

service d'infrastructure
de la défense Nord-ouest

cahier des clauses techniques particulières CCTP

Personne publique contractante – Représentant du pouvoir adjudicateur

ETAT – MINISTÈRE DES ARMÉES

Le Directeur du Service d'Infrastructure de la Défense Nord-Ouest
Quartier Margueritte – BP 14 – 35998 RENNES CEDEX 09

CHARGE DU SUIVI

Unité de Soutien d'Infrastructure de la Défense (USID) d'Évreux

Objet du marché

Marché de maintenance et tierce maintenance applicative des installations de contrôle d'accès, de détection intrusion et de vidéosurveillance (CADIVS) des sites de la BdD d'Évreux

SOMMAIRE :

1	OBJET	5
1.1	PERIMETRE.....	5
1.1.1	<i>Géographique</i>	<i>5</i>
1.1.2	<i>Normatif</i>	<i>6</i>
1.2	OBLIGATIONS COMMUNES.....	6
1.3	RESPONSABILITE DE L'ADMINISTRATION.....	7
1.4	OBLIGATION DU TITULAIRE	7
1.4.1	<i>Indisponibilité des installations CADIVS.....</i>	<i>7</i>
1.4.2	<i>Précautions particulières</i>	<i>8</i>
1.4.3	<i>Utilisation des matériels du client</i>	<i>8</i>
1.4.4	<i>Hygiène cyber et SII</i>	<i>8</i>
1.4.5	<i>Achat de matériels et de logiciels.....</i>	<i>14</i>
1.4.6	<i>Mise au rebut du matériel et maintenance externe</i>	<i>14</i>
1.4.7	<i>Objectifs de Résultats / de moyens</i>	<i>14</i>
1.4.8	<i>Exigence de conseil et d'assistance.....</i>	<i>15</i>
2	GENERALITES	16
2.1	HYGIENE ET SECURITE	16
2.1.1	<i>Tenue et comportement du personnel.....</i>	<i>16</i>
2.1.2	<i>Plan de prévention.....</i>	<i>16</i>
2.2	GESTION DES DECHETS.....	17
2.3	DISPOSITIONS ENVIRONNEMENTALES	18
2.4	MATERIAUX ET MATERIELS.....	18
2.5	PROCEDURES ORGANISATIONNELLES.....	18
2.6	NORME ET REGLEMENTATION	19
3	PRIX ET DISPOSITION FINANCIERE	19
3.1	PRIX.....	19
3.1.1	<i>Montage des prix</i>	<i>19</i>
3.1.2	<i>Prix des pièces du correctif</i>	<i>22</i>
4	QUALITE	24
5	DEFINITIONS DES PRESTATIONS.....	25
5.1	GESTION DU MARCHE	25
5.1.1	<i>Période de mise en place</i>	<i>25</i>
5.1.2	<i>La réalisation du planning de maintenance préventive et des trames des rapports de maintenance préventives demandés ;</i>	<i>25</i>

5.1.3	<i>État des lieux</i>	25
5.1.4	<i>Réversibilité des installations et transférabilité</i>	26
5.1.5	<i>GTP – outil de connaissance technique du SID</i>	27
5.1.6	<i>Réunions et livrables</i>	28
5.1.7	<i>Planning</i>	29
5.1.8	<i>Prestations dues au titre du marché</i>	29
5.2	MONOGRAPHIES / GMAO	31
5.3	CRITICITE/DELAIS D'INTERVENTION	31
5.4	MAINTENANCE PREVENTIVE	33
5.4.1	<i>Détecteurs, capteurs</i>	33
5.4.2	<i>Lecteurs de badges, claviers à code</i>	33
5.4.3	<i>Sirènes, dispositifs d'alarmes sonores</i>	33
5.4.4	<i>Nettoyer selon des prescriptions du fabricant</i>	33
5.4.5	<i>Vidéosurveillance</i>	33
5.4.6	<i>Interphonie et visiophonie</i>	34
5.4.7	<i>Tourniquets, tripodes</i>	34
5.4.8	<i>Maintenance préventive des composants actifs (switchs, serveurs, postes de travail, enregistreurs, pupitres, parefeux, diodes, imprimantes, UTL, centrales intrusion)</i>	34
5.5	MAINTENANCE CORRECTIVE	36
5.6	ASTREINTES/CENTRE DE SERVICE	36
5.7	MAINTENANCE APPLICATIVE – TIERCE MAINTENANCE	37
5.8	MAINTIEN EN CONDITION DE SECURITE	38
5.8.1	<i>Veille cyber sécurité</i>	38
5.8.2	<i>Volet technique MCS</i>	38
5.8.3	<i>Lutte contre les codes malveillants</i>	39
5.8.4	<i>Veille et traitement de l'obsolescence</i>	39
5.8.5	<i>Contrôle de conformité et audit de sécurité</i>	41

GLOSSAIRE ET TERMINOLOGIE

Notation CVSS : ce système de notation des vulnérabilités permet de disposer de trois notes numériques (base, temporelle et environnementale) comprises entre 0 et 10 et d'un vecteur représentant les critères utilisés pour calculer chaque note. La note de base permet de quantifier l'impact maximum théorique de la **vulnérabilité**. Elle s'appuie sur des éléments propres à la vulnérabilité. La note temporelle permet de pondérer la note de base en prenant en compte l'évolution de la vulnérabilité dans le temps. La note environnementale pondère à son tour les notes précédentes en tenant compte du contexte dans lequel est utilisé le système.

Occupant : Le personnel utilisant les bâtiments et immeubles de la base de défense de Rennes et de ses sites rattachés (appelés également *utilisateurs*)

RSSI : Responsable de la sécurité des systèmes d'information

Chef d'antenne : Représentant de proximité de l'USID sur un site excentré de Rennes qui a en charge la maintenance du site et d'autres entités. Il est un interlocuteur privilégié du titulaire sur le site. Surveillant la partie forfaitaire du contrat, il est responsable de la maintenance.

DRSD : Direction du Renseignement et de la Sécurité de la Défense, organisme militaire chargé notamment de la sécurité des sites militaires et qui a pouvoir d'enquêter sur les personnels ayant besoin d'accéder sur des sites sécurisés. Ce service réalise les *contrôles primaires*.

Maintien en condition opérationnelle (MCO) : il regroupe toutes les prestations qui consistent à conserver un bien dans un état lui permettant de remplir sa fonction. Ces prestations s'exécutent à titre préventif ou correctif. Elles peuvent concerner des prestations d'évolution de logiciels.

Maintien en condition de sécurité (MCS) : il regroupe l'ensemble des mesures organisationnelles et techniques concourant à maintenir le niveau de sécurité accepté lors de l'homologation, tout au long du cycle de vie d'un composant matériel ou logiciel.

Monographie : Liste détaillée des équipements à entretenir par type de matériel

SID : Service Infrastructure de la Défense

SII : Système Industriel d'Infrastructure

Tierce maintenance applicative : désigne les prestations qui consistent à conserver un système d'information dans un état lui permettant de remplir sa fonction. Ces prestations de maintien en condition opérationnelle et de maintien en condition de sécurité s'exécutent à titre préventif ou correctif. Elles peuvent également concerner des prestations d'évolution ou d'adaptation des logiciels. Ces services peuvent être rendus sur le site de l'acheteur ou à distance dans les locaux du titulaire. Des prestations de maintenance de matériel peuvent être incluses dans un marché de tierce maintenance applicative.

ANNEXE AU CCTP :

- Bon de travail SSI (compte rendu d'intervention).

1 Objet

Le marché a pour objet la réalisation de la maintenance des installations de contrôle d'accès, de détection intrusion et de vidéo surveillance ainsi que la tierce maintenance applicative des sites de la BdD d'Évreux hors DGA TH.

1.1 Périmètre

Le terme CADIVS regroupe l'ensemble des équipements, matériels, logiciels et installations constituant les sous-systèmes assurant les fonctions de contrôle d'accès, de détection intrusion, de vidéosurveillance, d'interphonie/visiophonie et de diffusion d'alerte, ainsi que les réseaux supports dédiés.

- Limite amont : à partir du disjoncteur du tableau électrique inclus
- Limite aval : jusqu'à l'équipement CADIVS inclus

Les équipements annexes sont également intégrés au présent marché et d'une manière générale tous les équipements secondaires et accessoires dédiés à la fonction « de contrôle d'accès, de détection intrusion, de vidéosurveillance et d'interphonie audio ou vidéo ».

La description et la spécification des équipements à maintenir sont celles décrites dans la monographie annexée au présent CCTP.

IMPORTANT : les prix forfaitaires resteront inchangés pour toute augmentation ou diminution de +/- 5% du nombre d'équipements recensés dans la monographie répartis sur un bâtiment et sur une année.

1.1.1 Géographique

Le présent marché concerne les sites suivants :

CNMO-TSR de Favières (28) :

- N° du site : 280 147 001 R
- Adresse : route de Courville – 28 170 FAVIERES

CNMO-TSR de Vernon (27) :

- N° site : 270 681 004 W
- Adresse : route de Magny – 27 200 Vernon

Base aérienne 105 et autres sites rattachés :

N° G2D du site	Description
270229009L	Dépôt munitions de SASSEY
270229012O	Base aérienne 105
760217502S	Sémaphore de Dieppe
760217503T	Brigade nautique de Dieppe

N° G2D du site	Description
760259501B	Sémaphore de Fecamp
760351503P	Immeuble du commandement de la marine
760351508U	Ilôt des remorqueurs
760540047H	Caserne d' Herbouville
760552506M	Sémaphore et station de la Heve
800039501B	Sémaphore d'Ault-Onival

1.1.2 Normatif

Le titulaire réalise la maintenance des niveaux 1 à 5 de la norme NF X 60 000.

Les prestations incluses dans le forfait comprennent le conseil, les études, les locations de matériel, la participation au réunion, la fourniture de livrable, participation aux CVPO.

Le présent marché comprend également des prestations de maintenance améliorative ayant pour objectif de faire évoluer le matériel pour s'adapter aux nouveaux besoins ou prévenir l'obsolescence.

1.2 Obligations communes

Le titulaire doit collaborer étroitement avec les représentants de l'administration et apporter son concours, chaque fois qu'elle lui en fera la demande sur l'ensemble des installations relevant du périmètre du marché. Il assure, sous sa responsabilité, l'exécution de l'ensemble des prestations du marché, conformément aux dispositions prévues et établies sur la base du CCTP et du BPU et se charge de leur préparation.

Le bénéficiaire et le titulaire doivent veiller à ce qu'aucune personne en dehors des préposés du titulaire, des représentants du bénéficiaire, des représentants habilités du ministère des Armées et de l'Unité du Service Infrastructure de la Défense (**USID**), ne puisse avoir accès aux locaux techniques concernés par le présent CCTP, aux documents, aux pièces du marché, ni intervenir dans le fonctionnement des installations.

Travaux d'amélioration : la personne publique est susceptible de faire effectuer des travaux sur les installations faisant l'objet du présent marché par un tiers.

Dans ce cas, la personne publique informe le titulaire des travaux qu'elle prévoit d'effectuer. Il appartient au titulaire de faire toutes les observations utiles sur l'état de l'équipement auprès de la personne publique avant les travaux.

Le titulaire peut être invité aux opérations préalables à la réception d'un nouvel équipement. Si, lors de cette étape, le titulaire juge que le nouvel équipement (ou son installation) ne peut être accepté en l'état, il en informe la personne publique. A l'issue de la réception, le titulaire

reconnait être parfaitement informé de la constitution et de l'état de l'équipement qu'il prend en charge.

Le Titulaire met, dans le cadre du présent marché, le personnel, les matériels et les documents liés au présent marché à la disposition de ces sociétés ou organismes pour qu'ils remplissent les missions qui leur sont confiées.

Le Titulaire en est informé par le maitre d'ouvrage avant les interventions.

1.3 Responsabilité de l'administration

L'USID mettra à la disposition du titulaire l'ensemble des documents utiles en sa possession pour la réalisation des prestations. La documentation sera à consulter dans les locaux de l'USID.

