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 000010

AVIS D'APPEL A MANIFESTATION D'INTÉRÊT N°...../AMI/MPT/SG/DAG/SDBM/SMA/2026 DU 02 AVR 2026, POUR LA PRESELECTION DES CABINETS OU BUREAUX D'ETUDES EN VUE DE LA REALISATION DE L'ETUDE DE MISE EN PLACE DE LA PLATEFORME NATIONALE DE SIGNALEMENT DES CONTENUS ILLICITES POUR LA PROTECTION DES ENFANTS EN LIGNE.

1. Contexte et justification

Les Technologies de l'Information et de la Communication (TIC) occupent aujourd'hui une place centrale dans les activités économiques, sociales, éducatives et culturelles. Elles offrent aux citoyens des opportunités inédites d'accès à l'information, de communication, de participation à la vie publique et de partage des connaissances.

Cependant, l'essor rapide du numérique et l'usage massif d'Internet s'accompagnent également de nombreux risques pour les usagers. Les espaces numériques sont devenus des environnements où circulent divers contenus et pratiques susceptibles de porter atteinte aux droits et à la sécurité des individus. Parmi ces dérives figurent notamment le cyberharcèlement, le grooming, la diffusion de contenus illicites ou inappropriés, la violation et l'utilisation abusive des données personnelles, la radicalisation en ligne, ainsi que les abus et exploitations sexuels.

Les couches vulnérables de la population, en particulier les enfants, les femmes et les personnes âgées, sont particulièrement exposées à ces menaces dans le cyberespace. Face à ces risques croissants, les pouvoirs publics camerounais ont engagé plusieurs initiatives visant à renforcer la protection des citoyens dans l'environnement numérique.

Dans cette perspective, un projet de loi portant Charte de protection des enfants en ligne, défendu par le Ministre des Postes et Télécommunications devant les deux chambres du Parlement, a été adopté. Cette initiative a conduit à l'élaboration d'un Plan d'Action National pour la Protection des Enfants en Ligne, piloté par le Ministère des Postes et Télécommunications (MINPOSTEL) en collaboration avec les administrations et partenaires concernés.

Toutefois, malgré ces avancées, la lutte contre les contenus illicites en ligne nécessite la mise en place de mécanismes opérationnels permettant aux citoyens de signaler facilement les contenus ou comportements préjudiciables rencontrés sur Internet, et aux autorités compétentes d'en assurer le traitement rapide et efficace.

C'est dans ce contexte que le MINPOSTEL envisage la mise en place d'une Plateforme Nationale de Signalement des Contenus Illicites en Ligne (PNSCIL). Cette plateforme constituera un outil stratégique permettant de centraliser les signalements des contenus illicites diffusés sur Internet, d'améliorer la coordination entre les différentes parties prenantes et de faciliter les actions de prévention, de retrait et de poursuite lorsque cela est nécessaire.

La mise en œuvre de cette plateforme poursuit notamment les objectifs suivants :

- Protéger les droits et libertés des citoyens : garantir la sécurité numérique des utilisateurs et préserver leur dignité, leur image et leurs données personnelles ;
- Faciliter le signalement des contenus illicites : offrir aux internautes un mécanisme accessible et sécurisé pour signaler les contenus ou comportements illégaux rencontrés en ligne ;
- Renforcer la lutte contre la diffusion de contenus illicites : améliorer la détection, l'analyse et le traitement rapide des contenus signalés ;

- Améliorer la sécurité de l'espace numérique national : contribuer à un environnement numérique plus sûr pour tous les usagers, notamment les populations vulnérables ;
- S'aligner sur les bonnes pratiques et normes internationales en matière de régulation des contenus en ligne et de protection des droits de l'homme dans l'espace numérique.

Ainsi, la Plateforme Nationale de Signalement des Contenus Illicites en Ligne s'inscrit comme un dispositif clé de la stratégie nationale de cybersécurité et de protection des usagers du cyberespace au Cameroun.

2. Consistance des prestations

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

Activité 1: Collecte des données et d'analyse des informations (Recensement des instruments juridiques et analyse des mécanismes de leurs mises en œuvre ; Consultations et entretiens avec les parties prenantes)

Activité 2: Benchmark des bonnes pratiques (Identification des expériences internationales pertinentes et Analyse des bonnes pratiques et enseignements tirés)

Activité 3: Fourniture des éléments de conception de la plateforme

A partir des études issues de la collecte des données et du benchmark, le prestataire devra :

