REQUEST FOR EXPRESSIONS OF INTEREST
(CONSULTING SERVICES – FIRMS SELECTION)

COUNTRY – Trinidad and Tobago
OECS Regional Health Project

Loan No. IDA-D5120
Project No.: P168539

Assignment Title: Consultancy to Conduct a Security Audit to Improve the IT capacity at CARPHA to host the DHIS-2 installation

Reference No. TT-CARPHA-227511-CS-CQS

The Caribbean Public Health Agency (CARPHA) has received financing from the World Bank toward the cost of the OECS Regional Health Project and intends to apply part of the proceeds for consulting services.

The consulting services ("the Services") include:

To test and analyze the security system to ensure data collected for the integrated surveillance platform will be secure such that no unauthorized individual or group can access CARPHA's external and internal networks with its main campuses at POS Trinidad connecting to St Lucia and Jamaica.

The detailed Terms of Reference (TOR) for the assignment is attached to this request for expressions of interest. (See Annex A)

The Caribbean Public Health Agency (CARPHA) now invites eligible consulting firms ("Consultants") to indicate their interest in providing the Services. Interested Consultants should provide information demonstrating that they have the required qualifications and relevant experience to perform the Services. The shortlisting criteria are:

- Interested firms must provide experience of having completed at least two (2) contracts similar in scope and nature with sufficient description (including location/country, name of the Employer/Client, type of services provided, period of contract, contract amount, starting and completion dates).
- Availability of appropriate skills/expertise among the consultant's staff to demonstrate technical capability of the firm. The following experts are required for the assignment: **Team Lead, Security Analyst** and **Security Auditor**. The general qualifications, Experience requirements of key staff are provided in the Terms of Reference.
- The consulting firm shall be legally registered by the regulatory authorities and the following documents shall be submitted;

  (i) A certificate of incorporation/registration for the firm.

The attention of interested Consultants is drawn to Section III, paragraphs, 3.14, 3.16, and 3.17 of the World Bank's "Procurement Regulations for IPF Borrowers" July 2016 ("Procurement Regulations"), setting forth the World Bank's policy on conflict of interest. In addition, please refer to the following specific information on conflict of interest related to this assignment (i.e., *3.17 of the Procurement Regulations)*.

Consultants may associate with other firms to enhance their qualifications but should indicate clearly whether the association is in the form of a joint venture and/or a sub-consultancy. In the case of a joint venture, all the partners in the joint venture shall be jointly and severally liable for the entire contract, if selected.

A Consultant will be selected in accordance with the **Consultant Qualification Selection method (CQS)** set out in Procurement Regulation.

Further information can be obtained at the address below during office hours 8:00am to 4:00pm Mondays to Fridays. Expressions of interest must be delivered in a written form to the address below by e-mail by 10th December 2021.

Caribbean Public Health Agency
Kern Cassell – Procurement Officer
16-18 Jamaica Boulevard, Federation Park
Port-of-Spain, Trinidad and Tobago
Tel: 1-868-622-4261
Fax: 1-868-622-2792
E-mail: casselke@carpha.org

Terms of Reference

Activity 2.1.3.3.2.1

Consultancy to Conduct a Security Audit
to Improve the IT capacity at CARPHA
to host the DHIS-2 installation.

1. Background

The Caribbean Public Health Agency (CARPHA) is a regional Institution of the Caribbean Community, formerly established on July 4, 2011 through the ratification of an Inter-Governments Agreement (IGA) by Heads of Member States of CARICOM in January 2013. The Agency is the Caribbean's collective response to addressing public health issues including those related to Communicable and Non-Communicable diseases; mental health, disaster response, injuries and violence and workers health.

In so doing, CARPHA has subsumed the functions of the previous five Regional Health Institutions (RHI) – The Caribbean Epidemiology Centre (CAREC), the Caribbean Food and Nutrition Institute (CFHI), the Caribbean Health Research Council (CHRC), the Caribbean Regional Drug Testing Laboratory (CRDTL) and the Caribbean Environmental Health Institute (CEHI). The agency began operation in January 2013 with Headquarters in Port of Spain Trinidad and offices in Saint Lucia and Jamaica.

