



ESID de Bordeaux - Mai 2021

EXIGENCES D'HYGIENE CYBER DES S2I

(systèmes industriels d'infrastructure)

Annexe relative aux marchés de prestations intellectuelles MOP et MMOA

1. Information sur la démarche d'homologation des systèmes industriels d'infrastructures (S2I)

Le présent projet, objet du marché, s'inscrit dans une démarche d'homologation pour chaque système industriel d'infrastructure (S2I) mis en place (du type gestions techniques, CVC, contrôle d'accès, vidéo surveillance, détection d'intrusion, traitement de l'eau et de l'incendie, ...), ainsi que tous les systèmes informatiques communs inhérents au fonctionnement de la supervision tel que les serveurs, les sauvegardes, la gestion du réseau IP ...

La démarche d'homologation est une démarche qualité appliquée à la sécurité.

Ce dossier est ensuite certifié par une décision délivrée par une autorité d'homologation (autorités responsables des S2I au niveau centrale du MINARM).

Cette décision d'homologation atteste que le système d'information considéré est apte à traiter des informations d'un niveau de classification donné, conformément aux objectifs de sécurité visés, et que les risques de sécurité résiduels sont acceptés et maîtrisés.

La démarche d'homologation des systèmes industriels d'infrastructures s'inscrit dans la mission de base du maître d'œuvre. Dans le cadre d'un mandat de maîtrise d'ouvrage, le mandataire devra assurer la prise en compte et le suivi de cette démarche. L'appel d'offres travaux devra stipuler que le ou les titulaires des lots concernés par la problématique cyber devront organiser les éléments liés à cette démarche et, de ce fait, devront posséder les compétences nécessaires au respect des exigences dites de cybersécurité.

A ce titre, les actions du titulaire du marché de maîtrise d'œuvre sont les suivantes :

En phase conception : inclure les exigences techniques imposées par la maîtrise d'ouvrage en termes de certifications des équipements par exemples, et de validation ANSSI pour ce qui est des systèmes et logiciels ainsi que de l'architecture des systèmes proposée.

En phase réalisation :

° Transmettre aux entreprises les modèles de documents fournis par le maître d'ouvrage et relatifs aux équipements installés (fiches produits et fiches de validation types, par exemple) ;

° Collecter et vérifier les informations et les documents complétés auprès des entreprises.

En phase de réception : assister le maître d'ouvrage dans la réalisation des tests de sécurité, lors des opérations préalables à la réception, obtenir un DOE et des cartographies exhaustifs, adaptés et strictement représentatifs des installations et systèmes mis en œuvre.

L'ensemble des informations et documents recueillis par le maître d'œuvre permettront au maître d'ouvrage de réaliser les livrables de la démarche d'homologation.

Toutes les informations relatives à la démarche d'homologation des systèmes industriels d'infrastructures sont consultables sur le site de l'ANSSI (Agence National en Sécurité des Systèmes d'Information).

Le candidat devra notamment prendre connaissance des documents intitulés « la démarche d'homologation en 9 étapes simples », « maîtriser la SSII pour les systèmes industriels » et « exigences de cybersécurité pour les prestataires d'intégration et de maintenance de systèmes industriels ».

2. Exigences relatives aux marchés de prestations intellectuelles MOP et MMOA

	Exigences	Pénalités ou retenues
1	<p>Le titulaire devra désigner en son sein un point de contact Cyber (POC cyber) pour les besoins de ses prestations ; celui-ci sera garant des obligations contractuelles de cybersécurité de l'entreprise et de ses sous-traitants. Son niveau minimal requis correspond à la formation en ligne de l'ANSSI dite MOOC ("massive on line open course" = cours en ligne), gratuite. Le programme de la formation sera à communiquer à l'ESID pour validation s'il est différent du MOOC de l'ANSSI.</p> <p>Une attestation de désignation du POC cyber devra être fournie dans l'offre par le titulaire ou, au plus tard, avant la notification du marché. En cas de changement de ce POC en cours d'opération, une nouvelle attestation devra être fournie.</p>	Sans objet.
2	<p>Toute documentation relative au dossier cybersécurité du système industriel fera l'objet d'une mention de protection au minimum de type "Diffusion restreinte", exigeant un poste de travail isolé ou connecté à un réseau interne de niveau DR dans l'entreprise (aucune connexion à internet). Les exigences de l'instruction interministérielle 901 (II 901) devront être appliquées.</p> <p>Le chiffrement de fichiers sera utilisé pour tous les échanges sensibles sur des réseaux non protégés (Internet...). Le logiciel de chiffrement, à la charge de l'entreprise, devra être autorisé par l'ANSSI (ZED par exemple, ou ACID).</p> <p><i>Nota : La solution ACID est à privilégier.</i></p>	Pénalité forfaitaire de 500 € HT à chaque manquement.
3	<p>Seuls les médias amovibles (clef USB, disques durs, carte SD...) dédiés aux systèmes du MINARM (c'est-à-dire étiquetés comme tels) pourront se connecter sur nos systèmes. L'utilisation de ces médias pour tout autre usage est interdite. Réciproquement, l'utilisation de tout autre média est interdite.</p> <p>Les médias amovibles seront fournis par le titulaire. Ils seront préparés par le BSSI-L avant toute utilisation.</p> <p>Ces médias amovibles devront passer par un sas antiviral (ordinateur de l'USID dit "station blanche") avant d'être connecté au système. Si l'accès à un sas antiviral n'est pas possible, le titulaire s'engagera auprès de l'administration à ce que les médias utilisés ont été vérifiés et sont sains.</p>	Pénalité forfaitaire de 1000 € HT à chaque manquement.