REPUBLIQUE DU CAMEROUN
Paix-Travail-Patrie

MINISTERE DES POSTES ET TELECOMMUNICATIONS

SECRETARIAT GENERAL

REPUBLIC OF CAMEROON
Peace-Work-Fatherland

MINISTRY OF POSTS AND TELECOMMUNICATIONS

GENERAL SECRETARIAT

0 0 0 0 0 0 1 0 AVIS D'APPEL A MANIFESTATION D'INTÉRÊT N°...../AMI/MPT/SG/DAG/SDBM/SMA/2024 DU 23 AVR 2024, POUR LA PRESELECTION DES CABINETS OU BUREAUX D'ETUDES EN VUE DE LA REVISION DE LA POLITIQUE NATIONALE DE SECURITE DES RESEAUX DE COMMUNICATIONS ELECTRONIQUES ET DES SYSTEMES D'INFORMATION.

Financement : FSE, Exercice 2024

1. <u>Contexte et justification</u>

Les frontières de la sécurité des réseaux et des systèmes d'information s'étendent. Avec chaque nouvel appareil connecté, des découvertes numériques ou des processus automatisés, de nouvelles vulnérabilités et des préoccupations de sécurité émergent. Le paysage de la cybersécurité est en constante évolution, mais ce qui est évident, c'est que les cybermenaces deviennent de plus en plus graves et se produisent de plus en plus fréquemment.

Au Cameroun, une politique nationale de sécurité des réseaux de communications électroniques et des systèmes d'information a été élaborée en 2018 et mise en œuvre sur instruction du Premier Ministre Chef du Gouvernement. Elle a pour but de mettre en place un cadre référentiel national basé sur les standards et normes de sécurité adapté au contexte camerounais et international. Elle donne des orientations sur les activités de la sécurité des réseaux de communications électroniques et des systèmes d'information. Cette politique qui reflète la compréhension à l'échelon national des menaces et des risques qui pèsent sur le contexte de la sécurité du cyberespace, prenait son ancrage aussi bien dans le Document de Stratégie pour la Croissance et l'Emploi (DSCE) que dans la stratégie de développement de l'Economie Numérique et celle du domaine des Télécommunications et TIC qui constituaient ainsi un cadre de référence pour la période allant de 2010 à 2019.

Cependant, ladite politique nationale étant élaborée, il y'a cinq ans (05), ne tient plus compte de la sophistication des nouvelles attaques. En plus, elle n'est pas suffisamment connue et appropriée de toutes les parties prenantes par manque de vulgarisation. Le nouveau cadre de référence pour la période allant de 2020 à 2030 (SND 30) étant élaboré, il serait pertinent de s'assurer que la politique nationale de sécurité des réseaux de communications électroniques et des systèmes d'information cadre avec cette nouvelle vision de l'Etat. Suite aux évolutions socio-politiques, et technologique, ce qui a été valable pour un moment dans l'histoire ne trouve plus forcément sa légitimation à un autre moment d'où la possibilité voire la nécessité de réviser de temps en temps les textes. Des adaptations et ajustements sont à apporter. Aussi, les documents de politique ne tenaient pas en compte d'une politique de gestion des risques liés à la cybersécurité. En outre, il a été recommandé au Cameroun lors de l'évaluation de la maturité de ses capacités en matière de cybersécurité par des experts de la Banque Mondiale de :

- réviser et mettre à jour le projet de stratégie de cybersécurité et son plan d'actions, l'objectif étant de s'assurer que leur contenu tienne non seulement compte des composantes de référence, mais soit également en phase avec les besoins et priorités actuels du Cameroun dans le domaine de la cybersécurité.
- préciser les fonctions du CIRT-CM en matière d'intervention en cas d'incident au niveau national.

- établir des normes de cybersécurité claires dans les secteurs des infrastructures critiques concernées et veiller à la mise en place du mécanisme réglementaire approprié pour les faire respecter ;
- répertorier officiellement les infrastructures de communication critiques utilisées pour la gestion des urgences et des crises, et en informer toutes les parties prenantes.

