



**MINISTÈRE
DES ARMÉES
ET DES ANCIENS
COMBATTANTS**

*Liberté
Égalité
Fraternité*

**Service d'infrastructure de la Défense
SID Sud-Est**

DAF_2026_000642

MARCHE PUBLIC DE PRESTATIONS INTELLECTUELLES

Cahier des Clauses Techniques Particulières (CCTP)

MAITRE D'OUVRAGE

ETAT

**MINISTÈRE DES
ARMÉES**

.....

CONDUCTEUR D'OPÉRATION :

**SERVICE D'INFRASTRUCTURE DE LA
DÉFENSE SUD-EST**



OBJET DU MARCHÉ :

CASTRES (81) – 8^{ÈME} RPIMA – QUARTIER PESQUIE – SCORPION

**MISSION D'ASSISTANCE À MAITRISE D'OUVRAGE (AMO) CYBER ((SID-SE
26 165 ; 461650)**

NON PROTEGE

1. DOCUMENTS DE RÉFÉRENCE

- Directive n°2014/24/UE, du 26 février 2014, relative à la passation des marchés publics
- Code de la commande publique (CCP)
- Arrêté du 30 mars 2021 portant approbation du cahier des clauses administratives générales applicables aux marchés publics de prestations intellectuelles
- Arrêté du 30 septembre 2021 modifiant les cahiers des clauses administratives générales des marchés publics
- Instruction ministérielle n°1707/ARM/CAB relative aux infrastructures du ministère de la défense du 25 octobre 2021 **[IM-1707]**
- Instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale du 09/08/2021 **[IGI-1300]**
- Instruction ministérielle n°900 du 15/03/2021, relative à la protection du secret et des informations Diffusion et sensibles **[IM-900]**
- Instruction ministérielle n°7326/ARM/CAB relative à la politique de sécurité des systèmes d'information du ministère des armées du 25 juin 2018 **[PSSI-M]** et son volet technique du 21 juillet 2021 **[PSSI-M-T]**
- Directive n°27/ARM/DGNUM portant sur l'homologation des systèmes d'information du ministère des armées, édition 3 du 7 juin 2022 **[DIR-27]**
- Directive n°39/ARM/DGNUM relative à la sécurité numérique des systèmes industriels, édition 2 du 9 juin 2023 **[DIR-39]**

2. OBJET DU PRÉSENTE CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

Le présent CCTP concerne l'exécution de prestations intellectuelles ayant pour objet une mission d'assistance à maîtrise d'ouvrage en cybersécurité (AMO CYBER) lors de l'exécution des phases de conception et réalisation des systèmes industriels d'infrastructure, autres que ceux dédiés à la sécurité protection (SECPRO) du site, qui seront installés au cours de la construction de la zone technique Scorpion au camps du Causse à Castres au profit du 8^e RPIMa.

Intervenant en amont, notamment par l'élaboration du cahier des charges et des exigences de cybersécurité de l'opération, la mission de l'AMO CYBER se poursuit jusqu'à la réception de l'opération et l'homologation de sécurité des systèmes industriels d'infrastructure.

Le titulaire du présent marché est appelé dans la suite du document « l'AMO CYBER ».

3. LE PROJET

Le programme d'armement nommé « Scorpion » (Synergie de COnтакт Renforcée par la Polyvalence et l'InfovalorisatiON) consiste à équiper les Groupements Tactiques Interarmées de l'Armée de Terre (GTIA) française, de véhicules blindés de nouvelle génération qui intègrent des matériels liés à l'entraînement et à la simulation embarquée.

Il développe un matériel évolutif et totalement interopérable. Le système de combat SCORPION vise la plus grande efficacité opérationnelle en intégrant les problématiques capacitaires, d'interopérabilité, d'entretien et de simulation. Ce système de combat est articulé autour d'engins de combat et de moyens d'information et de communication de nouvelle génération.

Dans ce contexte, chaque régiment bénéficiera d'une mise à niveau des infrastructures techniques pour qu'elles disposent des capacités nécessaires au maintien en condition opérationnelle, à la remise en condition, au stationnement des matériels, à la formation et à l'entraînement des équipages.

