

**REPUBLIQUE DE GUINEE**

Travail – Justice – Solidarité

-----  
**Ministère des Postes, des Télécommunications et de l'Économie Numérique**

-----  
**Unité de Gestion du Projet**

**Projet de Transformation Numérique pour l'Afrique / Programme Régional d'Intégration Numérique de l'Afrique de l'Ouest (DTfA/ WARDIP).**

**SOLLICITATION DE MANIFESTATIONS D'INTERET**

**RECRUTEMENT D'UN CABINET OU D'UNE FIRME POUR LA REVUE DU CADRE JURIDIQUE DE LA CYBERSECURITE ET DE LA LUTTE CONTRE LA CYBERCRIMINALITE EN REPUBLIQUE DE GUINEE**

**Début : 16/ Septembre / 2024 ; Date limite : 07 / Octobre / 2024**

1. Le Gouvernement de la République de Guinée a reçu un financement de l'Association internationale de développement (IDA) dans le cadre du Projet Transformation Numérique pour l'Afrique / Programme Régional d'Intégration Numérique de l'Afrique de l'Ouest (DTfA/ WARDIP), et à l'intention d'utiliser une partie du montant de ce don pour effectuer les paiements au titre du contrat suivant : **Recrutement d'un Cabinet ou d'une Firma pour la Revue du Cadre Juridique de la Cybersécurité et de la Lutte contre la Cybercriminalité en République de Guinée.**
2. L'Objectif de Développement du Projet (ODP) est d'accroître l'accès aux services haut débit et numériques grâce au développement et à l'intégration des marchés numériques dans la région Afrique de l'Ouest.

Pour atteindre cet objectif, le projet mettra en œuvre un ensemble d'activités organisées au tour des (5) composantes ci-après :

❖ **Composante 1 : Développement et intégration du marché de la connectivité**

Cette composante soutient les réformes visant à réduire les obstacles liés à la fourniture de services de télécommunications transfrontaliers par le biais de marchés ouverts ainsi qu'au déploiement d'infrastructures de connectivité à large bande dans le cadre d'une approche MFD. Cette composante vise à favoriser la concurrence dans le secteur des télécommunications, la baisse des coûts d'accès à internet, etc.

❖ **Composante 2 : Développement et intégration du marché des données**

Cette composante permet l'échange, le stockage et le traitement sécurisés des données à travers les frontières pour soutenir le déploiement régional et l'accès aux services, à l'innovation et à l'infrastructure basée sur les données par la réduction des restrictions régionales sur la libre circulation des données et l'augmentation des investissements dans ce domaine. Un marché des données plus intégré en Afrique de l'Ouest pourrait stimuler l'innovation et améliorer l'analyse des données, ce qui se traduirait par des avantages économiques et sociaux importants et des gains d'efficacité dans pratiquement tous les secteurs. Conformément aux objectifs régionaux, cette composante pourrait éventuellement inclure un soutien aux objectifs nationaux qui seraient essentiels pour tracer la voie de l'intégration.

❖ **Composante 3 : Développement et intégration du marché en ligne**

Cette composante soutient le développement et l'intégration du marché en ligne, ce qui créera un environnement propice à la fourniture et à l'accès transfrontaliers de biens ou de services numériques. Cette composante aiderait les gouvernements, les entreprises et les citoyens des pays participants à accéder et à fournir des services privés et publics en ligne, ainsi qu'à effectuer des achats en ligne de manière transparente à partir de n'importe où dans la région.

#### ❖ **Composante 4 « Gestion du projet »**

Elle porte sur la mise en place d'une unité d'exécution du projet, qui sera responsable de la mise en œuvre de toutes les activités.

#### ❖ **Composante 5. « Composante d'intervention d'urgence contingente CERC. »**

En reconnaissance de la vulnérabilité actuelle de la région et des pays aux chocs, une composante d'intervention d'urgence contingente (CERC) est ajoutée à la structure du projet pour fournir un soutien aux pays participants pour répondre rapidement aux crises et aux urgences, y compris les catastrophes climatiques et naturelles et les urgences de santé publique.