De l'analyse de tout ce qui précède, il serait judicieux de réviser la politique nationale de sécurité des réseaux de communications électroniques et des systèmes d'information afin de prendre en compte l'ensemble des manquements constatés dans la politique actuelle et de l'adapter à l'environnement cybernétique actuel et futur.

2. Consistance des prestations

Le Cabinet ou bureau d'études aura pour mission d'accompagner le MINPOSTEL dans l'exécution des activités suivantes:

- l'évaluation de la mise en œuvre de la politique nationale de sécurité des réseaux de communications électroniques et des systèmes d'information ;
- la mise à jour de l'état des lieux et diagnostic ;
- la mise à jour de la stratégie nationale de sécurité des réseaux de communications électroniques et des systèmes d'information ;
- la mise à jour du Plan d'actions et dispositifs de mise en œuvre, de suivi et d'évaluation de la stratégie ;
- la mise à jour du projet de déclaration de la politique ;
- la réalisation des ateliers d'échanges.

3. Participation

Pour faire acte de candidature, les Cabinets ou Bureaux d'Etudes, devront justifier d'une compétence avérée et une expérience avérée dans les domaines des télécommunications, de la sécurité des réseaux et des systèmes d'information, de la cybersécurité, de la formation dans le domaine de sécurité des réseaux et systèmes d'informations et la lutte contre la cybercriminalité et dans l'élaboration des politiques de sécurité des systèmes d'information.

4. Composition du dossier de candidature

Le dossier de sollicitation à manifestation d'intérêt comprend un dossier administratif et un dossier technique.

4.1. Dossier administratif (enveloppe A)

Il 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) copie timbrée de l'attestation d'immatriculation ;
c) copie du registre du commerce, certifiée au greffe du tribunal de 1ère instance ;
d) copie timbrée de l'attestation de conformité fiscale;
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 1ère instance.

NB : En cas d'absence ou de non validité d'une pièce ci-dessus énumérées entrainera la non recevabilité du dossier.

4.2. Dossier technique (enveloppe B)

L'enveloppe B contiendra les informations suivantes :

- la présentation du cabinet ainsi que les domaines d'action et d'intervention ;

- la liste du personnel clé proposé avec les copies des diplômes et des CV signés par chaque expert ;
- les références du Cabinet d'Etudes pour les prestations similaires réalisées au cours des trois (03) dernières années ;
- la compréhension du mandat de mission (TDR).

En cas de groupement, tous les membres dudit groupement devront présenter les pièces b), c), d), e) et f).

5. Évaluation des offres et sélection des candidats

Les offres seront évaluées conformément aux critères ci-après :

5.1 Critères éliminatoires

N°	Désignations
01	Dossier administratif incomplet
02	Fausse déclaration, document falsifié
03	Note technique inférieure à 75 points sur 100

5.2 Critères de qualifications

a) **Expérience générale du cabinet .....30 points.**

- Au moins deux références dans l'élaboration des politiques de sécurité des systèmes d'information ...20 points.
- Au moins deux références dans le domaines des télécommunications, de la sécurité des réseaux et des systèmes d'information, de la cybersécurité, de la formation, de sécurité des réseaux et systèmes d'informations et la lutte contre la cybercriminalité .....10 points.

b) **Compréhension du mandat de mission (TDR).....20 points .**

- Bonne compréhension du travail demandé, bonne organisation du travail, planning de réalisation des prestations adéquat.....05 pts ;
- Cohérence dans la répartition des tâches entre le personnel.....05 pts ;
- Pertinence de la méthodologie proposée.....05 pts ;
- Pertinences des observations sur le TDR.....05 pts.

c) **Qualifications et compétence du personnel clé pour la mission .....50 points.**

