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

00000014 AVIS D'APPEL A MANIFESTATION D'INTÉRÊT N°...../AMI/MPT/SG/DAG/SDBM/SMA/2024 DU 28 JUIN 2024 POUR LA PRESELECTION DES CABINETS OU BUREAUX D'ETUDES EN VUE DE L'ELABORATION D'UN MANUEL DE PROCEDURES D'INVESTIGATION NUMERIQUE

Financement : FSE, Exercice 2024

1. Contexte et justification

Les réseaux de communications électroniques et les Technologies de l'Information et de la Communication (TIC) sont devenus des outils indispensables pour les gouvernements, les entreprises, la société civile et les individus à travers le monde. Ces technologies ont favorisé un développement économique considérable, ont augmenté la libre circulation des informations, et ont contribué à des gains réels sur le plan du rendement, de l'efficacité, de la productivité et de la créativité à travers le monde.

L'utilisation des TIC, internet en particulier, est devenue une question d'importance stratégique pour les pays. Un internet ouvert et sécurisé représente un moteur de croissance économique et du développement social qui facilite la communication, l'innovation, la recherche scientifique et la transformation des administrations et des entreprises.

Cependant, l'utilisation croissante de l'internet a conduit à de nouveaux défis pour la communauté nationale et internationale. En effet, plus nous sommes connectés, plus nous nous exposons aux menaces cybernétiques. Par ailleurs, l'évolution rapide de l'internet a créé de nouvelles opportunités pour commettre des activités de cybercriminalité à grande échelle. Des individus tapis dans l'ombre utilisent les TIC pour poser des actes malveillants aux conséquences dommageables pour les administrations, les entreprises et les usagers. Les plaintes des victimes concernent notamment la diffamation, l'usurpation d'identité, les menaces, les violences verbales, les insultes, les arnaques, le piratage de données, le montage de photos ou vidéos à l'effet de nuire.

A titre d'illustration sur l'ampleur du phénomène de cybercriminalité au Cameroun, quelques statistiques obtenues des services compétents révèlent 3 388 cas d'usurpation d'identités en 2018, 2050 plaintes relatives au scamming et au phishing dont environ 5 milliards FCFA de perte financière, près de 6 milliards de pertes relatives aux fraudes bancaires, 11 617 vulnérabilités détectés sur les sites webs des administrations publiques en 2019.

Face à tous ces maux, le gouvernement du Cameroun n'est pas resté inerte. Pour lutter efficacement contre les actes déviants perpétrés par les cybercriminels dans le cyberespace camerounais, il a mis en place un cadre stratégique, juridique et institutionnel. Cependant, malgré toutes les solutions mises en place, les magistrats et les officiers de police judiciaire éprouvent des difficultés pour appréhender les concepts nouveaux relatifs à la cybersécurité et à la cybercriminalité d'une part, et à la conduite des investigations numériques d'autre part. Ces derniers ont évoqué ces difficultés lors du forum national sur la cybersécurité et la lutte contre la cybercriminalité qui s'est tenu du 03 au 05 novembre 2020 au Palais des Congrès de Yaoundé. Ils ont affirmé qu'il n'existe pas un cadre formel qui explique les différentes étapes d'une investigation numérique. Or, le Ministère des Postes et

Télécommunications est entre autres chargé de promouvoir la sécurité des réseaux et des systèmes d'information. Il est par ailleurs chargé de la coordination des activités de sécurité des réseaux et des systèmes d'information. Fort de ces constats, le forum susmentionné a préconisé comme recommandation « l'élaboration d'un manuel de procédures en matière d'investigations numériques ».

Par ailleurs, la justification de la nécessité d'un manuel standardisé pour les procédures d'investigation numérique au Cameroun repose sur plusieurs points clés, entre autres :

- l'uniformisation des Pratiques : un manuel standardisé permet d'assurer que toutes les enquêtes numériques suivent les mêmes protocoles, garantissant ainsi une approche cohérente et professionnelle ;
- la conformité légale : le manuel aidera à aligner les pratiques d'investigation avec les lois nationales et internationales, réduisant ainsi les risques de non-conformité ;
- la formation et les compétences : il servira de référence pour la formation des enquêteurs, assurant que le personnel possède les compétences nécessaires pour mener des investigations efficaces ;
- la qualité et l'intégrité des enquêtes : le manuel contribuera à maintenir un haut niveau de qualité et d'intégrité dans les enquêtes, ce qui est essentiel pour la crédibilité des résultats ;
- l'efficacité et la rapidité : des procédures claires et bien définies permettent de gagner du temps et d'accroître l'efficacité des enquêteurs face à des incidents numériques ;
- l'adaptabilité et l'évolution : un manuel standardisé peut être régulièrement mis à jour pour s'adapter aux évolutions technologiques et aux nouvelles menaces ;
- la coopération internationale : il facilitera la collaboration et l'échange d'informations avec d'autres pays et organisations internationales dans la lutte contre la cybercriminalité ;
- la confiance du Public : un manuel transparent et accessible renforce la confiance du public dans les capacités d'investigation numérique du pays...

