



MINISTÈRES
ÉDUCATION
JEUNESSE
SPORTS
ENSEIGNEMENT
SUPÉRIEUR
RECHERCHE

*Liberté
Égalité
Fraternité*

Direction du numérique
pour l'éducation
Sous-direction
des services numériques
(DNE SN)

61-65, rue Dutot
75732 Paris Cedex 15

Service de l'action
administrative et des
moyens
Sous-direction des achats
(SAAM B)
Bureau de la stratégie
et de l'ingénierie des achats
(SAAM B1)

61-65, rue Dutot
75732 Paris Cedex 15

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

Procédure : MEN-SG-AOO-25030

Objet : Réalisation de prestations d'infogérance des infrastructures de sécurité pour l'administration centrale du ministère de l'éducation nationale, du ministère des sports, de la jeunesse et de la vie associative et du ministère de l'enseignement supérieur, de la recherche et de l'espace.

ARTICLE 1. PREAMBULE	7
ARTICLE 2. OBJET DU MARCHÉ	7
ARTICLE 3. PRESENTATION DU PROJET	7
3.1. LES ACTEURS DU PROJET	7
3.1.1. PRESENTATION DE L'ADMINISTRATION CENTRALE DU MINISTERE	7
3.1.2. PRESENTATION DE LA DIRECTION DU NUMERIQUE POUR L'EDUCATION (DNE)	7
3.2. PRESENTATION DU CONTEXTE SI	8
3.2.1. ENTITES ET PERSONNES CONCERNEES	8
3.2.2. INFRASTRUCTURES	9
3.2.2.1. Infrastructures d'hébergement.....	9
3.2.2.2. Architecture d'ensemble, réseaux étendus	9
3.2.2.3. Télécommunications entre le titulaire et le ministère	9
3.2.2.4. Environnement d'exécution des prestations.....	9
3.2.2.5. Périmètre infogéré	10
ARTICLE 4. OBJECTIFS	10
ARTICLE 5. CADRE GENERAL D'EXECUTION DES PRESTATIONS	11
5.1. NATURE ET ETENDUE DES PRESTATIONS	11
5.2. CONTRAINTES ET EXIGENCES.....	11
5.2.1. RESPECT DES REFERENTIELS	11
5.2.2. RESPECT DES PREREQUIS MINISTERIELS	12
5.2.3. QUALIFICATION DES INTERVENANTS	12
5.2.4. ÉVOLUTIONS PREVUES ET PREVISIBLES DU PERIMETRE DU MARCHÉ.....	12
5.3. PILOTAGE ET CONDUITE DES PRESTATIONS	12
5.3.1 MODALITES DES ECHANGES ENTRE LE TITULAIRE ET LE MINISTERE.....	12
5.3.2 MOYENS TECHNIQUES.....	13
5.3.2.1. Moyens mis à la disposition du titulaire	13
5.3.2.1.1. Logiciels.....	13
5.3.2.1.2. Interventions sur sites.....	13
5.3.2.1.3 Gestion documentaire	13
5.3.2.2. Moyens mis à la disposition du ministère par le titulaire	13
5.3.2.2.1. Outil de supervision.....	13
5.3.2.2.2. Outil de gestion des tickets et de suivi des incidents.....	14
5.3.2.2.3. Outil de gestion des configurations	14

