EASTERN CARIBBEAN SECURITIES EXCHANGE

REQUEST FOR PROPOSAL

Network Security Assessment and Penetration Testing

Issue Date: January 22, 2024

Deadline for Clarification Questions: February 5, 2024

Deadline for Submission of Proposals: March 1, 2024

EASTERN CARIBBEAN SECURITIES EXCHANGE LTD REQUEST FOR PROPOSAL – NETWORK SERCURITY ASSESSMENT AND PENETRATION TESTING

1. Purpose

The Eastern Caribbean Securities Exchanges Ltd ("ECSE") Group is seeking to engage an independent service provider ("ISP") for the following.

1. To perform a comprehensive network security assessment\penetration test to determine the effectiveness of the ECSE's perimeter\external and internal network security and its alignment with best practices relating to system network security processes and procedures.
2. To perform a penetration test of the ECSE's website to determine the ability for attackers to gain administrative access to the website, perform denial-of-service (DoS) attacks against the website or compromise the integrity of information published on the website.
3. Test and verify the security of the Information technology systems and network to ascertain the effectiveness of deployed security measures.
4. Assess the ability of the ECSE group to respond in the event of an intrusion of the corporate computer network.
5. Identify any issues that may compromise the security of the ECSE's computer network.
6. Submit the findings of the assessment along with relevant recommendations in both executive level and technical level reports.

This activity is a part of the ECSE's ongoing risk management program and is focused on identifying the risk level that the group is currently exposed to so that an appropriate response plan to identified threats can be developed.

2. Background

The Eastern Caribbean Securities Exchange (ECSE) is a fully electronic regional exchange operating within the eight member states of the Eastern Caribbean Currency Union (ECCU). The ECSE, together with its wholly-owned subsidiary, the Eastern Caribbean Central Securities Depository (ECCSD), provides the infrastructure for the trading, clearance and settlement of financial assets on the Eastern Caribbean Securities market (ECSM) and the issuance of securities on Regional Government Securities Market (RGSM).

The markets were developed in response to identified gaps in the financial infrastructure in, where financial intermediation was based primarily on bank financing, leading to a bank-centric financial system. Additionally, there were limited investment opportunities, inadequate pricing and distribution mechanisms for securities, and minimal capital flows across ECCU.

The objectives of the ECSE are to provide the Eastern Caribbean Currency Union with an accessible marketplace in which to issue and trade securities, to clear settle trades, and to register companies in a transparent, seamless, confidential, and secure manner. The ECSE aims to be the medium of

choice for wealth creation and capital-raising in the Eastern Caribbean Currency Union.

The ECSE has a staff complement of 17 who operate within four (4) divisions or units , the Office of the Managing Director, the Accounting and Finance Division, the Operations Division, and the Custody Services Unit.

Further information on the structure of ECSE Group can be found in the latest Annual Report, which is available on our website www.ecseonline.com.

3. Technical Contact

Any question on the technical specifications of Statement of Work (SOW) requirements, contract terms and conditions or proposed format must be directed via email to the following

- Email Subject: Query re: Network Security Assessment and Penetration Testing
- Email address: ecse-IT@ecseonline.com

4. Scope of Works

The scope of the assessment will include the following but not be limited to:

1. A comprehensive assessment of the ECSE's network perimeter. This includes but is not limited to performing external port scanning and penetration testing of the ECSE's network perimeter. The assessment should include all public facing systems.
2. A comprehensive assessment of network systems for potential vulnerabilities.
   A count of the total number of servers, workstations switches and other network devices on the internal network will be made available upon request. All servers and workstations are to be considered within the scope of this assessment if they can be accessed from offsite through an identified vulnerability.
   Intrusive scans that may potentially cause any denial-of-services or other interruptions to critical systems should only be performed outside of the normal operating hours of the ECSE.
   The ECSE will provide the rules of engagement (ROE) to the successful applicant.
3. A penetration test of the ECSE website to determine the ability of an attacker to perform the following web application attacks.
   a. Cross-Site scripting
   b. Cross-Site request forgeries
   c. Injection attacks
   d. Brute-Force and Dictionary attacks
   e. Any Denial of Service (DoS) attacks that does not involve exploiting the underlying network or hosting environment.
4. Identify, analyze and confirm vulnerabilities found during the assessment.
   The proposer is expected to provide evidence of successful penetration tests (screenshots, files, etc.) as opposed to only a list of open ports, missing patches, or possible vulnerabilities.

