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

00 000011 AVIS D'APPEL A MANIFESTATION D'INTÉRÊT N°...../AMI/MPT/SG/DAG/SDBM/SMA/2026 DU ..0..2..AVR..2026..., POUR LA PRESELECTION DES CABINETS OU BUREAUX D'ETUDES EN VUE DE LA REALISATION DE L'ETUDE POUR L'ACQUISITION ET LA PROMOTION D'UN OUTIL DE CONTRÔLE PARENTAL POUR LES DISPOSITIFS EN LIGNE.

1. Contexte et justification

L'environnement numérique désigne l'ensemble des outils, des ressources et des services de communications électroniques mis à la disposition des utilisateurs pour communiquer, échanger et collaborer. Cet environnement a permis une diffusion rapide des informations à travers le monde avec un accès illimité à Internet. Aujourd'hui, enfants et adolescents grandissent connectés. Jeux, réseaux sociaux, apprentissage, tout passe par Internet. Cette immersion dans le monde en ligne ouvre d'immenses possibilités, mais soulève aussi des préoccupations majeures en matière de sécurité parmi lesquelles :

- **la cyberintimidation**: insultes, moqueries, harcèlement… Les réseaux sociaux et messageries en ligne peuvent devenir des terrains de malveillance persistante, avec un impact émotionnel profond.
- **l'exposition à des contenus inappropriés**: violence, pornographie, discours haineux ces contenus peuvent apparaître même sans recherche intentionnelle.
- **la manipulation et le leurre**: des individus malveillants peuvent se faire passer pour d'autres enfants ou adultes bienveillants afin de gagner la confiance de leur cible (on parle alors de grooming).
- **la surexposition des données personnelles**: en partageant leur nom, leur école, leurs photos ou leur localisation, les enfants peuvent involontairement alimenter des bases de données ou devenir des cibles.
- **l'addiction aux écrans**: les jeux en ligne et les réseaux sociaux peuvent générer une utilisation excessive, nuisant au sommeil, à la concentration ou aux interactions sociales réelles.
- **les arnaques et escroqueries**: certains sites ou applications incitent les jeunes à effectuer des achats, à divulguer des informations bancaires ou à cliquer sur des liens malveillants.

Les enfants représentant l'avenir d'une nation, assurer leur protection numérique est donc devenu une priorité pour les parents, les éducateurs, les entreprises technologiques et les gouvernements. Comprendre le contexte de leur protection, c'est poser les bases d'une sensibilisation efficace et de stratégies de protection adaptées à un environnement en constante évolution.

C'est fort de ce qui précède que le Cameroun a entrepris des grands chantiers sur les plans institutionnel, réglementaire et infrastructurel devant conduire vers l'émergence numérique à l'horizon 2035, notamment :

- la mise sur pied au sein du Ministère des Postes et Télécommunications (MINPOSTEL), d'une direction chargée de la sécurité des réseaux et des systèmes d'information (DSR) qui a entre autres, pour missions principales de :
  - Coordonner sur le plan national les activités concourant à la sécurisation et à la protection des réseaux de communications électroniques et des systèmes d'information ;
  - Vulgariser les mesures de protection des populations contre les actes de criminalité cybernétiques.

- l'adoption de la loi N°2023/009 du 25 juillet 2023 portant charte de la protection des enfants en ligne. Cette loi spéciale instaure un ensemble de mesures salutaires qui visent tant à prévenir qu'à réprimer les infractions contre les enfants en ligne.

Dans son article 4, la loi sus citée prévoit l'élaboration et la mise en œuvre par le MINPOSTEL, en collaboration avec les autres Administrations concernées, d'un Plan d'Actions National de Protection des Enfants en Ligne. La vision est de « Faire de l'écosystème numérique national un environnement sûr, sécurisé et sain pour tout enfant vivant au Cameroun ». Ce plan d'actions, après son élaboration et son examen par le comité et l'ensemble des parties prenantes dans la protection des enfants en ligne, propose plusieurs activités notamment l'acquisition des outils de contrôle parental pour les dispositifs en lignes et l'organisation de campagnes de sensibilisation et d'appropriation des pairs éducateurs, parents et personnel enseignant à l'usage de ces outils.