- proposer une architecture technique de fonctionnement de la plateforme, cette architecture devra être fiable, sécurisée et évolutive garantissant la confidentialité des signalements, la protection des données personnelles et la traçabilité des traitements ;
- proposer une architecture logicielle de la plateforme intégrant les fonctionnalités issus des besoins exprimés dans l'activité 1;
- présenter les fonctionnalités nécessaires permettant le signalement, la gestion, le traitement et le suivi des contenus illicites par les citoyens, les autorités compétentes et les partenaires concernés ;
- proposer les possibilités d'interconnexion et d'échange de données entre la future plateforme nationale et les systèmes d'information des institutions partenaires (forces de sécurité, autorités judiciaires, régulateurs, plateformes numériques, opérateurs de télécommunications, etc.), afin de faciliter la transmission, le traitement et le suivi des signalements ;
- définir les procédures de réception, de qualification, de transmission et de traitement des signalements entre les différentes institutions compétentes ;
- proposer des options d'hébergement de la plateforme ;
- identifier les ressources humaines, techniques, organisationnelles et financières nécessaires pour le développement, l'exploitation et la maintenance de la plateforme ;
- définir un dispositif de gouvernance permettant une coordination efficace entre les institutions impliquées dans la lutte contre les contenus illicites en ligne ;
- proposer une stratégie de sensibilisation et de communication visant à informer les citoyens sur l'existence de la plateforme, les encourager à signaler les contenus illicites et promouvoir un usage responsable d'Internet ;
- proposer une stratégie de pérennisation de la plateforme.

Activité 4: Estimation des coûts de développement de la plateforme

Le prestataire devra faire une analyse afin de proposer une estimation de coût de mise en place de la plateforme.

Il devra élaborer les éléments de maturité relatifs au développement et au déploiement de la solution à savoir :

- ✓ les TDR assortis d'une feuille de route de développement de la plateforme ;

✓ la note conceptuelle relative à la mise en place de cette plateforme.

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 référence).

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 TDR (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 : Expert en gouvernance du numérique** .....**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 aux TIC ou aux systèmes d'information ou à la transformation numérique. 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 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.

- **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 en analyse des processus et transformation numérique..... 05 points ;

Etre titulaire d'un diplôme Bac+5 ou Master en systèmes d'information ou management.

Justifier d'une expérience professionnelle d'au moins dix (10) ans dans l'analyse et la modélisation des processus. Avoir participé à la réalisation d'au moins deux (02) projets dans la conception de workflows et la transformation numérique des organisations.

- Expert en communication et sensibilisation numérique..... 05 points ;
Etre titulaire d'un diplôme Bac+5 ou Master en communication ou sciences sociales.
Justifier d'une expérience professionnelle d'au moins cinq (05) ans dans la communication institutionnelle ou les campagnes de sensibilisation. Avoir participé à la réalisation d'au moins deux (02) projets dans la conception de workflows et la transformation numérique des organisations au cours des cinq (05) dernières années.

- Expert juriste en droit du numérique et cybersécurité..... 05 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.

NB : Le personnel proposé par le Candidat ne sera évalué que si les justificatifs ci-après ont été produits : copie certifiée du diplôme, curriculum vitae dûment signé et daté par l'expert, justificatifs des expériences déclarées (Contrat travail/certificat de travail/ Attestation de service …).

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	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 ...4 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 DE MISE EN PLACE DE LA PLATEFORME NATIONALE DE SIGNALEMENT DES CONTENUS ILLICITES POUR LA PROTECTION DES ENFANTS 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

Libom Li Likong
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

00000010 CALL FOR EXPRESSION OF INTEREST, No...../AMI/MPT/SG/DAG/SDBM/SMA OF 02 AVR 2026..., FOR SHORTLISTING FIRMS OR CONSULTING FIRMS TO CARRY OUT THE STUDY ON THE IMPLEMENTATION OF THE NATIONAL PLATFORM FOR REPORTING ILLEGAL CONTENT FOR THE PROTECTION OF CHILDREN ONLINE.

1. Background and justification

Information and Communication Technologies (ICT) now play a central role in economic, social, educational and cultural activities. They offer citizens unprecedented opportunities to access information, communicate, participate in public life and share knowledge.

However, the rapid growth of digital technology and the widespread use of the internet also bring with them numerous risks for users. Digital spaces have become environments where various forms of content and practices circulate that may infringe upon individuals' rights and compromise their safety. These abuses include, in particular, cyberbullying, grooming, the dissemination of illegal or inappropriate content, the violation and misuse of personal data, online radicalisation, as well as sexual abuse and exploitation.

Vulnerable sections of the population, particularly children, women and the elderly, are particularly exposed to these threats in cyberspace. In response to these growing risks, the authorities of Cameroon have launched several initiatives aimed at strengthening the protection of citizens in the digital environment.

With this in mind, a draft law on the Charter for the Protection of Children Online, presented by the Minister of Posts and Telecommunications to both houses of Parliament, has been adopted. This initiative led to the development of a National Action Plan for the Protection of Children Online, spearheaded by the Ministry of Posts and Telecommunications (MINPOSTEL) in collaboration with the relevant government departments and partners.