5.3.3 MOYENS ORGANISATIONNELS DE PILOTAGE.....	14
5.3.3.1. Réunions de travail.....	14
5.3.3.2. Instances de pilotage.....	14
5.3.4 INDICATEURS DE PERFORMANCE.....	15
5.3.5 PLAN DE PROGRES.....	15
5.3.5.1. Contenu du plan de progrès.....	15
5.3.5.2. Mise en œuvre du plan de progrès.....	15
5.3.5.2.1. Élaboration du plan de progrès.....	15
5.3.5.2.2. Suivi et pilotage du plan de progrès.....	16
5.4. LANGUE DE TRAVAIL	16
5.5. LIEUX D'EXECUTION DES PRESTATIONS	16
5.5.1. PRESTATIONS.....	16
5.5.2. REUNIONS.....	17
5.6. EXIGENCES LIEES AUX PERSONNELS DU TITULAIRE ET DE SES SOUS-TRAITANTS	17
5.7. STANDARDS ET NORMES – PLANS D'ASSURANCE QUALITE ET SECURITE.....	17
5.8. LIVRAISON, VERIFICATION ET ADMISSION DES PRESTATIONS.....	17
5.8.1. CONDITIONS DE LIVRAISON.....	17
5.8.2. CONDITIONS DE VERIFICATION ET D'ADMISSION DES PRESTATIONS.....	18
ARTICLE 6. NATURE DES PRESTATIONS ATTENDUES.....	18
6.1. MISSION 1 : INITIALISATION ET PRISE EN CHARGE DU MARCHE	19
6.1.1. OBJET DE LA MISSION 1.....	19
6.1.2. DESCRIPTION DES SERVICES ATTENDUS.....	19
6.1.2.1. Réunion de lancement (M1.1).....	19
6.1.2.2. Prise de connaissance du contexte du marché (M1.2).....	20
6.1.2.3. Mise en place de l'organisation et de la gouvernance du marché (M1.3).....	21
6.1.2.3.1. Élaboration du référentiel documentaire du marché.....	21
6.1.2.3.2. Finalisation du plan d'assurance qualité (PAQ).....	21
6.1.2.3.3. Finalisation du plan d'assurance sécurité (PAS).....	22
6.1.2.3.4. Finalisation de la convention de service.....	23
6.1.2.3.5. Mise en place du processus d'échanges et de suivi des prestations.....	23
6.1.2.4. Réunion de clôture de la phase de prise en charge (M1.4).....	24
6.1.3. ROLES ET RESPONSABILITES	25
6.1.4. NIVEAUX DE SERVICE	25
6.1.5. UNITES D'ŒUVRE.....	25

6.1.6. LIVRABLES.....	26
6.1.7. DELAIS D'EXECUTION ET D'ADMISSION.....	26
6.2. MISSION 2 : PILOTAGE DE L'INFOGERANCE	27
6.2.1. OBJET DE LA MISSION 2.....	27
6.2.2. DESCRIPTION DES SERVICES ATTENDUS.....	28
6.2.2.1. Synthèse de la gouvernance attendue	29
6.2.2.2. Comités.....	29
6.2.2.3. Rapports	31
6.2.2.3.1. Rapport de crise	31
6.2.2.3.2. Rapport mensuel	31
6.2.2.3.3. Rapport semestriel	32
6.2.2.3.4. Rapport continu	32
6.2.2.4. Retours d'expérience.....	32
6.2.2.5. Documentation.....	33
6.2.3. ROLES ET RESPONSABILITES	33
6.2.4. NIVEAUX DE SERVICE ATTENDUS.....	34
6.2.5. UNITES D'ŒUVRE	35
6.2.6. LIVRABLES.....	35
6.2.7. DELAIS D'EXECUTION ET D'ADMISSION.....	35
6.3. MISSION 3 : INFOGERANCE DES INFRASTRUCTURES DU MINISTERE.....	36
6.3.1. OBJET DE LA MISSION 3.....	36
6.3.2. DESCRIPTION DES SERVICES ATTENDUS.....	36
6.3.2.1. Prestations récurrentes mensuelles	36
6.3.2.1.1. Service de supervision, support et maintenance (M3 PR01).....	37
6.3.2.1.2. Service d'administration et d'exploitation (M3 PR02)	40
6.3.2.1.3. Services du centre de sécurité opérationnel (SOC).....	44
6.3.2.1.4. Modalités d'exécution des services	46
6.3.2.1.5. Audit de la qualité des prestations	48
6.3.2.2. Prestations à la demande	48
6.3.3. ROLES ET RESPONSABILITES	48
6.3.3.1. Services de supervision, de support et de maintenance	48
6.3.3.2. Services d'administration et d'exploitation	52
6.3.3.3. Services du centre de sécurité opérationnel	54
6.3.4. NIVEAUX DE SERVICE ATTENDUS.....	56
6.3.4.1. Services de supervision, de support et de maintenance	56
6.3.4.2. Services d'exploitation et d'administration	58
6.3.4.3. Services du SOC	60