Les outils de contrôle parental sont des logiciels ou des fonctionnalités intégrées qui permettent aux parents de surveiller et de gérer l'utilisation d'Internet et des appareils numériques utilisés par leurs enfants. Ils offrent des moyens de filtrer le contenu inapproprié, de limiter le temps d'écran, de bloquer certaines applications ou sites web, et de contrôler les informations partagées.

En outre ces outils permettent notamment de :

- **filtrer le contenu** : empêcher l'accès à des sites web, des applications ou des contenus spécifiques considérés comme inappropriés pour l'âge de l'enfant ;
- **gérer le temps d'écran** : définir des limites de temps pour l'utilisation de l'appareil ou de certaines applications ;
- **surveiller l'activité** : consulter l'historique de navigation, les applications utilisées, et parfois même le contenu des messages ;
- **contrôler les achats** : empêcher les achats intégrés dans les applications ou les achats en ligne non autorisés ;
- **configurer des restrictions d'âge** : définir des restrictions basées sur l'âge pour les jeux, les applications et les contenus ;
- **localiser l'appareil** : dans certains cas, suivre la position géographique de l'appareil de l'enfant.

Cet instrument se présente donc comme un élément incontournable pour assurer aux enfants une sécurité optimale dans le cyberespace nécessaire à leur épanouissement. Toutefois il existe déjà une pléthore d'outils de control parental sur le marché mondial et même camerounais d'où la nécessité pour le Ministère des Postes et Télécommunications, de mener une étude préalable à ***« l'acquisition et la promotion d'un outil de control parental pour les dispositifs en ligne »***. La présente étude vise à fournir à l'État camerounais les besoins d'ordre techniques fonctionnels, opérationnels et financiers d'aide à la décision nécessaires pour la mise en œuvre efficace, équitable et durable de ce projet.

2. Consistance des prestations

Le Cabinet ou bureau d'études aura pour mission d'exécuter les activités suivantes:

Phase 1 : Etat des lieux et diagnostic

Il s'agit de collecter des données relatives aux outils et mécanismes de contrôle parental au Cameroun

a) États des lieux

- identifier les structures qui œuvrent dans la protection des enfants ;
- identifier les structures qui proposent des outils de control parental au Cameroun ;
- identifier l'expertise camerounaise à développer la solution ;
- identifier les différents modules contenus dans un outil de control parental ;
- recenser tous les outils de control parental existant au Cameroun ;
- collecter les données relativement à la taxation des différents outils de control parental (tarif moyen des outils, les différents services proposés, etc.) ;

- identifier les usages actuels d'Internet et des outils numériques par les enfants ;
- identifier les principaux risques en ligne auxquels les enfants sont exposés;
- identifier tous les textes réglementaires en rapport avec la protection des enfants ;
- relever les pertes de toute natures engendrés par l'absence d'outil de control parental dans le cyber espace national ;
- faire un benchmark des pratiques pour l'acquisition et la promotion d'un outil de control parental dans les pays de niveau de développement comparable au Cameroun.

b) Diagnostic

- exploiter et analyser les données issues de la collecte ;
- comparer les outils de contrôle parental existants (fonctionnalités, coûts, accessibilité, limites) ;
- analyser le marché et ressortir un plan de pérennisation de l'outil ;
- évaluer le niveau de connaissance et de sensibilisation des parents, des pairs éducateurs et du personnel enseignant en matière de protection en ligne ;
- ressortir les forces, les faiblesses, les opportunités et les menaces des outils collectés ;
- ressortir les enjeux économiques de l'acquisition et de la promotion d'un outil de control parental.

Phase 2 : propositions des mécanismes administratifs, techniques et opérationnels.
Il s'agira pour cette phase de proposer un plan stratégique pour l'achat d'un outil existant et la conception, le développement d'un nouvel outil.
Chacun de ces plans devra être accompagné d'un plan de déploiement, de maintenance et de promotion de l'outil de contrôle parental et des coûts y relatifs.
-Elaboration d'un plan stratégique pour l'achat accompagné d'un plan de déploiement et de maintenance de l'outil de control parental et des coûts y relatifs
-Elaboration d'un plan stratégique pour la conception et le développement accompagné d'un plan de déploiement et de maintenance de l'outil de control parental et des coûts y relatifs ;
Elaboration d'un plan de promotion de l'outil et du coût y relatif .