Le SID est doté d'un logiciel de Gestion Technique du Patrimoine nommé « Outil GTP ». Ce logiciel est aussi gestionnaire des ordres d'intervention (OI) de dépannage.

L'accès à GTP ne peut être fait que via l'intranet du Ministère des Armées (appelé INTRADEF), à partir d'un poste dédié, mis à disposition par l'USID.

Il est prévu qu'au cours du marché, le titulaire disposera d'un poste informatique équipé du logiciel et d'un compte GTP.

Une formation sera dispensée au titulaire par le SID.

1.4 Obligations du titulaire

La télémaintenance des installations est interdite.

1.4.1 Indisponibilité des installations CADIVS

Le Titulaire doit informer le maitre d'ouvrage de l'indisponibilité d'une installation CADIVS via une fiche d'interruption de service et lui en communiquer la durée prévisible.

Cette fiche comportera notamment les indications suivantes :

- La nature de l'opération entraînant l'interruption de service et la désignation du local ou de la zone concernée ;
- Les dates et heures de l'interruption ;
- La désignation éventuelle des organes à consigner pour la réalisation des prestations.

Cette fiche d'interruption de service doit être soumise à l'accord de l'administration au moins 15 jours ouvrés avant la date de l'intervention effective, afin que le maitre d'ouvrage puisse la communiquer aux services concernés avant la date d'intervention.

Dans le cas où une prestation ne pourrait pas être réalisée à la date définie du fait de l'administration, il s'engage à en avertir le Titulaire au plus tard 5 jours ouvrés avant sans que cela ne puisse avoir une incidence financière.

1.4.2 Précautions particulières

Lors de l'exécution des prestations du marché, toutes précautions doivent être prises pour assurer la protection des ouvrages fonciers et immobiliers ainsi que des équipements, qu'il s'agisse de mobiliers ou d'équipements.

Afin d'éviter les contestations ultérieures, un état des lieux préalable à toute intervention qui le justifie peut être demandé par le maître d'ouvrage ou par le titulaire. L'état des lieux correspondant est dressé contradictoirement par les deux parties, il ne donne pas lieu à facturation.

1.4.3 Utilisation des matériels du client

Il appartient au Titulaire d'avertir son personnel que l'usage des matériels et équipements que renferment les locaux et bureaux, notamment des appareils téléphoniques, matériels informatiques et machines à photocopier lui est strictement interdit sauf dérogation particulière ou autorisation formelle du Client.

1.4.4 Hygiène cyber et SII

Le Titulaire doit respecter les règles de protection des informations et supports en vigueur au sein du ministère des Armées.

Le Titulaire conserve et traite les données du Client de manière séparée de ses propres données ou de données d'autres clients du Titulaire. Le Titulaire doit restreindre l'accès aux données du Client suivant le principe de restriction au besoin d'en connaître.

Le Titulaire s'assure de la non divulgation, à des tiers non autorisés, des informations traitées dans le cadre du présent marché.

Le Titulaire garantit que les modalités de stockage et d'échanges d'informations numériques permettent d'en assurer la confidentialité et l'intégrité (utilisation d'Acid Cryptofiler).

Le Titulaire garantit que les supports échangés ou à connecter sur les systèmes n'intègrent aucun code malveillant et ont fait l'objet d'un test d'innocuité positif au moyen d'une attestation à fournir au Client.

Toute transmission de fichiers sur un support physique (USB, DAT, CDROM, etc.), par courrier externe ou par porteur, donne lieu à l'établissement d'un bordereau de prise en compte.

De plus, l'ensemble des opérations de transferts de disques durs, supports d'archives ou de sauvegarde doit être tracé en précisant :

- L'émetteur et le destinataire,
- Le détail des opérations de transferts et notamment le nombre, la date,
- Sur simple demande, ce registre est mis à la disposition du Client par le Titulaire.

Le Titulaire applique les règles de marquage sur les ressources techniques (matériels et logiciels informatiques, supports de stockage) et les supports papier pour faire savoir au personnel autorisé que ces éléments contiennent des informations sensibles.

Le Titulaire conserve en lieu sûr les supports de stockage de données en fin de vie hébergeant des données du Client, en attendant de procéder à leur effacement sécurisé ou à leur

destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée ne puisse être récupérée.

Le cas échéant, le Titulaire ne met pas au rebut ou ne fait pas emporter par une société de maintenance, ou encore ne réutilise pas ces supports de sauvegarde à d'autres fins que celles prévues initialement sans l'autorisation expresse du Client.

Le Titulaire maintient à jour et est en mesure de mettre à disposition du Client toutes les données relatives à la prestation.

En cas de non reconduction ou en cas de résiliation du contrat, le Titulaire restitue sous un mois au Client l'intégralité des données confiées dans le cadre de la prestation. Une fois la restitution effectuée, le Titulaire doit détruire dans un délai de 8 jours, les éventuelles copies de données détenues, y compris les données ayant fait l'objet de sauvegardes ou d'un archivage. Les procédés de destruction sont conformes aux réglementations en vigueur au sein du ministère des Armées (Instruction Générale Interministérielle 1300 et Instruction Interministérielle 901). La restitution et la destruction des données seront constatées par un procès-verbal daté et signé par le Titulaire.

1.4.4.1 Sécurité des réseaux et de l'exploitation du réseau

Le Titulaire est garant du bon cloisonnement (physique ou logique) des environnements utilisés dans le cadre de la prestation.

Les postes d'administration utilisés pour les prestations sont dédiés aux systèmes et ne doivent faire l'objet d'aucune tentative de connexion à Internet ou à tout autre infrastructure bureautique du Client ou du Titulaire.

Le Titulaire s'assure de l'acquisition et de la bonne installation et mise à jour d'une solution de lutte contre les codes malveillants sur tous les postes de travail et serveurs dont il est responsable dans le cadre des prestations.

La désactivation, même temporaire, d'un antivirus sur un serveur utilisé dans le cadre de la prestation devra avoir été préalablement notifiée au Client.

L'installation, l'exploitation et l'administration des moyens mis en œuvre dans le cadre des prestations sont conformes aux bonnes pratiques et aux règles de sécurité et d'exploitation établies par le maître d'ouvrage. Toute exception fera l'objet d'un accord préalable écrit des équipes du Client.

Le Titulaire gère les mises à jour et l'application des correctifs de sécurité et des mises à jour antivirales, pour assurer le maintien en condition opérationnelle de l'ensemble de ses équipements pour les services fournis au Client.

1.4.4.2 Gestion des accès logiques aux données

Le Titulaire s'assure que son personnel devant accéder à des ressources informatiques ou réseau dans le cadre des prestations (qu'elles soient hébergées chez le Titulaire ou chez le maître d'ouvrage) dispose d'un compte nominatif et d'un mot de passe qui lui sont personnels et qui sont utilisés uniquement par cette personne tout au cours de la vie du compte.

Le Titulaire s'assure de la suppression de tous les comptes d'accès inutiles ou obsolètes. De même, les mots de passe par défaut d'usine devront être systématiquement modifiés, sauf demande notifiée du Client.

Dans le cadre de la cartographie des systèmes, le Titulaire doit fournir un inventaire justifié des comptes techniques nécessaires à la réalisation des prestations objet du présent marché.

Le Titulaire tient à jour la liste exhaustive des comptes d'accès aux systèmes ainsi que des rôles et privilèges qui y sont associés.

Le Titulaire effectue et formalise une revue périodique des comptes d'accès aux serveurs et autres ressources utilisées dans le cadre de la prestation par une revue « d'emploi » ou une revue de « besoin », a minima annuelle de son personnel et ceux de ses sous-traitants.

Le Titulaire s'assure que tous les comptes d'accès des intervenants dans le cadre des prestations sont déclarés selon le principe du moindre privilège.

Les moyens d'authentification mis en place par le Titulaire (sur ses serveurs, applications et postes de travail) incluent une protection contre les attaques en essai et erreur sur les secrets d'authentification.

Le Titulaire collecte et stocke à minima les informations suivantes :

- Connexion et déconnexion aux équipements et applications,
- Informations concernant les accès fructueux et infructueux (identifiant de l'utilisateur, date, heure) aux serveurs du Titulaire.

Les traces enregistrées par le Titulaire doivent être imputables à un individu, elles sont par ailleurs horodatées selon une référence horaire commune à l'ensemble des équipements d'un même réseau.

Le Titulaire respecte la politique d'exigence de complexité, de durée de vie, d'historisation des mots de passe sur l'ensemble des comptes d'accès utilisateurs aux postes de travail et applications sous la responsabilité du Titulaire et mis en œuvre dans le cadre des prestations.

Le Titulaire dispose des sources d'installation des logiciels utilisés dans le cadre des prestations, lorsque ces logiciels ne sont pas mis à disposition par le maître d'ouvrage.

1.4.4.3 Politique, organisation et gouvernance de la sécurité

Le Titulaire met en place, applique et fait appliquer à ses sous-traitants une politique de sécurité dans le cadre du présent marché. Cette politique traite notamment des thèmes suivants :

- Organisation de la sécurité des systèmes d'information ;
- Application de la Politique de Sécurité des systèmes d'information ;
- Évaluation de la sensibilité et protection des documents ;
- Gestion des ressources humaines ;
- Sécurité physique des locaux et des salles informatiques ;
- Architecture et exploitation des SI (réseaux, systèmes) ;
- Sécurité des postes de travail ;
- Sécurité des supports numériques ;
- Gestion des autorisations et contrôle d'accès logique aux ressources ;
- Maintenance des systèmes ;
- Gestion des incidents de cyber sécurité et des alertes ;
- Gestion de la continuité d'activité des systèmes d'information ;
- Localisation des données.

Le Titulaire définit une organisation de la sécurité au sein de son organisme afin de respecter l'ensemble des contraintes émises par le maître d'ouvrage.

Le Titulaire désigne parmi son personnel un correspondant sécurité des systèmes d'information pour toute la durée de la prestation. Ce correspondant est notamment :

- L'interlocuteur privilégié du Client pour toutes les questions relatives à la sécurité des systèmes d'information de la prestation, notamment dans le cadre d'investigations initiées par le maître d'ouvrage ou le Titulaire suite à des incidents de sécurité opérationnels ;
- Joignable du lundi au jeudi de 08h30 à 17h30 et le vendredi de 08h30 à 16h30 par téléphone ou messagerie. Tout remplacement de ce correspondant doit être notifié au Client. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son indisponibilité.

Si le Titulaire fait appel à des sous-traitants ou sociétés partenaires (fabricants, fournisseurs), il précise leur rôle dans le cadre des prestations d'administration, de MCO et MCS.

1.4.4.4 Sensibilisation et formation à la protection des données numériques et cyber sécurité

Le Titulaire sensibilise son personnel et celui de ses sous-traitants, intervenant dans le cadre des prestations, à la sécurité numérique et aux règles du ministère des Armées.

Le Titulaire doit s'assurer, pour chaque prestation, que les intervenants désignés pour réaliser la prestation ont les compétences requises en matière de cyber sécurité.

De ce fait, les intervenants doivent avoir suivi, en fonction de leur domaine d'emploi, une formation ou une sensibilisation minimale en cyber sécurité des systèmes industriels telle que le MOOC gratuit de l'ANSSI.

Le Titulaire doit être en mesure de justifier les compétences détenues ou formations suivies par les intervenants de sa responsabilité dans le domaine de la cyber sécurité et de l'administration des réseaux, systèmes informatiques et des systèmes industriels.

Le Titulaire met en place une charte de bonne conduite informatique et s'assure de la signature de celle-ci par tous les intervenants, sous-traitants compris.

1.4.4.5 Agrément, habilitations et compétences attendues

Le Titulaire est garant du bon niveau d'habilitation et de compétences du personnel intervenant sur les systèmes, y compris les sous-traitants auxquels il fait appel.