Elle aura une valeur initiale nulle mais pourra être financée pendant la mise en œuvre du projet pour permettre une réponse agile aux événements émergents, avec des fonds redirigés depuis d'autres composantes. L'inclusion du CERC au stade de la préparation, bien qu'avec un financement nul, offre la flexibilité nécessaire pour répondre à une urgence imminente ou réelle (telle que la COVID-19). Les dépenses de réponse à la crise pourraient couvrir, par exemple, la facilitation des paiements d'urgence aux groupes vulnérables de la population en utilisant l'argent mobile ; assurer la continuité des activités des fonctions gouvernementales essentielles, lorsque les fonctionnaires sont tenus de continuer à travailler à domicile ; ou le soutien aux MTPE, en particulier les plus touchées, pour résoudre leurs problèmes de liquidité immédiats, réduire les licenciements et éviter les faillites.

Le CERC n'est pas censé financer des travaux de génie civil pouvant induire des risques et/ou des impacts environnementaux et sociaux négatifs.

### **3. OBJECTIF DE MISSION**

#### **3.1 : Objectif Général**

L'objectif général de la présente mission est d'évaluer les besoins pour l'élaboration et l'instauration d'un cadre juridique spécifique et robuste en matière de cybersécurité en République de Guinée. Il s'agit de proposer à cet effet, au regard des besoins, et en tenant compte des récentes évolutions du numérique et des menaces émergentes ou des nouvelles formes de menaces en matière de sécurité des systèmes d'information ou de cybersécurité en général d'une part, et des bonnes pratiques juridiques en ce domaine au niveau sous-régional, continental et/ou international, les textes législatifs et/ou réglementaires nécessaires ou utiles pour la mise en place de ce cadre juridique d'autre part.

La mission est réalisée au nom, pour le compte et au profit du gouvernement guinéen, à travers le ministère des postes, des télécommunications et de l'économie Numérique, qui est aussi le destinataire primaire des livrables qui seront issus de la mission.

La mission profitera également à l'agence nationale de sécurité des systèmes d'information (ANSSI), placée sous la tutelle technique du ministère précité des postes, des télécommunications et de l'économie Numérique. Cette agence a la charge sur le territoire guinéen de la cybersécurité en général.

### **4. ETENDUE DE LA MISSION**

Le cabinet ou la firme qui sera recruté(e) devra, tout en tenant dûment compte cependant des engagements sous-régionaux, continentaux et/ou internationaux auxquels la République de Guinée aurait souscrits dans le domaine de la cybersécurité et/ou en ce qui concerne les règles, prescriptions et directives qui auraient été émises ou adoptées dans ce domaine par les organisations sous-régionales, continentales et/ou internationales dont la République de Guinée serait partie, réaliser ou exécuter les missions spécifiques ci-après :

- Procéder à l'identification des besoins pour l'élaboration et l'instauration d'un cadre juridique spécifique et robuste en matière de cybersécurité en République de Guinée, au regard notamment des meilleures pratiques existantes ou des meilleurs cadres juridiques existant en la matière au niveau sous-régional,

continental et/ou international ;

- Formuler des propositions et recommandations pertinentes sur textes législatifs et/ou règlementaires à initier, prendre et/ou adapter et à mettre en œuvre pour l'instauration du cadre juridique nécessaire pour le renforcement de la cybersécurité et de la cyber-résilience sur le territoire guinéen, et ce, y compris du point de vue institutionnel, technique, technologique, opérationnel, juridique, administratif, économique et financier, ;
- Soumettre ses propositions et recommandations visées au point précédent ou à la boulette précédente, aux autorités compétentes au sein du ministère des postes, des télécommunications et de l'économie Numérique, en l'occurrence au ministre ou à la ministre en charge de ce ministère, et/ou aux représentants autorisés ou désignés dudit Ministre ou de ladite Ministre, aux fins de la validation ou de l'approbation préalable du contenu des propositions ou recommandations formulées par le Cabinet ou la firme ;
- Rédiger et élaborer les propositions de textes législatifs et/ou règlementaires qui auront été identifiés pour l'instauration du cadre juridique susvisé de la cybersécurité en République de Guinée, et soumettre ces propositions aux autorités susmentionnées du ministère des postes, des télécommunications et de l'économie Numérique, pour validation ou approbation préalable ;
- Produire un rapport final d'exécution de la mission.