3. Financement

Les prestations objet du présent Appel à Manifestation d'Intérêt seront financées par le Compte d'Affectation Spécial du Trésor pour **les Activités de Sécurité Électronique (FSE),** Exercice **2026**.

4. Participation

Pour faire acte de candidature, les Cabinets ou Bureaux d'Etudes, devront justifier d'une compétence avérée et une expérience pertinente dans les domaines des TIC, de la sécurité des réseaux et des systèmes d'information et le développement d'applications et des logiciels.

5. Composition du dossier de candidature

Les dossiers de candidature sont divisés en deux sections et comprennent les pièces administratives (Section 1) et le Dossier technique (Section 2), enregistrés sur clé USB ou CD/DVD.

Section 1 : Pièces administratives
Cette section 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) Attestation d'immatriculation (NIU);
c) Copie du registre du commerce, certifiée au greffe du tribunal de 1ère instance ;
d) Attestation de conformité fiscale ;
e) Attestation de soumission signée par la Caisse Nationale de prévoyance sociale;
f) Attestation de non faillite (original ou copie certifiée par le greffe du tribunal de 1ère instance ;
g) Attestation de non exclusion des marchés publics délivrée par l'ARMP ;

Section 2 : Dossier technique

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 dans la réalisation des prestations similaires datant de moins de cinq (05) ans ;
- la compréhension du mandat de mission (TDR).

6. Critères d'évaluation et de sélection des cabinets

6.1. Critères éliminatoires :

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

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

6.2.Critères de qualifications

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

Au moins deux références dans la conception, le développement, le déploiement et la sécurisation des systèmes d'information de complexité similaire (applications, logiciel et progiciel) réalisées au cours des cinq (05) dernières années. ...(15 points par références).

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

N°	Désignation de l'activité		Note
1	Qualité de la solution proposée (Adéquation de la solution aux objectifs spécifiques, richesses fonctionnelles additionnelles, qualité de l'architecture technique) (2 pts)		/2
2	Observations et suggestions sur les termes de référence (2 pts)	0,5 pt/commentaire sur le besoin en personnel	/1
		0,5 pt/commentaire sur les TDR	/1
3	Approche méthodologique proposée en adéquation avec les TDR (8 pts)	Compréhension des objectifs de la mission (la compréhension des objectifs est jugée très bonne lorsque tous ceux-ci sont énumérés et mis en évidence)	/4
		Approche technique et méthodologie d'exécution (cette approche est jugée très bonne lorsqu'elle ne présente aucune ambiguïté)	/4
4	Plan de travail (8 pts)	Planning de réalisation adéquat des prestations (Cohérence entre l'organisation d travail et le planning de réalisation des prestations)	/4
		Planning de mobilisation du personnel	/4
	NB : Les appréciations ci-après seront portées par sous-critère : ***-Mauvais =0 ; moyen =2 ; bon=4.***		

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

- **Chef de mission : ....15 points.**

Etre titulaire d'un diplôme Bac+5 ou Master en informatique ou télécommunications. Justifier d'au moins quinze (15) ans d'expérience professionnelle dans le domaine des TIC, Télécommunications et Informatique, dont cinq (05) ans dans la conduite de projets liés à la sécurité des réseaux et des

systèmes d'information. Avoir participé à l'exécution d'au moins trois (03) projets dans le domaine des systèmes d'information, de conception des systèmes d'information de developpement de plateformes, de la sécurité des réseaux au cours des cinq (05) dernières années en qualité de chef de mission. Etre titulaire de la certification Project Management Professional (PMP) et d'au moins l'une des certifications suivantes : CISSP ou CISM ; Cisco Certified Internetwork Expert Security, Cisco ? PECB ISO2700X, EC-COUNCIL, ISACA .

