportunity, affirmation action, and payments to influence Federal transactions.

12. Employee Compliance – The Bidder warrants that it will require all employees, entities and individuals providing services in connection with the performance of an DAI Purchase Order to comply with the provisions of the resulting Purchase Order and with all Federal, State, and local laws and regulations in connection with the work associated therein.

By submitting a proposal, offerors agree to fully comply with the terms and conditions above and all applicable U.S. federal government clauses included herein, and will be asked to sign these Representations and Certifications upon award.

9.7 Attachment G: Travel and International Air Transportation

TRAVEL AND INTERNATIONAL AIR TRANSPORTATION (DECEMBER 2014)

a. TRAVEL COSTS

All travel costs must comply with the applicable cost principles and must be consistent with those normally allowed in like circumstances in the recipient's non-USAID-funded activities. Costs incurred by employees and officers for travel, including air fare, costs of lodging, other subsistence, and incidental expenses, may be considered reasonable and allowable only to the extent such costs do not exceed reasonable charges normally allowed by the recipient in its regular operations as the result of the recipient organization's written travel policy and are within the limits established by the applicable cost principles.

In the absence of a reasonable written policy regarding international travel costs, the standard for determining the reasonableness of reimbursement for international travel costs will be the Standardized Regulations (Government Civilians, Foreign Areas), published by the U.S. Department of State, as from time to time amended. The most current Standardized Regulations on international travel costs may be obtained from the AO. In the event that the cost for air fare exceeds the customary standard commercial airfare (coach or equivalent) or the lowest commercial discount airfare, the recipient must document one of the allowable exceptions from the applicable cost principles.

b. FLY AMERICA ACT RESTRICTIONS

(1) The recipient must use U.S. Flag Air Carriers for all international air transportation (including personal effects) funded by this award pursuant to the Fly America Act and its implementing regulations to the extent service by such carriers is available.

(2) In the event that the recipient selects a carrier other than a U.S. Flag Air Carrier for international air transportation, in order for the costs of such international air transportation to be allowable, the recipient must document such transportation in accordance with this provision and maintain such documentation pursuant to the Standard Provision, "Accounting, Audit and Records." The documentation must use one of the following reasons or other exception under the Fly America Act:

(i) The recipient uses a European Union (EU) flag air carrier, which is an airline operating from an EU country that has signed the US-EU "Open Skies" agreement (http://www.state.gov/e/eb/rls/othr/ata/i/ic/170684.htm).

(ii) Travel to or from one of the following countries on an airline of that country when no city pair fare is in effect for that leg (see http://apps.fas.gsa.gov/citypairs/search/):

a. Australia on an Australian airline,
b. Switzerland on a Swiss airline, or
c. Japan on a Japanese airline;

(iii) Only for a particular leg of a route on which no US Flag Air Carrier provides service on that route;

(iv) For a trip of 3 hours or less, the use of a US Flag Air Carrier at least doubles the travel time;

(v) If the US Flag Air Carrier offers direct service, use of the US Flag Air Carrier would increase the travel time by more than 24 hours; or

(vi) If the US Flag Air Carrier does not offer direct service,

a. Use of the US Flag Air Carrier increases the number of aircraft changes by 2 or more,

b. Use of the US Flag Air Carrier extends travel time by 6 hours or more, or
c. Use of the US Flag Air Carrier requires a layover at an overseas interchange of 4 hours or more.

c. DEFINITIONS

The terms used in this provision have the following meanings:

(1) “Travel costs’’ means expenses for transportation, lodging, subsistence (meals and incidentals), and related expenses incurred by employees who are on travel status on official business of the recipient for any travel outside the country in which the organization is located. “Travel costs” do not include expenses incurred by employees who are not on official business of the recipient, such as rest and recuperation (R&R) travel offered as part of an employee’s benefits package that are consistent with the recipient’s personnel and travel policies and procedures.

(2) “International air transportation" means international air travel by individuals (and their personal effects) or transportation of cargo by air between a place in the United States and a place outside thereof, or between two places both of which are outside the United States.

(3) "U.S. Flag Air Carrier" means an air carrier on the list issued by the U.S. Department of Transportation at http://ostpxweb.dot.gov/aviation/certific/certlist.htm. U.S. Flag Air Carrier service also includes service provided under a code share agreement with another air carrier when the ticket, or documentation for an electronic ticket, identifies the U.S. flag air carrier’s designator code and flight number.

(4) For this provision, the term “United States” includes the fifty states, Commonwealth of Puerto Rico, possessions of the United States, and the District of Colombia.

9.8 Attachment H: Proposal Checklist

Offeror: _____

Have you?

- ☐ Submitted your proposal to DigitalFrontiers@dai.com as specified in General Instructions above?
- ☐ Submitted Separate Technical and Cost proposal email attachments?

Does your proposal include the following?

- ☐ Signed Cover Letter *(use template in Attachment B)*
- ☐ Technical Proposal not exceeding five (5) pages
- ☐ Past Performance Matrix *(use template in Attachment E)*
- ☐ CVs/bios of Team lead and staff
- ☐ Cost Proposal including budget and budget narrative *(use templates in Attachment C)*