However, despite these advances, the fight against illegal online content requires the establishment of operational mechanisms enabling citizens to easily report harmful content or behaviour encountered on the internet, and allowing the competent authorities to deal with it swiftly and effectively.

It is in this context that MINPOSTEL is planning to establish a National Platform for Reporting Illegal Online Content (PNSCIL). This platform will serve as a strategic tool to centralise reports of illegal content disseminated on the internet, improve coordination between the various stakeholders, and facilitate preventive measures, removal and prosecution where necessary.

The implementation of this platform aims, in particular, to achieve the following objectives:

- Protect citizens' rights and freedoms: guarantee users' digital security and safeguard their dignity, reputation and personal data;
- Facilitate the reporting of illegal content: provide internet users with an accessible and secure mechanism to report illegal content or behaviour encountered online;
- Strengthening the fight against the dissemination of illegal content: improving the detection, analysis and rapid processing of reported content;
- Improving the security of the national digital space: contributing to a safer digital environment for all users, particularly vulnerable groups;

- Aligning with international best practices and standards regarding the regulation of online content and the protection of human rights in the digital space.

Thus, the National Platform for Reporting Illegal Online Content is a key component of the national strategy for cybersecurity and the protection of cyberspace users in Cameroon.

2. Description of services

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

Activity 1: Data collection and information analysis (Survey of legal instruments and analysis of their implementation mechanisms; Consultations and interviews with stakeholders)

Activity 2: Benchmarking of best practices (Identification of relevant international experiences and analysis of best practices and lessons learnt)

Activity 3: Provision of the platform's design elements

Based on the studies resulting from the data collection and benchmarking, the service provider must:

- propose a technical architecture for the platform's operation; this architecture must be reliable, secure and scalable, ensuring the confidentiality of reports, the protection of personal data and the traceability of processing operations;
- propose a software architecture for the platform incorporating the functionalities derived from the requirements set out in Activity 1;
- present the necessary functionalities enabling the reporting, management, processing and monitoring of illegal content by citizens, the competent authorities and the relevant partners;
- propose options for interconnection and data exchange between the future national platform and the information systems of partner institutions (law enforcement agencies, judicial authorities, regulators, digital platforms, telecommunications operators, etc.), in order to facilitate the transmission, processing and follow-up of reports;
- define procedures for the receipt, classification, transmission and processing of reports between the various competent institutions;
- propose options for hosting the platform;
- identify the human, technical, organisational and financial resources required for the development, operation and maintenance of the platform;
- establish a governance framework to ensure effective coordination between the institutions involved in combating illegal online content;
- propose an awareness-raising and communication strategy aimed at informing the public about the platform's existence, encouraging them to report illegal content, and promoting responsible use of the internet;
- propose a strategy to ensure the platform's long-term sustainability.

Activity 4: Estimation of the platform's development costs

The service provider must carry out an analysis to provide a cost estimate for setting up the platform.

They must draw up the maturity elements relating to the development and deployment of the solution, namely:

- ✓ the terms of reference (ToR) accompanied by a platform development roadmap;
- ✓ the concept note relating to the implementation of this platform.

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: Expert in digital governance** .....**15 points.**

Be holder of a GCE A/L+5 years university studies or Master's degree in computer science or telecommunications. Demonstrate at least fifteen (15) years' professional experience in the field of ICT, telecommunications and computer science, including five (05) years in the management of projects related to ICT, information systems or digital transformation. Must have participated in the execution of at least three (03) projects in the field of information systems, information systems design or platform development over the last five (05) 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

- **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.

- **Expert in process analysis and digital transformation..... 05 points;**

Be holder of a fGCE A/L + 5 years university studies or Master's degree in information systems or management. Demonstrate at least ten (10) years' professional experience in process analysis and modelling. Must have participated in the delivery of at least two (02) projects involving workflow design and the digital transformation of organisations.

- **Expert in digital communication and aware-raising..... 05 points;**

Be holder of a GCE A/L+5 years university studies or Master's degree in communications or social sciences. Demonstrate at least five (5) years' professional experience in corporate communications or awareness-raising campaigns. Must have been involved in the delivery of at least two (02) projects relating to workflow design and the digital transformation of organisations over the last five (05) years.

- **Legal expert in digital law and cybersecurity…….. 05 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.

NB : The staff proposed by the Candidate will only be assessed if the following supporting documents have been provided: a certified copy of the degree, a curriculum vitae duly signed and dated by the expert, and evidence of the experience declared (employment contract/certificate of employment/certificate of service, etc.).

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 2020 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 OF ……., FOR SHORTLISTING FIRMS OR CONSULTING FIRMS TO CARRY OUT THE STUDY ON THE IMPLEMENTATION OF THE NATIONAL PLATFORM FOR REPORTING ILLEGAL CONTENT FOR THE PROTECTION OF CHILDREN ONLINE.
"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

LE MINISTRE
The Minister

Libom Li Likeng
née Mendoma Minette