- **Ingénieur en Informatique** ..... **10 points ;**

Etre titulaire d'un diplôme Bac+5 ou Master en Télécommunications ou en Informatique, génie logiciel ou systèmes d'information. Justifier d'au moins dix (10) ans d'expérience dans le domaine des systèmes d'information. Avoir participé à la réalisation d'au moins deux (02) projets dans la conception d'architectures applicatives et l'intégration de systèmes au cours des cinq (05) dernières années. Etre titulaire de certifications en sécurité des réseaux (PECB, ISACA, EC-COUNCIL…).

- **Expert en cybersécurité et protection des données**..... **10 points ;**

Etre titulaire d'un diplôme Bac+5 ou Master en télécommunications, cybersécurité, sécurité informatique. Justifier d'au moins dix (10) ans d'expérience dans le domaine de sécurité de réseaux et cybersécurité. Avoir participé à la réalisation d'au moins deux (02) projets de sécurité des systèmes d'information ou de mise en œuvre de politiques de sécurité et de protection des données au cours des cinq (05) dernières années. Etre titulaire de deux (02) certifications en sécurité des réseaux (PECB, ISACA, EC-COUNCIL…). CISSP ou CISM ; Cisco Certified Internetwork Expert Security, Cisco Certified Network Associate.

- **- Expert juriste en droit du numérique et cybersécurité**..... **7.5 points ;**

Etre titulaire d'un diplôme Bac+5 en droit. Justifier d'une expérience professionnelle d'au moins cinq (05) ans dans les questions juridiques liées aux TIC, à la cybercriminalité, à la protection des données et à la régulation des contenus en ligne. Avoir participé à la réalisation d'au moins une ou deux projets en droit du numérique, droit des TIC ou cybersécurité au cours des cinq (05) dernières années.

- **Ingénieur statisticien** ..... **7.5 points ;**

Etre titulaire d'un diplôme d'Ingénieur Statisticien ou Economiste, Financier, Gestion (BAC+5) ou équivalent. Justifier d'au moins cinq (05) ans d'expérience dans le domaine d'analyse économique ou financière, des Technologies de l'Information et de la Communication. Avoir participé à la réalisation d'au moins deux (02) projets dans le domaine des TIC et dans l'élaboration des stratégies de sécurité des réseaux et des systèmes d'information au cours des trois (03) dernières années.

NB : Le personnel proposé par le Candidat ne sera évalué que si les justificatifs ci-après ont été produits : copie du diplôme, curriculum vitae dûment signé et daté par l'expert, justificatifs des expériences déclarées.

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**

NB : 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.

7. Dépôts des dossiers

Les dossiers de candidature devront être transmises par le soumissionnaire sur la plateforme COLEPS. Chaque offre rédigée en français ou en anglais devra faire l'objet d'une soumission en ligne au plus tard le ….14 MAI 2026 à **14 heures précises**, heure locale, à l'adresse www.marchespublics.cm. Dans les mêmes délais, une copie de sauvegarde dudit dossier enregistrée sur clé USB ou CD/DVD et sous pli scellé sera déposée au Ministère des Postes et Télécommunications, Direction des Affaires Générales (Service des marchés publics 1er étage, porte 162), avec la mention :

AVIS D'APPEL A MANIFESTATION D'INTÉRÊT N°……/AMI/MPT/SG/DAG/SDBM/SMA/2026 DU ……., POUR LA PRESELECTION DES CABINETS OU BUREAUX D'ETUDES EN VUE DE LA REALISATION DE L'ETUDE POUR L'ACQUISITION ET LA PROMOTION D'UN OUTIL DE CONTRÔLE PARENTAL POUR LES DISPOSITIFS EN LIGNE.

« A n'ouvrir qu'en séance de dépouillement »

8. 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.

9. Publication des résultats

Le résultat du présent Avis d'Appel à Manifestation d'Intérêt sera publié dans le JDM et sur la plateforme COLEPS./-

Le Ministre des Postes et Télécommunications

LE MINISTRE The Minister

Mme Libom Li Likong née Mendoma Minette

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

00 000011 CALL FOR EXPRESSION OF INTEREST No. ...../AMI/MPT/SG/DAG/SDBM/SMA/2026 OF 10 2 AVR 2026 ....., FOR SHORTLISTING FIRMS OR CONSULTING FIRMS TO CARRY OUT A STUDY FOR THE ACQUISITION AND PROMOTION OF A PARENTAL CONTROL TOOL FOR ONLINE DEVICES.