Le présent marché de maintenance et tierce maintenance applicative fait appel à 3 profils professionnels différents liés :

- À l'infrastructure informatique support, exploitée dans un environnement virtualisé, qui nécessite des compétences en informatique générale pour l'administration des systèmes, réseaux, environnements virtualisés Windows et Linux, parefeux applicatifs ou matériels, bases de données, ... ;
- Aux logiciels de supervision, contrôle/commande des métiers de l'infrastructure qui nécessitent des compétences en informatique industrielle ;

- Aux automates associés aux procédés industriels de l'infrastructure et les outils logiciels permettant d'assurer les opérations d'ingénierie/ maintenance/ développement qui nécessitent des compétences en automatisme et informatique industrielle appliquée aux gestions techniques et automates.

Le Titulaire possède pour lui-même ou son personnel les agréments correspondants aux installations et types de matériels existants sur lesquels il doit intervenir.

Au sein du ministère des Armées, le personnel assurant des tâches d'administration sur les systèmes d'information doit détenir un niveau d'habilitation n+1 par rapport à la sensibilité des données traitées. Dans le cadre du présent marché, les gestions techniques sont de niveau Diffusion Restreinte. Par conséquent, pour tout le personnel du Titulaire ou de ses sous-traitants qui réalise des activités d'administration informatique, une habilitation de niveau **SECRET** est requise. Elle sera présentée au SID-NO au plus tard la deuxième semaine de la période de mise en place.

Le Titulaire réalise les procédures d'habilitation pour son personnel et fournit au Client, le certificat de sécurité attestant du bon niveau d'habilitation détenu, **annuellement**.

1.4.4.6 Bonnes pratiques

Au même titre que les agents de l'administration, le Titulaire doit prendre connaissance et appliquer les règlements internes du ministère des Armées (PSSI (Politique de Sécurité du Système Informatique), directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, etc.).

Le Titulaire doit respecter les standards et les méthodologies préconisés au sein du ministère des Armées.

Les intervenants appliquent les bonnes pratiques en matière de cyber sécurité lors de leurs interventions sans que celles-ci ne soient systématiquement rappelées par le maître d'ouvrage, et notamment en :

- Ne tentant pas d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation ;
- Ne divulguant pas, à des personnes non autorisées, des informations sensibles liées au marché ;
- Connectant sur les réseaux internes du Client uniquement des équipements fournis par le maître d'ouvrage ou acheter pour le compte du Client. Cela comprend tout type de matériel y compris les supports de stockage amovibles (clés USB ou disques dur externes, etc.) ;
- Signalant au Client, des situations anormales qu'il aurait constatées, présentant des risques en termes de cyber sécurité ;
- S'assurant de l'innocuité de tous les supports préalablement à leur connexion sur un composant du système ou à leur remise au Client ;
- Ne tentant pas d'extraire des données physiques ou numériques contenues dans le système ;
- Conservant sur le site d'exécution de la prestation les plans, notices techniques et toute documentation ou information sensible soumis à une consultation sur place et donc non expressément autorisés à quitter le site.

La connexion sur le système de toutes tablettes, ordinateurs, téléphones portables, smartphones, ou tous supports informatiques personnels est formellement proscrite.

L'installation, l'exploitation et l'administration des moyens mis en œuvre dans le cadre des prestations sont conformes aux bonnes pratiques et aux règles de sécurité et d'exploitation établies par le ministère des Armées. Toute exception fait l'objet d'un accord préalable écrit des équipes du Client.

La connexion sur les systèmes industriels de tous moyens informatiques extérieurs non dédiés est proscrite. Les équipements dédiés seront maintenus sur le site. En cas de remplacement, le Titulaire s'assure de la réalisation des opérations d'effacement sécurisé de toutes les données du Client contenues dans les dispositifs de stockage ou de mémoire.

1.4.4.7 Gestion des incidents de sécurité et gestion de crise

Durant toute la durée du marché, le Titulaire s'assure de la disponibilité des données du Client (quel que soit leur support) hébergées dans ses locaux.

1.4.4.8 Incidents de sécurité affectant les données du client

Le Titulaire alerte le maître d'ouvrage de toute suspicion de comportement anormal sur ses installations utilisées dans le cadre des prestations, de tout vol ou perte d'informations sensibles appartenant au Client (équipements et documentations techniques en particulier).

Le Titulaire prévoit une procédure de traitement d'incident, contenant notamment, un chapitre sur la préservation des traces éphémères (volatiles) en cas de suspicion d'attaque cyber sécurité. Une trace volatile est une trace potentiellement utile pour l'analyse forensique d'une attaque informatique mais qui ne peut pas, par nature, être journalisée (contenu de la RAM, du swap, journal des transactions d'un système de fichier, diverses dates liées aux fichiers, clés de registres...). La procédure établit le mode opératoire pour limiter l'activité susceptible de détruire ces traces éphémères.

Le Titulaire s'assure de l'enregistrement et de la traçabilité des incidents de sécurité.

Le Titulaire contacte le correspondant sécurité désigné du Client pour signaler tout incident de sécurité des systèmes d'information susceptible d'affecter les données ou le système d'information du Client. De plus :

- si cet incident a lieu sur le système du Client, le Titulaire participera au traitement de l'incident ;
- si cet incident a lieu sur le système du Titulaire, le Titulaire autorisera le maître d'ouvrage ou un tiers désigné à participer au traitement de l'incident.

En cas d'incident affectant les données du Client, des réunions périodiques d'analyse post-incident devront être planifiées avec le maître d'ouvrage.

Le Titulaire capitalise les procédures de résolution des problèmes techniques récurrents dans une base de connaissance dédiée qu'il fournit au Client à la fin du marché dans le cadre de la réversibilité.

Tout échange électronique relatif au traitement d'un incident de sécurité fait l'objet au préalable d'un chiffrement à l'aide de l'outil ACID Crypto filer.

1.4.4.9 Gestion de crise

Le Titulaire doit posséder un processus formalisé et opérationnel de gestion de crise, apte à assurer le traitement d'événements remettant en cause de façon inacceptable pour le maître d'ouvrage, les engagements en termes de performances techniques, de sécurité et de continuité de services des systèmes du Client.

Ce plan précise au minimum :

- a. Les principes d'escalade (critères de déclenchement, synoptique d'escalade) ;
- b. La composition de la cellule de crise : fonctions et responsabilités des membres (Client et Titulaire) ;
- c. La liste nominative des membres et de leurs suppléants référencée dans un annuaire ;
- d. Les moyens dédiés à la gestion de crise (salle(s) de crise, procédures opérationnelles, moyens de communication).

1.4.5 Achat de matériels et de logiciels

Les produits objet du contrat doivent être, au jour de leur mise en production pour le maître d'ouvrage, dépourvus de toute faille, faiblesse ou défaut de conception portant atteinte à la sécurité des informations ou aux performances techniques du système considéré et être installé dans leur version la plus récente.

A la fin de la prestation ou en cas de non reconduction ou résiliation du contrat, le Titulaire doit restituer l'ensemble du matériel fourni par le maître d'ouvrage ou acheté pour le compte du Client.

1.4.6 Mise au rebut du matériel et maintenance externe

Dans le cadre d'une opération de maintenance dans un atelier externe au site d'exploitation ou d'une mise au rebut, le Titulaire a l'obligation de procéder à l'effacement sécurisé de toutes les données sensibles contenues avant l'envoi en maintenance ou la mise au rebut de tout dispositif à mémoire du Client. Dans ce cas, l'Entrepreneur fournit au Client un document attestant la réalisation de cette opération d'effacement.

Si les données sensibles ne peuvent pas être effacées en totalité :

- L'envoi en maintenance externe est interdit ;
- Les dispositifs de mémoire sont retirés des équipements et restitués au Client, avant l'évacuation par le Titulaire du composant en panne.

1.4.7 Objectifs de Résultats / de moyens

Le titulaire doit assurer, à l'égard du Service Infrastructure de la Défense (SID), une obligation de résultats avec la mise en œuvre de moyens minimaux. Les prestations en maintenance préventive ou corrective visent à garantir les résultats suivants :

- La disponibilité et la pérennité des installations.
- La conservation et l'optimisation des performances.
- Le respect de la réglementation environnementale et du code du travail.
- Les économies d'énergie et le meilleur coût pour la qualité du service.

Le titulaire fournit à son équipe l'outillage nécessaire, courant ou spécialisé. Les outils spéciaux fournis par les constructeurs ou installateurs font partie intégrante de l'équipement et doivent être maintenus par le titulaire. L'utilisation des outils ou matériels du ministère des Armées est strictement interdite.

Pour assurer ses résultats, le titulaire peut faire intervenir les fabricants de matériels, dont les prestations doivent être incluses dans le prix du marché. Il définit et met en œuvre les moyens en personnels et matériels nécessaires à l'exécution des prestations demandées.

Le titulaire s'engage à nommer un responsable unique du marché, qui sera l'interlocuteur principal de l'USID, ainsi qu'un suppléant. Le nom et la qualification exacte du responsable doivent être communiqués au client dès la notification du marché. Ce responsable est chargé de l'organisation, de l'encadrement des agents, du suivi des prestations, des sous-traitants éventuels et de la supervision des outils informatiques. Il doit :

- Être qualifié et autorisé à prendre toute décision immédiate et à signer les plans de prévention et les compte-rendus.
- Être habilité SECRET conformément à l'IGI 1300 du 9 août 2021.
- Être en mesure de répondre à toute demande de l'USID sur les domaines couverts par le marché.
- Assister aux réunions programmées et sur demande de l'USID.
- Être joignable à tout moment pendant les heures ouvrées.

Le titulaire est autorisé à faire intervenir des fournisseurs d'équipements particuliers (fabricants), sous réserve de détention des agréments nécessaires, pour remplir ses obligations de résultat. Les coûts associés à ces interventions ne sont pas à la charge de l'administration. Pour les interventions hors forfait, l'accord préalable du client est requis après présentation d'un devis détaillé.

Le titulaire réalise au minimum les gammes de maintenance décrites par le maître d'ouvrage, qui ne sont pas exhaustives. Ces gammes constituent l'ensemble des tâches de maintenance requises. L'entrepreneur est chargé de réaliser les opérations nécessaires au respect des performances attendues et doit respecter la réglementation et les règles de l'art.

Le titulaire doit mettre en place une politique de maintenance préventive pour garantir les résultats demandés et limiter les interventions de maintenance curative. Il doit adapter et améliorer les gammes de maintenance en fonction des exigences spécifiques des installations et de l'expérience acquise, se conformer aux notices techniques des constructeurs, et mettre à disposition du représentant du client les gammes de maintenance proposées pour validation.

Le maître d'ouvrage peut demander le remplacement du personnel d'intervention à tout moment, sans justification, dans un délai de 5 jours ouvrés. En cas de faute grave caractérisée, le maître d'ouvrage peut expulser tout agent sans délai.

1.4.8 Exigence de conseil et d'assistance

Le Titulaire reconnaît être tenu à une obligation générale de conseil et d'assistance, au titre de laquelle il doit fournir au Client l'ensemble des conseils, mises en garde et recommandations nécessaires notamment en termes de qualité de services, de sécurité, de mise à l'état de l'art.

Le Titulaire doit tout au long du marché assurer la fonction de conseil auprès du Client pour tout ce qui concerne :

- L'obsolescence des matériels ou équipements, suite à l'arrêt de production des équipements par les fabricants et la fin programmée de disponibilité de pièces détachées ;
- La vétusté importante d'un équipement ou logiciel qui pourrait remettre en cause les résultats exigés au titre du présent marché et qui a un taux de pannes important ;
- Le choix des éléments constituant les lots de rechanges ;
- L'optimisation des systèmes, objet du présent marché.

Cette exigence de conseil permet au Client de pouvoir programmer en investissement le remplacement des équipements ou matériels concernés par ces signalements. Ces remplacements seront réalisés dans le cadre de marchés de travaux indépendants du présent marché de maintenance.

2 Généralités

2.1 Hygiène et sécurité

2.1.1 Tenue et comportement du personnel

Il est précisé que le personnel du Titulaire ou de ses sous-traitants intervenant dans le cadre des prestations doit être vêtu de manière uniforme selon la nature des fonctions exercées et identifiable facilement (le nom de l'entreprise devra figurer de manière apparente sur les vêtements).