Dans le cadre de ce programme, les anciens véhicules devenus inadaptés tels que le VAB (véhicule de l'Avant Blindé) sont voués à être remplacés par le SERVAl et le VBAE entre autres.

L'objectif principal à atteindre dans cette opération, est de réaliser toutes les infrastructures nécessaires à l'arrivée des véhicules SERVAL et VBAE sur le site du Camp Capitaine TOURRET à Castres (81) au profit du 8ème RPIMa.

L'ensemble des installations pour le 8^e RPIMA sera à livrer pour la fin du 1er trimestre 2029.

Toutes les infrastructures à réaliser dans le cadre de la présente opération permettront de regrouper l'ensemble des infrastructures de la zone technique du régiment en un même lieu.

Les nouvelles installations seront implantées au Camp Capitaine TOURRET aussi nommé camp du Causse, à 5 kilomètres du camp FAYOLLE.

L'ensemble des travaux de l'opération comprend :

- La construction d'un bâtiment regroupant le magasin multi technique et l'atelier NTI1 multi technique;
- La construction d'un bâtiment regroupant le l'atelier NTI1 et la station entretien;
- La construction d'une aire de lavage;
- La création des voiries et réseaux ;

4. MISSIONS DE L'AMO CYBER

Le rôle général de l'AMO CYBER est d'appuyer le SID dans la conduite de la démarche d'homologation des S2I déployés au titre de l'opération de construction de la ZT Scorpion jusqu'à obtenir leur homologation.

4.1. DESCRIPTION GÉNÉRALE

- D'une manière générale, sur l'ensemble de la phase de réalisation définie par l'[IM 1707] qui couvre les étapes de conception (APD – PRO), réalisation, réception, l'AMO CYBER assurera :
- Le contrôle de la conformité des mesures de sécurité mises en œuvre pour satisfaire les exigences de sécurité préalablement définies ;
- La rédaction des documents nécessaires à la démarche d'homologation ;
- Le contrôle de la documentation produite par les industriels et liée à l'exploitation de la sécurité des systèmes industriels ;
- L'expertise nécessaire au RSSI-P tout au long de la démarche d'homologation ;
- L'accompagnement du RSSI-P à la conduite de la commission d'homologation.

La mission d'AMO CYBER sera assurée par les personnes physiques nommément désignées. La bonne exécution des prestations dépend essentiellement de la personne qui se trouve nommément désignée pour en assurer la conduite.

4.2. DÉCOMPOSITION DES MISSIONS EN PARTIES TECHNIQUES

Les missions de l'AMO CYBER sont réparties en cinq (5) parties techniques (PTx) (au sens de l'article 22 du CCAG/PI), selon la description du tableau suivant :

4.2.1. 2.1. CONCEPTION (PRO)

La maîtrise d'œuvre réalise ses études de conception d'un niveau PRO en respectant les objectifs de réalisation selon le triptyque « coût – délai – performance ».

Cyber : L'AMO CYBER apporte son expertise dans l'analyse des éléments en lien avec la cybersécurité fournis par la maîtrise d'œuvre au stade PRO afin de s'assurer qu'ils sont satisfaisants au regard des exigences de sécurité définies dans le programme de l'opération.

Livrables :

- Cartographies des S2I
- Réponses intermédiaires aux exigences de sécurité (*CUC ou PDS intermédiaires*)

4.3. EXÉCUTION (EXE)

Ce stade correspond au suivi de l'exécution des travaux de réalisation. Il a pour objectif de mettre en œuvre la stratégie et les modalités définies lors des phases de conception.

Cyber : L'AMO CYBER apporte son expertise dans l'analyse et la vérification des éléments fournis par le soumissionnaire et notamment les différents éléments de cartographies des S2I et les réponses aux exigences de sécurité afin de vérifier leur conformité aux éléments décrits dans le programme technique détaillé de l'opération (PTD). Ces éléments lui permettent de rédiger les livrables nécessaires au processus d'homologation des S2I.

