MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Secrétariat général

Cahier des clauses techniques particulières (CCTP)

Accord-cadre relatif à l'acquisition, l'installation et le maintien en condition opérationnelle d'une solution logicielle d'intelligence artificielle de vidéo-protection

Lot 1 : Déploiement dans la région Île-de-France

Lot 2 : Déploiement dans les régions Provence Alpes Côte d'Azur, Rhône-Alpes, Outre-mer et Corse

Lot 3 : Déploiement dans une autre région de la France métropolitaine

Lot 4 : Déploiement sur des transports en commun et infrastructures associées (gares, stations)

SOMMAIRE

INTRODUCTION

CADRE JURIDIQUE DU MARCHE

Le législateur a autorisé, à titre expérimental jusqu'au 31 mars 2025, à la seule fin d'assurer la sécurité de manifestations sportives, récréatives ou culturelles, qui, par leur ampleur ou leurs circonstances sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes (notamment dans le cadre des prochains jeux Olympiques de 2024), de recourir à des traitements algorithmiques portant sur les images captées dans les lieux accueillant ces manifestations, à leurs abords ainsi que dans les moyens de transport et sur les voies les desservant, au moyen de systèmes de vidéo-protection et de caméras installées sur des aéronefs autorisés par le code de la sécurité intérieure.

Ces traitements ont pour unique objet de détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler ces risques et de les signaler, aux forces de sécurité intérieure, aux services de police municipale, aux services de la sécurité civile en charge des secours ou aux services internes de sécurité de la RATP ou de la SNCF, qui pourront confirmer l'alerte et prendre les mesures adaptées.

Les évènements prédéterminés sont en lien avec les finalités autorisées par la loi, à savoir la détection de risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes. La liste de ces évènements est fixée par le décret en cours de publication relatif aux modalités de mise en œuvre des traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, pris en application de l'article 10 de la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions. Ces évènements sont les suivants :

Label	Description
• Sens de circulation	• Non-respect du sens de circulation commun par une personne ou un véhicule
• Franchissement	• Franchissement ou présence d'une personne ou d'un véhicule dans une zone interdite ou sensible
• Mouvement de Foule	• Mouvement de foule
• Densité	• Densité trop importante de personnes
• Objets abandonnés	• Présence d'objets abandonnés
• Armes	• Présence ou utilisation d'une arme, parmi celles mentionnées à l'article R. 311-2 du code de la sécurité intérieure
• Personne au sol	• Présence d'une personne au sol à la suite d'une chute
• Feu	• Départ de feu

Ces traitements n'utiliseront aucun système d'identification biométrique, ne traiteront aucune donnée biométrique et ne mettront en œuvre aucune technique de reconnaissance faciale. Ils ne pourront procéder à aucun rapprochement, aucune interconnexion ni aucune mise en relation automatisée avec d'autres traitements de données à caractère personnel.

Ils procéderont exclusivement à un signalement d'attention, en temps réel et strictement limité aux événements prédéterminés qu'ils ont été programmés pour détecter. Ils ne produiront aucun autre résultat et ne pourront fonder, par eux-mêmes, aucune décision individuelle ou acte de poursuite.

Ils demeureront en permanence sous le contrôle des personnes chargées de leur mise en œuvre.

La loi impose que cette expérimentation se déroule sous le contrôle étroit de l'Etat qui seul peut acquérir une ou plusieurs solutions algorithmiques et qui devra attester de leur conformité aux exigences techniques et éthiques imposées par le VI de l'article 10 de la loi. Ces exigences sont cumulatives et impératives

- Des garanties devront être apportées afin que les données d'apprentissage, de validation et de test soient pertinentes, adéquates et représentatives ;
- Le traitement des données d'apprentissage, de validation et de test devra être loyal, reposer sur des critères objectifs et permettre d'identifier et prévenir l'occurrence de biais et d'erreurs ;
- Ces données font l'objet de mesures de sécurisation appropriées ;
- Le traitement devra comporter un enregistrement automatique des signalements des évènements prédéterminés détectés permettant d'assurer la traçabilité de son fonctionnement ;
- Le traitement devra permettre des mesures de contrôle humain et un système de gestion des risques permettant de prévenir et de corriger la survenue de biais éventuels ou de mauvaise utilisation ;
- Le traitement pourra être arrêté à tout instant ;
- Le traitement devra être accompagné d'une documentation technique complète.
- Le traitement fait l'objet d'une phase de test conduite dans des conditions analogues à celles de son emploi autorisé par le décret mentionné au V de l'article 10 de la loi, attestée par un rapport de validation.

En troisième lieu, l'État devra être en mesure de mettre cette (ces) solution (s) à disposition des services utilisateurs concernés par la sécurisation des manifestations accueillant les épreuves des prochains jeux olympiques et paralympiques, mais également d'autres manifestations sportives, récréatives et culturelles exposées à un risque d'actes de terrorisme ou d'atteintes à la sécurité des personnes et pouvant se tenir pendant la durée de l'expérimentation, soit jusqu'au 31 mars 2025.

Ces services sont limitativement énumérés dans la loi, à savoir ses propres services (Police nationale, Gendarmerie nationale, Sécurité civile) des services de police municipale, les services d'incendie et de secours, les services de sécurité interne de la RATP ou de la SNCF.
Cette mise à disposition sera autorisée par arrêté du préfet du lieu de la manifestation culturelle, sportive ou récréative, pour une durée et un périmètre limités. Une fois commandée par l'État, la solution devra donc pouvoir être installée et désinstallée au fur à mesure des besoins et au plus près de la fin de la manifestation. En cas de manifestations récurrentes en un même lieu, mais espacées dans le temps, les traitements pourront être désactivés plutôt que désinstallés.

Les traitements y compris pendant leur phase de conception sont régis par les dispositions applicables du règlement (UE) n° 2016/679 relatif à relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD) et de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le fournisseur du traitement devra présenter des garanties de continuité, d'assistance et de contrôle humains en vue notamment de procéder à la correction d'erreurs ou de biais éventuels lors de la mise en œuvre et prévenir leur itération.

Enfin, les opérations de captation, de transmission ou d'enregistrement des images sur lesquelles porteront les traitements algorithmiques sont soumises aux règles applicables en matière de vidéoprotection fixées par :
- les articles L. 251-1 à L. 251-8 et L. 223-1 à L. 223-9 du code de la sécurité intérieure ;
- le titre V du livre II de la partie réglementaire du code de la sécurité intérieure ;
- l'arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance.