Le personnel doit avoir un comportement exempt de tous reproches.

En particulier, les règles suivantes doivent être respectées :

- Interdiction de fumer ou de vapoter dans les locaux et, d'une manière générale, en dehors des zones autorisées lorsqu'il en existe ; doit se conformer au règlement intérieur du client.
- Tenue vestimentaire uniforme en état correct de propreté, identifiant la société ; redondant
- Interdiction d'introduire et de consommer des boissons alcoolisées dans les locaux ou d'y pénétrer en état d'ivresse ; doit se conformer au règlement intérieur du client.
- Interdiction de tenir des réunions, en dehors de celles prévues par le présent marché, dans l'enceinte des sites ;
- Interdiction d'introduire des marchandises destinées à la vente ;
- Interdiction de solliciter ou de recevoir de quiconque un pourboire quelconque.

Le Titulaire doit disposer d'une charte d'éthique, reprenant ces règles, que l'ensemble de ses intervenants (y compris sous-traitants éventuels) doit signer.

2.1.2 Plan de prévention

L'établissement du plan de prévention fait préalablement l'objet d'une inspection commune (Client/ Titulaire) des lieux d'exécution des prestations (inspection de prévention préalable

IPP) à l'issue de laquelle une analyse des risques est réalisée. Elle inclut également une analyse des aspects et impacts environnementaux concernant le présent contrat.

Le plan de prévention doit prendre en compte les consignes de sécurité communiquées par le maître d'ouvrage et doit comporter au moins des dispositions dans les domaines suivants :

- La définition des zones ou locaux dangereux ;
- La définition des phases d'activités dangereuses et des moyens spécifiques correspondants ;
- L'adaptation des matériels, installations et dispositifs relatifs à l'opération ;
- Les instructions à donner aux salariés ;
- L'organisation des secours ;
- Les visites périodiques ;
- Les dispositions à prendre en matière de protection de l'environnement.

En outre, lorsque les prestations objet du présent marché sont exécutées de nuit ou dans un lieu isolé ou à un moment où l'activité de l'établissement concerné est interrompue, le Titulaire doit prendre toutes les mesures nécessaires pour qu'aucun salarié de son entreprise ne travaille isolément en un point où il ne peut être secouru à bref délai en cas d'accident.

Le Titulaire informe ses salariés et fait signer le plan de prévention à ses propres sous-traitants avant tout début de prestation.

Une fois établi, le plan de prévention est remis au Client pour approbation.

Le Titulaire a l'obligation d'informer ses salariés des dangers spécifiques auxquels ils sont exposés et les mesures prises pour les prévenir en application du plan de prévention. Ils doivent être informés des zones dangereuses ainsi que des moyens mis en œuvre pour les matérialiser (affiches, consignes). Ils doivent être informés des dispositifs de protection collective et individuelle et des accès de secours.

A ce titre, le Titulaire communique au Client le contenu précis des formations et informations communiquées à ses salariés en matière de prévention.

En outre, le Titulaire signale au Client, dans un délai de 24 heures, tout accident du travail dont est victime un de ses salariés dans l'exécution des prestations objet du présent Marché.

Le plan de prévention est mis à jour conjointement par le maître d'ouvrage et le Prestataire au fur et mesure de la prise en compte des installations et des évolutions des risques au cours de la réalisation du marché. Ces prises en compte et évolutions sont communiquées par le prestataire au fur et à mesure de leur survenance.

2.2 Gestion des déchets

Le Titulaire évacue et détruit selon la législation en vigueur les déchets issus de ses propres activités dans le cadre de l'exécution du marché.

En application des articles R. 541-43 et suivants du Code de l'environnement, de l'annexe III de la directive 2008/98/CE des déchets dangereux et de l'annexe IV du règlement (UE) 2019/1021 pour les déchets POP, le Titulaire informera l'administration (USID d'Evreux) dans le cas de déchets dangereux et/ou POP.

- Les articles cités, prévoient de nouvelles modalités de gestion des bordereaux de suivi des déchets dangereux et des déchets POP, qui s'appuient sur le télé-service « Trackdéchets », récemment développé par le Ministère de l'Ecologie.
- Ces nouvelles exigences sont applicables depuis le 01/01/2022. Elles impactent notamment les pratiques
- Fourniture de l'ensemble des FDS pour les produits utilisés par le titulaire. Avant utilisation, ces fiches seront validées par le maitre d'ouvrage.

Cette obligation s'applique à l'ensemble des sociétés intervenant dans le cadre du marché, jusqu'à l'opération finale de traitement des déchets. Le Titulaire du marché devra s'assurer de l'utilisation de ce télé-service par les sociétés auxquelles il recourt pour collecter et traiter ces déchets.

Aucun matériel ou produit ne doit être stocké ou abandonné dans les locaux et/ou bâtiments concernés par le présent marché sous peine de son évacuation sans préavis par le maitre d'ouvrage et aux frais du Titulaire.

2.3 Dispositions environnementales

Le titulaire devra prendre toutes les dispositions pour limiter l'impact de ses prestations et du fonctionnement des installations sur l'environnement. Dans la mesure du possible :

- Les fournitures, le matériel commandé devront être conditionnés dans un système d'emballage recyclable et limitant la quantité de déchets ;
- Dans la mesure du possible les fournitures et le consommable seront recyclables ;
- Les produits détenant un label environnemental seront privilégiés.

2.4 Matériaux et matériels

- Label et pièces de rechanges

Pour toutes les pièces remplacées lors d'une intervention de maintenance préventive, les provenances, les qualités, les caractéristiques, les types, dimensions, les procédés de fabrication, les modalités d'essais, de marquage, de contrôle et de réception des matériaux seront conformes aux normes françaises homologuées ou réglementaires en vigueur et seront à minima de performance équivalente.

- Exigences particulières sur du matériel à faible impact environnemental

Le titulaire mettra en place autant que faire se peut tout matériel ayant l'impact environnemental le plus faible possible aux conditions actuelles de l'application du présent marché.

2.5 Procédures organisationnelles

Le titulaire mettra en place des procédures organisationnelles permettant d'avoir une traçabilité et/ou de limiter les impacts sur l'environnement.

Le titulaire doit mettre en place des procédures organisationnelles permettant de limiter les discriminations et de promouvoir l'égalité homme/femme. Ces procédures sont à insérer à la charte d'éthique.

Le Titulaire et les sous-traitants éventuels, ainsi que l'ensemble des personnels respectifs, doivent se soumettre sans contrepartie, à toute directive émanant du service de sécurité de la personne publique et à toute obligation résultant des plans d'hygiène et de sécurité.

2.6 Norme et réglementation

Le titulaire doit respecter l'ensemble des directives européennes, des lois, décrets, arrêtés, règlements, circulaires et tous textes administratifs nationaux ou locaux applicables dans le cadre de l'exécution du présent marché pour autant qu'ils soient d'ordre public ou qu'ils suppléent au silence des autres pièces contractuelles.

Le Titulaire s'engage à appliquer toute la documentation technique relative à l'installation, la configuration, l'administration, l'exploitation, la maintenance et la résolution d'incidents de tous les équipements objet du présent marché, dans le respect des règles de sécurité exigées au sein du ministère des Armées.

[DIRMCS] Directive n°47/ARM/DGNUM/SDSNUM/DR du 04 juin 2020 portant sur le maintien en condition de sécurité (MCS) des systèmes d'information du ministère des Armées.

[IM2476] Instruction ministérielle n°2476/ARM/CC6/NP du 29 avril 2019 portant sur la conduite des projets SIC au sein du ministère des armées.

[GCSSI] Guide des clauses de sécurité des systèmes d'information type à intégrer dans les marchés publics version juillet 2019.

[PSSIA] Politique SSI des Armées (PSSIA). V3.20 n°D-16-007151 du 08 Juillet 2016.

[ANSSI] Guide ANSSI « exigences de cyber sécurité pour les prestataires d'intégration et de maintenance de systèmes industriels ».

[IGI1300] Protection du secret de la défense nationale

[IM900] Protection de la défense

[ISO15408] Norme ISO 15408 : critère d'évaluation de la sécurité des technologies de l'information.

[NF X 60 000] Maintenance industrielle – fonction maintenance

[NF EN 13306] Maintenance – terminologie de la maintenance

[ANSSI] Cyber sécurité des SI – mesures détaillées

[ANSSI] Recommandations de sécurité pour la mise en œuvre de dispositifs de vidéo protection N° 524/ANSSI/SDE ;

[ANSSI] Exigences cyber sécurité pour les prestations d'intégration

3 Prix et dispositions financières

3.1 Prix

3.1.1 Montage des prix

Les prix sont constitués de prix unitaires (commandés par des bons de commande) relatifs :

- À des prestations forfaitaires pour :
 - L'Astreinte,

- La Maintenance préventive par bâtiment,
- La Tierce maintenance applicative et maintien en condition de sécurité par site,
- À des prestations unitaires pour :
 - La Prise en compte des installations
 - La Restitution des installations
 - Les interventions de maintenance corrective
 - La maintenance améliorative

Il n'est pas prévu de prix spécifique pour les prestations suivantes qui sont inclus dans les prix figurant dans le bordereau de prix unitaires :

- Les frais de déplacements aller-retour par tout moyen
- Les moyens d'élévation pour l'accès au travail en hauteur si nécessaire ;
- Tous les moyens en outillage ;
- La participation à l'inspection de prévention préalable pour l'établissement du Plan de Prévention, (Arrêté du 19 mai 2020 relatif aux modalités d'application des règles relatives aux interventions d'entreprises extérieures et aux opérations de bâtiment et de génie civil dans un organisme du ministère de la défense) ;
- L'ensemble de la main d'œuvre (toutes qualifications comprises) nécessaire à la réalisation des prestations hors maintenance corrective et améliorative ;
- L'accompagnement des sous-traitants dans le cadre de leurs interventions ;
- La fourniture de la liste du personnel et de celui des sous-traitants ayant accès aux équipements ;
- La rédaction et fourniture de tous les compte-rendu d'intervention, rapports, plans de tests de non-régression, plans d'action et toutes les informations (tableaux de bord, indicateurs et tous livrables prévus au marché) ;
- La mise en place et la tenue à jour des registres d'interventions dans les locaux du Client ;
- La fourniture dans un format numérique grand public (pdf, dwg, xls, doc, ...) et papier de l'ensemble des documents et fichiers mis à jour ou générer dans le cadre de l'exécution du présent marché.
- L'ensemble des prestations réalisées par le responsable du marché dans le cadre de la gestion du marché
- L'ensemble de la main d'œuvre inhérente à l'exploitation de l'outil GTP,
- La mise en service / paramétrage d'un équipement mise en place dans le cadre du marché
- Conseils et études
- Location de matériels
- Participations aux réunions et aux CVPO
- Actions de formation et de sensibilisation

Les documents nécessitant des mises à jour et validations techniques (plans, DOE, monographie ...) sont fournis au Client dans un délai de **15 jours** ouvrés à l'issue de la mise en place des équipements concernés

Il est rappelé que le type de la main-d'œuvre (interne, sous-traitance, fabricant,) est un choix du titulaire et ne peut faire l'objet de prix différenciés pour l'administration.

3.1.1.1 Maintenance préventive

Dans le cadre de la maintenance préventive, le titulaire prendra en compte dans son offre :

- le déplacement et la main d'œuvre,
- toutes les opérations nécessitant le remplacement des consommables,
 - o Piles de 3ème source, autant de fois que nécessaire et au moins une fois pendant la période du marché ;
 - o Les batteries d'accumulateurs, autant de fois que nécessaire et au moins une fois pendant la période du marché ;
 - o Voyant, bouton de commande, etc...

Et des pièces ou matériels dont le coût unitaire est inférieur ou égal à 500 € HT (deux cent cinquante euros hors taxe) prix fournisseur avec facture pro-forma faisant foi sans majoration d'aucune sorte,

- les diagnostics de panne,
- l'outillage individuel et collectif,
- les démontages et remontages connexes,
- toutes sujétions inhérente à la continuité de service.

