UNODC
United Nations Office on Drugs and Crime

Southern Africa

CORE VALUES: INTEGRITY, PROFESSIONALISM, RESPECT FOR DIVERSITY

CONSULTANCY ANNOUNCEMENT

TERMS OF REFERENCE

POSITION TITLE	:	GPML Cybercrime Consultant
ORGANIZATION	:	United Nations Office on Drugs and Crime
TYPE OF CONTRACT	:	Individual Contract
REGIONAL OFFICE		Pretoria, South Africa
DUTY STATION		Home-based (with the possibility of in-person after travel restrictions)
TITLE OF SUPERVISOR	:	Lindy Muzila (Anti-Money Laundering Project Coordinator)
PROPOSE PERIOD	:	28 August – 19 October 2020
ACTUAL WORK TIME	:	42 days
Fee Range		C

---

1. BACKGROUND OF THE ASSIGNMENT:

UNODC is supporting the Asset Recovery Interagency Network of Southern Africa, (ARINSA), initiative, which is an informal professional network of practitioners dealing with all aspects of tackling the proceeds and instrumentalities of crime. On 23-24 March 2009 delegates from law enforcement and prosecution agencies from nine countries in the eastern and southern African region met in Pretoria to discuss the creation of a new, informal network of investigators and prosecutors. Countries represented at the conference were: Botswana, Lesotho, Namibia, South Africa, Swaziland, Tanzania, Zambia and Zimbabwe. It was agreed that an informal network based on the CARIN model would be of considerable help to prosecutors and investigators working on cases involving the identification, tracing, freezing, seizure, confiscation and recovery of proceeds and instrumentalities of crime, and that such a network, established in accordance with the parameters set out below, should be established without delay.

The aim of ARINSA is to increase the effectiveness of members' efforts, individually and collectively, on a multi-agency basis, in depriving criminals of instrumentalities of crime and illicit profits,

In addressing the need of law enforcement authorities, as expressed through the ARINSA platform, UNODC is advertising this consultancy to focus on the following key issues:

i. What cyber-related threats law enforcement officials can expect in the COVID-19 era;
ii. How law enforcement officials can safely work online;

2. PURPOSE OF THE ASSIGNMENT:

The COVID-19 pandemic was initially seen as purely a health-related problem. However, the threat of cybercrime emanating from the pandemic has become apparent. Cyber criminals are ceasing the opportunity created by the pandemic to exploit available vulnerabilities and achieve profit.

Under the overall guidance and supervision of UNODC Project Coordinator, dealing with ARINSA project, the Consultant will carry out his/her assignment as follows:

The purpose of the assignment is to inform local law enforcement as to the likely cybercrime threats that may be introduced in the COVID-19 era and how to stay safe during these times while working

from home. It will assist to inform them of preventive measures that can be taken to curb and curtail any potential vulnerabilities that cyber criminals would likely take advantage of. The consultancy will be carried out under the overall guidance of the UNODC Global Programme against Money laundering (GPML) and the direct supervision of the relevant UNODC Project Coordinator.

3. SPECIFIC TASKS TO BE PERFORMED BY THE CONSULTANT:

- Prepare and deliver a three-day online or in person training session for the Gauteng National Prosecuting Authority (NPA), and the Financial Intelligence Centre (FIC) with a focus on cybercrime in South Africa. Presentation should provide recommendations on preventive and other measures in addressing this threat.
- Prepare and deliver a three-day online or in person training session for the Western Cape NPA with a focus on cybercrime in South Africa.
- Prepare and deliver a webinar presentation and facilitate Q&A session with a focus on how cyber criminals in the Southern African region are exploiting the COVID-19 pandemic for profit.
- Provide legislative and policy review towards the development of the Eswatini cybercrime bill.

4. DATES AND DETAILS OF DELIVERABLES/PAYMENTS:

Deliverable	Output	Days Worked	To be accomplished by:
A.	• Preparatory work and delivery of online or in-person three-day training session for Gauteng NPA on the cyber criminality threat for law enforcement and possibly FIC.	**Eight (8) days**	Eight working days after signing the contract
B.	• Preparatory work and delivery of online or in-person three-day presentation and discussion session for Western Cape NPA on the cyber criminality threat for law enforcement	**Eight (8) days**	Nineteen working days after signing the contract
C.	• Preparatory work and delivery of a regional webinar on the COVID-19 related cyber criminality threat for law enforcement	**Six (6) days**	Twenty-seven working days after signing the contract
D.	• Report detailing legislative and policy review of Eswatini new Cybercrime bill.	**Twenty (20) days**	Forty-seven working days after signing the contract
Total		**42 days**	

The payment fee will be paid as per the common UN rules and procedures and in two instalments:

- The first instalment of the total cost of the contract will be paid after the delivery of the online or in-person three-day training sessions for Gauteng and Western Cape NPA.