6.3.5. UNITES D'ŒUVRE	61
6.3.5.1. Unités d'œuvre des prestations récurrentes	61
6.3.5.2. Unités d'œuvre des prestations à la demande	61
6.3.6. LIVRABLES.....	62
6.3.7. DELAIS D'EXECUTION ET D'ADMISSION.....	63
6.4. MISSION 4 : FOURNITURE DE SOLUTIONS DE MAINTIEN EN CONDITION OPERATIONNELLE ET D'EVOLUTION DES INFRASTRUCTURES ET SERVICES.....	64
6.4.1. OBJET DE LA MISSION 4.....	64
6.4.2. DESCRIPTION DES SERVICES ATTENDUS.....	64
6.4.3. ROLES ET RESPONSABILITES	65
6.4.4. NIVEAUX DE SERVICE	65
6.4.5. UNITES D'ŒUVRE	65
6.4.6. LIVRABLES.....	68
6.4.7. DELAIS D'EXECUTION ET D'ADMISSION.....	68
6.5. MISSION 5 : SERVICES CONSTRUCTEURS	69
6.5.1. OBJET DE LA MISSION 5.....	69
6.5.2. DESCRIPTIONS DES SERVICES ATTENDUS.....	69
6.5.3. ROLES ET RESPONSABILITES	70
6.5.4. NIVEAUX DE SERVICE	70
6.5.5. UNITES D'ŒUVRE	70
6.5.6. LIVRABLES.....	70
6.5.7. DELAIS D'EXECUTION ET D'ADMISSION.....	71
6.6. MISSION 6 : REVERSIBILITE.....	71
6.6.1. OBJET DE LA MISSION 6.....	71
6.6.2. SERVICES ATTENDUS	71
6.6.3. ROLES ET RESPONSABILITES	73
6.6.4. NIVEAUX DE SERVICE	73
6.6.5. UNITES D'ŒUVRE	73
6.6.6. LIVRABLES.....	73
6.6.7. DELAIS D'EXECUTION ET D'ADMISSION.....	74
ARTICLE 7. GLOSSAIRE	75

Annexe	Intitulé
1	Inventaire matériel-GTR
2	Liste des sites

ARTICLE 1. **PREAMBULE**

Dans le cadre du présent cahier des clauses techniques particulières (CCTP) :

- le terme « **ministère** » désigne les ministères chargés de l'éducation nationale (MEN), des sports, de la jeunesse, de la vie associative (MSJVA) et de l'enseignement supérieur, de la recherche et de l'espace (MESRE).
- le terme « **titulaire** » désigne l'entreprise ou le groupement d'opérateurs économiques retenu pour exécuter les prestations ainsi que son ou ses représentant(s).

ARTICLE 2. **OBJET DU MARCHÉ**

Le présent marché a pour objet la réalisation de prestations d'infogérance des infrastructures de sécurité pour l'administration centrale du ministère de l'éducation nationale, du ministère des sports, de la jeunesse et de la vie associative et du ministère de l'enseignement supérieur, de la recherche et de l'espace.

ARTICLE 3. **PRESENTATION DU PROJET**

3.1. LES ACTEURS DU PROJET

3.1.1. PRESENTATION DE L'ADMINISTRATION CENTRALE DU MINISTERE

L'administration centrale des ministères comprend :

- l'inspection générale de l'administration de l'éducation nationale et de la recherche ;
- le médiateur de l'éducation nationale et de l'enseignement supérieur ;
- le haut fonctionnaire de défense et de sécurité ;
- les bureaux des cabinets ;
- le secrétariat général ;
- l'inspection générale de l'éducation nationale ;
- la direction générale de l'enseignement scolaire ;
- l'inspection générale des bibliothèques ;
- le conseil national d'évaluation du système scolaire ;
- le conseil supérieur des programmes
- l'observatoire national de la sécurité et de l'accessibilité des établissements d'enseignement ;
- la direction générale pour l'enseignement supérieur et l'insertion professionnelle ;
- la direction générale pour la recherche et l'innovation ;
- la direction de la jeunesse, de l'éducation populaire et de la vie associative ;
- la direction des sports.

