AFRICAN UNION
الاتحاد الأفريقي

UNION AFRICAINE

UNIÃO AFRICANA

Date: 25 August, 2023

REQUEST FOR EXPRESSIONS OF INTEREST

(CONSULTING SERVICES – INDIVIUDAL CONSULTANT SELECTION)

Project Name: Capacity Building to the African Union Project

Project Id: P-Z1-K00-122

Grant Number: 2100155041317

Assignment Title: Senior Cyber-Security Consultant (2)

The African Union (AU) has received financing from the Africa Development Bank towards implementing the Institutional Capacity Building for the African Union Project in which the African Union Commission (AUC) is a beneficiary of the grant component and intends to apply part of the proceeds for consulting services.

The overall objective of the consultancy service is to recruit Senior Cyber Security Consultant to assist the Africa Union Commission (AUC), Management of Information Services Directorate (MISD) on Cyber Security matters at the AUC Headquarters, Addis Ababa, Ethiopia

The scope of work will include:

- Safeguard information system assets by identifying and solving potential and actual security problems.
- Protect the system by defining access privileges, control structures and resources.
- Recognize problems by identifying abnormalities and reporting violations.
- Implement security improvements by assessing current situation, evaluating trends and anticipating requirements.
- Determine security violations and inefficiencies by conducting periodic audits.
- Upgrade system by implementing and maintaining security controls.
- Keep users informed by preparing performance reports and communicating system status.
- Maintain quality service by adhering to organization standards.
- Maintain technical knowledge by attending educational workshops and reviewing publications.
- Contribute to team effort by accomplishing related results as needed.

- Implement the Standard Operation Procedures (SOP) related to Cyber-security.
- Provide guidance and recommendation related to new technologies trends in the improvement of the AU Cyber-security.
- Utilize the existing monitoring tools to anticipate and propose remedial plans in cyber-threats.
- Exchange information with the Cyber threats Intelligence unit of MISD

The expected duration of the assignment will initially be for six (6) months with possibility of extension for another six (6) months subject to satisfactory performance, fund availability and deliverables**.**

The eligibility criteria, the establishment of a short list and the selection procedure shall be in conformity with the Bank's Procurement Policy and Procedure for selection of Individual Consultants.

Further information can be obtained at the address below during office hours *i.e. 0900 to 1700 hours*.

The **African Union Commission** now invites eligible individual consultants to indicate their interest in providing the Services. The detailed Terms of Reference for the Individual Consultants are attached to this request for expressions of interest.

Qualifications and Experience: Interested Consultants should provide information demonstrating that they have the required qualifications and relevant experience to perform the Services. The shortlisting criteria are as follows:

- A Master's degree in Computer Science, Cyber-Security, Cryptography, Cybercrime, Data Analysis, or other Information Technology related fields.
- At least seven years' practitioner experience, in which three years should be in senior operational level in cyber-security, cyber-threats assessment or cybercrime within an International Organization, Think Tank, Centre of Excellence or similar institution OR a University Bachelor's degree plus at least 10 years' experience, out of which five years should be in senior operational level.
- Strong background in Qualitative and Quantitative data analysis methodology required.
- Proof of cyber investigation cases resolved and implementation of remedial plan.
- Strong experience in Cyber threat intelligence analysis.
- Advanced certifications such as SANS GIAC/GCIA/GCIH, CISSP, CASP, SIEM-specific training, CEH, CND, CISSP, CHFI, CISA and any other relevant certification in Cyber-security.
- A higher qualification and experience in any related field would be an added advantage.
- Verifiable references and membership of professional organization(s).

- Previous work experience in projects funded by the African Development Bank and World Bank would be an added advantage.