- Cartographies finales des S2I
- Réponses finales aux exigences de sécurité (*CUC ou PDS finaux*)
- Procédures d'exploitation de sécurité (*PES*)

4.4. EXÉCUTION STADE FINAL (EXE)

Au cours de ce stade, le service constructeur contrôle la réalisation et vérifie sa conformité vis-à-vis du programme avant mise en service.

Cyber : L'AMO CYBER contrôle que les besoins de sécurité sont bien couverts par les mesures de sécurité mis en œuvre.

Lorsque des risques de sécurité préalablement identifiés n'ont pu recevoir une réponse organisationnelle ou technique, ils sont listés afin d'être présentés à l'autorité d'homologation et potentiellement traités ultérieurement.

Livrables :

- Rapport de conformité (vérification du CUC ou rapport de l'audit de sécurité)
- Liste des risques résiduels

4.5. MISE EN SERVICE (EXE)

Cette dernière étape de la phase réalisation correspond à la mise en service de l'infrastructure par le bénéficiaire. Elle peut nécessiter un processus de qualification avant la livraison définitive des ouvrages ou leur mise en service.

Cyber : La mise en service des systèmes industriels d'infrastructure est conditionnée à l'obtention de leur homologation.

Livrables :

- Synthèse de la démarche d'homologation et support de présentation pour la commission d'homologation

4.6. UTILISATION

Cette phase correspond à la prise en compte de l'ouvrage par l'utilisateur final, à la formation des utilisateurs sur la mise en œuvre des équipements, à la levée des réserves.

Cyber : Au début de cette phase, il s'agit de s'assurer de la prise en compte du maintien en condition de sécurité et opérationnelle des systèmes industriels d'infrastructure et d'initier le suivi dans le temps des mesures de sécurité à leur appliquer pour réduire les risques, traiter les non-conformités et les vulnérabilités tout au long de leur cycle de vie.

4.7. DÉROULEMENT DES MISSIONS

4.7.1. PHASE DE CONCEPTION FINALE PRO – VÉRIFICATION DES MESURES DE SÉCURITÉ PRÉVUES D'ÊTRE DÉPLOYÉES (PT1)

L'AMO CYBER analyse les études de conception finale (PRO) proposées par le maître d'œuvre afin de s'assurer de la cohérence de la réponse technique par rapport aux besoins de sécurité définis dans le programme technique détaillé de l'opération (PTD). Il recueille les documents relatifs à la sécurité des systèmes industriels d'infrastructure, notamment les différentes cartographies (physique, logique, applicative, matrice des flux, etc.) et s'assure que les mesures de sécurité répondent aux exigences de sécurité déterminées par le référentiel réglementaire en vigueur et les analyses de risques. Il suit et fait respecter le plan d'actions préalablement défini.

Livrables :

- Analyse des cartographies des S2I ;
- Réponses intermédiaires aux exigences de sécurité (CUC ou PDS intermédiaires) ;
- Mise à jour du plan d'actions de suivi des remarques de l'AH.

Les délais de fourniture des livrables sont précisés au CCAP.

L'AMO CYBER doit prévoir, dans le cadre de cette PT1, de participer à des réunions se déroulant à Montauban. Le nombre minimum de réunions pour cette partie technique est fixé à 2.

4.7.2. PHASE EXÉCUTION EXE – RÉDACTION DES DOCUMENTS DE SÉCURITÉ NÉCESSAIRES À LA DÉMARCHE D'HOMOLOGATION (PT2)

L'AMO CYBER apporte son expertise dans l'analyse et la vérification des éléments finaux fournis par le maître d'œuvre et notamment les différents éléments de cartographies des S2I et les réponses aux exigences de sécurité afin de vérifier leur conformité aux éléments décrits dans le programme. Ces éléments lui permettent de rédiger les livrables nécessaires au processus d'homologation des S2I.