## **5. QUALIFICATIONS ET EXPERIENCES REQUISES**

### **5.1 Expérience générale du cabinet Qualifications du Cabinet**

Le cabinet à recruter doit être doté de solides compétences en matière d'élaboration de textes légaux et règlementaires, et de préférence dans le domaine des Télécommunications/TIC, du numérique en général et de la cybersécurité, de la cybercriminalité et/ou de la protection des données à caractère personnel en particulier.

Le cabinet devra justifier d'une grande qualification, et de solides compétences, ainsi que d'une expérience avérée dans la conduite et la mise en œuvre de missions similaires ou analogues à la mission objet des présents Termes de Références (TDR).

Le cabinet devra en particulier justifier des critères d'expérience ci-après :

- **Expérience générale :**
  - Une expérience avérée d'au moins cinq (05) ans dans la rédaction ou la révision de textes législatifs et règlementaires dans le secteur de l'économie numérique ;
- **Expériences spécifiques :**
  - Avoir effectué au moins deux (02) missions similaires au cours des cinq (05) dernières années. Une expérience en Afrique, et surtout en Afrique de l'Ouest, serait un atout. Chaque mission supplémentaire sera aussi un atout ;
  - Avoir une expérience d'au moins cinq (05) ans dans l'analyse ou le développement de réglementations et/ou de législations sur la cybersécurité, la cybercriminalité, la protection des données à caractère personnel et/ou dans un domaine connexe ;
  - Avoir une bonne connaissance du cadre juridique sous-régional, continental et/ou international en matière de cybersécurité, de lutte contre la cybercriminalité et la protection des données personnelles. La connaissance du cadre juridique applicable au niveau de la CEDEAO en ces domaines, serait un atout ;

- Une bonne connaissance de l'industrie du numérique et notamment des questions liées à la cybersécurité et les enjeux y afférents ;
- Avoir une bonne connaissance de l'environnement juridique applicable aux télécommunications/TIC, aux transactions électroniques, à la cybercriminalité et/ou à la protection des données à caractère personnel en République de Guinée, serait aussi un atout.

**Les qualifications, compétences et expériences du cabinet ou du personnel dudit cabinet devront être justifiées par des certificats et attestations de bonne fin d'exécution ou par tout autre document de nature à justifier de ces qualifications, compétences et expériences, notamment les Curriculum Vitae (CV) et diplômes de ce personnel, ainsi que les fiches de tâches dudit personnel concerné et les qualifications requises.**

## **5.2. Personnel-Clé du Cabinet**

Le personnel clé du cabinet qui devra être recruté devra être composé au minimum des experts aux profils ci-après :

- ✓ Un (01) Juriste Senior (chef de mission);
- ✓ Un (01) juriste spécialiste du droit des télécommunications/TIC et du numérique en général, et notamment sur les questions de cybersécurité.;
- ✓ Un (01) expert en politiques et stratégies de protection et de sécurisation des systèmes d'information ;
- ✓ Un (01) ingénieur spécialiste de l'organisation et management de la sécurité des systèmes d'information ;
- ✓ Un (1) expert en Prospective et en Intelligence et Ingénierie Économique et Financière en matière de Cybersécurité.

Les experts précités doivent pour chacun d'entre eux, justifier de compétences et d'une expérience avérée dans les domaines d'activités suscités.

La connaissance de l'environnement de la cybersécurité en République de Guinée serait un plus ou un atout. Ces experts devront exécuter les tâches mentionnées ci-dessous dans le cadre de la mission, et pour se faire, disposer des qualifications minimales également décrites ci-dessous.

