MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

Clausier CYBER initial

octobre 2022

Référentiel intérimaire avant la mise en place du référentiel de maturité Cyber

Il est proposé que les documents de référence suivants soient accessibles sur https://armement.defense.gouv.fr (successeur IXARM) à l'appui des clauses Cyber suivantes :

- [Ref. 1] guide pour la spécification de la cybersécurité comme une performance
- [Ref. 2] guide d'identification des systèmes d'information névralgiques
- [Ref. 3] guide d'identification des composants critiques d'un point de vue cyber
- [Ref. 4] référentiel d'exigences de sécurisation de livraison (intégrant le modèle de certificat d'innocuité)

Clauses Cyber – Démarche d'homologation

	CCAP (clausier)	CCTP
Le Titulaire met en place une veille afin d'identifier les vulnérabilités et les obsolescences sur les composants applicatifs, firmwares ou matériels pouvant concerner les constituants du système objet du marché.		X
Le Titulaire réalise une analyse d'impact sur les vulnérabilités et obsolescences détectées.		X
Le Titulaire propose un plan de remédiation* pour les vulnérabilités et obsolescences identifiées.		X

**Les modalités de traitement (forfaitaire ou non) des vulnérabilités et obsolescences pourront être adaptées au contexte du marché concerné*

Clauses Cyber – management et qualité

	CCAP (clausier)	CCTP
Les revues d'avancement contractuelles * liées aux jalons programme incluent un volet cybersécurité.		X

**En l'absence de revues d'avancement programme (de type RCP, RCD…), des points d'avancement spécifiques cyber devront être mis en place*

Clauses Cyber – Cyber en tant que Performance

- En phase précontractuelle, le Titulaire réalisera :
  - une analyse fonctionnelle du système (si non réalisée par ailleurs), permettant d'identifier clairement les principales chaines fonctionnelles concourant à la réalisation des missions du système et intégrant la dimension cyber
  - une analyse EBIOS RM (Risk Manager) en mode plateau Industrie-Minarm permettant d'identifier les éléments importants pour la réalisation des missions (valeurs métier), les événements redoutés, le socle réglementaire minimum, les sources de risques, les objectifs visés et les scénarios stratégiques
  - une proposition de moyens techniques et RH à mettre en place pour estimer la résilience des performances opérationnelles à un environnement de menaces cyber
- Pour la phase contractuelle, le Titulaire proposera :
  - Une architecture et un dossier justificatif permettant de justifier la tenue des performances opérationnelles face à la menace cyber
  - Un planning de réalisation des tests de résilience des performances opérationnelles à la menace cyber, incluant des créneaux pour des tests étatiques
  - La réalisation de plateformes représentatives du système permettant la réalisation de ces tests de résilience

Pour ces travaux, le titulaire pourra s'appuyer sur le document [Ref. 1]

Clauses Cyber – Cyber en tant que Performance

	CCAP (clausier)	CCTP
Le Titulaire propose des éléments d'architecture technique en réponse aux performances cyber exprimées et aux exigences socle. *Il peut être nécessaire de réaliser plusieurs itérations besoins/exigences/architecture par exemple pour prendre en compte les compromis nécessaires entre les performances cyber et les autres performances du système, pour raffiner les scénarios de menace en fonction de l'architecture proposée. Le nombre minimum d'itérations prévues dans cette étude est de deux.*		X

Clauses Cyber – Systèmes d'Information névralgiques

	CCAP (clausier)	CCTP
A sa date de notification, les prestations du marché nécessitent le recours à des SI névralgiques. L'annexe [xx] : • identifie ces SI névralgiques pour le titulaire et les sous-traitants déclarés au marché ; • précise pour chacun des SI névralgiques du titulaire les mesures de sécurité mises en place pour les protéger contre les menaces cyber.	X	
Le titulaire demande à l'ensemble de ses sous-traitants de rang 1 de communiquer au MINARM, à une fréquence annuelle : • la mise à jour de la liste de leurs SI névralgiques ; • les mesures de sécurité mises en place pour protéger leurs SI névralgiques contre les menaces cyber. Le Titulaire demande à l'ensemble de ses sous-traitants de rang 1 de répercuter ces exigences vers leurs propres sous-traitants.	X	

Clauses Cyber – Systèmes d'Information névralgiques

	CCAP (clausier)	CCTP
Le titulaire demande à l'ensemble de ses sous-traitants de rang 1 de communiquer au MINARM : • tout incident affectant leurs SI névralgiques sous 72 heures. Le Titulaire demande à l'ensemble de ses sous-traitants de rang 1 de répercuter cette exigence vers leurs propres sous-traitants.	X	
Le Titulaire met à jour l'annexe [xx] du CCAP en suivant le guide d'identification des SI névralgiques (*) [annuellement] / [lors des jalons suivants : {liste de jalons}].		X

(*) cf. document [Ref. 2]

Clauses Cyber – Composants critiques

	CCAP (clausier)	CCTP
Le Titulaire détermine la liste des composants critiques d'un point de vue cyber du système objet du présent marché en suivant le guide d'identification des composants critiques d'un point de vue cyber (*). Cette liste est fournie à l'administration et mise à jour [annuellement] / [lors des jalons programmes suivants : {liste de jalons}].		X

(*) cf. document [Ref. 3]

Clauses Cyber – Sous-contractants critiques

	CCAP (clausier)	CCTP
Le marché comporte à sa date de notification les sous-contractants critiques d'un point de vue de cyber listés en annexe [yy]. Ces sous-contractants pourront faire l'objet d'audits cyber conduits par l'administration.	X	
Le Titulaire met à jour l'annexe [yy] d'identification des sous-contractants critiques d'un point de vue cyber [annuellement] / [lors des jalons programmes suivants : {liste de jalons}].		X
Le Titulaire s'attache à sélectionner des sous-contractants critiques présentant un niveau de maturité cyber adapté aux prestations qui lui sont confiées. Le Titulaire demande à l'ensemble de ses sous-contractants critiques de répercuter cette exigence vers leurs propres sous-contractants critiques.	X	

Clauses Cyber – Maîtrise du risque cyber dans les livraisons

	CCAP (clausier)	CCTP
Le Titulaire décrit l'organisation, les procédures et les moyens* mis en place pour assurer la cybersécurité des livraisons numériques** en conformité avec le modèle de certification d'innocuité (*).		X
Chaque livraison numérique** est accompagnée d'un certificat d'innocuité contenant au minimum les informations listées dans le modèle de certification d'innocuité (*).		X
L'administration se réserve le droit de refuser toute livraison numérique** si le certificat d'innocuité contient un élément signalé comme infecté, sauf s'il est formellement identifié comme « faux positifs » et accompagné des informations *ad hoc* demandées dans le référentiel d'exigences de sécurisation de livraison (*).	X	

**Via les outils du commerce (ex : station blanche…)*

***Via des supports IT (ex : disque dur…) ou transferts dématérialisés*

(*) cf. document [Ref. 4]

Clauses Cyber – Garantie des prestations

	CCAP (clausier)	CCTP
Pour les prestations, les matériels et logiciels, la garantie couvre les performances cyber*.	X (§ chapeau de l'article 7)	

**Dans les limites fixées par l'article ad-hoc du CCAP du marché concerné pour les garanties associées aux prestations, matériels et logiciels*