L'AMO CYBER recueille donc auprès du groupement titulaire du maître d'ouvrage l'ensemble des documents nécessaires à la rédaction des différents documents de sécurité qui seront soumis à approbation de l'autorité d'homologation et présentés lors de la commission d'homologation. Ces documents qui permettront de garantir la sécurité du système industriel d'infrastructure durant son cycle de vie seront délivrés au RSSI-A.

Livrables :

- Cartographies finales des S2I ;
- Réponses finales aux exigences de sécurité (CUC ou PDS finaux) ;
- Procédures d'exploitation de sécurité (PES) ;

Les délais de fourniture des livrables sont précisés au CCAP.

L'AMO CYBER doit prévoir, dans le cadre de cette PT2, de participer à des réunions se déroulant à Castres. Le nombre minimum de réunions pour cette partie technique est fixé à 2.

4.7.3. PHASE SUIVI FINAL DE RÉALISATION – CONTRÔLE DE LA CONFORMITÉ DES MESURES DE SÉCURITÉ DÉPLOYÉES SUR LES S2I (PT3)

L'AMO CYBER vérifie la conformité des mesures de sécurité mises en œuvre au cours de l'opération d'infrastructure soit au travers d'un contrôle pour les S2I de classe 1. Dans ce dernier cas, l'AMO CYBER fournira un rapport d'audit dans lequel seront identifiés les non-conformités et proposées les actions correctrices en cas de découverte de vulnérabilités.

L'AMO CYBER rédige la fiche de synthèse des risques résiduels. Cette fiche reprend les risques résiduels et élabore des scénarios d'attaque puis en chiffre les impacts sur le système industriel d'infrastructure.

Elle présente ensuite, sous forme synthétique, les résultats de l'analyse d'impacts et les préconisations résultantes. Elle permet à la commission d'homologation et à l'autorité d'homologation d'avoir une idée précise sur la gravité des risques résiduels et de statuer sur l'homologation du S2I.

Livrables :

- Liste des risques résiduels ;

Les délais de fourniture des livrables sont précisés au CCAP.

L'AMO CYBER doit prévoir, dans le cadre de cette PT3, de participer à des réunions se déroulant à Castres. Le nombre minimum de réunions pour cette partie technique est fixé à 2.

4.7.4. PHASE MISE EN SERVICE – ASSISTANCE À LA PRÉPARATION DE LA COMMISSION D'HOMOLOGATION (PT4)

L'AMO CYBER participe à la commission d'homologation et assiste le RSSI-P dans la présentation du dossier d'homologation. Il rédige le compte-rendu de la séance.

Livrables :

- Synthèse de la démarche d'homologation ;
- Support de présentation pour la commission d'homologation ;
- Compte-rendu de la commission d'homologation.

Les délais de fourniture des livrables sont précisés au CCAP.

L'AMO CYBER doit prévoir, dans le cadre de cette PT4, de participer à des réunions se déroulant à Castres notamment à la commission d'homologation sur site. Le nombre minimum de réunions pour cette partie technique est fixé à 1.

4.7.5. PHASE UTILISATION (PT5)

Lors de cette phase, l'AMO CYBER assiste l'ESID de Lyon afin de s'assurer que le maintien en condition de sécurité est bien pris en compte par le maître d'ouvrage pour la mise en œuvre du marché de maintenance.

Livrables :

- Plan d'amélioration continue de sécurité final ;

Les délais de fourniture des livrables sont précisés au CCAP.

L'AMO CYBER doit prévoir, dans le cadre de cette PT5, de participer à des réunions se déroulant à Castres. Le nombre minimum de réunions pour cette partie technique est fixé à 8 (1 réunion trimestrielle au minimum).

4.8. FORME DES LIVRABLES

L'AMO CYBER fournit chaque livrable en version informatique (fichier « .pdf » et fichier natif) ainsi qu'une version papier en un exemplaire si demandé. Les plans, documents, dossiers et supports informatiques sont soigneusement conditionnés. Les précisions suivantes figurent sur tous les documents remis :

- Nom du titulaire ;
- Date d'exécution des prestations ;
- Cartouche/nom et logotype du maître d'ouvrage ;
- Classification des documents.

