



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

**Secrétariat général de la défense
et de la sécurité nationale**

**Cahier des clauses
techniques particulières
n° 2026-12 du 23 juillet 2026**

Marché public de propriété intellectuelle

Pouvoir adjudicateur contractant :

L'État – Services du Premier ministre
Secrétariat général de la défense et de la sécurité nationale (SGDSN)
51, bd de La Tour-Maubourg - 75700 Paris 07 SP

Service bénéficiaire :

Agence nationale de la sécurité des systèmes d'information (ANSSI)
51, bd de La Tour-Maubourg - 75700 Paris 07 SP

Objet du marché :

Fourniture de prestations d'évaluation pour expérimenter la première démarche d'évaluation de produits ou systèmes intégrant un modèle d'Intelligence Artificielle issue du groupe de travail SEPIA.

SOMMAIRE

Article 1 -	Présentation générale du projet	3
Article 2 -	Prestations attendues.....	4
2.1	Généralités.....	4
2.2	Critères de vérification.....	4
2.3	Remarque sur la langue de travail	4
2.4	Réunions provoquées par l'ANSSI.....	4
2.5	Évaluation, selon le scénario 1, du produit retenu.....	4
2.5.1	<i>Objet de la prestation</i>	4
2.5.2	<i>Prestation attendue</i>	5
2.5.3	<i>Livrables attendus</i>	5
2.5.4	<i>Délai prévisionnel</i>	5
Article 3 -	Critères et délais de vérification	6
Article 4 -	Remarques sur les délais	6
4.1	Contenu de l'obligation	7
4.1.1	<i>Confidentialité</i>	7
4.1.2	<i>Secret</i>	7
4.2	Sanction du non-respect de l'obligation	7
Article 5 -	Droits d'utilisation.....	7
5.1	Droits du SGDSN et de l'ANSSI.....	7
5.2	Droits du titulaire.....	7

Article 1 - Présentation générale du projet

L'intelligence artificielle (IA) est en train de modifier en profondeur le numérique, elle intègre de plus en plus de solutions numériques y compris les produits de sécurité déployés dans les réseaux et de nombreux bénéficiaires de l'ANSSI sont en train de l'adopter progressivement. L'ANSSI est ainsi sollicitée pour apporter son expertise en matière de cybersécurité et d'IA.

Par ailleurs, la France est aujourd'hui un des principaux acteurs européens dans le domaine de la certification et l'évaluation de produits de cybersécurité. Son expertise est attendue pour prendre le virage de la certification de produits et systèmes intégrant l'IA. Cependant les modalités d'évaluations de ces types de produits et systèmes ne sont pas fixées à l'heure actuelle bien que différentes normes sur des périmètres très divers, sont déjà en cours d'élaboration.

L'ANSSI pilote ainsi, depuis début 2025, un groupe de travail nommé SEPIA (Sécurité des Produits IA) en charge d'élaborer des méthodes d'évaluation sur la cybersécurité des produits et systèmes intégrant de l'IA. Les travaux de ce groupe ont permis d'aboutir à un premier scénario d'évaluation (dit scénario 1) consistant à garantir que le modèle d'IA, même s'il est considéré comme non fiable ou potentiellement malveillant, ne puisse pas compromettre la sécurité du produit ou système qui l'intègre. Ce scénario apparaît particulièrement adapté lorsque le commanditaire de l'évaluation ne dispose pas des moyens pour faire analyser le modèle lui-même, mais souhaite tout de même évaluer la sécurité globale du produit ou système qui l'intègre.

L'objet de ce marché est d'expérimenter ce scénario 1 pour en valider l'intérêt et proposer d'éventuels compléments de la démarche d'évaluation proposée. Les résultats de cette expérimentation pourront également servir à la valorisation de cette approche dans les instances européennes et internationales, en coordination avec le groupe SEPIA. S'agissant d'une expérimentation, l'application du marché ne donnera pas lieu à l'édition, par l'ANSSI, d'une certification de sécurité au titre du décret n° 2002-535 du 18 avril 2002 modifié.

Cette expérimentation sera réalisée sur un produit et un périmètre d'évaluation proposés par le titulaire, qu'il soit développé par lui-même ou un tiers. Le développeur du produit, que ce soit le titulaire ou un tiers, devra être associé aux réunions de restitution et pourra valider le contenu des communications visant des publics hors ANSSI pour, le cas échéant, approuver le niveau d'anonymisation des informations publiées.

