REPUBLIQUE DE GUINEE

Travail-Justice-Solidarité

……

MINISTERE DES POSTES, DES TELECOMMUNICATIONS ET DE L'ECONOMIE NUMERIQUE (MPTEN)

……..

PROJET DE TRANSFORMATION NUMERIQUE POUR L'AFRIQUE/PROJET REGIONAL D'INTEGRATION NUMERIQUE EN AFRIQUE DE L'OUEST (WARDIP-GUINEE)

……

L'APPEL A MANIFESTATION D'INTERET POUR LE RECRUTEMENT D'UN CABINET POUR L'ASSISTANCE TECHNIQUE POUR LA GESTION DE PROJET, LA PLANIFICATION STRATEGIQUE ET LE PILOTAGE DE LA MISE EN ŒUVRE DU CERT/SOC

SERVICES DE CONSULTANT

Date début : 20 Octobre 2025 **Date limité : 17 Novembre 2025**

Contexte et justification de la mission

Selon le Global Cybersecurity Index (GCI) 2024 de l'Union Internationale des Télécommunications (UIT), la Guinée se situe au Niveau 3 – "Établissement" avec un score global de 56,39/100. Les points forts concernent les mesures juridiques (16,27/20) et organisationnelles (14,38/20), tandis que les notes les plus faibles concernent les mesures techniques (3,98/20) et le développement des capacités (9,74/20), indiquant un besoin accru de renforcement opérationnel et de formation.

Malgré l'adoption en 2016 de la loi L/2016/037/AN relative à la cybersécurité et à la protection des données personnelles, et la validation en avril 2022 d'un document de politique et stratégie nationale en cybersécurité par l'ANSSI pour la période 2022-2027, le pays reste confronté à des défis spécifiques : cybercriminalité financière, malwares, attaques sur les infrastructures critiques, fraude en ligne, infrastructures obsolètes, faible sensibilisation et pénurie de professionnels qualifiés.

À l'issue des études de faisabilité et dans le cadre de la prochaine mise en œuvre, une Assistance à Maîtrise d'Ouvrage (AMOA) sera sollicitée pour accompagner l'ANSSI dans le suivi de la mise en œuvre, la conduite du changement, la qualité des livrables et la conformité aux standards internationaux.

OBJECTIFS DE LA MISSION :

Le principal objectif de la mission d'Assistance à Maîtrise d'Ouvrage en Cybersécurité est de conseiller et d'accompagner l'ANSSI dans la définition, la mise en œuvre et le pilotage du projet de création du CERT/SOC.
Le prestataire AMOA agira comme un facilitateur et un intermédiaire clé entre les équipes métiers de l'organisation et la Maîtrise d'Œuvre (MOE) qui sera en charge de la réalisation technique.

OBJECTIFS SPÉCIFIQUES

Les objectifs spécifiques de la mission de l'AMOA sont :

- Examiner et Actualiser avec la MOE les propositions techniques issues des études précédentes, en veillant à leur alignement avec les besoins de l'ANSSI et les standards internationaux ;
- Accompagner, superviser et challenger la MOE dans la mise en œuvre technique du projet, en assurant le respect des délais, du budget et des exigences de sécurité ; ;
- Définir et piloter la phase de recette, en élaborant la stratégie de tests et en guidant les équipes de la MOE dans leur réalisation ;
- Renforcer les compétences et l'appropriation des équipes, via un plan de formation et un accompagnement structuré pour la conduite du changement ;
- Mettre en place des outils et supports pour pérenniser l'opérationnalisation et la capitalisation du CERT/SOC, garantissant l'autonomie et la montée en compétence des équipes de l'ANSSI.
- S'assurer que les conditions minimales d'adhésion au FIRST sont remplies et accompagner l'ANSSI dans la préparation du dossier de candidature.
- Promouvoir l'interopérabilité régionale et internationale du CERT/SOC en accompagnant l'ANSSI dans la mise en place de mécanismes de coopération et d'échanges avec les CERT d'Afrique de l'Ouest et les réseaux internationaux (OIC-CERT, ITU, etc.).
- Assurer l'interconnexion technique avec les plateformes de partage d'informations, notamment MISP (Malware Information Sharing Platform), pour garantir un échange fluide d'indicateurs de compromission (IoC) et une participation effective à la communauté mondiale de renseignement sur les menaces.