DEFINITIONS – LEXIQUE

Libellé	Définition
Faux positif	Détection à tort
Faux négatif	Absence de détection, à tort
Vrai positif	Détection à raison
Vrai négatif	Absence de détection, à raison
Incident critique	Comportement anormal apparaissant et rendant inopérant tout ou partie des signalements dans le VMS
Incident majeur	Comportement anormal apparaissant ayant un impact sur la qualité des détections. Cette notion inclut les incidents de nature technique mais aussi les biais dans le fonctionnement de l'algorithme
Incident mineur	Comportement anormal apparaissant ayant un impact sur lesystème et n'étant ni majeur, ni critique. Cette notion inclut les incidents de nature technique mais aussi les erreurs dont les faux négatifs ou positifs lorsqu'ils sont d'une incidence mineure
Classification	La classification réside dans l'identification de la catégorie à

	laquelle un nouvel élément appartient, sur la base d'un data set d'entraînement de données contenant des observations (ou instances) dont la catégorie est connue
Service prescripteur	Entité de l'État qui passe un bon de commande avec un titulaire
Soumissionnaire	Entreprise (fournisseur) qui soumet une réponse à l'appel d'offre
Service utilisateur ou Exploitant	Entité qui met en œuvre la solution
Titulaire	Entreprise attributaire d'un lot du marché
Déploiement	Installation, mise en service, utilisation, puis désactivation ou démontage sur un site pour une période donnée.
Heures ouvrées	8H à 19h les jours ouvrés
Jours ouvrés	Lundi à vendredi hors jours fériés
Heures nocturnes	Période de 19h à 8h
Jours fériés	1er janvier, lundi de Pâques (1er avril en 2024), 1er mai, 8 mai, jeudi de l'ascension (9 mai 2024), lundi de Pentecôte (20 mai 2024), 14 juillet, 15 août, 1er novembre, 11 novembre, 25 décembre

Dans la suite du document, les exigences sont classées de la manière suivante :

F0	Exigence impérative impliquant l'irrégularité de l'offre en cas de non conformité . Le soumissionnaire décrit comment il couvre l'exigence
F1	Exigence importante n'impliquant pas l'irrégularité de l'offre : le soumissionnaire signale s'il est ou non capable de satisfaire l'exigence dans sa réponse, et décrit comment il couvre l'exigence.

DESCRIPTION DES PRESTATIONS POUR L'ENSEMBLE DES LOTS

Toutes les prestations sont à engagement de résultat.

PLANNING DE DEPLOIEMENT

Les déploiements prévus sont les suivants :

- Déploiement dès le mois de novembre 2023 pour encadrer les manifestations liées à la période de Noël (notamment marchés de Noël, transports associés à la période de Noël) ;

- Puis déploiements pour d'autres manifestations récréatives, sportives ou culturelles, notamment mais pas exclusivement liés aux Jeux Olympiques.

Un déploiement consiste en une phase d'installation, une phase de mise en service, une phase de fonctionnement à blanc, une phase opérationnelle et une phase de démontage ou de désactivation.
Le titulaire est présent sur site sur les phases d'installation, de mise en service et de démontage. Il assure un support téléphonique dans les autres phases.
Afin de planifier les déploiements qu'il sera possible d'organiser, il est nécessaire de connaître les durées nécessaires pour réaliser l'installation et la mise en service en fonction :

- Du nombre de flux à surveiller dans le déploiement ;
- Du nombre de sites à déployer en simultané.

Cas pratique :

- *déploiement pour 50 flux ;*
- *Période d'installation et de test en conditions analogues : dans la semaine qui précède le début du festival ;*
- *Festival ayant lieu du 30 mars au 14 avril 2024 ;*
- *A quelle date au plus tard doit être notifié le bon de commande ? Sur quelle période est livré et installé le matériel ? Sur quelles périodes sont réalisées les formations et mises en service ?*
- *Quelle modification des dates en fonction du volume de flux commandé ?*
- *Combien de commandes similaires sur la même période mais sur un autre site géographique peuvent elles être assumées avec le dispositif proposé ?*

Le titulaire, lorsqu'une demande de faisabilité lui est transmise, précise au demandeur les limites éventuelles lors de l'installation et la mise en service de sa solution, en fonction des contraintes de délais nécessaires et de déploiement simultané. Lorsqu'il juge les limites annoncées incompatibles avec les besoins du service utilisateur, le service prescripteur peut recourir au titulaire de rang suivant.

PRESTATION 1 : FOURNITURE D'UNE SOLUTION ALGORITHMIQUE

Exigences techniques de la solution algorithmique

Évènements couverts

Voici les 8 types d'évènements à détecter :

Label	Description
Sens de circulation	Non-respect du sens de circulation commun par une personne ou un véhicule
Franchissement	Franchissement ou présence d'une personne ou d'un véhicule dans une zone interdite ou sensible
Mouvement de Foule	Mouvement de foule
Densité	Densité trop importante de personnes
Objets abandonnés	Présence d'objets abandonnés
Armes	Présence ou utilisation d'armes, parmi celles mentionnées à l'article R. 311-2 du code de la sécurité intérieure
Personne au sol	Présence d'une personne au sol à la suite d'une chute
Feu	Départ de feu

Exigences	Clauses et conditions	Fi
Exigence n°1	La détection générique de ces évènements peut être adaptée aux besoins métier,des utilisateurs, par exemple en configurant le signalement d'attention sur certaines situations relevant d'un même évènement. Des paramètres métiers pourront être ajustés dans la solution.	F1
Exigence n°2	Le titulaire doit proposer des solutions pour les évènements obligatoires de chaque lot, selon le tableau ci dessous	F0
Exigence n° 3	Le titulaire peut proposer une solution fonctionnelle pour les évènements optionnels selon le tableau ci-dessous	F1

Évènements	**Lot 1**	**Lot 2**	**Lot 3**	**Lot 4**
Sens de circulation	obligatoire	obligatoire	obligatoire	optionnel
Franchissement	obligatoire	obligatoire	obligatoire	obligatoire
Mouvement de Foule	obligatoire	obligatoire	obligatoire	obligatoire