1. Background and justification

The digital environment refers to the range of tools, resources and electronic communication services made available to users for communicating, exchanging information and collaborating. This environment has enabled the rapid dissemination of information across the globe with unlimited access to the internet. Today, children and teenagers are growing up connected. Games, social media, learning – everything happens online. This immersion in the online world opens up immense possibilities, but also raises major safety concerns, including:

- **cyberbullying**: insults, mockery, harassment… Social media and online messaging platforms can become breeding grounds for persistent malice, with a profound emotional impact.
- **exposure to inappropriate content**: violence, pornography, hate speech – such content can appear even without an intentional search.
- **manipulation and deception**: malicious individuals may pose as other children or caring adults in order to gain their target's trust (this is known as grooming).
- **over-sharing of personal data**: by sharing their name, school, photos or location, children may unwittingly feed into databases or become targets.
- **Screen addiction**: online games and social media can lead to excessive use, affecting sleep, concentration or real-life social interactions.
- **Scams and fraud**: certain websites or apps encourage young people to make purchases, disclose banking details or click on malicious links.

As children represent the future of a nation, ensuring their digital protection has therefore become a priority for parents, educators, technology companies and governments. Understanding the context of their protection lays the foundations for effective awareness-raising and protection strategies adapted to a constantly evolving environment.

It is against this backdrop that Cameroon has undertaken major initiatives at the institutional, regulatory and infrastructural levels, aimed at achieving digital emergence by 2035, notably:

- the establishment within the Ministry of Posts and Telecommunications (MINPOSTEL) of a Directorate responsible for network and information system security (DSR), whose main tasks include:
  - Coordinating, at national level, activities aimed at securing and protecting electronic communications networks and information systems;
  - Raising public awareness of measures to protect people against cybercrime.
- The adoption of Law No. 2023/009 of 25 July 2023 establishing a charter for the protection of children online. This special law introduces a set of beneficial measures aimed at both preventing and punishing offences against children online.

In Article 4, the aforementioned law provides for the development and implementation by MINPOSTEL, in collaboration with other relevant government departments, of a National Action Plan for the Protection of Children Online. The vision is to 'make the national digital ecosystem a safe, secure and healthy environment for every child living in Cameroon'. Once this action plan has

been drawn up and reviewed by the committee and all stakeholders involved in child protection online, it proposes a number of activities, including the provision of parental control tools for online platforms and the organisation of awareness-raising campaigns to help peer educators, parents and teaching staff become familiar with the use of these tools.

Parental control tools are software programmes or built-in features that allow parents to monitor and manage their children's use of the internet and digital devices. They provide ways to filter inappropriate content, limit screen time, block certain apps or websites, and control the information shared.

In addition, these tools enable users to:

- **filter content**: prevent access to websites, apps or specific content deemed inappropriate for the child's age;
- **manage screen time**: set time limits for the use of the device or certain apps;
- **monitor activity**: view browsing history, apps used, and sometimes even the content of messages;
- **control purchases**: prevent in-app purchases or unauthorised online purchases;
- **set age restrictions**: define age-based restrictions for games, apps and content;
- **locate the device**: in some cases, track the geographical location of the child's device.

This tool is therefore essential for ensuring that children enjoy the optimal online safety they need to thrive. However, there is already a plethora of parental control tools on the global market and even in Cameroon, hence the need for the Ministry of Posts and Telecommunications to conduct a preliminary study on ***"the acquisition and promotion of a parental control tool for online devices"***. This study aims to provide the Cameroonian government with the technical, functional, operational and financial requirements necessary for decision-making to ensure the effective, equitable and sustainable implementation of this project.