CARPHA'S mission is to provide strategic direction, in analysing, defining and responding to public health priorities of Member States to prevent disease promote health and respond to public health emergencies.

To support the operation and implementation of the integrated surveillance strategy, and thereby strengthen CARPHA's and CMS capacity to respond to COVID-19 and other public health emergencies, there is a crucial need to strengthen the data framework for the various systems, as well as to move towards integration of communicable, non-communicable and environmental health disease/condition surveillance systems. Integration of the regional surveillance systems, supported by strengthened data standards and policies, and further enabled by capacity-building within the Agency and its CMS, will ensure a routine consolidated overview of the status of public health in the region and support the detection of, preparedness and response to public health threats and emergencies from the wide range of possible sources. The DHIS2 is one of the tools that will be used as part of the integrated surveillance platform.

DHIS2 is a tool for collection, validation, analysis, and presentation of aggregate and patient-based statistical data, tailored (but not limited) to integrated health information management activities. It is a generic tool rather than a pre-configured database application, with an open meta-data model and a flexible user interface that allows the user to design the contents of a specific information system without the need for programming. DHIS2 is a modular web-based software package built with free and open source Java frameworks.

DHIS2 is open source software released under the BSD license and can be obtained at no cost. It runs on any platform with a Java Runtime Environment (JRE 7 or higher) installed.

DHIS2 is developed by the Health Information Systems Programme (HISP) as an open and globally distributed process with developers currently in India, Vietnam, Tanzania, Ireland, and Norway. The development is coordinated by the University of Oslo with support from NORAD and other donors.

CARPHA implemented the DHIS2 application in 2012 with the implementation of a server at its Port-of-Spain office in Trinidad and Tobago. The application currently is mainly being used internally, however there are plans to expand access to CARPHA Member States.

CARPHA is seeking to engage a Firm to conduct a Security Audit to Improve the IT capacity at CARPHA to host the DHIS-2 installation.

Approved in 2019, the Organisation of Eastern Caribbean States (OECS) Regional Health Project (RHP), is a five (5) year project funded by the World Bank. The overall objective of the project is to (i) improve preparedness capacities of health systems for public health emergencies in the OECS region, and (ii) provide a response in the event of eligible crises or emergencies. The OECS RHP is implemented by four CARPHA member states (Dominica, Grenada, Saint Lucia and Saint Vincent and the Grenadines), CARPHA and the OECS Commission.

The areas of focus revolve around improving International Health Regulations (IHR) core capacities in the areas of surveillance, laboratories, workforce development and emergency management. There are four Components under this project; (i) Improved Health Facilities and Laboratory Capacity, (ii) Public Health Surveillance, Preparedness and Response (iii) Institutional Capacity Building, Project Management and Coordination, and the Contingency Emergency Response Component (CERC) implemented at country level.

The primary functions of this Audit are to evaluate the systems that are in place to guard CARPHA's information under the integrated surveillance platform. The audits will be used to evaluate CARPHA's ability to protect its information assets and to properly dispense information to authorised parties.

This Consultancy is in alignment with Component 2 of the OECS RHP Project, which is representative of the key requirements to support the implementation and coordination of the project.

The project activities under Component 2 supports the IT capacity at CARPHA to host DHIS-2 installation associated with the CARPHA integrated surveillance system.