### **1. L'Expert Juridique Senior et Chef de Mission**

#### **Tâches du Chef de Mission :**

L'Expert Juridique Senior et Chef de Mission aura pour tâches, de :

- Coordonner et gérer l'exécution de la mission ;
- Diriger l'équipe d'experts en charge de la mission;
- Gérer la planification des activités de la mission et/ou le planning desdites activités ;
- Allouer les ressources et s'assurer de la bonne exécution de la mission ;
- Être le premier et principal interlocuteur du client dans le cadre de la mission et assurer toutes interactions entre le client et le cabinet ;
- Analyser les enjeux et la portée de la mise en œuvre des dispositions régionales en matière de cybersécurité et de garantir l'achèvement de la mission dans les délais impartis, et dans le strict respect des objectifs spécifiques assignés et susmentionnés de la mission, ainsi que des résultats et livrables attendus et également mentionnés ci-dessus ;

- Coordonner, gérer et faciliter les interactions entre les experts du cabinet intervenant dans l'exécution de la mission, ainsi que les interventions desdits experts d'une part, mais aussi en ce qui concerne leurs interactions avec les équipes ou services concerné(e)s du client d'autre part ;
- Coordonner et assurer la liaison et les communications entre le cabinet et l'UGP – WARDIP GUINEE d'une part, et avec le client (le MPTEN) d'autre part, dans le cadre ou au titre de la mission ;
- Assurer le reporting régulier de l'exécution de la mission ou concernant cette exécution, à l'UGP – WARDIP GUINEE et au client (le MPTEN).

### **Qualifications du Chef de Mission :**

L'Expert Juridique Senior et Chef de Mission doit avoir les qualifications minimales ci-après :

- Éducation/Formation : Avoir au moins un Master en droit ou dans un domaine connexe ;
- Expérience professionnelle générale : Avoir au moins dix (10) années d'expérience professionnelle dans la pratique du droit en général et l'élaboration de cadres juridiques et/ou réglementaires en particulier. Des compétences en légistique serait un atout ;
- Expérience(s) professionnelle(s) spécifique(s) : avoir conduit au cours des cinq (05) dernières années, au moins une (01) mission d'élaboration de cadres juridiques et/ou réglementaires au niveau national, sous-régional, régional et/ou international, dans le secteur de l'économie numérique, et notamment dans le domaine des télécommunications, des technologies de l'information et de la communication (TIC), de la cybersécurité, de la lutte contre la cybercriminalité et/ou de la protection des données à caractère personnel;
- Compétences additionnelles ou particulières : la connaissance de l'environnement juridique du secteur de l'économie numérique, et notamment des télécommunications, des technologies de l'information et de la communication (TIC), de la cybersécurité, de la lutte contre la cybercriminalité et/ou de la protection des données à caractère personnel, au niveau sous-régional ou de l'Afrique de l'Ouest, continental et/ou international, serait un atout.

### **2. L'Expert Juridique spécialiste du droit des télécommunications/TIC et du numérique en général**

#### **Tâches de L'Expert Juridique spécialiste du droit des télécommunications/TIC et du numérique en général**

L'Expert Juridique spécialiste du droit des télécommunications/TIC et du numérique en général aura, sous l'autorité, la coordination et la supervision du Chef de Mission, pour tâches, de :

- Fournir au nom et pour le compte du cabinet et notamment aux autres experts au sein du cabinet, mais aussi au client et/ou à ses équipes ou services concernés, son expertise juridique, des conseils juridiques et/ou toutes autres tâches de nature juridique en rapport avec la mission ou en lien avec celle-ci ;
- Assister le chef de mission et les autres experts intervenant dans le cadre de leurs missions, tâches ou activités, dans la mise en œuvre desdites missions, tâches ou activités, et ce, y compris en ce qui concerne :
  - ✓ L'état des lieux du cadre juridique qui existerait en République de Guinée en matière de cybersécurité et/ou dans tous autres domaines connexes, annexes ou ayant un lien ou un impact avéré ou potentiel avec ce cadre juridique;
  - ✓ La réalisation d'études comparatives (benchmarkings) sur les environnement et cadres juridiques de référence (cas de bonnes pratiques) existant au niveau sous-régional ou de l'Afrique de l'Ouest, continental et/ou international, en matière de cybersécurité ;

- ✓ La rédaction et l'élaboration des propositions de textes législatifs et/ou réglementaires devant constituer et consacrer le cadre juridique attendu par le client au titre de la mission, et en matière de cybersécurité en l'occurrence, et/ou de tous autres livrables connexes ou annexes à ce cadre juridique ;
- ✓ Contribuer à l'élaboration des rapports d'étape attendus par le client dans le cadre de l'exécution de la mission ;
- Exécuter toute autre tâche ou activité en lien avec sa mission, ses tâches ou activités, son profil, ses compétences et/ou ses qualifications, qui est ou serait nécessaire pour la bonne exécution de la mission ou pour la réussite de ladite mission.

