



000000017  
2.2.2020  
**AVIS D'APPEL A MANIFESTATION D'INTERET  
/AMI/MPT/SG/DAG/SDBM/SMA/2020 DU  
POUR LA PRESELECTION DES CABINETS D'ETUDES OU  
ENTREPRISES EN VUE DU RENFORCEMENT DES CAPACITES DES PERSONNELS  
POUR LA REALISATION DE LA MISSION DE VEILLE SECURITAIRE.  
« EN PROCEDURE D'URGENCE »**

**1. Contexte et justification**

Le CIRT est une structure de l'ANTIC constituée de seize (16) personnels chargés au quotidien de la prévention et de la réponse aux actes cybercriminels au Cameroun. Afin de remplir convenablement ses missions, le CIRT a besoin de personnels compétents dans différents domaines de la cybersécurité. A cet effet, le renforcement des capacités est une activité continue au sein du CIRT et permet de maintenir les personnels à la hauteur des enjeux auxquels ils font face au quotidien.

**2. Consistance des prestations**

Les prestations portent sur la formation et la présentation aux examens de certification dans les domaines suivants :

- Ethical Hacking ;
- Les investigations numériques ;
- L'analyse des programmes malveillants ;
- La sécurité des infrastructures critiques ;
- La protection des postes clients ;
- La collecte des informations à travers les outils OSINT et le Dark web ;
- La protection des infrastructures critiques.

**3. Participation**

Pour faire acte de candidature, tout Cabinet d'Etudes ou Entreprise, devra justifier d'un agrément du MINEFOP ou disposer de la tutelle d'une institution de l'Etat et être accrédité par au moins une organisation internationale opérant dans le domaine de la sécurité des TIC (EC Council, ISACA, institute Of Internal Auditors, Internal Control Institute,...).

**4. Composition du dossier de candidature**

Le dossier d'Avis à Manifestation d'Intérêt comprendra les sections suivantes :

- Section 1 : Pièces administratives ;
- Section 2 : Dossier technique.

**4.1. Section 1 : pièces administratives (enveloppe A)**

La section 1 comprend les pièces administratives (originales ou leurs copies certifiées conformes datant de moins de trois (03) et valables pour l'exercice en cours) suivantes :

- a) lettre de motivation dûment signée du soumissionnaire ;
- b) Une attestation de soumission signée des services de la Caisse Nationale de Prévoyance Sociale certifiant que le soumissionnaire a satisfait à ses obligations vis-à-vis de ladite caisse datant de moins de trois mois
- c) copie du registre du commerce, certifiée au greffe du tribunal de 1<sup>ère</sup> instance ;
- d) attestation de non redevance (copie certifiée, par le service des impôts) ;



- e) attestation de non exclusion des marchés publics délivrée par l'ARMP ;
- f) attestation de non faillite (original ou copie certifiée par le greffe du tribunal de 1<sup>ère</sup> instance.

**4.2. Section 2 : dossier technique (enveloppe B)**

L'enveloppe B contiendra les informations suivantes :

- la présentation du cabinet ainsi que les domaines d'action et d'intervention ;
- l'agrément et accréditation ;
- la liste des formateurs avec les copies des diplômes et des CV datés et signés par chaque expert ;
- les références du Cabinet d'Etudes pour les prestations similaires réalisées au cours des cinq (05) (marchés et lettres commande...);
- la compréhension du mandat de mission (TDR) .

**5. Critères d'évaluation et de sélection des cabinets**

**5.1. Critères éliminatoires :**

- Dossier administratif ou technique incomplet ;
- Fausse déclaration, document falsifié ;
- Note technique inférieure à 75 points sur 100.

**5.2. Critères de qualification**

Les offres techniques seront présentées en fonction des principaux critères ci-après :

- a) **Expérience générale .....20 points ;**
  - Être une entreprise de droit camerounais disposant d'un agrément du MINEFOP ou disposer de la tutelle d'une institution de l'Etat.....5 points ;
  - Etre accrédité par au moins une organisation internationale opérant dans le domaine de la sécurité des TIC (EC Council, ISACA, Institute Of Internal Auditors, Internal Control Institute,...) .....10 points ;
  - Disposer d'une expérience d'au moins 05 ans dans les formations professionnelles en audit et cybersécurité et dans la préparation des certifications en audit des systèmes d'information, cybersécurité et sécurité des systèmes .....5 points ;
- b) **Expérience du formateur clé.....50 points ;**

Poste	Qualifications	Notation
<b>Formateur N°1 CEHv10</b>	- BAC+3 minimums ; - Justifier d'une expérience professionnelle d'au moins cinq (05) ans dans la cyber sécurité; - Disposer de la certification CEHv10 ; - Être titulaire d'au moins deux (02) des certifications suivantes (CISM, CISA, CSA, FCSA, LPT, VWCP, CCNA, CCNP, MCSA, ...); -avoir dispensé au moins deux (02) sessions de formations en rapport avec la cyber sécurité.	<b>12.5 points</b>
<b>Formateur N°2 CHFIv9</b>	- BAC+3 minimums ; - Justifier d'une expérience professionnelle d'au moins cinq (05) ans dans la cyber sécurité; - Disposer de la certification CHFIv9 ; - Être titulaire d'au moins deux (02) des certifications suivantes (CEH, CISM, CISA, CSA, ECSA, LPT, VWCP, CCNA, CCNP, MCSA, ...); -avoir dispensé au moins deux (02) sessions de formations en rapport avec la cyber sécurité.	<b>12.5 points</b>