Densité	obligatoire	obligatoire	obligatoire	obligatoire
Objets abandonnés	optionnel	optionnel	optionnel	obligatoire
Armes	optionnel	optionnel	optionnel	optionnel
Personne au sol	optionnel	optionnel	optionnel	optionnel
Feu	optionnel	optionnel	optionnel	optionnel

Périmètre technique de la solution

Exigences	Clauses et conditions	Fi
Exigence n°4	Compatibilité des solutions avec les caméras installées . Lors d'une demande de faisabilité, le service utilisateur fournit la liste des modèles de caméra qui seront utilisés pour générer les flux vidéo et les configurations techniques associées. Le titulaire signale s'il existe des incompatibilités de fonctionnement avec sa solution et précise l'impact de ces incompatibilités (impossibilité d'utiliser le flux correspondant ou utilisation dans un mode dégradé, ou nécessité de réaliser un paramétrage spécifique sur la caméra pour pouvoir fonctionner).	F0
Exigence n°5	La solution doit pouvoir fonctionner avec des flux RTSP MULTICAST, UNICAST UDP, UNICAST TCP.	F0
Exigence n°6	La solution devra fonctionner avec des caméras ayant une résolution 4CIF au minimum	F0
Exigence n°7	La solution doit accepter des flux vidéo d'entrée entre 12 et 25 images par seconde (avant d'éventuels retraitements au sein de la solution nécessaire à son bon fonctionnement)	F0
Exigence n°8	Pour les caméras déjà en place, la solution doit s'adapter à la perspective de l'image soit par paramétrage (via des IHM utilisée par l'exploitant), soit par auto-configuration (les caméras sont placées à des hauteurs, avec des angles, dans des conditions de luminosités, dans des conditions climatiques différent(e)s). La solution doit pouvoir fonctionner dans le cas où aucune modification des paramètres de la caméra ne sont possibles.	F0
Exigence n°9	La solution doit également pouvoir fonctionner avec une qualité suffisante avec des caméras installées spécialement pour le déploiement, dont l'emplacement sera ajusté lors de la mise en service ou la phase de fonctionnement à blanc. .	F0
Exigence n°10	La solution doit fonctionner avec une qualité suffisante avec des caméras pouvant changer d'angle de vue et de facteur de zoom.	F1

Dimensionnement du matériel

Exigences	Clauses et conditions	Fi
Exigence n°11	Le fournisseur décrit le matériel proposé pour traiter les N flux (N=8, 20, 50, 100 ou 200) sur les événements qu'il sait détecter.	F0

Exigence n°12	La sobriété numérique de la solution sera évaluée.	F1

Composants logiciels

Exigences	Clauses et conditions	Fi
Exigence n°13	La solution est livrée avec tous les composants (SDK, logiciels tiers) libres de redevance d'utilisation nécessaires ainsi que le système d'exploitation sur lequel la solution est installée.	F0

Diagnostic, analyse et reporting

Exigences	Clauses et conditions	Fi
Exigence n°14	Le traitement doit comporter un enregistrement automatique des signalements des évènements prédéterminés détectés permettant d'assurer la traçabilité de son fonctionnement : il devra être possible d'extraire les logs et les résultats des algorithmes dans une forme qui sera à définir conjointement répondant à un standard du marché (xls, csv, parquet, json, feather, …). Ces extractions doivent permettre de réaliser des analyses statistiques dans le temps	F0
Exigence n°15	Il est possible d'accéder aux données de la solution via des moyens documentés de façon automatisée et industrielle sans action humaine.	F1
Exigence n°16	Le titulaire doit proposer une méthode d'export sur un support amovible USB à la fin d'un déploiement de l'ensemble des logs et résultats d'algorithmes (vrais et faux positifs).	F0
Exigence n°17	Dans le cas où la solution sauvegarde les images, ces dernières doivent être conservées conformément à la réglementation applicable à la vidéoprotection	F0

Gestions des droits

Exigences	Clauses et conditions	Fi
Exigence n°18	Le dispositif doit permettre au moins trois niveaux de rôles : **- Niveau 3 :** Administrateur technique: il a la main sur l'infrastructure, le poste informatique et la maîtrise totale de la solution. Ce rôle est assumé par l'éditeur, et doit pouvoir être transféré sur demande, après formation à l'exploitant du site. Il peut ouvrir des comptes de rang inférieur ; **- Niveau 2 :** utilisateur avancé : assure les tracés des zones, franchissement/intrusion, les seuils de signalement et le moteur de règle logique. Ce rôle peut être partagé avec l'éditeur. Il peut ouvrir des comptes de rang inférieur ; **- Niveau 1 :** utilisateur standard: Observe les flux et les signalements.	F0

Exigence n°19	La(es) solution(s) doivent permettre de gérer des groupesd'utilisateurs.	F0
Exigence n°20	Il doit être possible de décliner différents types de profils permettant de gérer les droits des différents groupes d'utilisateurs.	F0
Exigence n°21	Il est possible pour un utilisateur avancé d'activer / désactiver l'utilisation de règles sur un flux mis à disposition via une interface simple d'utilisation (accessible en 1 ou 2 clics, réalisable en 2 ou 3 clics).	F1
Exigence n°22	La solution doit permettre l'ouverture de compte pour des administrateurs, utilisateurs avancés, et utilisateur standard	F0

La gestion de l'accès à la solution et de l'attribution des droits sera soit faite en local, soit à travers le système centralisé de l'exploitant, en accord avec celui-ci, et si la solution du titulaire est compatible avec ce système (cf exigence 117).