3.1.1.2 Astreinte

Les prix relatifs à l'astreinte comprennent :

- L'astreinte 365 j/365 j et 24h/24h (y compris centre d'appel)
- Le coût du déplacement et de la main d'œuvre pour assurer le diagnostic et le dépannage
- Le coût des pièces et des matériels nécessaires à la remise en service de la fonction dont le coût unitaire est inférieur ou égal à 500 € HT

3.1.1.3 Maintenance corrective et améliorative

Dans le cadre de la maintenance corrective et améliorative, l'intervention se fera après acceptation par l'administration du devis composé :

- Des prestations décrites au BPU
- Du coût de la main d'œuvre détaillé en quantité d'heure et prix horaire d'un technicien prévu au BPU majoré des plus-values E3 et E4 si nécessaire pour la main d'œuvre non prise en compte dans les prestations incluses au BPU
- Le coût unitaire des pièces décrites au BPU
- Le cout unitaire des pièces non décrites au BPU et excédant 500 € HT (facture pro-forma du fournisseur faisant foi) majoré du coefficient K prévu au BPU.

Nota : les plus-values sur la main d'œuvre pour les prestations urgentes ne sont pas utilisables avec les prestations incluses au BPU (lignes I du BPU). Ces dernières doivent intégrer cette éventuelle contrainte.

Exemple : nombre d'heures x (coût horaire d'un technicien + plus value pour intervention urgente) + (coût unitaire de la pièce hors BPU x coefficient (K) appliqué aux pièces hors BPU) + cout de la pièce au BPU

Le coût des pièces inférieur ou égal à 500€ HT (et ne faisant pas parti du bordereau de prix) ainsi que la location de matériel, les consommables et tout ce qui est nécessaire à l'intervention sera compris dans le prix de la main d'œuvre du bordereau.

L'administration se réserve le droit de demander au titulaire une décomposition détaillée qu'elle jugera utile.

Le délai de remise du devis sera de 10 jours ouvrés après réception de la demande de devis par le représentant de l'acheteur. Le bon de commande vaut accord et notification au titulaire des prix proposés pour les pièces dans le devis.

Prix des pièces du correctif :

Les prestations suivantes font l'objet d'un prix unitaire dans le BPU :

- Pièces spécifiques
- Les éléments suivants de MCS et de tierce maintenance applicative. Attention, ces prix sont complets et comprennent la main d'œuvre et toutes sujétions :

Remplacement d'un bloc alimentation sur un switch

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer le bloc alimentation, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'une carte contrôleur sur un switch réseau

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer la carte contrôleur, assurer le recyclage du matériel hors service, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'un disque dur sur un poste de supervision client

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer le disque dur, réintégrer le poste dans le réseau, réaliser la restauration des données à partir des sauvegardes, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'un bloc alimentation sur un poste de supervision client

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer le bloc alimentation, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'un écran sur poste informatique

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer l'écran, assurer le recyclage du matériel hors service, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'une carte contrôleur sur un poste de supervision client

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer un contrôleur, assurer le recyclage du

matériel hors service, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'un bloc ventilation sur un poste de supervision client

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer le ventilateur, assurer le recyclage du matériel hors service, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'une batterie d'alimentation sur un PC portable

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer la batterie, assurer le recyclage du matériel hors service, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'un ventilateur sur un PC portable

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer la batterie, assurer le recyclage du matériel hors service, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'un disque dur sur un serveur

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer le disque dur, réintégrer le poste dans le réseau, réaliser la restauration des données à partir des sauvegardes, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'un bloc alimentation sur un serveur

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer le bloc alimentation, assurer le recyclage du matériel hors service réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'une carte contrôleur sur un serveur

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer la carte contrôleur, assurer le recyclage du matériel hors service, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'un bloc ventilation sur un serveur

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer le ventilateur, assurer le recyclage du matériel hors service, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'une carte contrôleur sur un SAN

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer la carte contrôleur, assurer le recyclage du matériel hors service, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'un disque dur sur un SAN

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer le disque dur, restauration des données à partir des sauvegardes, s'assurer de la bonne reconstruction du RAID, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'un bloc alimentation sur un SAN

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer le bloc alimentation, assurer le recyclage du matériel HS, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'un bloc alimentation sur un NAS

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer le bloc alimentation, assurer le recyclage du matériel hors service, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'une carte contrôleur sur un NAS

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer la carte contrôleur, assurer le recyclage du matériel hors service, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'un disque dur sur un NAS

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer le disque dur, restauration des données à partir des sauvegardes, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

Remplacement d'un module de communication sur un automate programmable, UTL ou centrale de détection intrusion

La prestation comprend toute la main d'œuvre qualifiée, frais de déplacement et tous les matériels nécessaires pour remplacer la pile, assurer le recyclage du matériel hors service, assurer les restaurations de paramètres nécessaires, réaliser les tests de bon fonctionnement, rédiger et fournir le compte-rendu final.

4 Qualité

Le maître d'ouvrage peut faire procéder, à tout moment, par ses services techniques ou par un organisme d'audit extérieur, à toute vérification et à tout contrôle des prestations, sans pour autant déléguer la responsabilité du Titulaire qui demeure pleine et entière.

Dans ces conditions, le Titulaire doit se conformer aux instructions des vérificateurs chargés de contrôler l'exécution du marché et leur transmettre tout document nécessaire à la réalisation de leur mission de vérification.

5 Définitions des prestations

5.1 Gestion du marché

5.1.1 Période de mise en place

La période de mise en place est de deux mois à compter de la date de notification de l'accord-cadre.

Elle porte sur la structuration et la mise en œuvre de l'organisation générale et, notamment :

- La réalisation de l'état des lieux
- La mise en place des outils informatiques (ceux que le Prestataire estime nécessaires à l'exécution des prestations demandées dans le cadre du marché, sous réserve de déclaration préalable du fait de la sensibilité des sites) ;

5.1.2 La réalisation du planning de maintenance préventive et des trames des rapports de maintenance préventives demandés ;

- mettre en place les procédures d'astreinte ;
- finaliser ses gammes de maintenance ;
- fournir les chartes d'éthique et de bonne conduite informatique signées par son personnel et celui de ses sous-traitants ;
- fournir toute autre information jugée utile par le Titulaire.

Durant le premier mois de la période de mise en place, le Titulaire initie, en priorité, les demandes de contrôle primaire (CPR) pour tous les intervenants (personnels du Titulaire et de ses sous-traitants) et les demandes d'habilitation.

Le Titulaire propose les éléments formels (outils, modélisation d'indicateurs, modèle de rapports, procédures, numéro d'appel, GMAO, etc.) au Client qui les valide.

Durant le deuxième mois de la période de mise en place, le Titulaire produit les éléments retenus et les teste.

Deux mois après la date de notification du marché, l'ensemble est opérationnel et le système de pénalités entre en vigueur.

5.1.3 État des lieux

L'état des lieux est prévu pour une durée de deux mois à compter de la date de notification de l'accord-cadre. Il est attendu du Titulaire qu'il réalise un état des lieux qualitatif et quantitatif des installations comprises au titre de ce marché.

Durant cette période, l'Entrepreneur effectue un inventaire initial (état des lieux) qui comprend :

- le recensement physique de l'ensemble des installations et équipements compris dans le marché,

- une expertise technique de l'état général de chaque installation ou équipement, qui permet d'affecter une classe d'état de référence (exemple : bon état, état standard, nécessitant des réparations, hors service).

A l'issue de l'inventaire initial, le Titulaire dispose d'un délai d'un mois pour remettre au Client un rapport initial et signaler par écrit d'éventuelles réserves constituant une sujétion soit pour l'obtention des objectifs de résultats qui lui sont assignés, soit sur la quantité des matériels. Au-delà de ce délai, il ne pourra se prévaloir d'une quelconque anomalie pour élever une réclamation ou ne pas satisfaire à ses obligations.

L'inventaire aura le même format que la monographie et le niveau de détail sera également le même. Les équipements annexes ne sont pas à répertorier lors de l'inventaire. Ils peuvent faire l'objet d'un autre inventaire. Le titulaire ajoutera une colonne « observation à la prise en compte des installations » et ajoutera les nouveaux équipements en fin de tableau.

Le maître d'ouvrage reste l'unique arbitre de l'acceptation des réserves émises par le Titulaire.

Les inventaires et descriptifs succincts, joints aux pièces du marché sont communiqués à titre indicatif.

5.1.4 Réversibilité des installations et transférabilité

La **réversibilité** désigne les opérations de retour de responsabilité, par lesquelles le maître d'ouvrage ou un tiers désigné reprend les prestations qu'il avait confiées au Titulaire dont le contrat arrive à terme. Les modalités organisationnelles et techniques de la réversibilité figurent dans un plan de réversibilité.

La période de réversibilité ou de transférabilité est la période couvrant le retour ou le transfert de responsabilité précédemment définis. Le plan de réversibilité ou de transférabilité est le document qui décrit la durée et les conditions de mise en œuvre de la réversibilité ou de la transférabilité.

Compte tenu de la spécificité et de la technicité des prestations à réaliser dans le cadre du marché, **la période de réversibilité aura une durée maximale de deux mois.**

La mise en œuvre de la réversibilité devra être effective au plus tard un mois avant date de fin d'exécution du dernier bon de commande dans le cadre normal de la fin de marché et se poursuivra au plus un mois après la reprise des prestations par le titulaire entrant.

Le partage des responsabilités et des obligations durant cette phase de réversibilité sera le suivant :

- **Jusqu'à l'expiration du marché**, les responsabilités et les obligations (résultats et moyens) du marché subsistent pour le titulaire sortant, le titulaire entrant n'ayant qu'une obligation de moyens consistant uniquement à la mise en place de ses propres équipes ;
- **À l'expiration du marché**, les responsabilités et les obligations du titulaire sortant (résultats et moyens) sont transférées au titulaire entrant, le titulaire sortant n'ayant plus qu'une obligation de moyens portant uniquement sur la mise en place du personnel nécessaire et suffisant pour poursuivre le transfert de la connaissance des installations et infrastructures.

La réversibilité devra permettre de manière non limitative :

- La mise en place d'une méthodologie de transfert des programmes de maintenance spécifiques aux installations,
- La mise en œuvre d'une assistance technique et administrative sur toute la période de réversibilité,
- L'établissement des inventaires complets et détaillés :
 - o De l'ensemble des installations et équipements compris dans le marché (le format sera celui de l'inventaire d'état des lieux auquel on ajoutera une nouvelle colonne « observation à la restitution des installations »),
 - o De la documentation technique et fonctionnelle,
 - o Des identifiants login/mots de passe des comptes techniques de tous les équipements et logiciels,
 - o Des pièces de rechange et plateforme de pré-production,
 - o Des gammes de maintenance à jour et mises en œuvre dans le cadre de la maintenance préventive,
 - o Des dates de renouvellement des licences.
- Les accès au comptes permettant la gestion des licences,
- La fourniture des clés de licences des logiciels,
- La fourniture de la nomenclature à jour des équipements et logiciels,
- La connaissance de l'historique des incidents importants résolus ou en cours, y compris base de connaissance,
- La mise à disposition des fichiers sources (DAU, fiches de procédure, fichiers de paramétrage, scripts, plans, ...) suivant un ou plusieurs formats documentés et exploitables en dehors du service fourni ou des moyens propres au Titulaire,
- Les informations sur les actions conduites dans le cadre d'un plan de remplacement d'un équipement ou d'un logiciel (gestion de l'obsolescence) afin de permettre leur reprise par le maître d'ouvrage ou le titulaire entrant,
- La restitution des équipements composant les plateformes de tests propres au Client,
- Toutes les informations jugées utiles au suivi des actions en cours.

Durant la période de réversibilité le Titulaire aura l'obligation de mettre en œuvre tous les moyens supplémentaires nécessaires afin d'assurer cette tâche dans les délais impartis tout en continuant à assumer les prestations dont il a la charge jusqu'à l'échéance du contrat.