En somme, un manuel standardisé est un outil indispensable pour structurer et guider les efforts d'investigation numérique au Cameroun, en vue de répondre efficacement aux défis de la cybercriminalité et de tirer parti des opportunités offertes par le numérique pour la sécurité et le développement national.

2. Consistance des prestations

Le Cabinet ou bureau d'études aura pour mission de réaliser les prestations à travers les activités suivantes:

- identifier les différents types d'investigations numériques ;
- dresser un état des lieux des méthodes existantes en matière du déroulement des investigations numériques auprès des parties prenantes (SED, DGSN, DGRE, INTERPOL, ANTIC, MINJUSTICE, etc);
- répertorier tous les cas d'investigations numériques existantes ; identifier les procédures déjà mises en place ; demander aux acteurs de décrire leurs activités et de fournir tous les documents liés à chaque activité ; analyser les informations collectées pour identifier les forces et faiblesses des procédures existantes ainsi que les risques associés ;
- décrire l'ensemble des étapes à parcourir pour mener avec efficacité chaque cas d'investigation numérique rencontrée ;
- faire un inventaire des équipements utilisés au cours de chaque cas d'investigation numérique ainsi que les spécifications techniques de ces équipements ; de même que les outils et logiciels

recommandés pour les différentes étapes d'une investigation numérique ; les méthodes et techniques proposées tiendront compte de l'acquisition et de l'analyse des données, l'analyse du trafic réseau, l'analyse des systèmes de fichiers, l'analyse des e-mails et des communications, l'analyse de la mémoire, l'analyse des malwares, etc..... ;

- ressortir les précautions à observer au cours du déroulement des investigations numériques ;
- identifier les différents intervenants dans le cadre du déroulement de chaque cas d'investigation numérique et de définir leur rôle et responsabilité ;
- ressortir les compétences requises des responsables en charge des investigations numériques ;
- proposer des modules de renforcement des capacités en matière d'investigation numérique, les coûts, les lieux et les établissements possibles de formation ;
- proposer des procédures pour la révision périodique et la mise à jour du manuel en fonction de l'évolution technologique et législative ;
- élaborer le manuel de procédures d'investigation numérique ;
- organiser un atelier de validation dudit manuel ;
- traduire, concevoir, produire et multiplier le manuel de procédures d'investigations numériques.

3. Participation

Pour faire acte de candidature, les Cabinets ou Bureaux d'Etudes, devront justifier d'une compétence avérée et une expérience pertinente dans l'élaboration des stratégies de sécurité des réseaux et des systèmes d'information et l'investigations numériques.

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 stratégies de sécurité des réseaux et des systèmes d'information réalisés au cours des cinq (05) dernières années...15 points.
- Au moins deux références dans le domaine d'investigations numériques réalisés au cours des cinq (05) dernières années ...15 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 informatique ou télécommunications (BAC+5) ou Master en Télécommunications ou en Informatique, ayant une expertise en management des projets. Justifiant d'une expérience d'au moins dix (10) ans dans l'élaboration des stratégies de sécurité des réseaux et des systèmes d'information, certifié en gestion de projet (PMP ou PRINCE2) et ayant conduit au moins deux (02) projets en tant que Chef de mission au cours des cinq dernières années. ..... 20 points ;
- Un (01) Ingénieur Télécommunications ou informatique (BAC +5 ou équivalent). Justifiant d'une expérience d'au moins huit (08) ans dans la réalisation de projets similaires, certifié en en cybersécurité (deux certificats au moins) et ayant participé à la réalisation d'au moins deux (02) projets en matière investigations numériques au cours des cinq (05) dernières années .....10 points ;
- Un (01) Ingénieur en Informatique (BAC+5) ou Master en Informatique, Expert en cybercriminalité. Ayant au moins huit (08) ans d'expérience dans l'élaboration des stratégies de sécurité des réseaux et des systèmes d'information, titulaire de certifications en cybersécurité et ayant participé à la réalisation d'au moins deux (02) projets d'investigation numérique au cours des cinq (05) dernières années; ..... 10 points ;
- Un (01) Ingénieur en Informatique (BAC+5) ou Master en Informatique. Expert en sécurité informatique. Ayant au moins huit (08) ans d'expérience dans l'élaboration des stratégies de sécurité des réseaux et des systèmes d'information, titulaire de certifications en cybersécurité et ayant participé à la réalisation d'au moins deux (02) projets dans le domaine de la protection des infrastructures numériques et la prévention des intrusions au cours des cinq (05) dernières années..... 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 05 AOUT 2024 14 heures, heure locale et devra porter la mention :