- **Un (01) Chef de mission,** Ingénieur en Télécommunication ou Informatique, (BAC+5) ou Master en Télécommunications ou en Informatique, ayant une expertise en management des projets. Justifiant d'une expérience d'au moins quinze (15) ans dans le domaine de la sécurité des réseaux et système d'information et ayant conduit au moins deux (02) projets similaires en tant que Chef de mission. ..... 20 points ;
- **Un (01) Ingénieur en informatique, (BAC +5) ou Master en informatique,** ayant au moins dix (10) ans d'expérience en audit de sécurité des systèmes d'information et ayant participé à au moins deux (02) projets dans le domaine de la sécurité des systèmes d'informations. Certifié en audit ou sécurité des S.I. - CISA ou CISM ..... 10 points ;
- **Un (01) ingénieur en Télécom, BAC + 5 ou Master en Télécom,** justifiant d'au moins huit (08) ans d'expérience dans le domaine des communications électroniques et ayant participé à la réalisation d'au moins deux (02) projets dans le domaine de la sécurité des systèmes d'informations. Certifié en sécurité des systèmes d'information. (EC-Council et/ou ISACA, ISO 2700x, CISCO etc....)..... 10 points ;

- **Un (01) Ingénieur Statisticien** (BAC+5), ayant au moins cinq (05) ans d'expérience et ayant participé à la réalisation d'au moins deux (02) projets dans l'élaboration des stratégies de sécurité des réseaux et des systèmes d'information..... 10 points ;

Récapitulatif des critères de qualification

N°	Critères	Points
1	**Expérience générale du cabinet** (Références dans les prestations similaires)	30
2	Compréhension du mandat de la mission (contexte, objectifs, méthodologie, résultats, planning de réalisation)	20
3	Qualification et compétences du personnel pour la mission	50
Total		**100**

Seuls les candidats ayant totalisé, à l'issue de l'évaluation, une note technique au moins égale à 75 points sur 100, seront retenus pour participer à l'appel d'offres restreint.

6. **Dépôts des dossiers**

Les dossiers de candidature seront remis en cinq (05) exemplaires dont un (01) original et quatre (04) copies marquées comme tels, sous pli fermé scellé et comportant deux enveloppes distinctes à la Direction des Affaires Générales, Service des Marchés (porte 162), au Ministère des Postes et Télécommunications, au plus tard le 3 JUIN 2024 14 heures, heure locale et devra porter la mention :

AVIS D'APPEL A MANIFESTATION D'INTÉRÊT
N°00010/AMI/MPT/SG/DAG/SDBM/SMA/2024 DU 23 Avr 2024 POUR LA PRESELECTION DES CABINETS OU BUREAUX D'ETUDES EN VUE DE LA REVISION DE LA POLITIQUE NATIONALE DE SECURITE DES RESEAUX DE COMMUNICATIONS ELECTRONIQUES ET DES SYSTEMES D'INFORMATION.
« A n'ouvrir qu'en séance de dépouillement »

7. **Renseignements complémentaires**

Les candidats intéressés peuvent obtenir des renseignements complémentaires auprès au Ministère des Postes et Télécommunications, Direction de la Sécurité des Réseaux et des Systèmes d'Information, bâtiment annexe porte 108. Tél : 222 23 29 75 / 242 74 27 67.

8. **Publication des résultats**

L'Avis d'Appel d'Offres National Restreint (AONR) fera office de publication des résultats du présent avis d'Appel à Manifestation d'Intérêt./-

Le Ministre des Postes et Télécommunications

Minette Li Likeng
née Mendoma

REPUBLIQUE DU CAMEROUN
Paix-Travail-Patrie

MINISTERE DES POSTES ET TELECOMMUNICATIONS

SECRETARIAT GENERAL

REPUBLIC OF CAMEROON
Peace-Work-Fatherland

MINISTRY OF POSTS AND TELECOMMUNICATIONS

GENERAL SECRETARIAT

CALL FOR EXPRESSION OF INTEREST No. 0...1...AMI/MPT/SG/DAG/SDBM/SMA/2024 OF 23 AVR 2024 FOR THE ESTABLISHMENT OF A SHORTLIST OF FIRMS OR CONSULTING FIRMS WITH A VIEW TO REVISING THE NATIONAL POLICY ON THE SECURITY OF ELECTRONIC COMMUNICATIONS NETWORKS AND INFORMATION SYSTEMS.