5.1.5 Le maître d'ouvrage GTP – Outil de connaissance technique du SID

Le titulaire, en complément de la GMAO dont il est libre de disposer, doit utiliser le logiciel « GTP » du SID afin d'assurer le suivi des installations concernées par le présent marché.

Il sera responsable de la bonne tenue du suivi des installations concernées.

- A ce titre, le titulaire sera responsable à minima, de renseigner les OI après chaque intervention, dans un délai maximal de cinq jours ouvrables après la fin de chaque intervention, notamment :
 - Présenter les actions menées dans l'onglet ECHANGE,
 - Mettre à jour le statut de la tâche et les dates réelles,
 - Joindre les comptes rendus d'intervention de dépannage et de maintenance,
 - Enregistrer le devis correctif.

En aucun cas le suivi des installations sur « l'outil GTP » ne saurait se substituer au carnet d'entretien que doit renseigner le titulaire lors de chaque intervention sur les installations, ainsi qu'à la fourniture des rapports de contrôles (bons de travaux SSI en annexe) et des registres dont il a la charge.

Les demandes d'intervention seront transmises au titulaire via « l'outil GTP ».

En cas de non-respect de cette obligation, le titulaire peut s'exposer aux pénalités prévues au CCAP du présent marché pour non remise de documents.

5.1.6 Réunions et livrables

Le responsable du marché désigné par le Titulaire doit être obligatoirement présent aux réunions de synthèse organisées et planifiées par le maître d'ouvrage, en vue de la vérification de l'état d'avancement des diverses prestations.

La fréquence des réunions est annuelle. Celles-ci sont tenues dans les locaux de l'USID d'Evreux. Au fur et à mesure de l'avancement du marché, la fréquence peut être adaptée en fonction des nécessités du service et à l'initiative du Client.

Toutes les pièces justificatives sont alors présentées, et notamment les rapports d'activité.

Le Titulaire est chargé de la production des comptes rendus. Ceux-ci doivent être représentatifs de l'ensemble des remarques émises lors de la réunion et soumis à l'approbation du Client dans un délai maximum de 15 jours ouvrés à compter de la tenue de la réunion. En cas de désaccord sur le contenu du compte rendu le Titulaire doit le reprendre dans un délai maximum de 5 jours ouvrés après avis du Client prononcé au plus tard 15 jours ouvrés après réception dudit compte rendu.

À l'issue de ce délai, l'application des pénalités est automatique selon les modalités définies au CCAP.

Un support de réunions est réalisé par le Titulaire au format informatique et remis au Client au moins 5 jours ouvrés avant la réunion. Il comprendra les éléments suivants :

- La date de réunion ;
- La liste des participants ;
- Un rapport d'inventaire initial (lors de la 1^{ière} réunion)
- Un planning de maintenance préventive (lors de la 1^{ière} réunion)
- Un tableau récapitulatif des maintenances préventives non réalisées afin qu'une décision soit prise en réunion par le maître d'ouvrage sur leurs reports éventuels ou non ;
- Un tableau de suivi des opérations de maintenance corrective en cours en précisant la date de remise en service prévisible ;
- Un tableau de suivi des anomalies de fonctionnement non résolues et rencontrées lors des opérations de maintenance préventives ;
- Un tableau des pièces achetées forfaitairement ou non ;
- Un tableau récapitulatif de suivi et de comptabilisation des pénalités sur l'année qui sera validé par le maître d'ouvrage ;
- Un tableau de suivi des devis émis et réalisés, les travaux commandés, en attente et facturés, ainsi que le montant des pièces remplacées comprises dans le forfait (inférieur au seuil en € H.T : prix unitaire de la pièce) et hors forfait ;

- Un tableau de suivi de la veille sécurité (cyber sécurité)
- Un tableau de suivi des obsolescences
- Un plan de réversibilité pour la fin de contrat (dernière réunion)
- Les faits marquants.

Un rapport annuel des activités par période réalisé par le Titulaire est remis au Client, au plus tard le dernier jour du premier mois qui suit la fin de l'exercice.

Ce document comprend pour l'exercice écoulé, les points suivants :

- Les éléments demandés dans le support de réunion et mis à jour suite à la réunion ;
- Un bilan de l'ensemble des lignes de prix commandées ;
- ***un bilan économique faisant ressortir en toute transparence, l'ensemble des coûts forfaitaires ou non (fournitures, licences, main d'œuvre, frais variables, frais fixes, marge) ;***
- éventuellement, la nature de tout ce qui n'est pas conforme à la réglementation.

Dans le cadre de sa mission, le prestataire assure au fil de l'eau, la gestion de la documentation technique qui comprend la mise à jour des plans, schémas et documents concernés après toute modification des installations réalisée par le prestataire au format définie par l'USID :

- dgn de microstation pour les plans
- pdf pour les autres documents

Un plan ou document non mis à jour dans un délai de 15 jours ouvrés est considéré comme un document non remis.

Les documents techniques et la documentation maintenance relatifs aux installations maintenues, en possession de la personne publique, sont tenus à la disposition du titulaire dans les locaux de l'administration après la notification du présent marché.

Durant la durée du marché, toute la documentation technique des installations, les plans et gammes, programmes et planning de maintenance préventive, les comptes rendus d'intervention (joindre les bons de travaux SSI en annexe du CCTP) ainsi que toutes les bases de données saisies par le titulaire restent la propriété de la personne publique.

5.1.7 Planning

Pendant la période de mise en place et à chaque fin d'année civile, le titulaire proposera un planning pour les maintenances préventives et la tierce maintenance applicative au client pour validation.

5.1.8 Prestations dues au titre du marché

- Vérifier la conformité des schémas et synoptiques des installations ;
- Vérifier et modifier les fiches de consignes mis à disposition des exploitants si nécessaires ;
- Vérifier les documents d'exploitation (utilisation, administration, maintenance) et les mettre à jour au besoin ;
- Changer les libellés des événements et alarmes remontés sur les supervisions (suppression, ajout, modification) pour correspondre à l'existant sur le terrain ;

- Réorganiser l'ergonomie de l'affichage sur les écrans (vignettes, mosaïque, etc.) selon le besoin exprimé par le Représentant de la personne publique ;
- Intégrer, modifier ou supprimer dans les bases de données des logiciels CADIVS, les consignes ou fiches consignes à appliquer par les exploitants ;
- Assurer les arrêts et redémarrages des installations dans le cadre des maintenances annuelles des sites ou des contrôles et vérifications périodiques obligatoires (CVPO) ;
- Réaliser les extractions des variables (états, alarmes, mesures, ...) issues des logiciels et matériels en vue d'analyse (extractions/requêtes dans les bases de données de tout type) à la demande de l'autorité contractante ;
- Supprimer ou requalifier la priorité de certaines alarmes ou événements à la demande de l'autorité contractante (modification des priorités) ;
- Mettre à jour les plans modifiés suite au rajout ou à la suppression d'équipements dus à l'initiative du Titulaire ou du Représentant de la personne publique. Ces mises à jour sont réalisées et fournies sur plans papiers (modification de l'existant) et en version informatique (.DWG et .DGN) ;
- Gérer et mettre à jour les plans d'adressage IP, monographies, inventaires des matériels et logiciels, synoptiques des réseaux informatiques ;
- Mettre à jour les synoptiques et vues des installations dans les logiciels CADIVS ;
- Gérer les configurations appliquées (versions des logiciels et firmwares installées dans les équipements, schémas de flux réseau, identification des points de connexion sur les EAR dans les baies techniques). Le Titulaire transmet un état des configurations appliquées une fois par an ou à la demande du Représentant de la personne publique, sous un format numérique grand public et par voie numérique sécurisée (ACID ou Prim'X Zed !) ;
- Marquer les équipements (sensibilité des données, nommage réseau normalisé, identification) ;
- Gérer les licences, contrats de maintenance, redevances, renouvellements clé de licence des logiciels listés dans les présentes Clauses Techniques Particulières (annexe xxx) en :
 - o s'assurant de leur validité ;
 - o réalisant les actes administratifs nécessaires à l'acquisition ou au renouvellement des licences et contrat de maintenance (acquittement des redevances) ;
 - o réalisant toutes les opérations techniques liées à la récupération et à l'installation des nouvelles clés de licences sur les composants du système ;
 - o fournissant au Client, **annuellement**, un état inventaire des validités des licences et contrats de maintenance ;
 - o fournissant au Client les identifiants d'accès aux comptes client des différents éditeurs pour permettre le suivi des licences.
- Mettre à jour et livrer au Client la documentation fonctionnelle d'installation, d'administration et d'utilisation impactée par les maintenances et modifications effectuées ;
- Assurer une assistance aux utilisateurs sur l'emploi des logiciels CADIVS déployés ;
- Dispenser une formation complémentaire, 1 fois par an (au besoin), aux exploitants des logiciels CADIVS ;

- Participer à des réunions (groupes de travail) dans le cadre de futures opérations d'infrastructure impactant les CADIVS ;
- Assurer l'administration fonctionnelle des CADIVS pour garantir leur disponibilité, leur optimisation. Cette prestation correspondra aux interventions permettant d'optimiser le fonctionnement des programmes applicatifs, des logiciels et des systèmes d'exploitation constituant le parc informatique objet du présent accord-cadre.
- Remplir les bons de travaux SSI conformément à l'annexe jointe au CCTP et à remettre à chaque compte rendu d'intervention en maintenance préventive et corrective.

A ce titre, le Titulaire doit détenir toutes les compétences nécessaires pour réaliser toutes les opérations dites d'administration technique et fonctionnelle, pour l'ensemble des installations, notamment les activités suivantes sur les composants actifs (liste non exhaustive) :

- administration des réseaux informatiques (routage, intégration réseau, ...), des services communs (AD, sauvegarde, authentification, NTP, stockage, ...),
- administration des bases de données SQL ou propriétaires,
- administration des systèmes informatiques (systèmes d'exploitation clients et serveurs, processus, fichiers, utilisateurs, paramètres système, ...),
- administration des logiciels et applications CADIVS correspondant au parc objet du présent accord-cadre,
- administration des logiciels et applications d'informatique générale (bureautique, navigateurs Web, ...),
- administration des supports de desserte des réseaux informatiques (brassage, ...),
- administration de la sécurité (serveurs antivirus, parefeux, gestion de certificats),
- administration des automates programmables industriels (UTL, centrales détection intrusion,).

Le Titulaire doit être en mesure de présenter les certifications et attestations justifiant les compétences détenues.

5.2 Monographies / GMAO

Le Titulaire doit l'accès au Client à un système d'informations (GMAO) permettant le suivi des faits techniques et interventions sur les installations objet du présent marché. Les informations contenues ne doivent en aucun cas présenter un caractère sensible.

Dans le cadre du présent marché, aucune interconnexion entre la GMAO et les systèmes du Client n'est autorisée.

Lors de la prise en charge / compte des installations, le titulaire se basera sur le fichier de la monographie de la consultation auquel il ajoutera une colonne « commentaires ». Les équipements manquants seront ajoutés avec une précision en commentaire. Les équipements inexistants ne seront pas supprimés de la monographie mais feront l'objet d'un commentaire.

5.3 Criticité/délais d'intervention

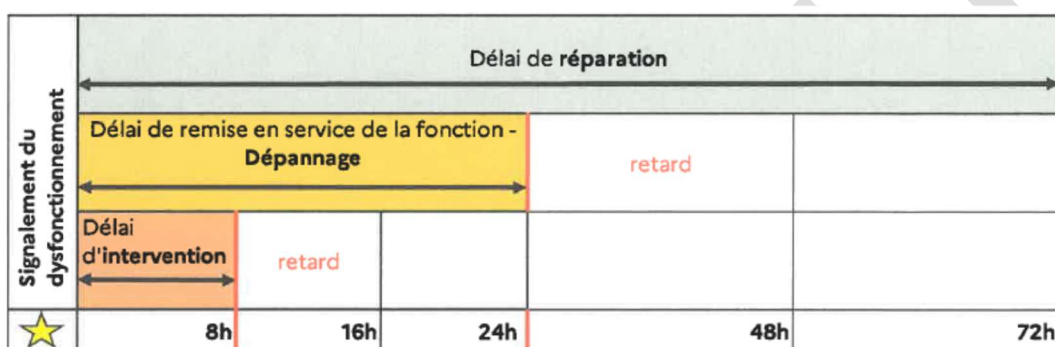
Le titulaire doit garantir la continuité du service pour répondre aux besoins de fonctionnement des installations. Les intervenants doivent connaître parfaitement les installations à dépanner et recevoir une information adaptée sur chaque site.