Le présent document constitue le cahier des clauses techniques particulières du marché (dénommé « CCTP ») et a pour objet de décrire les prestations et livrables demandés dans le cadre de l'expérimentation d'une évaluation selon le scénario 1 produit par SEPIA (numéro de référence 72222300-0 – Services de technologies de l'information – de la nomenclature CPV).

Article 2 - Prestations attendues

2.1 Généralités

Dans le cadre de l'exécution technique du marché, le pouvoir adjudicateur sera représenté par un membre de la Division Produits et Services de Sécurité (PSS) de la sous-direction Expertise (SDE) de l'ANSSI, désigné dans le présent document comme « le commanditaire ».

L'objectif de la prestation consiste :

- à appliquer la méthode d'évaluation du scénario 1 de SEPIA sur le produit et le périmètre retenus ;
- à rédiger une analyse critique de la démarche du scénario 1 et à proposer des axes d'améliorations.

Pour piloter les prestations du marché, le titulaire désignera, dès la notification du marché, un représentant garantissant la permanence et l'unité de sa représentativité auprès de l'autre partie au marché, désigné comme « le chef de projet ».

La décision d'arrêter l'exécution des prestations interviendra sans formalités autres que la notification de cet arrêt et ne donnera lieu à aucune indemnité.

2.2 Critères de vérification

L'ANSSI effectuera la revue des livrables fournis par le titulaire. Celle-ci donnera lieu à une restitution entre le titulaire et l'ANSSI, dans les locaux de cette dernière. La revue permettra la validation des travaux du titulaire, elle portera sur son exhaustivité et sa cohérence par rapport aux attentes de l'ANSSI.

2.3 Remarque sur la langue de travail

Le titulaire devra être en capacité de fournir des livrables en langues française et anglaise. De plus le personnel technique impliqué dans les travaux d'évaluation devra être en capacité de participer à des réunions de restitution orale des travaux en français.

2.4 Réunions provoquées par l'ANSSI

Le titulaire s'engage à assister également aux réunions provoquées par l'ANSSI afin de réunir l'ensemble des parties prenantes du projet représentées dans SEPIA.

2.5 Évaluation, selon le scénario 1, du produit retenu

2.5.1 Objet de la prestation

L'objet de la prestation est de réaliser l'évaluation du périmètre d'évaluation validé au titre de la réponse au marché selon le processus et les règles associés au scénario 1 décrit par SEPIA et de fournir un retour d'expérience sur la mise en œuvre de cette démarche d'évaluation.

2.5.2 Prestation attendue

Le titulaire devra réaliser l'évaluation du produit selon le périmètre retenu conformément aux attentes du scénario 1, en s'aidant de tout support qu'il jugera pertinent au regard des spécificités du produit et de la démarche d'évaluation. Une seule passe d'évaluation sera réalisée au titre du marché : il n'est pas attendu d'itération du processus d'évaluation.

L'évaluation du périmètre retenu doit être réalisée par du personnel du titulaire faisant partie du centre d'évaluation agréé par l'ANSSI pour le domaine « équipements matériels avec boîtier sécurisé ».

À l'issue de l'évaluation, le titulaire remettra à l'ANSSI un rapport d'évaluation, ainsi qu'une analyse de la pertinence de la démarche, éventuellement accompagnée de propositions d'amélioration de cette approche.

La prestation inclut une réunion de restitution orale, en français, des travaux réalisés par le titulaire, accompagné des agents impliqués dans le suivi de l'évaluation, à l'ANSSI, ainsi qu'une présentation au groupe SEPIA sur la base des éléments communicables.

La prestation inclut la production d'éléments de communications publique adressant la présentation du cas concret d'application de la démarche, éventuellement anonymisée de la référence au produit.

2.5.3 Livrables attendus

Les livrables attendus au titre du poste sont :

- la spécification détaillée de la portée de l'évaluation, rédigée en anglais, basée dans la mesure du possible sur ce qui est attendu au titre d'une cible de sécurité Critères Communs et sur des particularités du scénario 1. Ce document décrira au moins, le produit, le périmètre d'évaluation retenu et les objectifs de sécurité (spécifiques au scénario 1 et complémentaire à celui-ci) étudiés ;
- un rapport d'évaluation, en anglais ;
- une analyse de la démarche décrite par le scénario 1 (dont les éventuelles difficultés liées à l'instrumentation du produit pour répondre aux particularités du scénario 1), et le cas échéant, des propositions d'amélioration de celle-ci, en anglais ;
- une réunion de fin de projet au groupe SEPIA, en français, sur la base des éléments identifiés comme publiables : retour d'expérience, critique du scénario 1 et suites éventuelles, etc. ;
- des supports de communication publique adressant la présentation du cas concret d'application de la démarche, éventuellement anonymisé.