Fonctionnement de la solution

Exigences	Clauses et conditions	Fi
Exigence n°23	La solution doit produire des logs applicatives des évènements majeurs et critiques pouvant impacter son bon fonctionnement.	F0
Exigence n°24	Les logs applicatives doivent être accessibles à un administrateur côté exploitant.	F0
Exigence n°25	Une IHM de la solution permet d'avoir une idée du bon fonctionnement des différents composants (ex : un code couleur Vert / jaune / rouge)	F1
Exigence n°26	En cas de redémarrage du serveur, la solution doit se relancer automatiquement.	F0
Exigence n°27	En cas de coupure électrique sans onduleur, la solution doit se relancer automatiquement.	F0
Exigence n°28	Le titulaire respecte son taux de disponibilité de la solution sur lequel il s'engage (CRT), le taux étant calculé sur la phase de déploiement opérationnel.	F1
Exigence n°29	En cas de perte du flux vidéo, la solution doit pouvoir reprendre automatiquement ses analyses dès retour de celui ci.	F0
Exigence n°30	Une IHM (ou autre solution) permet de réaliser des backups manuel du paramétrage avec un compte ayant des droits adaptés.	F1
Exigence n°31	Une IHM permet de paramétrer des backups automatiques du paramétrage avec un compte ayant des droits adaptés.	F1
Exigence n°32	Les IHM de la solution permettent aux utilisateurs de paramétrer les conditions de déclenchement complexes par composition logique de conditions simples.	F1

Paramétrage

Exigences	Clauses et conditions	Fi
Exigence n°33	Les IHM de la solution doivent permettre à l'utilisateur de gérer les caméras (ajout, suppression de caméras).	F0
Exigence n°34	La solution ne doit comptabiliser les licences que sur les flux / les caméras / films actifs dans la solution (les licences devront être flottantes).	F0
Exigence n°35	Les IHM de la solution permettent à l'utilisateur d'activer / désactiver une caméra ou un fichier vidéo dans un format standard type MP4.	F1
Exigence n°36	Les IHM de la solution doivent permettre de spécifier des zones d'analyse dans l'image en positionnant des points représentant une ligne / une forme libre.	F0
Exigence n°37	Les IHM de la solution permettent à l'utilisateur de tester un paramétrage sur une scène pré enregistrée (pour vérifier le bon fonctionnement ou comprendre les faux positifs / faux négatifs).	F1
Exigence n°38	La solution permet le paramétrage des algorithmes (conditions de déclenchements complexes) au travers d'IHM ergonomiques et complètes	F1
Exigence n°39	Les IHM de la solution doivent permettre aux utilisateurs de vérifier les signalements déclenchées.	F0
Exigence n°40	Les IHM de la solution permettent aux utilisateurs de visualiser les résultats des détections en temps réel ainsi que les données associées aux détections (encadrement des formes identifiées).	F1
Exigence n°41	Les IHM de la solution doivent permettre aux utilisateurs de paramétrer les jours / heures sur lesquelles les signalements sont actifs.	F0
Exigence n°42	Les IHM de la solution doivent permettre aux utilisateurs de visualiser les résultats des algorithmes de comptage ou de densité.	F0
Exigence n°43	Les IHM de la solution doivent permettre d'administrer les délais de rétention des signalements et des données permettant de qualifier leur pertinence.	F0
Exigence n°44	Les IHM de la solution permettent d'administrer les durées de rétention des logs de connexion et d'usage de la solution.	F1
Exigence n°45	Les IHM de la solution sont en français	F0
Exigence n°46	Les IHM doivent permettre de désactiver à tout moment la solution, ou la possibilité de désactiver certains évènements par le service utilisateur	F0

Classification

Exigences	Clauses et conditions	Fi
Exigence n°47	La solution classifie différents types « d'objets » (au sens de l'analyse d'image : véhicule, mobilier urbain, , *ie* pas au sens objet abandonné).	F1
Exigence n°48	Le soumissionnaire fournit la liste de tous les « objets » pouvant	F1

	être classifiés par la solution.	
Exigence n°49	Le soumissionnaire détaillera les modalités et délais pour créer une nouvelle classe (ex : trains).	F1
Exigence n°50	Le soumissionnaire détaille les prérequis nécessaires à la création d'une nouvelle classe (volume de données, informations associées, …).	F1
Exigence n°51	Le soumissionnaire peut réaliser la création de classe ou l'amélioration de classe dans un local du service utilisateur en utilisant les datasets mis à disposition par le service utilisateur sous réserve de disponibilité de ces datasets.	F1

Évolutions logicielles

Exigences	Clauses et conditions	Fi
Exigence n°52	Le titulaire s'engage à assurer la compatibilité du paramétrage lors des montées de version. Si le paramétrage évolue, la solution devra être livrée avec des scripts de mise à jour du paramétrage Si l'évolution de paramétrage n'est pas réalisable par scripts, le titulaire s'engage à prendre à sa charge la mise à jour du paramétrage.	F0
Exigence n°53	Le titulaire s'engage à assurer la compatibilité du(es) logiciel(s) avec les mises à jour du socle (ex : KB windows) et les évolutions de version du socle (ex : Windows serveur 2019).	F0
Exigence n°54	Le titulaire s'engage à mettre à jour avec les dernières versions logiciels du socle et de la solution lors de chaque mise en service (lignes B2-X ou B4). La solution devra être testée préalablement par le titulaire afin de garantir l'absence de régression lors de cette montée de version.	F0
Exigence n°55	La mise à jour du produit et de tous ses composants doit être simple à mettre en œuvre, et la plus automatisée possible.	F0

Pérennité logicielle

Exigences	Clauses et conditions	Fi
Exigence n°56	Si des composantes logicielles de la solution ne sont plus supportées par leurs éditeurs ou sont dépréciées par le socle hébergeant la solution, le titulaire doit fournir un plan d'action permettant de remplacer ces composantes et de gérer les éventuelles vulnérabilités de sécurité le temps de la transition.	F0

Support pendant toute la durée du marché

-

Exigences	Clauses et conditions	Fi
Exigence n°57	Le titulaire s'engage à assurer un support technique en langue française.	F0