À cet effet, le titulaire devra fournir le numéro téléphonique et une adresse de messagerie de son service de dépannage. Ce service devra être accessible 365j/365j et 24h/24h. Le délai de dépannage débute à compter de l'heure d'envoi de la demande d'intervention par message électronique ou téléphonique au titulaire.

Suite à la sollicitation par le représentant local de l'USID ou par l'astreinte technique de l'USID au service de dépannage, le titulaire devra se conformer aux délais présentés ci-dessous. Les délais sont en heures calendaires. Le représentant local de l'USID sera le seul à juger du seuil d'urgence du dysfonctionnement et du déclenchement de l'astreinte.

Après chaque intervention, le titulaire prendra contact avec le représentant local de l'USID. Ils vérifieront ensemble le bon fonctionnement des installations remises en service.

Le délai NORMAL d'intervention, de dépannage et de réparation doit respecter le schéma suivant :



Le délai d'intervention est le délai imparti au titulaire incluant le déplacement pour le diagnostic, soit un maximum de huit heures (8 h).

Le délai de remise en service de la fonction ou de dépannage, soit un maximum de vingt-quatre heures (24 h). Dans ce délai est inclus l'intervention.

Le délai de réparation est le délai imparti au titulaire pour la remise en service définitive des installations. Ce délai est fixé au maximum à soixante-douze heures (72h00) après le signalement du dysfonctionnement par le représentant local de l'USID.

Le délai URGENT d'intervention, de dépannage et de réparation doit respecter le schéma suivant :



Le délai de remise en service de la fonction/dépannage inclut le déplacement pour le diagnostic et l'intervention sous huit heures (8 h).

Ce délai d'intervention et dépannage restreint sous 8h00 impliquera l'application d'une plus-value inscrite au BPU.

Le délai de réparation est le délai imparti au titulaire pour la remise en service définitive des installations. Ce délai est fixé au maximum à soixante-douze heures (72h00) après le signalement du dysfonctionnement par le représentant local de l'USID

5.4 Maintenance préventive

Le Titulaire réalise forfaitairement sur toutes les installations une **maintenance préventive courante**. Les gammes de maintenance devront contenir les opérations suivantes qui ne constituent pas une liste exhaustive et devront être complétées par le Titulaire au besoin pour couvrir les attendus du marché.

Toutes les opérations pourront être effectuées avec de l'outillage courant disponible dans le commerce. Si des moyens spéciaux sont nécessaires ils seront fournis, par le Titulaire.

5.4.1 Détecteurs, capteurs

- Contrôler le bon fonctionnement et l'état général ;
- Régler la sensibilité des appareils et leur positionnement ;
- Procéder aux essais de masquage et de détection ;
- Contrôler les témoins lumineux de détection ;
- Vérifier les autoprotections ;
- Nettoyer selon des prescriptions du fabricant.

5.4.2 Lecteurs de badges, claviers à code

- Contrôler le bon fonctionnement et l'état général ;
- Tester la fonction d'enrôlement et d'édition de badges ;
- Mettre à jour les firmwares ;
- Nettoyer selon des prescriptions du fabricant.

5.4.3 Sirènes, dispositifs d'alarmes sonores

- Contrôler le bon fonctionnement par essai et l'état général ;
- Contrôler l'audibilité dans les zones concernées ;

5.4.4 Nettoyer selon des prescriptions du fabricant.

5.4.5 Vidéosurveillance

- Vérifier le bon fonctionnement des caméras et la visualisation des scènes sur les écrans ;
- Vérifier les embases de raccordement, la connectique, les supports de transportant des flux vidéo ;
- Vérifier l'état et le bon fonctionnement des convertisseurs de signal analogique/numérique ;

- Vérifier le bon fonctionnement des systèmes d'éclairage associés ;
- Vérifier l'état et le bon fonctionnement des joysticks ;
- Vérifier et resserrer les supports de fixation ;
- Vérifier et régler l'azimut, les angles de vues et champs des caméras (si nécessaire) ;
- Vérifier et régler la netteté et la mise au point (si nécessaire) ;
- Vérifier et régler les détecteurs vidéo,
- Mettre à jour les firmwares ;
- Nettoyer tous les équipements constituant l'installation (caméras, objectifs, caissons, coffrets de caméras, ...).

5.4.6 Interphonie et visiophonie

- Vérifier l'état et le bon fonctionnement par appel (netteté, qualité sonore, etc.) ;
- Nettoyer selon des prescriptions du fabricant.

5.4.7 Tourniquets, tripodes

- Contrôler le bon fonctionnement général ;
- Contrôler les sécurités ;
- Vérifier les organes et armoire de commande (connectique, câblage, cartes, fusibles) ;
- Vérifier les détecteurs actifs ;
- Vérifier la filerie, les boîtes à bornes ;
- Vérifier le débrayage manuel ;
- Vérifier les organes de fin de course ;
- Contrôler de la motorisation ;
- Vérifier les fixations ;
- Vérifier les articulations ;
- Vérifier la signalisation et le pupitre de commande.

Le prestataire devra le réglage, le serrage, le nettoyage et la lubrification de tous les composants le nécessitant.

5.4.8 Maintenance préventive des composants actifs (switchs, serveurs, postes de travail, enregistreurs, pupitres, parefeux, diodes, imprimantes, UTL, centrales intrusion)

Pour cette catégorie de composants, le Titulaire réalise forfaitairement sur toutes les installations une **maintenance préventive courante**. Les gammes de maintenance devront contenir les opérations suivantes qui ne constituent pas une liste exhaustive et devront être complétées par le Titulaire au besoin pour couvrir les attendus du marché.

- Vérifier par contrôle visuel, s'assurer de l'intégrité physique des matériels, câbles et cordons de raccordement informatique et électrique (embases de raccordement, languettes de verrouillage, ...), réaliser les remplacements nécessaires ;

- Vérifier « l'état de santé » des serveurs physiques et virtuels, ainsi que des postes de travail (utilisation mémoire, utilisation processeur, taux d'occupation espace disque, latences, temps de réaction, ...) ;
- Optimiser le fonctionnement des programmes, des applicatifs et des systèmes d'exploitation (purge des fichiers, inspection, réorganisation des fichiers, ...) ;
- Vérifier le bon fonctionnement des logiciels, des matériels et des machines virtuelles (bilan des événements, purge des fichiers, ...) ;
- Contrôler la bonne exécution des échanges protocolaires et réaliser les essais de transmission de données entre les composants (analyse des réseaux de communication) ;
- Réaliser les essais de remontées d'alarmes vers les postes de supervision ;
- Contrôler et changer les cartes électroniques défectueuses ;
- Sauvegarder les programmes, configurations et paramètres des API, des logiciels métier, éléments actifs de réseau, des parefeux, ... ;
- Vérifier la synchronisation des équipements et machines virtuelles avec les horloges de référence si existantes ;
- Mettre à jour les équipements non connectés aux horloges de référence et s'assurer du bon passage heure hiver/été des serveurs NTP source et des équipements ;
- Contrôler la bonne exécution des tâches planifiées notamment les sauvegardes, jobs de journalisation, purges, scripts, ... ;
- Contrôler la qualité des sauvegardes par restauration sur les plateformes de pré-production, si existantes ;
- Vérifier la bonne historisation des données ;
- Vérifier le bon paramétrage et fonctionnement des redondances applicatives ou physiques (basculement de serveurs, reprises de services, ...) ;
- Vérifier l'état des bases de données métier et réaliser les purges nécessaires, en respectant une rétention des données de 12 mois minimum, si la tâche n'est pas automatisée ;
- Relever, analyser et corriger les alarmes et défauts sur les matériels ;
- Relever, analyser les journaux d'événements des équipements et traiter les anomalies constatées ;
- Tester les imprimantes et accessoires ;
- Vérifier l'état des écrans, la qualité image, la luminosité, le contraste ;
- Vérifier et remplacer, en fonction des préconisations des constructeurs, les moyens permettant la conservation, hors tension, des paramètres dans les équipements (piles, batteries, accumulateurs électriques) ;
- Contrôler les tensions et protections ;
- Contrôler les fixations, serrage des bornes ;
- Apporter toutes les actions correctrices aux anomalies, écarts, dysfonctionnements constatés durant la maintenance pour garantir le bon fonctionnement de l'ensemble ;
- Vérifier et assurer le nettoyage, dépoussiérage interne et externe des équipements, périphériques associés (claviers, souris, écrans, ...) et des ventilateurs.

5.5 Maintenance corrective

La **maintenance corrective** regroupe les opérations non programmées, exécutées pour assurer la remise en état d'un composant, d'un sous-système, d'une fonction ou d'une installation en fonctionnement après une défaillance constatée par l'Administration ou par le Titulaire lors de l'exécution de la maintenance préventive.

Elle inclut par ailleurs pour les composants actifs :

- Toutes les actions permettant de corriger les logiciels CADIVS en vue de remédier à des dysfonctionnements ou des anomalies de traitement en vue d'une remise en état définitive ;
- Toutes les opérations de sauvegarde de données stockées sur les systèmes ou de reconstitution des fichiers, des données, ou encore de programmes altérés ou perdus suite à une défaillance des systèmes.

La maintenance corrective comprend les prestations suivantes :

- La prise en compte et le traitement de l'incident ;
- L'astreinte ;
- L'établissement du diagnostic (détection, localisation, analyse) ;
- L'information de l'Administration concernant la durée probable d'immobilisation ;
- Le dépannage et la main d'œuvre pour la mise en place de toute pièce, et/ou la réparation du système et/ou de l'équipement, les réglages et la remise en service

La prestation de maintenance corrective inclut également, pour les composants actifs, les prestations :

- De sauvegarde/restauration des données stockées sur les systèmes objet du présent accord-cadre ;
- De reconstitution des fichiers, des données, ou encore des programmes altérés ou perdus suite à une défaillance des systèmes.

5.6 Astreintes/centre de service

Le Titulaire doit mettre en place un centre de service doté des procédures, moyens et qualification des personnels nécessaires pour gérer les incidents remontés par le personnel du site (USID ou sécurité) ou le personnel de maintenance. Ce centre de service assure également un service d'astreinte 365 jours par an, 24h/24, accessible par un numéro de téléphone unique, non surtaxé, pour l'ensemble des installations et équipements compris dans ce marché. Ce dispositif est essentiel pour la continuité de service et la gestion des cas de force majeure.

Le centre de service fournit au Client :

- Un numéro d'appel unique non surtaxé et disponible 365 jours par an, 24h/24.
- Un moyen de traçabilité des appels (appellant, date/heure d'appel, numéro d'incident, qualification du fait technique et toutes les informations techniques définissant la défaillance et sa résolution).
- Un suivi statistique des interventions (fréquence, type d'intervention et durée d'indisponibilité par installation).

- Le statut de la demande d'intervention (prise en compte, en cours, suspendue ou clôturée).

Le centre de service est responsable de déclencher les interventions de l'astreinte en cas de besoin. Le personnel du centre de service et de l'astreinte sera soumis aux mêmes exigences et niveau d'habilitation que ceux demandés aux agents de maintenance dédiés au site. Ils devront avoir la connaissance des installations et des procédures d'intervention.

Le dimensionnement et l'organisation des moyens humains seront prévus pour répondre à la fiabilité (criticité, performance, disponibilité, gestion des incidents, etc.) et réactivité demandées au marché.

Le centre de service est accessible 24/7 via un numéro de téléphone et une adresse de messagerie fonctionnelle. Le décroché se fera en moins de 3 minutes. Ce centre de service doit être opérationnel dès la notification de l'accord-cadre pour vérifier son bon fonctionnement et enregistrer les délais d'intervention/réparation.