### **Qualifications de L'Expert Juridique spécialiste du droit des télécommunications/TIC et du numérique en général**

L'Expert Juridique spécialiste du droit des télécommunications/TIC et du numérique en général doit avoir les qualifications minimales ci-après :

- Études/formation : Master en droit, et ou en droit des télécommunications, de l'informatique, des technologies de l'information et de la communication (TIC), du numérique et/ou dans tout autre domaine connexe en particulier;
- Expérience professionnelle générale : avoir au minimum Cinq (05) années d'expérience professionnelle dans la pratique du droit en général et l'élaboration de cadres juridiques et/ou réglementaires en particulier.;
- Expérience(s) professionnelle(s) spécifique(s) : avoir élaboré au cours des cinq (05) dernières années, au moins un (01) cadre juridique et/ou réglementaire majeur ou d'importance au niveau national, sous-régional, régional et/ou international, dans le secteur de l'économie numérique, et notamment dans le domaine des télécommunications, des technologies de l'information et de la communication (TIC), de la cybersécurité, de la lutte contre la cybercriminalité et/ou de la protection des données à caractère personnel.
- Compétences additionnelles ou particulières : la connaissance des instruments juridiques des organisations sous-régionales, continentales et internationales auxquelles la République de Guinée est partie, en matière de cybersécurité, de cybercriminalité et de protection des données à caractère personnel, est exigée.

La connaissance de l'environnement juridique global du secteur de l'économie numérique, et notamment des télécommunications, des technologies de l'information et de la communication (TIC), de la cybersécurité, de la lutte contre la cybercriminalité et/ou de la protection des données à caractère personnel, à l'échelle des pays de la sous-région ouest-africaine, du continent africain et/ou au niveau international, serait un atout.

### **3. L'Expert en Politiques et Stratégies de Protection et de Sécurisation des Systèmes d'Information**

#### **Tâches de l'Expert en Stratégies de Protection et de Sécurisation des Systèmes d'Information:**

L'expert en stratégies de protection et de sécurisation des systèmes d'information aura, sous l'autorité, la coordination et la supervision du Chef de Mission, pour tâches, de :

- Faire l'état des lieux des stratégies qui existeraient, auraient été initiées ou seraient déjà mises en œuvre à la date de démarrage de la mission en République de Guinée, y compris par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) et/ou par toutes autres entités publiques, en matière de sécurité ou de sécurisation des systèmes d'information ou de cybersécurité en général;

- Réaliser des études comparatives (benchmankings) sur les bonnes stratégies (cas de bonnes pratiques) en vigueur au niveau sous-régional ou de l’Afrique de l’Ouest, continental et/ou international, en matière de protection ou de sécurisation des systèmes d’information ou de cybersécurité en général ;
- Proposer, y compris aux autres experts de l’équipe projet ou en charge de la mission, des stratégies pertinentes de sécurisation des systèmes d’information, en vue de leur déclinaison et de leur codification dans le cadre juridique et notamment des textes législatifs et/ou règlementaires qui sera ou qui seront rédigé(s) ou élaboré(s) au titre de la mission ou à l’issue de celle-ci ;
- Assister au besoin, dans le cadre de ses attributions et tâches, les autres experts ou membres de l’équipe-projet ou en charge de la mission, dans l’exécution de leurs missions, tâches ou activités ;
- Contribuer à l’élaboration des rapports d’étape attendus par le client dans le cadre de l’exécution de la mission ;
- Exécuter toute autre tâche ou activité en lien avec sa mission, de ses tâches ou activités, son profil, ses compétences et/ou ses qualifications, qui est ou serait nécessaire pour la bonne exécution de la mission ou pour la réussite de ladite mission.