2. Description of services

The firm or consulting firm will be tasked with carrying out the following activities:

Phase 1: inventory and diagnosis

This involves collecting data on parental control tools and mechanisms in Cameroon

a) Current situation

- identify organisations working in the field of child protection;
- identify organisations offering parental control tools in Cameroon;
- identify Cameroonian expertise to develop the solution;
- identify the various modules contained within a parental control tool;
- catalogue all existing parental control tools in Cameroon;
- collect data on the pricing of various parental control tools (average cost of tools, the different services offered, etc.);
- identify children's current use of the internet and digital tools;
- identify the main online risks to which children are exposed;
- identify all regulatory texts relating to child protection;
- identify losses of all kinds caused by the absence of parental control tools in the national cyberspace;
- conduct a benchmarking exercise of practices for the acquisition and promotion of parental control tools in countries with a level of development comparable to that of Cameroon.

b) Diagnosis

- Extract and analyse the data collected;
- Compare existing parental control tools (features, costs, accessibility, limitations);
- Analyse the market and develop a plan for the tool's long-term sustainability;

- Assess the level of knowledge and awareness among parents, peer educators and teaching staff regarding online protection;
- identify the strengths, weaknesses, opportunities and threats of the tools collected;
- highlight the economic implications of acquiring and promoting a parental control tool.

Phase 2: proposals for administrative, technical and operational mechanisms.
This phase will involve proposing a strategic plan for the procurement of an existing tool and the design and development of a new tool.
Each of these plans must be accompanied by a plan for the deployment, maintenance and promotion of the parental control tool, along with the associated costs.
- Development of a strategic plan for the purchase, accompanied by a plan for the deployment and maintenance of the parental control tool and the associated costs
- Development of a strategic plan for the design and development, accompanied by a plan for the deployment and maintenance of the parental control tool and the associated costs;
Development of a promotion plan for the tool and the associated costs.

3. Financing

The services covered by this Call for Expressions of Interest will be financed by the Treasury's Special Earmarked Account for **Electronic Security Activities (FSE), 2026** Financial Year.

4. Participation

To apply, consultancies or engineering firms must demonstrate proven expertise and relevant experience in the fields of ICT, network and information systems security, and the development of applications and software.

5. Application file

Application files are divided into two sections and comprise administrative documents (Section 1) and the Technical Documents (Section 2), saved on a USB stick or CD/DVD.

Section 1: Administrative documents
This section 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) Registration certificate (NIU);
c) Copy of the commercial register, certified by the clerk's office of the court of first instance;
d) Certificate of tax compliance;
e) Certificate of submission signed by the National Social Security Fund;
f) Certificate of non-bankruptcy (original or copy certified by the Clerk's Office of the Court of First Instance;
g) a certificate of non exclusion from public contracts issued by the ARMP;

Section 2: Technical file
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 from the consulting firm for similar services provided within the last five (05) years;
- Understanding the mandate of the mission (ToR).

6. Evaluation and selection criteria of firms

6.1. Eliminatory criteria:

No.	Designations
01	Incomplete administrative document

02	False declaration, forged document
03	Technical score below 75 points out of 100

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

6.2.Selection Criteria

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

At least two references in the design, development, deployment and security of information systems of similar complexity (applications, software and software packages) completed within the last five (05) years. ...(15 points per reference).

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

No	Designation of the activity		Score
1	Quality of the proposed solution (Adequacy of the solution to the specific objectives, additional functional richness, quality of the technical architecture)(2 pts)		/2
2	Comments and suggestions on the TOR (2 pts)	0.5 pt/comment on staffing requirements	/1
		0, 5 pt/comment on the ToR	/1
3	Proposed methodological approach in line with the ToR (8 pts)	Understanding of the mission's objectives (the understanding of the objectives is deemed to be very good when all of them are listed and highlighted).	/4
		Technical approach and implementation methodology (this approach is deemed to be very good when it is unambiguous)	/4
4	Work plan (8 pts)	Adequate schedule for carrying out the services (consistency between the organisation of the work and the schedule for carrying out the services)	/4
		Staff mobilisation schedule	/4
	NB : The following assessments will be made for each sub-criterion: ***-Poor =0; average =2; good=4.***		

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

- **Mission Head: .....15 points.**

Be holder of a GCE A/L+5 years university studies or Master's degree in computer science or telecommunications. Must have at least fifteen (15) years' professional experience in the field of ICT, Telecommunications and Computer Science, including five (5) years in managing projects related to network and information system security. Must have participated in the delivery of at least three (3) projects in the field of information systems, information systems design, platform development and network security over the last five (5) years in the role of project manager. Be holder the Project Management Professional (PMP) certification and at least one of the following certifications: CISSP or CISM; Cisco Certified Internetwork Expert Security, Cisco? PECB ISO2700X, EC-COUNCIL, ISACA .