Exigence n°58	Les incidents et difficultés de fonctionnement sont communiqués au titulaire : • soit directement à son personnel lorsqu'il est présent sur place • soit à travers le service de support utilisateur qu'il met à disposition	F0
Exigence n°59	Le titulaire doit proposer une assistance téléphonique. Il peut également mettre en place une assistance par tchat ou par courriel pour faciliter l'interaction avec accord de l'exploitant. Dans ce cas, des salons de tchat seront ouverts par l'administration ou l'exploitant sur demande.	F0
Exigence n°60	Le titulaire s'engage à un temps de réponse technique argumenté (échange oral avec une assistance experte) de 4h en jours et heures ouvrés sur un incident critique de l'application.	F0
Exigence n°61	Le titulaire s'engage à un temps de réponse technique argumenté (échange oral avec une assistance experte) de un jour ouvré sur un incident majeur de l'application.	F0
Exigence n°62	Le titulaire s'engage à un temps de réponse technique argumenté (échange oral avec une assistance experte) de une semaine sur un incident mineur de l'application.	F0
Exigence n°63	Dans le cas d'un incident critique, le titulaire s'engage à intervenir dans le premier jour ouvré suivant la prise en compte pour corriger ou apporter un contournement accepté par l'exploitant.	F0
Exigence n°64	Dans le cas d'un incident majeur, le titulaire s'engage à intervenir dans les 5 jours ouvrés suivants la prise en compte pour corriger ou apporter un contournement accepté par l'exploitant.	F0
Exigence n°65	Le titulaire doit disposer d'une méthodologie prévoyant les mesures qu'il prendra pour corriger et prévenir les erreurs et les biais qui seraient détectées dans le fonctionnement du traitement, si nécessaire en procédant à une phase de réentrainement, le cas échéant dans le cadre prévu par le e décret en cours de publication relatif aux modalités de mise en œuvre des traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, pris en application de l'article 10 de la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions	F0
Exigence n°66	Dans le cas d'un incident mineur, le titulaire s'engage à convenir avec l'exploitant d'une planification de la livraison des corrections, ou de l'abandon de celle-ci en cas d'accord écrit (par courriel) du service utilisateur.	F0
Exigence n°67	Le titulaire doit assurer la traçabilité des incidents rencontrés et de leur résolution. Le titulaire animera tous les trimestres une réunion de suivi des incidents et corrections d'incidents s'il y en a.	F0
Exigence n°68	Lors de toute proposition de solution palliative à un problème rencontré, le titulaire doit tester préalablement cette solution, et détailler à l'exploitant les modalités précises de mise en œuvre et les précautions à prendre.	F0

Sous-prestation 1.1 : Fourniture d'une licence flottante sur la période d'expérimentation pour un (1) flux vidéo

Exigences	Clauses et conditions	Fi
Exigence n°69	Le titulaire fournit un droit d'usage de sa solution (licence flottante) pour toute la durée de l'expérimentation. Ce droit d'usage est facturé par flux et est transférable d'un site de déploiement à l'autre.	F0
Exigence n°70	Cette licence flottante doit permettre de mutualiser les licences sur l'ensemble des déploiements du lot,et être réaffectée à un nouveau flux à la volée. Sur un déploiement (même site), il n'y a pas besoin de recours au service commercial ou technique pour faire cette réallocation.	F0
Exigence n°71	Cette licence contient également tous les correctifs rendus nécessaires sur la période, que cela soit pour corriger les dysfonctionnements ou les vulnérabilités de cybersécurité, ou pour améliorer les performances du produit. Il installe les correctifs à chaque mise en service, et conformément aux exigences pour les incidents majeurs et critiques.	F0

Sous-prestation 1.2 : Location des serveurs et terminaux

N= 8, 20, 50, 100, 200 en fonction de la ligne de commande.

Exigences	Clauses et conditions	Fi
Exigence n°72	Le titulaire doit fournir une réponse à la demande de faisabilité couvrant les prestations et les équipements nécessaires pour la mise en œuvre de N flux sur un site, pendant la période de l'expérimentation.	F0
Exigence n°73	Les équipements doivent pouvoir être transférés successivement sur plusieurs sites pendant la période de l'expérimentation.	F0
Exigence n°74	Les équipements doivent permettre d'installer la solution algorithmique et de réaliser l'ensemble de l'architecture permettant l'interconnexion avec le système de vidéoprotection du site.	F0
Exigence n°75	Le titulaire doit fournir un poste de supervision (ou poste opérateur) doté de deux écrans de taille adaptée en mesure	F0

	d'afficher 9 tuiles vidéos par écran, qui sera interconnecté avec la solution du titulaire.	
Exigence n°76	Si en fin de marché, la commande de la prestation achat de serveur n'est pas émise, le titulaire doit décommissionner en fin de contrat le matériel en suivant les exigences techniques. Dans tous les cas, les stockages de masse sont livrés en fin de marché à l'exploitant.	F0
Exigence n°77	Le titulaire en fin de marché transfère la propriété du matériel à l' Etat si la commande d'achat est émise. L'ensemble des logiciels installés sont à jour lors du transfert de propriété.	F0

Livrables

Exigences	Clauses et conditions	Fi
Exigence n°78	La solution doit être livrée avec la documentation administrateur des différents composants logiciels en Français ou anglais et libre de redevance.	F0
Exigence n°79	La solution est livrée avec la documentation utilisateur avancé des différents composants logiciels en Français ou anglais et libre de redevance.	F1
Exigence n°80	La solution doit être livrée avec la documentation utilisateur standard des différents composants logiciels en Français ou anglais et libre de redevance.	F0
Exigence n°81	La solution est livrée avec la documentation des gestes de maintenance nécessaires au maintien en condition opérationnelle (purge de logs, redémarrages, …).	F1
Exigence n°82	La solution est livrée avec la documentation d'installation de la solution.	F1

Exigences et livrables spécifiques de la conception de la solution :

Exigence n°83	Le titulaire doit documenter les moyens organisationnels mis en œuvre pour veiller à la protection des données à caractère personnel et à l'éthique de la solution	F0
Exigence n°84	Le titulaire doit disposer d'une description du (ou des) jeu(x) de données utilisé(s) lors des phases d'entraînement, de validation et de test de la solution, d'informations relatives à leur provenance, leur portée et leurs principales caractéristiques, ainsi que la manière dont elles ont été obtenues et sélectionnées et peut fournir une description des caractéristiques des images ou captations vidéo constituant ce(s) jeu(x) de données ainsi que les données qui leur sont associées (ex : annotations, métadonnées, etc.)	*Fo*
Exigence n°85	Le titulaire doit décrire le modèle d'apprentissage utilisé pour la solution	F0
Exigence n°86	Le titulaire doit expliquer les mesures mises en œuvre pour que le jeu de données utilisé pour la conception soit représentatif, pertinent et adéquat	F0

Exigence n°87	Le titulaire doit décrire les mesures mises en œuvre pour identifier et prévenir l'occurrence de biais et d'erreurs lors la conception de la solution	F0
Exigence n°88	Le titulaire doit décrire les modalités prévues dans le fonctionnement de la solution pour garantir le contrôle humain	F0
Exigence n°89	Les algorithmes devront pouvoir fonctionner sans exploitation de données biométriques ni de reconnaissance faciale (la solution déployée ne doit pas présenter ce type d'analyse, ni comporter des capacités d'activation de ces capacités).	F0
Exigence n°90	Les livrables (documentations (exigence 78 à 82), dossier de conception (exigence 83 à 89), PAQ (exigence 92 & 93)) doivent être transmis dans le mois qui suit la notification du marché. Chaque mise à jour majeure nécessitant une reprise des livrables est suivie d'une livraison de ceux-ci avant mise en service de la mise à jour.	F0
Exigence n°91	A chaque livraison d'une prestation, un bordereau de livraison doit être transmis au service prescripteur.	F0