### **Qualifications de l’Expert en Stratégies de Protection et de Sécurisation des Systèmes d’Information**

L’Expert en Stratégies de Protection et de Sécurisation des Systèmes d’Information doit avoir les qualifications minimales ci-après :

- Études/formation : Master ou ingénierie en Informatique et/ou en Technologies de l’information et de la communication (TIC) ;
- Expérience professionnelle générale : minimum de six (06) années d’expérience professionnelle dans le domaine de l’Informatique, des Technologies de l’information et de la communication (TIC), du numérique et/ou de la cybersécurité ou de la sécurité des systèmes d’information, avec une bonne maîtrise des enjeux stratégiques liés à la sécurisation et à la protection des systèmes d’information, et à fortiori des stratégies à implémenter et/ou à mettre en œuvre pour la sécurisation et la protection desdits systèmes ;
- Expérience(s) professionnelle(s) spécifique(s) : avoir participé au cours des cinq (05) dernières années à élaboration une ou des stratégie(s) de sécurisation et de protection des systèmes d’information ou en matière de cybersécurité.
- Compétences additionnelles ou particulières : la connaissance des enjeux et défis liés à la sécurisation et à la protection des systèmes d’information ou en matière de cybersécurité en général au sein des organisations sous-régionales, continentales et internationales auxquelles la République de Guinée est partie, en ce domaine, serait un atout.

### **4. L’Ingénieur Spécialiste en Organisation et Management de la Sécurité des Systèmes d’Information :**

#### **Tâches de l’Ingénieur Spécialiste en Organisation et Management de la Sécurité des Systèmes d’Information:**

L’Ingénieur Spécialiste en Organisation et Management de la Sécurité des Systèmes d’Information aura, sous l’autorité, la coordination et la supervision du Chef de Mission, pour tâches, de :

- Faire la revue ou l’état des lieux technique, technologique et opérationnel existant à la date de démarrage de la mission, en matière de protection et de sécurisation des systèmes d’information ou de cybersécurité en général, mais aussi en ce qui concerne les infrastructures, équipements, matériels, outils et systèmes entrant dans le cadre de cette protection et sécurisation, ainsi que sur les normes, standards, référentiels, procédures et pratiques existants ou en vigueur en ce domaine ;

- Réaliser des études comparatives (benchmarks) sur les cas de bonnes pratiques en termes d'infrastructures, d'équipements et de technologies déployés et/ou mis en œuvre en vigueur au niveau de la sous-région ouest-africaine, du continent africain et/ou au niveau international, en matière de protection ou de sécurisation des systèmes d'information ou de cybersécurité en général, mais aussi en ce qui concerne les aspects techniques et opérationnels et sur les normes, standards, référentiels, procédures et pratiques existants ou en vigueur en ce domaine au sein de ces sphères géographiques ;
- Proposer ou recommander, suite à l'état des lieux et aux études comparatives (benchmarks) précité(s), et en lien avec l'Expert en Stratégies de Protection et de Sécurisation des Systèmes d'Information :
  - ✓ des mesures pertinentes, efficaces et efficientes à déployer et/ou mettre en œuvre en République de Guinée, du point de vue technique et opérationnel, pour une bonne protection des systèmes d'information sur le territoire guinéen ;
  - ✓ Les infrastructures, équipements, matériels, outils et systèmes à acquérir, déployer et/ou à mettre en œuvre en République de Guinée, pour une protection et une sécurisation efficace et efficiente des systèmes d'information en République de Guinée, et ce, en, vue de leur encadrement juridique au besoin, et notamment en ce qui concerne leur installation, leur utilisation ou leur exploitation ;
  - ✓ les normes, standards, référentiels, procédures et bonnes pratiques à implémenter, déployer et/ou mettre en œuvre pour l'atteinte de cet objectif de protection et de sécurisation desdits systèmes d'information ;
- Assister au besoin, dans le cadre de ses attributions et tâches, les autres experts ou membres de l'équipe-projet ou en charge de la mission, dans l'exécution de leurs missions, tâches ou activités ;
- Contribuer à l'élaboration des rapports d'étape attendus par le client dans le cadre de l'exécution de la mission ;
- Exécuter toute autre tâche ou activité en lien avec sa mission, ses tâches ou activités, son profil, ses compétences et/ou ses qualifications, et qui est ou serait nécessaire pour la bonne exécution de la mission ou pour la réussite de ladite mission.