2. Objective(s) of the Assignment

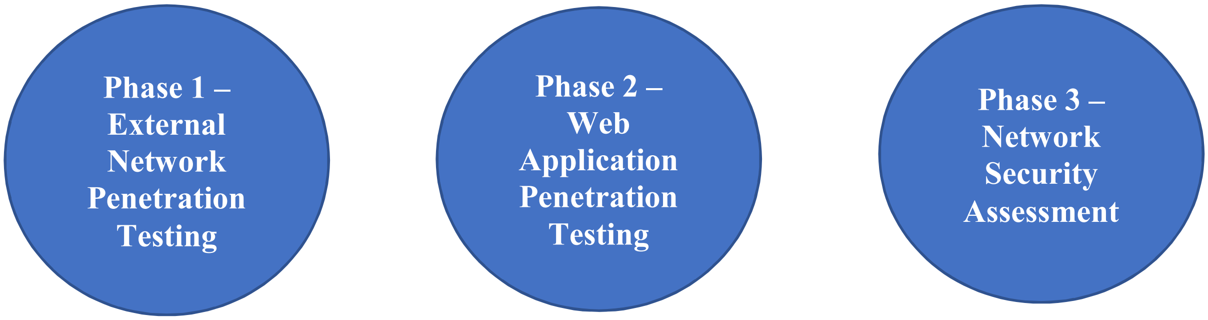
The **objective** of this Assignment is to test and analyze the security system to ensure data collected for the integrated surveillance platform will be secure such that no unauthorized individual or group can access CARPHA's external and internal networks with its main campuses at POS Trinidad connecting to St Lucia and Jamaica.

The **purpose** of this consultancy is to ensure that the requisite elements and commitments are enabled to conduct an Audit of the existing Information Technology infrastructure to host an integrated surveillance platform including, but not limited to the DHIS2 application.

CARPHA is seeking to engage a Firm to perform an Information System audit to assess CARPHA existing security posture by conducting external network penetration testing, web application penetration testing, and network penetration testing.

3. Scope of Services, Tasks (Components) and Expected Deliverables:

The Assignment will be conducted in three independent phases :


Phase 1 – External Network Penetration Testing
Phase 2 – Web Application Penetration Testing
Phase 3 – Network Security Assessment

Each of these phases of this assessment should be considered and itemised as independent modules of the overall evaluation.

Phase 1 - External Network Penetration Test

An external penetration test will be performed on externally available hosts accessible from the internet. Testing during this phase should represent an uninformed anonymous threat targeting the CARPHA external infrastructure. The in-scope infrastructure for CARPHA's external penetration testing phase includes five public-facing application with addresses to be provided. CARPHA assumes the following:

- Identified vulnerabilities will be exploited to demonstrate impact to the organisation except for denial of service (DoS) attacks.
- Heavy load brute force or automated attacks will not be performed.
- The vendor agrees to notify CARPHA of any portion of the assessment resulting in a disruption of service.
- Both parties will sign a mutual non-disclosure agreement to ensure the confidentiality of information exposed and proprietary tools and techniques used during these assessments.
- The vendor will immediately notify CARPHA of any security vulnerability threatening critical business processes or IT services.
- Indicate if software agents will be installed on our devices during the testing period and if/when they will be confirmed as removed.

Phase 2 - Web Application Penetration Test

A web application penetration test provides an independent verification of the security status of an organisation's web application(s). This test determines whether web-based applications (customer, patient, other) present an exploitable risk to the organisation. CARPHA assumes the following:

- Determines if vulnerabilities exist in an application by testing each interface to the application, including server operating system, application platform, and database.
- Denial of Service (DOS) attacks will not be performed.
- Three-phased structure methodology for application penetration testing that includes enumeration, vulnerability assessment, and exploitation.
- Identification of prioritised remediation needs, requirements, and associated risk.

Phase 3 - Network Security Assessment

A network security assessment will be performed in two phases. The initial assessment will be performed to simulate an attack by an untrusted outsider or an unauthenticated user with no working knowledge of CARPHA's network. The second phase of the assessment will be performed with low-level credentials, an authenticated user. This penetration style test should assess the security of all networked assets, including servers, desktops, firewall, network devices, wireless infrastructure and network monitoring & management. Testing during the internal network vulnerability assessment will be performed on CARPHA's corporate office located in Trinidad and Tobago

Additional Information :

Existing Technology Environment :

1. LAN type
2. Server operating system
3. Desktop operating system
4. Development platforms

***** Specific Details on the Technical Environment will be provided upon shortlisting.***

Expected Deliverables Include::