Plan d'assurance qualité

Exigences	Clauses et conditions	Fi
Exigence n°92	Le titulaire met à disposition un plan d'assurance qualité s'il en a un.	F1
Exigence n°93	Le soumissionnaire fournit à titre informatif le PAQ dont il dispose.	F1

PRESTATION 2 : INSTALLATION ET DEMONTAGE DE LA SOLUTION

Exigences	Clauses et conditions	Fi
Exigence n°94	L'intervention sur les infrastructures de l'exploitant doit se dérouler en présence de l'exploitant et doit respecter les normes et usages de ce dernier. Aucune intervention ne pourra être faite sans son accord ou sans supervision de sa part.	F0

Installation de la solution sur un site (sans considération du nombre de flux)

Exigences	Clauses et conditions	Fi
Exigence n°95	Lors de l'installation sur site, le titulaire doit assurer le transfert et la livraison du matériel nécessaire sur le site. Il doit installer l'ensemble des logiciels nécessaires à la mise en œuvre de la solution.	F0
Exigence n°96	Il raccorde sa solution au réseau de vidéosurveillance et au VMS du site en respectant les exigences de cybersécurité. Il suit les consignes de raccordement qui lui sont fournies par l'exploitant	F0

Préparation à la mise service de la solution

Exigences	Clauses et conditions	Fi
Exigence n°97	Lors de la préparation à la mise en service, le titulaire doit vérifier le bon fonctionnement de la solution, et s'assure de la capacité à configurer la solution (choix des flux, paramétrage et calibration). Il s'assure de la pertinence des détections réalisées par rapport aux besoins métiers. Il construit les patterns de détection permettant de réaliser les détections pertinentes. Il est présent sur site lors de cette prestation. La prestation est forfaitaire, en fonction du nombre de flux concernés. A charge au titulaire d'accompagner les utilisateurs sur la durée nécessaire à la mise au point, qui ne doit pas être supérieure à quelques jours.	F0

Démontage de la solution pour un site

Exigences	Clauses et conditions	Fi
Exigence n°98	Lors du démontage de la solution, le titulaire doit débrancher la solution du réseau de l'exploitant. Le titulaire démonte la solution, la transporte soit sur un nouveau site de déploiement,	F0

	soit sur un lieu de stockage sous responsabilité du titulaire jusqu'au prochain déploiement.	

Désactivation et réactivation de la solution sur un même site entre deux manifestations

Exigences	Clauses et conditions	Fi
Exigence n°99	Lors de la désactivation de la solution, l'exploitant doit mettre la solution du titulaire en sommeil pour une période entre deux manifestations. Lors de la réactivation, si c'est nécessaire, le titulaire garantit la mise à jour MCO/MCS de la solution. La prestation de préparation à la remise en service, si elle est rendue nécessaire par un changement du besoin métier (zone couverte différente, besoin de détection différent), sera facturée sur la prestation 4.	F0
Exigence n°100	Le titulaire forme l'exploitant à la désactivation, et autorise l'exploitant à réaliser cette désactivation lui-même. Le titulaire forme l'exploitant à la ré activation et autorise l'exploitant à réaliser cette ré activation lui-même. Si une prestation du titulaire est nécessaire, celle-ci sera facturée sur la prestation 4.	F1

Fonctionnement avec le VMS existant

Exigences	Clauses et conditions	Fi
Exigence n°101	Lors du déploiement sur un site, la solution est raccordée au VMS existant. La solution doit être compatible avec les VMS Genetec et Milestone.	F0
Exigence n°102	Sur certains sites de déploiement, d'autres VMS peuvent être déployés. Le raccordement à un de ces VMS sera précisé lors de la demande de faisabilité, et le titulaire pourra décliner s'il n'est pas en capacité de se raccorder à ce VMS. Dans ce cas, le recours au titulaire du rang suivant pourra être fait .	F1
Exigence n°103	Des échanges de flux de contrôle doivent être possibles avec le VMS. La liste des flux de contrôle doit être documentée.	F0
Exigence n°104	Les éléments utilisés pour caractériser et déclencher l'alerte sont visibles lors de la relecture de la séquence vidéo.	F1
Exigence n°105	Les flux vidéos doivent pouvoir être transmis par le VMS existant du site à la solution déployée par le titulaire.	F0

Délais d'exécution

- Le titulaire définit son délai N d'installation et de mise en service, exprimé en jours ouvrés dans sa réponse à la demande de faisabilité.

- Commande non anticipée : La date souhaitée de livraison du matériel et de mise en service de la solution sur un site est précisée lors de la demande de faisabilité. Si le titulaire n'est pas en capacité de livrer les prestations prévues dans le délai imparti, l'administration peut requérir les services du titulaire du rang suivant, selon les règles de rang prévues dans le CCAP.

- Commande anticipée : une commande peut être réalisée sans précision de la date de livraison ou d'installation. Dans ce cas, un ordre de service est notifié au titulaire au moins N jours ouvrés avant la date de mise en service souhaitée.

- La désactivation de la solution doit être effective dès la fin de l'autorisation préfectorale d'usage de la solution.

- le titulaire dispose de 5 jours ouvrés pour démonter la solution à partir de la date définie avec l'exploitant.

Mesures de cybersécurité

Objectifs de sécurité

Le principal objectif de sécurité visé consiste à ce que la solution fournie et déployée par le titulaire du présent marché ne puisse pas nuire au bon fonctionnement, à la disponibilité et à la protection des données des systèmes de vidéoprotection historiquement mis en œuvre par les entités utilisatrices. Les systèmes de vidéoprotection en production doivent impérativement rester opérationnels pour permettre aux services utilisateurs d'assurer leurs missions. Plus particulièrement, dans l'hypothèse d'une prise de contrôle malveillante de la solution du titulaire, il ne doit pas être possible de compromettre le système de vidéoprotection avec lequel il est interconnecté afin, par exemple, de le rendre indisponible ou d'exfiltrer les images vidéo.