Skills and Competencies Required:

- System administration
- Network security and Problem solving
- Information security policies
- On-call network troubleshooting
- Firewall administration (Cisco Firepower, FortiNet, Palo Alto)
- Advanced understanding of TCP/IP, common networking ports and protocols, traffic flow, system administration, OSI model, Defense-in-depth and common security elements.
- Hands-on experience in analysing high volumes of logs, network data (e.g. Netflow, FPC) and other attack artifacts in support of incident investigations
- Experience with vulnerability scanning solutions
- Familiarity with the DOD Information Assurance Vulnerability Management program.
- Proficiency in Anti-Virus, HIPS, ID/PS, Full Packet Capture, Host-Based Forensics, Network Forensics, and RSA Security
- In-depth knowledge of architecture, engineering, and operations of at least one enterprise SIEM platform (e.g. Nitro/McAfee Enterprise Security Manager, Kaspersky, ArcSight, QRadar, LogLogic, Splunk)
- Experience developing and deploying signatures (e.g. YARA, Snort, Suricata, HIPS)
- Understanding of mobile technology and OS (i.e. Android, iOS, Windows), VMware technology, and Unix and basic Unix commands
- Strong knowledge in Routers, WIFI controllers and switches configuration
- Capacity to exploit information sharing in Darkweb concerning new Cyber-threats intelligence
- Digital investigation using triage tools such MobilEdit, SPEKTOR or any other related tool.
- Strong knowledge in Stealthwatch, ISE, Graylog, TITUS and MISP are an advantage.
- Strong knowledge in XDR and CTI tools.

Expressions of Interest (CV and Cover letter) must be submitted in a written form to the address below (in person, by mail, or e-mail by the **11 September 2023 before or at 04.00 pm**, Addis Ababa time zone (GMT+3) :

African Union Commission,
Attn: Head of Supply Chain Management Division
Building C, 3rd Floor
P.O. Box 3243, Roosevelt Street
Addis Ababa, Ethiopia
Tel: +251 (0) 11 551 7700 – Ext 4305
Fax: +251 (0) 11 551 0442; +251 11-551-0430
E-mail: tender@africa-union.org

(CONSULTING SERVICES– INDIVIDUAL CONSULTANT)

TERMS OF REFERENCE

SENIOR CYBER-SECURITY CONSULTANT (2)

A. BACKGROUND

The African Union, established as a unique Pan African continental body, is charged with spearheading Africa's rapid integration and sustainable development by promoting unity, solidarity, cohesion and cooperation among the peoples of Africa and African States as well as developing a new partnership worldwide. Its Headquarters is located in Addis Ababa, capital city of Ethiopia.

In seeking to achieve this objective, the African Union intends to strengthen its capacity to deliver by, among others, the implementation of its organizational structure and the filling of all vacant posts. Therefore, the Management of the Information System Directorate (MISD) is one the crucial department in the achievement of the Strategic objectives of the organization.

The Commission of the African Union invites applicants who are citizens of Member States for the consultancy service as Senior Cyber-security Consultant within the Management of Information System Directorate (MISD), Addis-Ababa, Ethiopia

B. OBJECTIVES

The overall objective of the consultancy service is to recruit Senior Cyber Security Consultant to assist the AUC MISD on Cyber Security assignment.

C. SCOPE OF WORK

The following are the major responsibilities of the consultant;

- Safeguard information system assets by identifying and solving potential and actual security problems.
- Protect the system by defining access privileges, control structures and resources.
- Recognize problems by identifying abnormalities and reporting violations.
- Implement security improvements by assessing current situation, evaluating trends and anticipating requirements.
- Determine security violations and inefficiencies by conducting periodic audits.
- Upgrade system by implementing and maintaining security controls.