Under the direct supervision of the IT Manager, CARPHA and in collaboration with other project officers, the Firm will be expected to execute the tasks and activities under each of the following Results:

- **Executive Report** of a maximum of 12 pages to be produced after **four (4) weeks** from the start of implementation. In the report, the Firm shall describe the initial findings, including summary of the scope and approach, findings, and recommendations.
- **Technical Report** of maximum of 12 pages to be produced after **six (6) weeks** from the start of implementation. In the report, the Firm will include testing methodology, strengths and weaknesses observed, detailed findings matrix, associated risk ratings of each finding, technical recommendations and appendices providing supporting documentation of each vulnerability identified.
- **Draft Final Report and Findings Presentation** to be submitted no later than **(1)** month before the end of the period of implementation of tasks. Upon the completion of the project, results will be shared via a teleconference call presentation to CARPHA Headquarters management. This presentation should provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.
- **Final report** with the same specifications as the draft final report, incorporating any comments received from the parties on the draft report. The deadline for sending the final report is **seven (7) working days** after receipt of comments on the draft final report. The detailed analyses underpinning the recommendations will be presented in annexes to the main report.

Confidentiality, Copyright and other Proprietary Rights:

i. The Firm shall maintain full confidentiality of all documentation shared and produced during the consultancy. The Firm may not utilize, without prior approval from CARPHA, the information for any purposes external to CARPHA.

4. Team Composition & Qualification Requirements for the Key Experts :

The work requires use of initiative and capacity to work without close supervision, use of judgement, tact, and diplomacy. There is also the need to analyse and respond rapidly for immediate resolution of challenges encountered and issues arisen.

A. Key Expert – Team Lead

Academic Qualifications:

i. An Undergraduate Degree in Computer Science, Software Engineering, Network or Computer Information Systems or Certification levels such as CISSP, HCISPP or SAN Certifications other industry recognized certifications.

Specific Experience:

i. Understanding of Computer Networks

ii. Exposure to and understanding of cryptography, reverse engineering, web applications, databases, and wireless technologies.

iii. Good knowledge of Linux and its security-oriented distributions

General Experience:

i. Experience in working in health care database

ii. Ability to use programming language

   a. Understanding of principles of secure, stable software design.

   b. Understanding of the software development process and lifecycle, including the design-develop-test-release-maintain cycle, and long-term lifecycle support and maintenance.

Languages:

i. Excellent knowledge of English – written and spoken

IT Skills:

i. Knowledge of various computer systems and Computer Network Knowledge programming languages, preferably in-demand ones such as SQL, Java, JavaScript, C# or C++, Python, ZODB object database, PHP, Ruby on Rails, or iOS.

Other requirements:

i. Excellent written and interpersonal communication with meticulous attention to detail.

ii. Excellent organizational, project management, multi-tasking and problem-solving skills

Key Expert - 1: Security Analyst

Academic Qualifications:

i. Undergraduate Degree in Computer Science, Networking, Accounting, Finance or a related field, or sufficient experience in Information Technology auditing, or other field that would provide the same basic knowledge

Specific Experience:

i. Understanding of Computer Networks

ii. Exposure to and understanding of cryptography, reverse engineering, web applications, databases, and wireless technologies.

iii. Good knowledge of Linux and its security-oriented distributions

General Experience:

i. A minimum of four years operational IT audit experience in an environment that provides exposure to complex information systems audit techniques, network security, technology infrastructure, software development, project management, or a related field for which Internal Audit has a need.

ii. Certification as a Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified Public Accountant (CPA), and/or specific to the information technology industry such as a Certified Network Engineer, Certified Security Professional, or other certification for which Internal Audit has a need.