Par ailleurs, la solution proposée par le titulaire doit être conçue et déployée pour se prémunir des événements redoutés suivants :

- Les flux vidéos sont interceptés et détournés par un acteur malveillant ;
- Un acteur malveillant compromet le système de vidéoprotection intelligent afin :
    - de modifier le comportement de l'IA et sa capacité à détecter les cas d'usages souhaités ;
    - d'envoyer de fausses alertes pour mobiliser inutilement les forces de sécurité (intérieure/civile) et créer des troubles à l'ordre public ;
    - par rebond de rendre le système de vidéoprotection de l'exploitant inopérant.
- Un acteur malveillant compromet les ressources permettant l'apprentissage de l'IA et/ou son maintien en condition opérationnelle et de sécurité afin de nuire à son bon fonctionnement de la solution.

Principe d'architecture visant à répondre aux objectifs de sécurité

Afin de répondre aux objectifs de sécurité indiqués ci-dessus, le titulaire doit s'appuyer sur les principes d'architecture suivants :

#001	Le système d'information de vidéo intelligent sera séparé du système d'information de production de la vidéoprotection
#002	Le système n'a pas de connexion avec l'extérieur (comprendre l'Internet). Il est dans une "bulle" isolée et indépendante". Tous les éléments constitutifs du SI vidéo intelligent seront déployés et hébergés sur des serveurs et équipements locaux sur le site du service utilisateur.
#003	L'acquisition de caméra n'est pas prévue dans le présent marché.
#004	Les caméras n'embarqueront pas d'algorithme d'intelligence artificielle, ni ne seront directement pilotés par des algorithmes d'IA.
#005	L'usage de service nuagique n'est pas autorisé.
#006	Il n'y a pas d'exigence concernant le cycle de développement des produits qui répondront au marché.
#007	Le serveur hébergeant les services de vidéo intelligente sera connecté sur un VMS sous responsabilité de l'exploitant.

Exigences de sécurité

Exigences	Clauses et conditions	Fi
Exigence 106	Assurer un cloisonnement optimal entre les composants du SI vidéo intelligent et ceux du SI de vidéoprotection existant, notamment en filtrant strictement les flux entre les composants ou en appliquant un cloisonnement applicatif (système, authentification, droits d'exécution, etc.). Lors de la préparation du déploiement, le titulaire confirme son architecture réseau avec l'exploitant pour s'assurer que cette exigence est bien remplie	F0
Exigence 107	Si possible les flux ne sont pas initiés par le SI vidéo intelligent.	F1
Exigence 108	Dans cet objectif de cloisonnement, le prestataire s'appuie : - sur le cloisonnement logiciel qui consiste en l'utilisation de mécanisme pour gérer des droits d'accès ; - sur le cloisonnement physique qui consiste en la séparation matérielle des composants ; -et sur le cloisonnement virtuel qui consiste en l'utilisation d'une technologie de virtualisation pour segmenter les composants.	F1
Exigence 109	En cas de dysfonctionnement ou de vulnérabilité, le prestataire doit veiller à ce que les composants de vidéo intelligent puissent être désactivés sans impact sur le SI de vidéoprotection existant	F0

Exigence 110	Tous les équipements constitutifs du nouveau SI vidéo intelligent doivent être déployés et hébergés localement sur le site du service utilisateur. Tout hébergement externe, notamment s'appuyant sur des infrastructures ou des services nuagiques, est interdit. Cela interdit également toute mise en œuvre de chaîne CI/CD visant à mettre à jour régulièrement les versions logicielles des équipements du SI vidéo intelligent.	F0
Exigence 111	Toutes actions d'administration, d'exploitation ou de supervision depuis Internet sont interdites.	F0
Exigence 112	Si le titulaire met en place des actions d'administration à distance, le système doit respecter le chapitre 12 du guide « Recommandations relatives à l'administration sécurisée des systèmes d'information ». L'exploitant se réserve le droit d'interdire les actions d'administrations à distance en cas d'insuffisance des mesures de protection proposées.	F1
Exigence 113	Les serveurs hébergeant les services de vidéo intelligente devront être connectés sur le VMS du site. Le stockage nécessaire à la solution doit être réalisé en local sur son architecture.	F0
Exigence 114	Assurer l'intégrité et la confidentialité des flux de contrôle des protocoles s'appuyant sur des mécanismes cryptographiques (cf. annexes du RGS et guide ANSSI sur les algorithmes cryptographiques). La mise en place du protocole sécurisé doit être confirmée lors des échanges préalables à l'installation.	F0
Exigence 115	Assurer l'intégrité et la confidentialité des flux vidéos avec des protocoles s'appuyant sur des mécanismes cryptographiques (cf. annexes du RGS et guide ANSSI sur les algorithmes cryptographiques).La mise en place du protocole sécurisé doit être confirmée lors des échanges préalables à l'installation.	F0
Exigence 116	Distinguer l'administration de l'infrastructure du SI vidéo intelligent d'une part, et d'autre part la gestion métier de ce nouveau SI. L'administration de l'infrastructure et la gestion métier du SI vidéo intelligent sont cloisonnées. .	F1
Exigences 117	S'assurer que l'ensemble des dispositifs déployés sont compatibles avec une gestion centralisée des identités et des droits (RBAC), par exemple au travers d'un référentiel d'identification et authentification.	F1
Exigence 118	L'ensemble des dispositifs constitutifs du SI vidéo intelligent se synchronise sur la même source de temps (serveur NTP du SI de l'exploitant).	F1
Exigence 119	Assurer la traçabilité des accès à l'infrastructure du SI vidéo intelligent, ainsi qu'aux vidéos.	F0
Exigence 120	S'assurer que le système permet de respecter le principe de moindre privilège (applications, tâches, actions, secteurs). Les droits et privilèges des utilisateurs et administrateurs sont configurés suivant le strict besoin opérationnel. Tous les comptes techniques du SI vidéo sont être distincts de ceux utilisés pour le SI de vidéoprotection existants.	F1