- **Computer Science Engineer ..... 10 points;**

Be holder of GCE A/L + 5 years university studies or a Master's degree in Telecommunications, Computer Science, Software Engineering or Information Systems. Must have at least ten (10) years' experience in the field of information systems. Must have participated in the delivery of at least two (02) projects involving application architecture design and systems integration over the last five (05) years. Be holder of certifications in network security (PECB, ISACA, EC-COUNCIL, etc.).

- **Expert in cybersecurity and data protection**..... **10 points;**

Be holder of a GCE A/L+5 years university studies or Master's degree in computer science Telecommunications sub-sector., security. Must have at least ten (10) years' experience in the field of network security and cybersecurity. Must have participated in the delivery of at least two (02) information systems security projects or the implementation of security and data protection policies over the last five (05) years. Be holder of two (02) network security certifications (PECB, ISACA, EC-COUNCIL, etc.). CISSP or CISM; Cisco Certified Internetwork Expert Security, Cisco Certified Network Associate.

- **Legal expert in digital law and cybersecurity**..... **7.5 points;**

Be holder of a GCE A/L+5 years university studies in Law. Demonstrate at least five (05) years' professional experience in legal matters relating to ICT, cybercrime, data protection and the regulation of online content. Must have participated in the implementation of at least one or two projects in digital law, ICT law or cybersecurity over the last five (05) years.

- **Statistical Engineer**..... **7.5 points;**

Be holder of a diploma in Statistical Engineering or Economics, Finance, Management (GCE A/L+5 years of higher education) or equivalent diploma. Demonstrate at least five (05) years' experience in the field of economic or financial analysis, or Information and Communication Technologies. Must have participated in the implementation of at least two (02) projects in the field of ICT and in the development of network and information system security strategies over the last three (03) years.

NB : The personnel proposed by the applicant will only be assessed if the following documents are submitted: copy of the diploma, curriculum vitae duly signed and dated by the expert, supporting documents for the declared experience.

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**

NB : 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.

7. Submission of files

Applications must be submitted by the tenderer via the COLEPS platform. Each tender, written in French or English, must be submitted online by no later than on ....4 MAI 2026..... at **2 p.m. prompt** local time on www.marchespublics.cm Within the same timeframe, a backup copy of the said application, saved on a USB stick or CD/DVD and placed in a sealed envelope, must be submitted to the Ministry of Posts and Telecommunications, Department of General Affairs (Public Contracts Service, 1st floor, room 162), labelled as follows :

CALL FOR EXPRESSION OF INTEREST
No. ...../AMI/MPT/SG/DAG/SDBM/SMA/2026 OF ....., FOR SHORTLISTING FIRMS OR CONSULTING FIRMS TO CARRY OUT A STUDY FOR THE ACQUISITION AND PROMOTION OF A PARENTAL CONTROL TOOL FOR ONLINE DEVICES.
"to be opened only during the bid-opening session"

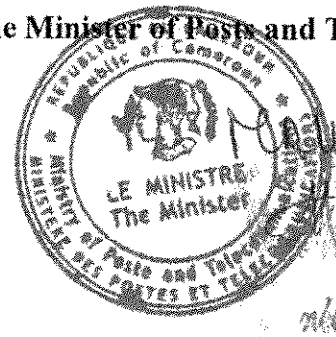
8. Additional information

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.: 222 23 29 75 / 242 74 27 67.

9. Publication of results

The result of this Call for Expressions of Interest will be published in the platform JDM and on the COLEPS platform /-.

The Minister of Posts and Telecommunications



Dr. Libom Li Likeng
née Mendoma Minette