La mission s'étend sur une période totale de 24 mois, incluant une phase de 12 mois après la mise en production dédiée à l'accompagnement de la stabilisation, de l'optimisation et de l'opérationnalisation du CERT/SOC.

RÉSULTATS ATTENDUS

Les résultats attendus de la mission d'AMOA sont :

- Le rapport d'étude technico-économique, la conception organisationnelle et technique du SOC et du CERT sont analysés et validés par l'ANSSI ;
- La conformité des équipements physiques acquis avec les spécifications techniques du projet est vérifiée et documentée ;
- Les outils métiers (SIEM, SOAR, etc.) recommandés par l'étude de faisabilité sont revus et adaptés aux besoins ;
- La cohérence entre les propositions techniques et les objectifs stratégiques définis, y compris la conformité à la norme ISO 27001 et les exigences du FIRST est vérifiée ;
- Un cahier des charges détaillé pour les éléments non couverts par les études initiales, traduisant les besoins métiers en exigences fonctionnelles et non fonctionnelles est élaboré et validé avec le MOE ;
- Le MOE est assisté dans la contractualisation des solutions logicielles (outils métiers) et des licences nécessaires ;
- Les instances de gouvernance du projet sont définies et mise en place avec clarification des rôles ;
- Des réunions de suivi et de coordination sont régulièrement tenues ;
- Un reporting régulier sur l'avancement, les risques et les écarts par rapport au planning et au budget est élaboré ;

- La supervision et la validation des phases d'intégration des infrastructures et des solutions de sécurité (SIEM, SOAR, Threat Intelligence, etc.) sont tenues ;
- Un plan de tests et une stratégie de validation sont élaborés ;
- Des scénarios de tests fonctionnels et techniques pour s'assurer que le CERT/SOC répond aux exigences sont rédigés et transmis ;
- Les équipes de l'ANSSI sont assistées dans l'exécution des tests et la qualification des anomalies ;
- L'ANSSI est appuyé dans la validation fonctionnelle et la réception provisoire et définitive des livrables de la MOE ;
- Un programme de formation adapté aux équipes de l'ANSSI portant sur des parcours de formation spécifiques pour les managers, les analystes SOC, les analystes CERT/CTI et les investigateurs numériques est développé et exécuté ;
- Un plan de conduite du changement pour accompagner les équipes opérationnelles est élaboré et mis en œuvre ;
- Un plan de communication et de sensibilisation destiné aux acteurs clés (OIV/IIC, secteur privé, grand public) est définit et mis en œuvre ;
- Un plan de gestion des risques cyber est élaboré et une organisation du suivi régulier pour sa mise à jour est réalisée ;
- Un support continu à l'opérationnalisation pour une durée de 12 mois après la mise en production du CERT/SOC est fourni ;
- Élaboration d'un plan d'interopérabilité régionale et internationale et mise en place de protocoles de coopération avec les CERT d'Afrique de l'Ouest et les réseaux internationaux ;
- Interopérabilité technique avec le MISP de FIRST, incluant l'échange d'IoC et la formation des analystes SOC/CERT pour exploiter ces flux de renseignements ;
- Des outils de documentation et de capitalisation des connaissances pour assurer une transition fluide vers l'exploitation autonome du CERT/SOC par les équipes du client sont mis en place.

Le Ministère des Postes, des Télécommunications et de l'Economie Numérique (MPTEN), représenté par le Projet WARDIP invite les firmes de consultants (« Consultants ») admissibles à manifester leur intérêt à fournir les services. Les consultants intéressés doivent fournir **en langue française** les informations démontrant qu'ils possèdent les qualifications requises et une expérience pertinente pour l'exécution des Services.

Les critères pour l'établissement de la liste restreinte sont :

I- <u>Expérience générale du cabinet</u> :

- Le prestataire devra justifier d'au moins 08 années d'expérience en assistance à maîtrise d'ouvrage (AMOA) dans le domaine de la cybersécurité ou sur des projets critiques (CERT, SOC, supervision bancaire, PSSI sectorielles, infrastructures critiques) ;
- Le prestataire devra fournir au moins trois (03) références AMOA cybersécurité
- Le prestataire devra fournir au moins trois (3) références portant spécifiquement sur un projet CERT et/ou SOC.
- Le soumissionnaire devra justifier de références pertinentes dans le domaine de la cybersécurité, dont au moins une expérience en Afrique subsaharienne, idéalement dans le secteur public ou e-Gov.