Financing: ESF, 2024 financial year

1. Background and justification

The boundaries of network and information system security are expanding. With each new connected device, digital discovery or automated process, new vulnerabilities and security concerns emerge. The cyber security landscape is constantly evolving, but what is clear is that cyber threats are becoming more serious and occurring more frequently.

In Cameroon, a national security policy for electronic communications networks and information systems was drawn up in 2018 and implemented on the instructions of the Prime Minister Head of Government. Its aim is to put in place a national reference framework based on security standards and norms adapted to the Cameroonian and international context. It provides guidelines for activities relating to the security of electronic communications networks and information systems. This policy, which reflects a national understanding of the threats and risks to security in cyberspace, was anchored both in the Growth and Employment Strategy Paper (DSCE) and in the Digital Economy and Telecommunications and ICT development strategies, which provided a reference framework for the period from 2010 to 2019.

However, as this national policy was drawn up five years ago (05), it no longer takes account of the sophistication of new attacks. What's more, it is not sufficiently well known or appropriated by all stakeholders due to a lack of publicity. Now that the new reference framework for the period from 2020 to 2030 (SND 30) has been drawn up, it would be appropriate to ensure that the national security policy for electronic communications networks and information systems is in line with this new vision of the State. As a result of socio-political and technological developments, what was valid at one time in history is no longer necessarily legitimate at another time, hence the possibility or even the need to revise texts from time to time. Adaptations and adjustments need to be made. Also, the policy documents did not take into account a cybersecurity risk management policy. In addition, during the assessment of the maturity of its cybersecurity capabilities by World Bank experts, Cameroon was recommended to :

- revise and update the draft cybersecurity strategy and its action plan, the aim being to ensure that their content not only takes account of the reference components, but is also in line with Cameroon's current cybersecurity needs and priorities.
- specify the functions of the CIRT-CM in terms of incident response at national level.
- establish clear cybersecurity standards for the critical infrastructure sectors concerned and ensure that the appropriate regulatory mechanism is put in place to enforce them;
- officially list the critical communications infrastructures used for emergency and crisis management, and inform all stakeholders.

Based on an analysis of all the above, it would be advisable to revise the national security policy for electronic communications networks and information systems in order to take into account

all the shortcomings observed in the current policy and to adapt it to the current and future cyber environment.

2. Description of services

The firm or consulting firm will be responsible for supporting MINPOSTEL in carrying out the following activities:

- assessing the implementation of the national policy on the security of electronic communications networks and information systems ;
- updating the inventory and diagnosis ;
- updating the national security strategy for electronic communications networks and information systems ;
- updating the action plan and mechanisms for implementing, monitoring and evaluating the strategy;
- updating the draft policy statement ;
- holding exchange workshops.

3. Participation

To apply, firms or consulting firms must have proven competence and experience in the fields of telecommunications, network and information system security, cyber security, training in network and information system security, the fight against cyber crime and the development of information system security policies.

4. Application file

The application file for an expression of interest comprises an administrative file and a technical file.

4.1. Administrative documents (envelope A)

It shall include 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) stamped copy of the registration certificate ;
c) a copy of the commercial register, certified by the Registry of the Court of First Instance;
d) stamped copy of the certificate of tax compliance;
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.

NB : If any of the documents listed above are missing or invalid, the application will not be accepted.

4.2. 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;
- the list of key staff proposed with copies of certificates and CVs signed by each expert;
- references of the consulting firm for similar works executed during the past three (03) years;
- Understanding the mandate of the mission (ToR).

In the case of a grouping, all the members of the grouping must submit documents b), c), d), e) and f).