00000017 CALL FOR EXPRESSION OF INTEREST  
/AMI/MPT/SG/DAG/SDBM/SMA/2020 OF 22 JUIL 2020 FOR  
THE ESTABLISHMENT OF A SHORT-LIST OF CONSULTING FIRMS OR  
COMPANIES FOR THE CAPACITY BUILDING OF THE PERSONNEL IN THE  
CREATION OF A SECURITY WATCH MISSION.  
"IN A PROCEDURE OF URGENCY"

**1. Background and justification**

The CERT is a structure of NAICT made up of sixteen (16) personnel responsible for the daily prevention and response to cybercrime in Cameroon. In order to properly carry out its missions, the CERT needs competent personnel in different areas of cybersecurity. To this end, capacity building is an ongoing activity within the CERT and helps to keep the personnel up to the challenges they encounter on a daily basis.

**2. Description of services**

The services include training and sitting in at certification examinations in the following areas:

- Ethical Hacking;
- Digital investigations;
- Malware analysis;
- Critical Infrastructure Security;
- The protection of client workstations;
- Data collection through OSINT tools and the Dark web;
- Protection of Critical Infrastructure

**3. Participation**

In order to apply, any Consulting Firm or Company must be approved by MINEFOP or have the supervision of a state institution and be accredited by at least one international organization operating in the field of ICT security (EC Council, ISACA, Institute Of Internal Auditors, Internal Control Institute, ...).

**4. Application file**

The application file of the Call for Expression of Interest shall include the following volumes:

- Volume 1 :Administrative documents;
- Volume 2:Technical documents.

**4.1. Volume 1: Administrative documents (envelope A)**

Volume 1 shall include the following administrative documents (originals and their certified true copies of not more than three (03) months and valid for the current financial year):

- a) A cover letter duly signed by the applicant;
- b) A signed attestation of tender provided by the National Social Security Fund certifying that the tenderer has fulfilled its obligations to the National Social Security Fund, dated less than three months ago.
- c) A copy of the commercial register, certified by the Registry of the Court of First Instance;
- d) tax clearance certificate (certified copy, by the tax service);
- e) a certificate of non exclusion from public contracts issued by the ARMP;



f) a certificate of non-bankruptcy (original or copy certified by the Registry of the Court of First Instance.

**4.2. Volume 2: Technical file (envelope B)**

Envelope B shall contain the following information:

- the presentation of the Firm or Consulting Firm as well as areas of action and intervention;
- Approval and accreditation;
- the list of trainers with copies of their certificates and CVs dated and signed by each expert;
- references of the consulting firm for similar services executed during the past five (05) years (contracts and letter of order.....);
- understanding the mandate of the mission (TOR);

**5. Evaluation and selection criteria of firms**

**5.1. Eliminary criteria:**

- Incomplete administrative or technical document;
- False declaration, forged document.
- Technical score below 75 points out of 100.

**5.2. Selection criteria:**

The technical bids shall be presented according to the main criteria below:

- a) **General Experience .....20 points;**
- Be a Cameroonian company under Cameroonian law holding a MINEFOP approval or be under the supervision of a state institution .....5 points ;
  - Be accredited by at least one international organisation operating in the field of ICT security (EC Council, ISACA, Institute Of Internal Auditors, Internal Control Institute,...) .....10 points ;
  - Have at least 05 years' experience in professional training in auditing and cybersecurity and in the preparation of certifications in information systems auditing, cybersecurity and systems security .....5 points;
- b) **Experience of key trainer.....50 points;**

Function	Qualifications	Rating
<b>Trainer No. 1 CEHv10</b>	<ul style="list-style-type: none"> <li>- at least GCE A/L +3</li> <li>- Proof of at least five (05) years of professional experience in cyber security;</li> <li>- Must have the CEHv10 certification;</li> <li>- Be a holder of at least two (02) of the following certifications (CISM, CISA, CSA, ECSA, LPT, VWCP, CCNA, CCNP, MCSA, ...);</li> <li>- Must have provided at least two (02) training sessions related to cyber security.</li> </ul>	<b>12.5 points</b>
<b>Trainer No. 2 CHFv9</b>	<ul style="list-style-type: none"> <li>- at least GCE A/L. +3</li> <li>- Proof of at least five (05) years of professional experience in cyber security;</li> <li>- Must have the CHFv9 certification;</li> <li>- Be a holder of at least two (02) of the following certifications (CEH, CISM, CISA, CSA, ECSA, LPT, VWCP, CCNA, CCNP, MCSA, ...);</li> <li>- Must have provided at least two (02) training sessions related to cyber security.</li> </ul>	<b>12.5 points</b>
<b>Trainer No. 3 ECSAv9</b>	<ul style="list-style-type: none"> <li>- at least GCE A/L +3</li> <li>- Proof of at least five (05) years of professional experience in cyber security;</li> <li>- Must have the ECSAv9 certification;</li> </ul>	<b>12.5 points</b>