(Deliverables A & B)

- The second and final instalment of the total cost of the contract will be paid after the delivery of the webinar and the review of the Eswatini cybercrime bill (Deliverables C & D) final report has been submitted, assessed and approved by UNODC ROSAF.

5. INDICATORS TO EVALUATE THE CONSULTANT'S PERFORMANCE:

Deliverables	Indicators
Three-day delivery of online or in-person training session for Gauteng NPA on the cyber criminality threat for law enforcement and possibly FIC. Presentations should provide recommendations to prevent and respond to this threat.	Successful presentation and increase in knowledge of participants, as evidenced by feedback provided in pre and post training evaluation questionnaires
Three-day online or in person training session for the Western Cape NPA with a focus on cybercrime in South Africa. Presentations should provide recommendations to prevent and respond to this threat.	Successful presentation and increase in knowledge of participants, as evidenced by feedback provided in pre and post training evaluation questionnaires
Webinar presentation on cyber-related threats to law enforcement officials in the COVID-19 era and how law enforcement officials can work safely at home and facilitation of a Q&A session after the webinar.	Successful presentation and increase in knowledge of participants, as evidenced by feedback provided in pre and post webinar evaluation questionnaires
A comprehensive legislative or policy report on cybercrime measures to be undertaken by Eswatini.	Detailed report approved by UNODC ROSAF, outlining specific elements to be amended in the bill and/or specific measures to be undertaken in improving the cybercrime bill

EVALUATION CRITERIA/EXPERTISE SOUGHT (REQUIRED EDUCATIONAL BACKGROUND, YEARS OF RELEVANT WORK EXPERIENCE, OTHER SPECIAL SKILLS OR KNOWLEDGE REQUIRED):

- An advanced university degree (Master's degree or equivalent) in the fields of law, criminology, public administration, political science, international relations or related fields of criminal justice, crime prevention and/or law enforcement is required. A first-level university degree OR equivalent academic education, professional training with certification from a recognized international/national police, customs or other staff training institution, with specialization in cyber forensics, border working techniques and/or other related areas, in combination with additional years of qualifying experience may be accepted in lieu of the advanced university degree. Certification or other qualification in training design and delivery is an advantage.
- At least 10 years of professional experience in the fight against cybercrime, financial crime and related areas is required.
- Previous experience in developing anti-cybercrime legislation is required
- Previous experience of providing anti-cybercrime technical assistance internationally is required.
- Specialist knowledge of fraud prevention and the conduct of successful cyber-criminal investigations is desirable.

- Intelligence collection, investigation or prosecution experience relating to cybercrime is desirable.
- Practical professional experience in the implementation of technical assistance, and design & delivery of training for law enforcement, particularly in Africa. Experience in Southern Africa would be an advantage.
- Oral and written fluency in English. Knowledge of other UN languages would be an asset.

APPLICATION REQUIREMENTS

A completed application must include: Financial and technical proposal, Cover letter, CV with three contactable referees, and Personal History profile (UNDP P11 Form). Personal History profile must include past work experiences, information on computer skills, samples of knowledge products (guides, toolkit, etc.) and include three contactable referees.

Interested candidates may send their completed application with the Subject line ***"UNODC Cybercrime Consultant"*** to Takalani Godobedza at takalani.godobedza@un.org (incomplete applications will not be considered). For enquiries, please contact Takalani at the provided email.

For technical queries, please contact Uyo Yenwong-Fai at uyo.yenwongfai@un.org
These TOR's will also be available on UNODC website:
https://www.unodc.org/southernafrica/en/consultancies-and-opportunities.html
Correspondence will be limited to shortlisted candidates only.
UNODC reserves the right not to make an appointment.

CLOSING DATE FOR APPLICATIONS: 15 August 2020