5. Evaluation of tenders and selection of candidates

Tenders will be evaluated in accordance with the following criteria:

5.1 Eliminatory criteria

No.	Designations
01	Incomplete administrative document
02	False declaration, forged document
03	Technical score below 75 points out of 100

5.2 Selection Criteria

a) **General experience of the firm .....30 points.**

- At least two references in the development of information systems security policies ...20 points.
- At least two references in the fields of telecommunications, network and information systems security, cybersecurity, training, network and information systems security and the fight against cybercrime .....10 points.

b) **Understanding of the mission (TOR).....20 points.**

- Proper understanding of the work requested, good organisation of the work, execution schedule of adequate services ..... 05 pts;
- Consistency in the distribution of tasks between the personnel.....05 pts;
- Relevance of the proposed methodology.....05 pts;
- Relevance of observations made on the TOR.....05 pts.

c) **Qualifications and skills of the key staff for the mission .....50 points.**

- One (01) **Mission Head,** telecommunications or IT engineer, (GCE A/L + 5 years university studies) or Master's degree in Telecommunications or IT, with expertise in project management. Proven experience of at least fifteen (15) years in the field of network and information system security and having led at least two (02) similar projects as Mission Head. ..... 20 points;
- **One (01) Computer Science Engineer (GCE A/L +5 years of university studies) or Master in Computer Science,** with at least ten (10) years' experience in information systems security audit and having participated in at least two (02) projects in the field of information systems security. Certified in I.S. audit or security. - CISA or CISM ..... 10 points;
- **One (01) telecoms engineer, GCE A/L + 5 years of university studies** or Master's degree in telecoms, with at least eight (08) years' experience in the field of electronic communications and having participated in at least two (02) projects in the field of information systems security.ity. Certified in information systems security. (EC-Council and/or ISACA, ISO 2700x, CISCO etc....)..... 10 points;
- **One (01) Statistical Engineer** (GCE A/L+5 years university studies), with at least five (05) years' experience and having participated in the implementation of at least two (02) projects in the development of network and information system security strategies..... 10 points;

Summary of the qualification criteria

No.	Criteria	Points
1	**General experience** of the firm (references for similar services)	30
2	Understanding the mandate of the mission (background, objective, methodology, results, implementation schedule)	20
3	Qualification and skills of the personnel for the mission	50
	Total	**100**

Only consultants with a technical score equal to at least a total mark of seventy (75) out of one hundred (100) points after the evaluation session shall be pre-selected for the limited invitation to tender.

6. **Submission of files**

Application files shall be submitted in five (05) copies including one (01) original and four (04) copies labelled as such, which shall be submitted in a sealed envelop containing two separate envelops to the Department of General Affairs, (room 162), at the Ministry of Posts and Telecommunications, not later than 3 JUIN 2024 at 2:30 pm, local time and shall carry the following label:

CALL FOR EXPRESSION OF INTEREST
No 00010 /AMI/MPT/SG/DAG/SDBM/SMA/2024 OF 23 Avril 2024 FOR THE ESTABLISHMENT OF A SHORTLIST OF FIRMS OR CONSULTING FIRMS WITH A VIEW TO REVISING THE NATIONAL POLICY ON THE SECURITY OF ELECTRONIC COMMUNICATIONS NETWORKS AND INFORMATION SYSTEMS.
"to be opened only during the bid-opening session"

7. **Additional information**

Interested candidates may obtain further information from the Ministry of Posts and Telecommunications, Department of Network Security and Information Systems, ancillary building, room 108. Tel.: 242 23 29 75 / 242 74 27 67.

8. **Publication of results**

The Restricted National Invitation to Tender shall be published as the result of this Call for Expression of Interest./-

The Minister of Posts and Telecommunications

REPUBLIQUE DU CAMEROUN Republic of Cameroon
LE MINISTRE The Minister
Ministry of Poste and Telecommunication MINISTERE DES POSTES ET TELECOMMUNICATIONS

Dr Libom Li Likeng
née Mendoma Minette