2.5.4 Délai prévisionnel

Le délai prévisionnel pour démarrer l'évaluation est de quatre semaines à compter de la notification du marché.

Le délai prévisionnel pour la première livraison du rapport d'évaluation sera déterminé lors de la réunion de lancement mais ne pourra être supérieur à trois mois calendaires après la validation de la spécification de la portée de l'évaluation. Idéalement, ce délai est de deux mois à compter de la notification du marché.

Les délais de vérification sont décrits à l'article 3.

Article 3 - Critères et délais de vérification

Les opérations de vérification nécessaires à la réception des prestations porteront sur :

- concernant la spécification de la portée de l'évaluation : conformité aux attentes du scénario 1, qualité technique et documentaire, cohérence interne, complétude ;
- concernant l'évaluation : respect des règles du scénario 1, qualité du rapport technique d'évaluation, de l'analyse critique de l'approche d'évaluation et des propositions d'améliorations formulées ;
- concernant les éléments de communication publique : qualité technique et pédagogique.

Les opérations de surveillance et de vérification seront réalisées par le commanditaire et consignées dans un procès-verbal de constatation des opérations de vérification mentionnant s'il y a lieu les réserves du titulaire. Il sera ensuite transmis au représentant du pouvoir adjudicateur.

Quels que soient les résultats des vérifications, les frais qu'elles entraînent sont à la charge du pouvoir adjudicateur pour les opérations qui, conformément aux stipulations du marché, doivent être exécutées dans ses propres locaux. Ils sont à la charge du titulaire dans les autres cas.

Le délai maximum imparti au pouvoir adjudicateur pour procéder aux opérations de vérification d'un livrable du marché est de quatre semaines calendaires à compter de sa date de livraison ou de son exécution.

Si les opérations de vérification sont négatives, le commanditaire prendra une décision d'ajournement assortie d'un délai de correction maximum de deux semaines calendaires au titulaire pour parfaire les prestations ; il est rappelé que ce délai ne justifie pas lui-même l'octroi d'une prolongation du délai contractuel d'exécution des prestations.

À l'issue de la livraison du livrable corrigé, le commanditaire dispose de nouveau d'un délai maximum de deux semaines calendaires pour reprendre les opérations de vérification.

En cas de nouvel échec, soit la même procédure sera reconduite, soit le représentant légal du pouvoir adjudicateur prononcera directement le rejet des prestations.

Article 4 - Remarques sur les délais

Le délai prévisionnel total est de six (6) mois à compter de la date de réunion de lancement de la prestation.

4.1 Contenu de l'obligation

4.1.1 Confidentialité

Le titulaire s'engage à ne pas divulguer toute information qui pourrait lui être parvenue soit avant la notification du marché soit au cours de l'exécution du marché, sauf pour l'exécution du marché.

4.1.2 Secret

Le titulaire est soumis aux obligations générales relatives à la protection du secret, notamment à celles qui concernent le contrôle du personnel ainsi qu'aux mesures de protection particulière à observer pour l'exécution du marché.

Il ne peut prétendre du chef des dispositions du présent article ni à prolongation du délai d'exécution ni à indemnité à moins que la notification d'avoir à se soumettre à ces mesures de protection du secret ne lui ayant été faite préalablement à la signature du marché, il ne rapporte la preuve que les obligations qui lui sont imposées à ce titre lui rendent l'exécution du marché plus onéreuse.

Le titulaire doit prendre toutes dispositions pour assurer la conservation et la protection des éléments du marché qui revêtent un caractère secret et aviser sans délai l'ANSSI de toute disparition et de tout incident pouvant révéler un risque de violation du secret.

L'obligation au secret perdure après la fin du marché.

4.2 Sanction du non-respect de l'obligation

En cas de violation par le titulaire des obligations mentionnées à l'article 4.1 et indépendamment des sanctions encourues, le titulaire s'expose à une résiliation du marché à ses torts, telle que définie au cahier des clauses administratives particulières.

Article 5 - Droits d'utilisation

5.1 Droits du SGDSN et de l'ANSSI

Le SGDSN et l'ANSSI peuvent librement utiliser les livrables visés à l'article 2.5.3 du présent CCTP et les informations qu'ils contiennent ainsi que les informations utiles qui lui sont communiquées par le titulaire.

5.2 Droits du titulaire

Le titulaire ne peut communiquer les livrables visés à l'article 2.5.3 du présent CCTP et les informations qu'ils contiennent, à titre gratuit ou onéreux, qu'avec l'autorisation de l'ANSSI.