Languages:

i. Excellent knowledge of English – written and spoken

IT Skills:

i. Understanding of concepts related to information systems audit, including security and control risks such as logical and physical access security, change management, information security, business recovery practices and network technology.

ii. Knowledge of various computer systems and Computer Network Knowledge programming languages, preferably in-demand ones such as SQL, Java, JavaScript, C# or C++, Python, ZODB object database, PHP, Ruby on Rails, or iOS.

iii. Strong analytical ability, including network and network systems design, capacity planning, operations methodology, error detection/resolution techniques, quality assurance techniques, and IT implementation and management methodologies.

iv. Knowledge of Control Objectives for Information and Related Technology, Accepted Auditing Standards, Standards for the Professional Practice of Internal Auditing

Other requirements:

iii. Excellent written and interpersonal communication with meticulous attention to detail.

iv. Excellent organizational, project management, multi-tasking and problem-solving skills

B. Key Expert - 2: Security Auditor

Academic Qualifications:

i. Bachelor's degree in Information Technology or, an Information Security related area such as Certification as a Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified Public Accountant (CPA), and/or specific to the information technology industry such as a Certified Network Engineer, Certified Security Professional, or other certification for which Internal Audit has a need.

Specific Experience:

iv. Understanding of Computer Networks

v. Exposure to and understanding of cryptography, reverse engineering, web applications, databases, and wireless technologies.

vi. Good knowledge of Linux and its security-oriented distributions

General Experience:

iii. A minimum of four years operational IT audit experience in an environment that provides exposure to sophisticated information systems audit techniques, network security, technology infrastructure, software development, project management, or a related field for which Internal Audit has a need.

Languages:

ii. Excellent knowledge of English – written and spoken

IT Skills:

v. Understanding of concepts related to information systems audit, including security and control risks such as logical and physical access security, change management, information security, business recovery practices and network technology.

vi. Knowledge of various computer systems and Computer Network Knowledge programming languages, preferably in-demand ones such as SQL, Java, JavaScript, C# or C++, Python, ZODB object database, PHP, Ruby on Rails, or iOS.

vii. Strong analytical ability, including network and network systems design, capacity planning, operations methodology, error detection/resolution techniques, quality assurance techniques, and IT implementation and management methodologies.

viii. Knowledge of Control Objectives for Information and Related Technology, Accepted Auditing Standards, Standards for the Professional Practice of Internal Auditing

Other requirements:

v. Excellent written and interpersonal communication with meticulous attention to detail.

vi. Excellent organizational, project management, multi-tasking and problem-solving skills

** An overview of other supporting members of the Firm's project team to complete CARPHA's technology security assessment should be provided.

5. Reporting Requirements and Time Schedule for Deliverables

This consultancy is expected to commence in January 2022 for a period of three (3) months. Reports will be submitted in electronic format to the ITS Manager, who will be responsible for approving all reports.

Table 2 below gives details of the reports required and the timeline for delivery:

Table 2 : Reports required and Timeline for Delivery

Name of Report	Content	Time of Submission
Executive Report	• Detailed workplan with timelines for completing the consultancy with key milestones and expected deliverables clearly identified	No later than four (4) weeks from the start date of the contract
Technical Report	• Detailed report summarizing the findings of the review of the current system initial findings, issues, challenges, the proposal with the course of action to address issues and challenges. • An annex should be provided as supporting evidence	No later than six (6) weeks from start of the contract
Draft Final Report	• Should contain descriptions of the progress made with implementation of the tasks set out in Section 3 above with a summary of	No later than four (4) weeks before the end of the

Table 2 : Reports required and Timeline for Delivery

Name of Report	Content	Time of Submission
	findings, issues and challenges experienced and recommendations and resolutions. • An annex should be provided as supporting evidence	implementation period of the contract
Final Report	• Same specifications as the Draft Final Report • Detailed report on all activities and undertakings of the Consultancy and a summary of outputs/outcomes and feedback. • An annex should be provided as supporting evidence	No later than seven (7) days before the end date of the Consultancy

6. Client's Input and Counterpart Personnel

i. Services, facilities and property to be made available to the Firm by the Client include:

   a. Access to application on the server (remote)

   b. No office accommodation will be provided by the Client.

   c. The Firm shall be required to utilise their computers (e.g. laptop or tablet) and Internet connectivity for use during this project

ii. Professional and support counterpart personnel to be assigned by the Client to the Firm: None