- Keep users informed by preparing performance reports and communicating system status.
- Maintain quality service by adhering to organization standards.
- Maintain technical knowledge by attending educational workshops and reviewing publications.
- Contribute to team effort by accomplishing related results as needed.
- Implement the Standard Operation Procedures (SOP) related to Cyber-security.
- Provide guidance and recommendation related to new technologies trends in the improvement of the AU Cyber-security.
- Utilize the existing monitoring tools to anticipate and propose remedial plans in cyber-threats.
- Exchange information with the Cyber threats Intelligence unit of MISD

D. QUALIFICATIONS AND EXPERIENCE

The Senior Cyber Security Consultant should have the following qualifications and experience:

- A Master's degree in Computer Science, Cyber-Security, Cryptography, Cybercrime, Data Analysis, or other Information Technology related fields.
- At least seven years' practitioner experience, in which three years should be in senior operational level in cyber-security, cyber-threats assessment or cybercrime within an International Organization, Think Tank, Centre of Excellence or similar institution OR a University Bachelor's degree plus at least 10 years' experience, out of which five years should be in senior operational level.
- Strong background in Qualitative and Quantitative data analysis methodology required.
- Proof of cyber investigation cases resolved and implementation of remedial plan.
- Strong experience in Cyber threat intelligence analysis.
- Advanced certifications such as SANS GIAC/GCIA/GCIH, CISSP, CASP, SIEM-specific training, CEH, CND, CISSP, CHFI, CISA and any other relevant certification in Cyber-security.
- A higher qualification and experience in any related field would be an added advantage.
- Verifiable references and membership of professional organization(s).
- Previous work experience in projects funded by the African Development Bank and World Bank would be an added advantage.

Skills and Competencies Required:

- System administration
- Network security and Problem solving
- Information security policies
- On-call network troubleshooting
- Firewall administration (Cisco Firepower, FortiNet, Palo Alto)
- Advanced understanding of TCP/IP, common networking ports and protocols, traffic flow, system administration, OSI model, Defense-in-depth and common security elements.
- Hands-on experience in analysing high volumes of logs, network data (e.g. Netflow, FPC) and other attack artifacts in support of incident investigations
- Experience with vulnerability scanning solutions

- Familiarity with the DOD Information Assurance Vulnerability Management program.
- Proficiency in Anti-Virus, HIPS, ID/PS, Full Packet Capture, Host-Based Forensics, Network Forensics, and RSA Security
- In-depth knowledge of architecture, engineering, and operations of at least one enterprise SIEM platform (e.g. Nitro/McAfee Enterprise Security Manager, Kaspersky, ArcSight, QRadar, LogLogic, Splunk)
- Experience developing and deploying signatures (e.g. YARA, Snort, Suricata, HIPS)
- Understanding of mobile technology and OS (i.e. Android, iOS, Windows), VMware technology, and Unix and basic Unix commands
- Strong knowledge in Routers, WIFI controllers and switches configuration
- Capacity to exploit information sharing in Darkweb concerning new Cyber-threats intelligence
- Digital investigation using triage tools such MobilEdit, SPEKTOR or any other related tool.
- Strong knowledge in Stealthwatch, ISE, Graylog, TITUS and MISP are an advantage.
- Strong knowledge in XDR and CTI tools.

E. DURATION AND TIMING

Contract duration will initially be for six (6) months with possibility of extension for another six (6) months subject to satisfactory performance, fund availability and deliverables**.**

F. INSTITUTIONAL AND ORGANIZATIONAL ARRANGEMENTS

The consultant will report functionally to the MISD Director in the AU Headquarter and administratively to the AfDB Capacity Development Project coordinator.

G. DUTY STATION

The consultant will be based in the African Union Commission Head Quarter Addis Ababa Ethiopia.

H. REMUNERATION

Remuneration is payable on a monthly basis. It is negotiable but based on qualifications and experience and the applicable AU rates for the level of the consultancy. Fees payable do not include costs associated with project related travels, coordination/organization of project related activities and events, stakeholder dialogues, consultations and workshops. These costs will be met by the AU.

I. FACULITIES TO BE PROVIDED BY THE AU

The following shall be made available by the MISD:

- Office accommodation;

- Computer, Photocopying, Stationary;
- Facilitation of Visa and
- Internet Access