Any vulnerabilities found on critical system should first be discussed with the ECSE before being exploited. This will minimize the risk of an in-depth analysis of any vulnerabilities found resulting in an extended outage of critical systems.

5. Items out of scope include attempting to exploit any denial of services vulnerabilities without the express written or otherwise communicated permission of the ECSE. Any vulnerability found outside of the SOW should also be first communicated to the ECSE before any exploitation is attempted.

5. Deliverables

At the conclusion of the assessment the ECSE requires written documentation of the approach, findings and recommendations associated with the project. A formal presentation of the findings and recommendations to senior management and other relevant personnel will also be required. The documentation should consist of the following:

- Detailed Technical Report – a document developed for the use of the ECSE's technical staff. This document should discuss:
    - The methodology employed.
    - Positive security features identified.
    - Detailed technical vulnerability findings with an assigned risk rating for each vulnerability based on the CVSS database and rating scale.
    - Supporting evidence and exhibits for vulnerabilities where appropriate.
    - Detailed technical and administrative remediation steps to address all of the vulnerabilities discovered during the assessment and penetration testing.

- Executive Summary Report – a document developed to summarize the scope, approach findings and recommendations in a high-level format suitable for senior management.

6. Proposal Requirements

These guidelines are offered as general information for the proposal preparation process. The sections listed below should be included in proposals, which should be brief. The review process may disqualify proposals that do not follow or comply with the required format.

The proposal should be submitted in English and must be accompanied by a properly executed proposal letter, which must bear the signatures of the individual or individuals authorized to legally bind the firm or company.

The ECSE reserves the right to

- Reject any or all offers and discontinue the RFP process without obligation or liability to any proposer.
- Accept any offer regardless of price.
- Award a contract based on the initial proposal received, without discussions or requests for best and final offers.

The proposal should be submitted as outlined below.

i. **Executive Summary**

A high-level synopsis of the proposers response to the RFP. This should be a brief overview of the engagement and should identify the main features and benefits of the proposed work.

ii. **Approach and Methodology**

Detailed testing procedures and technical expertise by phase. This section should also include a description of each major item as described in the scope of work above.

iii. **Project Deliverables**

Include descriptions of the types of reports that will be used to summarize and provide detailed information on the security risk, vulnerabilities and the necessary countermeasures and recommended corrective actions. Sample reports that show examples of the type of reports provided for this engagement can be included as attachments to the proposal.

iv. **Project Management Approach**

Describe the method and approach used to manage the overall project and client correspondence. Briefly describe how the assessment will proceed from beginning to end and the expected timelines for each phase.

v. **Detailed and Itemized Pricing**

Include a fee breakdown by project phase and estimates of all anticipated out of pocket expenses.

vi. **Appendix: References**

Provide three references for which you have provided similar services.

vii. **Appendix: Project Team Staffing**

Include short biographies which provides information on the relevant experience and qualifications of key staff and management personnel.

viii. **Appendix: Company Overview**

Provide the following for your company.

- Official registered name, address, telephone number(s) and website
- Key contact names, titles, telephone numbers and email addresses.
- The person authorized to contractually bind the organization for any proposal against this RFP.
- Brief history, including the year established and number of years your company has been offering Information Security related assessments and penetration testing.

7. Evaluation Criteria

The evaluation of the proposal will be based on the candidate's responsiveness to the terms of RFP, as well as the application of the evaluation criteria and points system as indicated below.

Criteria	Points Allocated
Experience of the proposer in providing the required services.	25
Suitability of the submitted proposal in meet the ECSE's needs.	30
Qualifications and experience of team members.	30
Pricing and fees	15
Total	**100**

8. Submission Details

Event	Date Due
RFP Issue Date	**22 January 2024**
Deadline for Clarification Questions from Proposers	**5 February 2024**
Response to Clarification Questions	**19 February 2024**
Last Day for Submission of Proposals	**1 March 2024**
Interviews for Shortlisted Proposals	**15 March 2024**
Successful Proposer Announced	**22 March 2024**

Proposals should be sent by email to info@ecseonline.com with the subject "**Security Assessment RFP 2024 - Proposal Enclosed.**"

The deadline for the receipt of proposals is **1 March 2024**. Any submissions made after the deadline will not be considered. The Proposer shall ensure delivery to the ECSE by the period specified for delivery.

Any delivery issues that result in a proposal being received after the specified due date and time are not the responsibility of the ECSE. Proposals must be sent before the deadline to be considered.

ECSE
January 2024