### **Qualifications de l'Ingénieur Spécialiste en Organisation et Management de la Sécurité des Systèmes d'Information :**

L'Ingénieur Spécialiste en Organisation et Management de la Sécurité des Systèmes d'Information doit avoir les qualifications minimales ci-après :

- Études/formation : Master ou ingénierie en Informatique et/ou en Technologies de l'information et de la communication (TIC) ;
- Expérience professionnelle générale : minimum de cinq (05) années d'expérience professionnelle dans le domaine de l'Informatique, des Technologies de l'information et de la communication (TIC), du numérique et/ou de la cybersécurité ou de la sécurité des systèmes d'information;
- Expérience(s) professionnelle(s) spécifique(s) : avoir exécuté au niveau national, sous-régional, régional et/ou international, au cours des cinq (05) dernières années, une mission similaire ou analogue à sa présente mission sus-décrite ou comprenant l'ensemble de ses tâches mentionnées précédemment, en son propre nom et/ou au nom et pour le compte d'un cabinet recruté ou mandaté à cet effet, et le cas échéant, avoir participé à l'exécution d'une telle mission ;
- Compétences additionnelles ou particulières : la connaissance des infrastructures, équipements, matériels, outils, technologies et systèmes, ainsi que des normes, standards, référentiels, procédures et bonnes pratiques en vigueur au sein des organisations sous-régionales, continentales et internationales auxquelles la République de Guinée est partie, ou qui seraient recommandés, prescrits ou exigés au sein



desdites organisations, dans le cadre de la sécurisation et de la protection des systèmes d'information ou en matière de cybersécurité en général, et ce, eu égard notamment aux politiques, stratégies et/ou aux instruments juridiques applicables au sein de ces organisations, serait un atout.

## **5. L'Expert en Prospective et en Intelligence et Ingénierie Économique et Financière en matière de Cybersécurité :**

### **Tâches de l'Expert en Prospective et en Intelligence et Ingénierie Économique et Financière en matière de Cybersécurité :**

L'Expert en Prospective et en Intelligence et Ingénierie Économique et Financière en matière de Cybersécurité aura, sous l'autorité, la coordination et la supervision du Chef de Mission, pour tâches, de :

- Faire la revue ou l'état des lieux des politiques, stratégies et/ou des instruments juridiques qui existeraient en République de Guinée, sur le plan économique et financier ou de ce point de vue, en matière de protection et/ou de sécurisation des systèmes d'information ou de cybersécurité sur le territoire guinéen en général;
- Réaliser des études comparatives (benchmarkings) sur les cas de bonnes politiques, stratégies et/ou sur les instruments juridiques pertinents en vigueur au niveau sous-régional ou de l'Afrique de l'Ouest, continental et/ou international, du point de vue économique et financier en matière de protection et/ou de sécurisation des systèmes d'information ou de cybersécurité en général ;
- Proposer, y compris aux autres experts de l'équipe-projet ou en charge de la mission, et à la suite de la revue ou de l'état des lieux ainsi que des études comparatives précitées, les politiques, stratégies et/ou les instruments juridiques pertinents à initier, adopter et/ou à mettre en œuvre en République de Guinée en matière économique et financière, dans le cadre de la protection et/ou de la sécurisation des systèmes d'information ou de la cybersécurité en général, et ce, en vue du renforcement de cette protection et de cette sécurisation, et de leur déclinaison et codification au besoin dans le cadre juridique et notamment des textes législatifs et/ou réglementaires qui sera rédigé ou qui seront rédigés ou élaboré(s) au titre de la mission ou à l'issue de celle-ci ;
- Assister au besoin, dans le cadre de ses attributions et tâches, les autres experts ou membres de l'équipe-projet ou en charge de la mission, dans l'exécution de leurs missions, tâches ou activités ;
- Contribuer à l'élaboration des rapports d'étape attendus par le client dans le cadre de l'exécution de la mission ;
- Exécuter toute autre tâche ou activité en lien avec sa mission, ses tâches ou activités, son profil, ses compétences et/ou ses qualifications, et qui est ou serait nécessaire pour la bonne exécution de la mission ou pour la réussite de ladite mission.