AVIS D'APPEL A MANIFESTATION D'INTÉRÊT
N°00000014/AMI/MPT/SG/DAG/SDBM/SMA/2024 DU 28 Juin 2024 POUR LA PRESELECTION DES CABINETS OU BUREAUX D'ETUDES EN VUE DE L'ELABORATION D'UN MANUEL DE PROCEDURES D'INVESTIGATION NUMERIQUE
« 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

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

Libom Li Likeng
née Mendoma Minette

REPUBLIC OF CAMEROON
Peace-Work-Fatherland

MINISTRY OF POSTS AND TELECOMMUNICATIONS

SECRETARIAT GENERAL

REPUBLIC OF CAMEROON
Peace-Work-Fatherland

MINISTRY OF POSTS AND TELECOMMUNICATIONS

GENERAL SECRETARIAT

00000014

CALL FOR EXPRESSION OF INTEREST
N°...AMI/MINPOSTEL/SG/DAG/SDBM/SMA/2024 OF 28 JUIN 2024 FOR THE ESTABLISHMENT OF A SHORTLIST OF FIRMS OR CONSULTING FIRMS WITH A VIEW TO DRAWING UP A HANDBOOK OF DIGITAL INVESTIGATION PROCEDURES

Financing: ESF, 2024 financial year

1. Background and justification

Electronic communications networks and Information and Communication Technologies (ICTs) have become indispensable tools for governments, businesses, civil society and individuals throughout the world. These technologies have fostered considerable economic development, increased the free flow of information, and contributed to real gains in performance, efficiency, productivity and creativity around the world.

The use of ICTs, and the internet in particular, has become an issue of strategic importance for countries. An open and secure Internet is an engine for economic growth and social development, facilitating communication, innovation, scientific research and the transformation of administrations and businesses.

However, the growing use of the Internet has led to new challenges for the national and international community. The more connected we are, the more exposed we are to cyber threats. In addition, the rapid evolution of the Internet has created new opportunities for large-scale cybercrime. Individuals lurking in the shadows are using ICTs to commit malicious acts with damaging consequences for public authorities, businesses and users. Complaints from victims include defamation, identity theft, threats, verbal abuse, insults, scams, data hacking, and photo or video editing to cause harm.

By way of illustration of the scale of cybercrime in Cameroon, some statistics obtained from the relevant services reveal 3,388 cases of identity theft in 2018, 2,050 complaints relating to scamming and phishing, including around CFAF 5 billion in financial losses, nearly CFAF 6 billion in losses relating to bank fraud, 11,617 vulnerabilities detected on public administration websites in 2019.

Faced with all these problems, the government of Cameroon has not remained inert. To effectively combat the deviant acts perpetrated by cybercriminals in Cameroonian cyberspace, it has put in place a strategic, legal and institutional framework. However, despite all the solutions that have been put in place, magistrates and judicial police officers are finding it difficult to grasp the new concepts relating to cybersecurity and cybercrime on the one hand, and the conduct of digital investigations on the other. These difficulties were discussed at the national forum on cybersecurity and the fight against cybercrime, held from 03 to 05 November 2020 at the Yaounde Conference Centre. They said that there was no formal framework explaining the various stages of a digital investigation. The Ministry of Posts and Telecommunications is responsible, among other things, for promoting the security of networks and information systems. It is also responsible for coordinating network and information system security activities. On the basis of these observations, the above-mentioned forum recommended "drawing up a procedures handbook for digital investigations".

