TERMS OF REFERENCE

Project Title: Information and Communication Technology

Statement of Work: Consultancy services to conduct network vulnerability and penetration testing on ECREEE's Network.

Starting Date: As soon as possible.

1. Background

The ECOWAS Centre for Renewable energy and energy Efficiency (ECREEE) was established in 2010 in response to the energy crisis faced by member states in the West Africa region. The overall objective of ECREEE is to contribute to the sustainable economic, social, and environmental development in West Africa by improving access to modern, reliable and affordable energy services, energy security and reduction of energy related externalities (GHG, local pollution). More specifically, ECREEE aims to create favorable framework conditions for regional Renewable Energy (RE) and Energy Efficiency (EE) markets by supporting activities directed to mitigate existing technological and financial barriers.

In pursuit of its mandate, ECREEE have acquired various information and Communication systems at it´s headquarter, to effectively support its business operations. Considering the current trend in Cyber Security, it is important to protect these systems and related information against cyber attacks and other security threats. One such means is to periodically assess its vulnerability and weaknesses, to effectively mitigate the likelihood of any attack. ECREEE is seeking the services of a qualified IT professional to perform a security assessment of its network.

2. Objectives

The Consultant will conduct a network vulnerability assessment and penetration testing to determine the weaknesses and exposure of ECREEE's network. He/she will conduct an independent analysis and review of ECREEE´s network security and processes to identify the network vulnerabilities, strength and weakness in detecting and preventing attacks against the network.

3. Scope of Work

The work will cover a complete external and internal Network Vulnerability assessment and penetration testing, not limited to: assessment of telephony, security awareness policy, physical security, network architecture designs, DMZ, Wireless, virtual infrastructure, Server, firewall, Router, switches, printers, computers, biometrics, and other network systems Configurations.

3.1 The vulnerability assessment shall include but not limited to:

Assessment of Internal and External security measures. Conduct vulnerability scans to identify any security vulnerability;

1. Assessment of the wireless security;
2. Review of all Information Technology assets;
3. The current network architecture security assessment;
4. Application security assessment;
5. Assessment of security awareness of ECREEE´s personnel;
6. Assessment of overall state of security measure in relation to current threats in cyber-security.

3.2 The penetration testing services will cover but not limited to:

1. Network penetration testing;
2. Web application testing;
3. Internal systems application testing;
4. Social engineering testing.

3.3 ECREEE´s Network

ECREEE´s network is a small-medium sized network composing of few servers, firewalls and switch in clusters. The network spans 4 floors with access layer switches in each. It has a wireless network composed of access points in each floor, all in a cluster, and the computers counts to 50 operational endpoints

4. Deliverables

The deliverable includes:

1. Network vulnerability assessment report and presentation.
2. Penetration testing report and presentation.
3. An overall detail report and presentations on the findings and recommendations, to include risk identified, their impact and the remediation actions. These actions will be detailed and prioritised according to their impact and importance, with detailed steps to mitigate all risks.

5. Qualification and Experience

Minimum requirements

- ✓ Minimum BSc. in Information Security, Cyber Security, Computer Information Systems, Management Information Systems or similar relevant field
- ✓ Six (6) years of experience conducting vulnerability security assessment and penetration testing.
- ✓ Excellent proven written and spoken English language proficiency

Preferred requirements

- ✓ Relevant cyber security and security audit certifications
- ✓ Demonstrated Excellent experience in assessing and developing mitigation strategies for networks, operating systems, and applications
- ✓ Experience in offensive security, with the ability to think like an adversary
- ✓ Strong experience in operating system and application security hardening and best practices
- ✓ Experience with multiple solutions from Microsoft, Cisco, and their related virtual applications
- ✓ Demonstrated experience working with government, regional or international organizations
- ✓ Working knowledge of French and/or Portuguese;
- ✓ Working experience in the ECOWAS region and knowledge or relevant experience in the energy sector is an advantage.

6. Application and Evaluation

Applicants should submit the following in English,

i. A technical proposal that captures a) the methodology to carry out the assignment and detailed implementation schedule.
ii. Financial proposal in US$ including all costs and taxes (i.e., a detailed work-time-expert-diagram indicating daily rates for individual team members).
iii. The consultant’s CV;
iv. Copies of academic certificates and any other relevant documents

Evaluation will be based on the Consultant´s qualification and experiences, quality & substantial responsiveness of the proposal, and cost.

7. Application Deadline

Applicants are requested to submit their proposals no later than 23:59 hrs (GMT) of 22 November 2022, to itsecurity@ecreee.org

For more information, send an email to jabdulrahman@ecreee.org and copy adeoliveira@ecreee.org

Disclaimer: The Consultant must explicitly agree that any information collected and analyzed during the contracting period is subject to a data privacy clause and a non -disclosure agreement. All products and services delivered under this contract shall pass into the exclusive ownership of ECREEE, including all use and distribution rights connected to it.