Certifications et accréditations

- Le cabinet devra être certifié ISO/IEC 27001 ou, à défaut, démontrer la mise en œuvre effective d'un SMSI aligné sur cette norme.
- De plus, au moins un (1) expert clé de l'équipe projet devra être certifié ISO/IEC 27001 Lead Implémenter ou Lead Auditor.

Compétences spécialisées

- Expérience avérée dans la mise en œuvre d'au moins deux solutions de sécurité opérationnelle (SIEM, SOAR, NDR, EDR) ;
- Maîtrise et expérience confirmée dans l'intégration et l'utilisation de solutions de gestion des accès et identités et de sécurité privilégiée, incluant :
    - Wallix Bastion (Privileged Access Management – PAM),
    - BestSafe (sécurité des postes de travail et protection avancée),
    - Trustelem (Identity as Service – IDaaS / fédération d'identités),
    - Compétences en investigation numérique et réponse à incident.
- L'expérience en audits de conformité (ISO) constituera un atout distinctif.

III. Capacité technique et administrative du cabinet (Agrément/ou organisation)

- ✓ Disposer d'une équipe multidisciplinaire avec des compétences techniques, juridiques et économiques.

Ce qui pourrait correspondre à la répartition ci-après : (i) Expérience générale… (20 points) ; Expériences spécifiques…… (70 points) ; et (iii) organisation… (10 points).

Personnel :

Le personnel clé ne sera pas évalué lors de l'établissement de la liste restreinte.

Il est porté à l'attention des Consultants que les dispositions des paragraphes 3.14, 3.16, et 3.17 de la Section III de : « BANQUE MONDIALE, Règlement de Passation des Marchés pour les Emprunteurs sollicitant le Financement de Projets d'Investissement (FPI) », Edition Septembre 2025, relatifs aux règles de la Banque mondiale en matière de conflit d'intérêts sont applicables.

Les Consultants peuvent s'associer avec d'autres cabinets pour renforcer leurs compétences respectives en la forme d'un Groupement ou d'un accord de sous-traitant. En cas de groupement, tous les membres de ce groupement restent conjointement et solidairement responsables de l'exécution de la mission au cas où le groupement sera sélectionné.

Un Consultant sera recruté selon la méthode de **Sélection fondée sur les qualifications du consultant (SQC)** en accord avec les procédures définies dans le Règlement de passation de marchés pour les Emprunteurs sollicitant le Financement de Projets d'Investissement (FPI) de la Banque mondiale, Édition Septembre 2025.

Les consultants intéressés peuvent obtenir des informations supplémentaires au sujet des documents de référence (TDR) à l'adresse mentionnée ci-dessous et aux heures suivantes :

Du lundi au jeudi : de 9 heures à 16 heures 30 mn Le vendredi : de 9 heures à 13 heures.

Les expressions d'intérêt doivent être déposées ou transmises par courriel à l'adresse mentionnée ci-dessous au plus tard le **17 Novembre 2025 à 12 h 00 mn GMT.** Les enveloppes doivent porter expressément la mention **« *Manifestation d'intérêt pour le Recrutement d'un cabinet pour l'assistance technique pour la gestion de projet, la planification stratégique et le pilotage de la mise en œuvre du CERT/SOC».***

À l'attention de : Monsieur le Coordonnateur par intérim du Projet Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP-GN).

L'adresse dont il est fait mention ci-dessus est : Projet Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP-GN), Quartier Kaporo, Commune de Ratoma-Conakry, Immeuble BAH Kadiatou, référence la Société Easycom et à proximité du pont Kiridi, **E-mail : coordonnateur@wardip.gn /spm@wardip.gn/ assistant.spm@wardip.gn avec copie obligatoire à : assistante.direction@wardip.gn**

Fait à Conakry, le 18 Octobre 2025

M. Fodé YOULA
Coordonnateur par intérim de WARDIP