Tous les incidents remontés devront être saisis dans un outil de gestion des tickets d'incident mis en place par le Titulaire. L'administration doit pouvoir accéder au suivi des incidents ouverts dans le cadre de la garantie et de la maintenance. Ces rapports doivent être produits sous un format exploitable depuis une suite bureautique standard.

5.7 Maintenance applicative – tierce maintenance

Le Titulaire est responsable de la récupération, de la fourniture et de l'installation des mises à jour des versions de logiciels et de firmwares des matériels en production et en stock, conformément aux recommandations des éditeurs ou constructeurs. Les mises à jour sont d'abord installées et testées dans un environnement de pré-production (maquette), s'il existe, avant d'être déployées en production.

Cette mise à jour sera effectuée à une périodicité trimestrielle.

Les maquettes sont prioritairement installées dans les locaux de l'administration. Cependant, à titre exceptionnel, elles peuvent être hébergées chez le titulaire du présent marché.

À la rédaction du présent marché, seule une installation est dotée d'une maquette. Cependant, dans le cadre de travaux sur les différents sites, de nouvelles maquettes pourront être confiées à la maintenance dans le cadre du présent marché.

Pendant la durée du marché, le Titulaire assure les mises à jour des logiciels tiers pour garantir la pérennité des installations et leur compatibilité avec les composants et protocoles en production (bases de données, interfaces web, etc.). Aucune mise à jour ne doit entraîner une régression de la sécurité ou des performances des installations.

Le Représentant de la personne publique peut décider de ne pas appliquer une mise à jour si son impact fonctionnel ou technique est jugé trop important. Dans ce cas, le Titulaire continue d'assurer ses obligations de maintenance pour la version en service. Pour chaque mise à jour logicielle, le Titulaire présente les nouvelles fonctionnalités aux utilisateurs sorties depuis la dernière mise à jour, si celles-ci ont un impact sur la supervision/exploitation.

Tous les trimestres, le titulaire à 7 jours calendaires pour réaliser la mise à jour.

5.8 Maintien en condition de sécurité

Le maintien en condition de sécurité vise à garantir un niveau de sécurité des installations face aux vulnérabilités identifiées affectant les composants actifs. Il comprend cinq volets : veille cyber-sécurité, volet technique, lutte contre les codes malveillants, veille et traitement de l'obsolescence, et contrôle de conformité.

5.8.1 Veille cyber sécurité

Il s'agit de toutes les opérations qui consistent à assurer une veille de sécurité permanente des logiciels et matériels, les plus exposés. Cette veille doit permettre d'identifier les nouvelles vulnérabilités et de déclencher les mesures correctrices et/ou mesures transitoires idoines.

La veille cyber sécurité doit permettre de classer les vulnérabilités selon 5 niveaux de criticité, en fonction de la note environnementale CVSS :

- nul,
- très faible,
- faible,
- fort,
- critique.

Cette veille fait l'objet d'un rapport de veille qui précise à minima :

- les matériels ou logiciels concernés,
- l'intitulé et référence des alertes et avis de sécurité,
- les sources de veille (adresse Web des sites éditeur),
- les notes CVSS de base et temporel lorsque celles-ci sont connues,
- les correctifs à appliquer ou mesures transitoires.

Dans le cadre du présent accord-cadre, le Titulaire assure la veille de vulnérabilité sur les composants suivants :

- les systèmes d'exploitation des serveurs et postes informatiques,
- les firmwares des serveurs et postes informatiques,
- les firmwares des API (UTL de contrôle d'accès, centrales de détection intrusion),
- les logiciels CADIVS (contrôle d'accès, détection intrusion, vidéosurveillance).

5.8.2 Volet technique MCS

Le Titulaire est responsable de toutes les opérations techniques qui consistent à réaliser le traitement des vulnérabilités, par l'intégration des correctifs de sécurité ou les mises à jour de version des logiciels ou firmwares recommandés par les éditeurs ou constructeurs. Le volet technique MCS fait partie intégrante des actions de maintenance préventive et adaptative.

Pour répondre au besoin, le Titulaire met en place l'organisation permettant :

- De réaliser l'acquisition des correctifs de sécurité ou mises à jour, en s'assurant de l'intégrité et de l'authenticité de la source de publication ;
- De vérifier que les correctifs de sécurité ou mises à jour n'impliquent pas de régression vis-à-vis des performances du système, de la sécurité du système ou des

fonctionnalités offertes aux utilisateurs. En cas d'incompatibilité avérée entre un correctif de sécurité et le système existant, avertir immédiatement par courrier électronique le maître d'ouvrage de l'incompatibilité rencontrée et des risques engendrés. Dans ce cas, proposer une solution palliative pour rendre les dispositifs en production compatibles avec le correctif de sécurité ou mises à jour, ou pour limiter les risques dans les délais définis en accord avec le maître d'ouvrage. Les tests de non régressions sont réalisés sur les plateformes de pré-production, si existantes ;

- Lorsqu'aucun correctif de sécurité ou mise à jour n'est disponible, de suivre les recommandations de l'éditeur ou du ministère des Armées dans le cadre d'une mesure transitoire. Si la mesure transitoire nécessite la désactivation d'une fonctionnalité indispensable, rendant ainsi impossible le fonctionnement nominal du système ou la correction partielle de la vulnérabilité, le Titulaire s'engage à proposer des mesures organisationnelles permettant d'éviter l'exploitation de la vulnérabilité et la poursuite de l'activité ;
- D'intégrer les correctifs de sécurité ou les mises à jour conformément à la politique de sécurité du système en production ;
- De respecter les exigences liées à, la vérification de l'innocuité du support d'intégration, l'utilisation des équipements dédiés aux systèmes (clés USB, PC de maintenance ou d'ingénierie), la traçabilité des actions ;
- De s'engager, à traiter les vulnérabilités selon leur niveau de criticité comme suit :

Tout traitement, qu'il soit transitoire ou pérenne doit faire l'objet d'une validation et d'une planification, en accord avec le Représentant de la personne publique.

L'homologation de la maquette du site de Vernon est en cours d'audit par le CASSIS, il s'agit d'un SII de classe 3.

5.8.3 Lutte contre les codes malveillants

Il s'agit d'assurer toutes les opérations techniques permettant :

- L'acquisition des fichiers de signatures des solutions antivirus déployées sur le système auprès des éditeurs officiels ;
- La réalisation des tests de non-régression sur les plateformes de tests si existantes et la fourniture des rapports de tests au Client ;
- L'installation, le déploiement des fichiers de signatures sur l'environnement de production (serveurs, postes de travail) ;
- La réalisation des tests de bon fonctionnement après déploiement.

5.8.4 Veille et traitement de l'obsolescence

Le Titulaire est responsable des opérations pour assurer le suivi de la maintenabilité des composants constituant les systèmes, permettant à l'Administration d'anticiper leur remplacement ou mise à niveau. La veille et le traitement de l'obsolescence complètent les mises à jour régulières de firmwares ou de logiciels et répondent aux impératifs d'anticipation de remplacement de matériels ou de mise à niveau de logiciels.

Pour répondre au besoin de veille de l'obsolescence, le Titulaire met en place l'organisation permettant :

- D'assurer une veille permanente des alertes d'obsolescences ou de fin de support émises par les éditeurs pour les équipements et les logiciels installés ;
- De fournir au Représentant de la personne publique une alerte d'obsolescence ou de fin de support dans les 30 jours suivant la date de réception ou de publication d'un avis d'obsolescence ou de fin de support d'un sous-traitant, d'un fournisseur ou d'un éditeur ;
- D'analyser l'obsolescence des matériels et logiciels constituant les systèmes. Les résultats de cette analyse fournis annuellement au Client, sous forme de rapport de suivi de l'obsolescence, présentent les composants selon :
 - les criticités suivantes :
 - obsolescent ou fin de support,
 - composant à pérennité faible (< 3 ans),
 - composant à pérennité moyenne (3-5 ans),
 - composant à pérennité forte (> 5 ans).
 - les catégories de traitement suivantes :
 - classe 1 : aucune action prévue en raison d'une consommation faible, d'un support soutien ou d'un stock existant suffisant pour assurer le service jusqu'à la fin de vie du système ;
 - classe 2 : remplacement du composant obsolète par un équivalent réel ayant pour seul impact sur le dossier industriel du système la spécification d'une nouvelle source d'approvisionnement, d'une nouvelle version du programme ;
 - classe 3 : remplacement du composant obsolète ou en fin de support par un nouveau composant correspondant à une évolution technique. Le Titulaire réalise l'étude préliminaire avec établissement d'une proposition technique, financière et calendaire pour l'étude complémentaire et les différentes répercussions sur le MCO ;
 - classe 4 : approvisionnement, sous réserve d'une commande par le Représentant de la personne publique, du composant avant son arrêt de production. Le Titulaire définit la quantité de composants à approvisionner en accord avec le Représentant de la personne publique.

Pour la catégorie de traitement de classe 3, le Titulaire s'engage à établir le rapport d'étude sous trois mois à compter de la notification de l'alerte obsolescence au Représentant de la personne publique.

La catégorisation en classe 3 est proposée, si le constructeur ou l'éditeur recommande impérativement le remplacement du matériel ou logiciel obsolète par un nouvel équipement ou la mise à niveau du logiciel en fin de support vers une nouvelle version majeure pour garantir la pérennité du système.

Les opérations de traitement de l'obsolescence, sont programmées dans le cadre de la maintenance adaptative des installations.

5.8.5 Contrôle de conformité et audit de sécurité

Pour s'assurer du maintien du bon niveau de sécurité des installations, l'Administration peut effectuer ou faire effectuer soit :

- des contrôles de conformité ;
- des audits de sécurité qui incluent un volet technique et/ou organisationnel du système, ainsi que des installations et locaux du Titulaire ayant trait au présent marché, par un prestataire d'audit de sécurité des systèmes d'informations (PASSI).

Le Titulaire s'engage, pour un audit, à fournir au PASSI, tous les documents et informations techniques et organisationnels nécessaires à la conduite de l'audit et met à disposition le personnel en fonction des profils requis pour les interviews.

Si les conclusions du contrôle de conformité ou du rapport d'audit mettent en évidence des manquements résultant de la non-exécution d'opérations prévues au présent contrat dans le cadre, du MCO, de la conduite des installations ou du MCS, le Titulaire s'engage à présenter un plan d'action dans les deux mois suivants les résultats et à corriger les écarts en s'assurant de la non-régression du système, sans frais supplémentaire pour l'Administration.

Le contrôle de conformité des installations par rapport aux exigences de cyber sécurité porte, a minima, sur :

- la gestion de l'authentification (politique de mots de passe, y compris l'authentification hors AD),
- la gestion des comptes d'accès nominatifs et techniques,
- la politique des gestions de mots de passe et identifiants techniques (gestion conteneur de mots de passe),
- l'application des mises à jour recommandées par les éditeurs ou constructeur pour la version du composant en exploitation,
- la gestion des mises à jour antivirales,
- l'application des stratégies de sécurité (GPO ou locales),
- les entrées dans les journaux de logs et d'évènements et leur exploitation,
- la désactivation des composants inutiles,
- le blocage physique ou logique des ports inutilisés,
- le durcissement des configurations des postes de travail, d'administration, d'ingénierie, de maintenance,
- la bonne application des exigences de cloisonnement logique,
- la bonne adéquation de la cartographie, monographie avec les installations déployées,
- le respect des PES1,
- la mise à jour de la documentation d'exploitation, d'administration et de sécurité.

Lorsque le Titulaire est mandaté par le Représentant de la personne publique pour réaliser un contrôle de conformité, le Titulaire rédige et fournit au Représentant de la personne publique, le rapport de conformité de sécurité et le plan d'action sous format numérique chiffré (ACID ou Prim'x ZED !). Ces derniers portent la mention Diffusion Restreinte.

¹ Procédures d'Exploitation de Sécurité

Le Titulaire régularise les écarts constatés par l'application du plan d'action dans un délai convenu en commun accord entre les deux parties.

PROJET