5. REMISE DES LIVRABLES AU MAÎTRE D'OUVRAGE

Chaque livrable est présenté au maître d'ouvrage lors d'une réunion organisée, à cet effet, entre les parties¹. Plusieurs livrables peuvent être présentés lors d'une même réunion, avec accord préalable du maître d'ouvrage.

6. DÉFINITIONS ET ATTENDUS SUR LES LIVRABLES

I.1. Stratégie d'homologation (SH)

La stratégie d'homologation est produite lorsque le S2I est de classe 2 ou 3. Elle formalise l'organisation et la procédure d'homologation qui est adoptée en identifiant les éventuels écarts ou adaptations retenues par rapport à la réglementation. Elle liste également les acteurs de la démarche d'homologation et fixe le périmètre concerné. Elle intègre, le schéma technico opérationnel obtenu à l'aide de l'outil VAUBAN du SID. Enfin elle présente les prescriptions retenues pour assurer le MCS.

I.2. Plan de sécurité des systèmes (PDS)

Le PDS décrit les mesures techniques et organisationnelles mises en œuvre pour répondre aux exigences de sécurité applicables au S2I considéré, compte tenu de sa classe de cybersécurité et de son contexte d'emploi.

Le PDS contient un paragraphe sur le maintien en condition de sécurité (MCS) du S2I concerné.

Le PDS évolue durant le projet jusqu'à sa version finale en passant par les phases suivantes :

- Préliminaire (initial) qui décrit la liste des exigences retenue par l'autorité cliente, à annexer au DCE du maître d'œuvre ;
- Provisoire (intermédiaire) qui intègre les études réalisées en vue de l'exécution des travaux ;
- Définitif (final) qui intègre notamment les recommandations de l'audit Cyber.

Le plan de sécurité des systèmes est produit par l'AMO CYBER en concertation avec le RSSIP.

I.3. Procédures d'exploitation de sécurité (PES)

Il s'agit du mode d'emploi de la sécurité du S2I. Les PES décrivent les règles de sécurité organisationnelles permettant de prendre en compte l'organisation cybersécurité qui a été formalisée pour le système.

Les PES doivent présenter notamment :

- L'organisation retenue au sein de l'autorité d'emploi ;
- Les procédures de maintenance (MCO/MCS) du S2I ;
- La gestion des accès logiques du S2I ;
- Les modes d'exploitation normal et dégradé, associés aux procédures de conduite correspondantes

La procédure d'exploitation de sécurité est produite par l'AMO CYBER, en concertation avec le RSSIP.

7. ADMISSION DES PRESTATIONS

L'admission des prestations remises par l'AMO CYBER est validée par une décision du maître d'ouvrage, notifiée par ordre de service dans un délai maximum de deux mois à compter de la date certaine de réception des prestations par le maître d'ouvrage.

Si cette décision n'est pas notifiée au titulaire dans les délais précédents, la prestation est considérée comme reçue tacitement, avec effet à compter de l'expiration du délai, conformément à l'article 29 du CCAG-PI.

8. CONTRÔLE DES LIVRABLES PAR LE MAÎTRE D'OUVRAGE

Les documents préparés par l'AMO CYBER font l'objet d'une validation par le maître d'ouvrage avant diffusion.

9. CONTRÔLE ET ACHÈVEMENT DE LA MISSION

9.1.1. CONTRÔLE

Tout au long des différentes phases, le maître d'ouvrage se réserve le droit d'effectuer, par les moyens qu'il juge adéquats et dont il est seul juge, les vérifications qu'il estime nécessaires quant au contrôle de la qualité des prestations effectuées par l'AMO CYBER.

À ce titre, ce dernier est tenu de lui laisser, ainsi qu'aux personnes qu'il aura désignées, le libre accès à tous documents requis.

9.1.2. ACHÈVEMENT DE LA MISSION

L'achèvement de la mission fait l'objet d'une décision établie par le pouvoir adjudicateur après demande du titulaire établie en application de l'article 28.4.2 du CCAG/PI pour la dernière partie technique du marché.