Exigence 121	Journaliser les actions sur le système.	F0
Exigence 122	Maîtriser les périphériques amovibles. Les périphériques sont identifiés. Seuls les périphériques identifiés peuvent être utilisés dans le cadre du bon fonctionnement de la solution. Les périphériques sont chiffrés pour limiter l'impact de la perte d'un périphérique. Les périphériques sont stockés de manière sécurisée. Les périphériques sont effacés de manière sécurisée après chaque utilisation.	F1
Exigence 123	Lors de l'installation des équipements du titulaire, procéder au chiffrement de tous les disques durs et de leurs partitions afin de protéger les données et rendre plus facile les opérations d'effacement des données.	F1
Exigence 124	Lors du décommissionnement, les unités de stockage des équipements doivent être conservés par l'exploitant. Tout support de stockage qui est raccordé à la solution ne doit pas sortir du site sans autorisation de l'exploitant.	F0
Exigence 125	Lors du démontage de la solution pour transfert sur un autre site, le titulaire doit prouver à l'exploitant qu'il a bien effacé tous les supports de stockage utilisés avec une procédure sécurisée	F0
Exigence 126	S'assurer que les flux vidéos et les flux de contrôle sont cloisonnés dans des canaux distincts.	F1
Exigence 127	Assurer la traçabilité des accès aux activités d'administration de l'infrastructure de la solution du titulaire.	F0
Exigence 128	Assurer la traçabilité des accès aux activités d'administration de gestion/administration de la solution du titulaire.	F0
Exigence 129	Les caméras ne devront ni embarquer d'algorithme d'intelligence artificielle, ni ne seront directement pilotés par des algorithmes d'IA. Il n'y aura pas de flux de contrôle permettant de piloter les caméras dont les flux sont récupérés.	F0
Exigence 130	La solution du titulaire ne doit pas pouvoir joindre les caméras directement.	F0
Exigence 131	Aucun apprentissage de l'IA n'est autorisé pendant le déploiement de la solution. Cela implique qu'aucune interconnexion extérieure visant à alimenter l'IA en données d'apprentissage ne devra être mise en œuvre. Un apprentissage local peut être réalisé par le titulaire pendant les phases de mises en service et à blanc, mais pas dans la phase d'exploitation.	F0
Exigence 132	La solution du titulaire doit être maintenue en condition opérationnelle et en condition de sécurité de manière régulière (au minimum à chaque mise en service ou réactivation) et tout au long du cycle de vie de l'expérimentation. Pour toutes vulnérabilités d'un score CVSS égal ou supérieur à 7, le titulaire devra mettre en œuvre les correctifs de sécurité ou les mesures palliatives dans un délai de 15 jours.	F0
Exigence 133	Des procédures de sauvegarde et de restauration doivent être formalisées, mises en œuvre et testées régulièrement (fréquence à préciser). Des sauvegardes hors ligne doivent avoir lieu (données de configuration et données métier).	F0
Exigence 134	La solution mise en œuvre doit être auditable par un tiers.	F0

Exigence 135	Si des composants sont déployés sur le SI de vidéoprotection, modifiant ainsi ses fonctionnalités, le titulaire devra garantir et démontrer l'innocuité des nouveaux composants installés	F0
Exigence 136	Les composants logiciels ne disposent pas de comptes et privilèges d'administrateur système (par exemple, « root » pour Linux). Des comptes et droits d'accès répondant au juste besoin sont utilisés.	F1
Exigence 137	La documentation (architecture, sécurité, etc.) doit être disponible et à jour. Cette documentation doit être assez précise techniquement pour détailler l'intégration des nouvelles fonctionnalités sur le SI de vidéoprotection et d'en déterminer les impacts.	F0
Exigence 138	Les secrets relatifs à la solution (interne à la solution, secret détenu par les utilisateurs, etc.) doivent être à l'état de l'art et conservé de manière sécurisée. Les secrets de la solution doivent être différents de secrets du SI de vidéoprotection existant. Les secrets d'authentification doivent être configurés par l'entité utilisatrice et non par le titulaire.	F0
Exigence 139	Le titulaire fournit tous les équipements nécessaires à la mise en conformité aux exigences de sécurité, et doit en assurer la configuration.	F1

PRESTATION 3 : FORMATION ET PRISE EN MAIN DES ACTEURS TERRAINS

Exigences	Clauses et conditions	Fi
Exigence n°140	Le titulaire doit réaliser une formation pour l'ensemble des opérateurs d'un site, à la manipulation, au paramétrage et à la calibration. La formation a lieu pendant la phase de mise en service sur un site. Les secrets d'authentification sont changés après la phase de formation.	F0
Exigence n°141	Le titulaire doit proposer des formations pour l'installation, le paramétrage simple et la maintenance de la solution et outils, le tout en langue française.	F0
Exigence n°142	Le titulaire doit indiquer les contenus des formations prévues. Ils seront validés par le service utilisateur avant toute ouverture des sessions concernées.Ces formations sont en évolution continue et sont adaptatives vis- à-vis des équipements déployés.Les sessions de formation sont dispensées localement et/ou dans les locaux du soumissionnaire.	F0

PRESTATION 4 : ACCOMPAGNEMENT A LA MISE EN ŒUVRE DE LA SOLUTION

Exigences	Clauses et conditions	Fi
Exigence n°143	L'accompagnement prend la forme d'une journée d'intervention sur site pour un profil expert de la solution.	F0
Exigence n°144	Il doit être également prévu la possibilité d'astreinte téléphonique de nuit (entre 19h et 8h) ou l'astreinte téléphonique pendant une journée non ouvrée. Il est nécessaire de fournir le cas échéant tout moyen permettant de résoudre le problème rencontré, selon les délais des exigences prévus au présent CCTP, mais sans la mention « ouvré » (les heures ouvrés et jours ouvrés deviennent des heures et jours, sans notion ni de plage horaire ni de jour de la semaine).	F0
Exigence n°145	L'astreinte commandée dans un bon de commande est valable pour l'ensemble des déploiements du titulaire pour l'ensemble des lots dont il est titulaire pour la période considérée.	F0

GUIDES PRATIQUES

Voici la liste des guides que le soumissionnaire puis les candidats peuvent consulter pour les aider protéger le système d'information livré, et à le maintenir en condition de sécurité :

- Recommandations relatives à l'administration sécurisée des systèmes d'information | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
- Recommandations relatives à l'authentification multifacteur et aux mots de passe | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
- Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
- Définition d'une politique de pare-feu | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
- Recommandations de sécurité relatives à IPsec | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
- Mécanismes cryptographiques | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
- Le Référentiel général de sécurité (RGS) | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
- Recommandations de sécurité pour l'architecture d'un système de journalisation | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)