### **Qualifications de l'Expert en Prospective et en Intelligence et Ingénierie Économique et Financière en matière de Cybersécurité**

L'Expert en Prospective et en Intelligence et Ingénierie Économique et Financière en matière de Cybersécurité, doit avoir les qualifications minimales ci-après :

- Études/formation : Master en Sciences Économiques, en Finances Publiques, ou en Ingénierie Économique et/ou Financière;
- Expérience professionnelle générale : minimum de six (06) années d'expérience professionnelle dans la pratique des sciences économiques, des finances publiques, et/ou dans le domaine de l'ingénierie économique et/ou financière ;
- Expérience(s) professionnelle(s) spécifique(s) : avoir déjà élaboré, au cours des cinq (05) dernières années, et à un niveau national, sous-régional, régional et/ou international, une ou des politiques, stratégies

et/ou des instruments juridiques en matière économique et/ou financière dans le domaine des Télécommunications, de l'Informatique, des Technologies de l'information et de la communication (TIC), et/ou du numérique en général.

Une telle expérience dans le cadre de la protection et/ou de la sécurité des systèmes d'information ou en matière de cybersécurité en général, serait un atout ;

- Compétences additionnelles ou particulières : la connaissance des enjeux et défis liés au financement de la protection et/ou de la sécurité des systèmes d'information ou en matière de cybersécurité en général au niveau de la sous-région ouest-africaine, du continent africain et/ou au niveau international, serait un atout.

La connaissance de ces enjeux et défis dans le contexte guinéen aussi, serait un atout.

## 6 DURE E DE LA MISSION.

La mission a une durée maximum de à **quatre-vingt-dix (90) jours calendaires** compter de la date de l'émission de l'Ordre de démarrage des Services qui notifie le début des prestations. La charge de travail est évaluée en « homme-jours » de prestations.

La mission se déroulera en **République de Guinée**, pour les réunions de cadrage, l'état des lieux, la collecte documentaire (au besoin) et la tenue de l'atelier susmentionné de vulgarisation et de formation sur les nouveaux textes juridiques qui seront adoptés.

## 7 PROCEDURE ET METHODE DE SELECTION

Le Cabinet sera recruté suivant la méthode de sélection fondée sur les Qualifications du Consultant (SQC) telle que décrites dans les Règlement de Passation des Marchés pour les Emprunteurs sollicitant de la Banque mondiale le financement de projets d'investissement Règlements de Passation des Marchés de l'IDA (Edition septembre 2023).

Les cabinets intéressé(e)s peuvent soumettre leur dossier et/ou obtenir des informations supplémentaires, au sujet des Termes de Reference à l'adresse ci-dessous et aux heures suivantes : [wardipguinee@gmail.com](mailto:wardipguinee@gmail.com), [cdiallo@hotmail.com](mailto:cdiallo@hotmail.com), Lundi au jeudi de 9h à 16h 00 et le vendredi de 9h à 13h 00, (+224) 622 84 54 04

*Les dossiers de soumission doivent être* déposés à l'adresse ci-dessous par courrier électronique ou en personne au plus tard le **7 Octobre 2024 à 14 heures**. [wardipguinee@gmail.com](mailto:wardipguinee@gmail.com), [cdiallo@hotmail.com](mailto:cdiallo@hotmail.com)

ou

**Projet de Transformation Numérique pour l'Afrique / Programme Régional d'Intégration Numérique de l'Afrique de l'Ouest (DTfA/ WARDIP)**, Commune de Ratoma ; Tel : (+224) 622 84 54 04.

Le dossier de candidature doit porter la mention « **Recrutement d'un Cabinet ou d'une Firma pour la Revue du Cadre Juridique de la Cybersécurité et de la Lutte contre la Cybercriminalité en République de Guinée** » en objet du courrier

Conakry, le 13 Septembre 2024

Le Coordonnateur



Cellou DIALLO