Furthermore, the justification for the need for a standardised manual for digital investigation procedures in Cameroon is based on several key points, including:

- Standardisation of Practices: a standardised manual will ensure that all digital investigations follow the same protocols, guaranteeing a consistent and professional approach;
- Legal compliance: the manual will help to align investigation practices with national and international laws, reducing the risk of non-compliance;
- Training and skills: it will serve as a reference for the training of investigators, ensuring that staff have the necessary skills to conduct effective investigations;
- quality and integrity of investigations: the manual will help to maintain a high level of quality and integrity in investigations, which is essential for the credibility of the results;
- efficiency and speed: clear, well-defined procedures save time and increase the effectiveness of investigators when dealing with digital incidents;
- Adaptability and evolution: a standardised manual can be regularly updated to adapt to technological developments and new threats;
- international cooperation: it will facilitate collaboration and the exchange of information with other countries and international organisations in the fight against cybercrime;
- Public confidence: a transparent and accessible manual strengthens public confidence in the country's digital investigation capabilities...

In short, a standardised manual is an essential tool for structuring and guiding digital investigation efforts in Cameroon, with a view to responding effectively to the challenges of cybercrime and taking advantage of the opportunities offered by digital technology for national security and development.

2. Description of services

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

- identifying the different types of digital investigation
- drawing up an inventory of existing methods for conducting digital investigations with stakeholders (SED, DGSN, DGRE, INTERPOL, NAICT, MINJUSTICE, etc);
- listing all cases of existing digital investigations; identifying the procedures already in place: asking the actors to describe their activities and provide all documents relating to each activity; analysing the information collected to identify the strengths and weaknesses of existing procedures and the associated risks;
- describing all the measures to be taken to carry out each digital investigation effectively;
- making an inventory of the equipment used during each digital investigation case, together with the technical specifications of this equipment: as well as the tools and software recommended for the various stages of a digital investigation; the proposed methods and techniques will take into account data acquisition and analysis, network traffic analysis, file system analysis, email and communications analysis, memory analysis, malware analysis, etc..... ;
- highlighting the precautions to be observed during the digital investigations;
- Identifying the various parties involved in each digital investigation and defining their roles and responsibilities;
- Identifying the skills required of those in charge of digital investigations;
- Proposing capacity-building modules for digital investigations, costs, possible training locations and institutions;
- Proposing procedures for periodically reviewing and updating the manual in line with technological and legislative developments;

- Drawing up the digital investigation procedures handbook;
- Organising a workshop to validate the handbook;
- Translating, designing, producing and disseminating the digital investigation procedures manual.

3. **Participation**

To apply, firms or consultancies must have proven skills and relevant experience in developing network and information system security strategies and digital investigations.

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 network and information system security strategies carried out within the last five (05) year...15 points.
- At least two references in the field of digital investigations carried out over the last five (05) years ...15 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 : Computer or telecommunications engineer (GCE A/L + 5 years university studies) or Master's degree in Telecommunications or Computer Science, with expertise in project management. Proof of at least ten (10) years' experience in developing network and information systems security strategies, certified in project management (PMP or PRINCE2) and must have led at least two (02) projects as Mission Head over the last five years. ..... 20 points;
- One (01) Telecommunications or IT Engineer (GCE A/L +5 or equivalent). Proof of at least eight (08) years' experience in carrying out similar projects, certified in cybersecurity (at least two certificates) and must have participated in at least two (02) digital investigations projects over the last five (05) years .....10 points ;
- One (01) Computer Engineer (GCE A/L+5) or Master's Degree in Computer Science, expert in cybercrime. Must have at least eight (08) years' experience in developing network and information system security strategies, must hold cybersecurity certifications and must have participated in at least two (02) digital investigation projects over the last five (05) years; ..... 10 points;
- One (01) Computer Engineer (GCE A/L+5) or Master's Degree in Computer Science. Expert in computer security. Must have at least eight (08) years' experience in developing network and information system security strategies, must hold cybersecurity certifications and must have participated in the completion of at least two (02) projects in the field of digital infrastructure protection and intrusion prevention over the last five (05) years:..... 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. <u>Submission of files</u>

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), of the Ministry of Posts and Telecommunications, not later than 05 AOUT 2024 at 2:30 pm, local time and shall carry the following label:

CALL FOR EXPRESSION OF INTEREST

No 0000014/AMPT/SG/DAG/SDBM/SAA/2024 OF 28 Juin 24 FOR THE ESTABLISHMENT OF A SHORTLIST OF FIRMS OR CONSULTING FIRMS WITH A VIEW TO DRAWING UP A HANDBOOK OF DIGITAL INVESTIGATION PROCEDURES

"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.: 222 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 Telecommunications
MINISTERE DES POSTES ET TELECOMMUNICATIONS

Ing. Libom Li Likeng
Mrs. Ndoma Minette