3.1.2. PRESENTATION DE LA DIRECTION DU NUMERIQUE POUR L'EDUCATION (DNE)

La direction du numérique pour l'éducation a pour mission l'impulsion et l'accompagnement de la transformation numérique du système éducatif, au bénéfice de la communauté éducative comme des agents.

Elle intervient au profit de l'ensemble du ministère, sur le périmètre des systèmes d'information à l'exception de ceux relevant de la zone fonctionnelle des ressources humaines du ministère.

Elle définit la politique de développement du service public du numérique éducatif. Elle en assure le déploiement et la valorisation.

Elle coordonne les actions du ministère, en matière de systèmes d'information, de développement de services numériques et d'innovation numérique, de développement de la culture numérique ainsi que de gestion des compétences numériques. A ce titre, elle représente le ministère auprès des structures interministérielles chargées du numérique et des systèmes d'information et de communication, sur le périmètre de ses attributions.

Elle coordonne le volet numérique de l'activité des opérateurs de l'enseignement scolaire, en lien avec la direction générale de l'enseignement scolaire, la direction générale des ressources humaines et la direction des affaires financières, et définit les orientations stratégiques dans ce domaine.

Elle prépare les orientations stratégiques et les éléments de programmation en matière de numérique pour l'éducation. Elle conduit la politique partenariale avec les acteurs publics et privés de la filière numérique.

Sans préjudice des compétences de la direction de l'évaluation, de la prospective et de la performance en matière de données statistiques, elle coordonne les actions en matière d'inventaire, de gouvernance, de production, de circulation et d'exploitation des données.

Pour le ministère, elle assure, sur le périmètre de ses attributions, le cadrage opérationnel, technique et juridique des projets numériques et pilote les relations avec les partenaires concernés.

Elle assure la maîtrise d'ouvrage, la mise en œuvre et la maintenance de l'infrastructure technique adaptée à ces projets.

Elle conçoit, met en œuvre et assure la maintenance des systèmes d'information et de communication relevant de ses attributions.

Elle élabore, en lien avec les maîtrises d'ouvrage, le schéma stratégique des systèmes d'information et des télécommunications et conduit sa mise en œuvre opérationnelle.

Elle assure la maîtrise d'œuvre des projets informatiques et numériques relevant de ses attributions et en propose la programmation budgétaire et à ce titre, elle a autorité fonctionnelle sur les équipes informatiques nationales implantées dans certaines académies.

Elle assure une mission de contrôle de gestion dans le domaine du numérique pour l'éducation.

Au sein de la DNE, la délégation de service numériques pour l'administration centrale (DNE AC) veille à la cohérence des choix techniques et définit le schéma directeur des infrastructures.

Elle assure la programmation financière des plans d'équipement techniques.

Elle assure l'équipement matériel et logiciel et l'assistance aux utilisateurs de l'administration centrale.

Au sein de la DNE, la délégation des services numériques pour l'administration centrale (DNE AC) assure la conception et le développement des services numériques et des systèmes d'information pour l'administration centrale des ministères.

À ce titre, et en collaboration avec la sous-direction des achats, le bureau DNE AC1 est l'interlocuteur principal du titulaire du présent marché.

3.2. PRESENTATION DU CONTEXTE SI

3.2.1. ENTITES ET PERSONNES CONCERNEES

L'administration centrale du ministère est implantée sur plusieurs sites dont la liste figure en annexe 2 au présent document et représente un effectif d'environ 4 500 personnes.

Au sein du bureau DNE AC1, le pôle d'ingénierie réseau et télécom du ministère est l'interlocuteur du titulaire sur les sujets suivants :

- maîtrise d'ouvrage du marché ;
- suivi du service rendu ;
- gestion des changements.

Le titulaire est en relation directe avec :

- les collaborateurs du bureau DNE AC1 habilités à transmettre les incidents pour leur prise en compte par le titulaire ainsi que les demandes de changement (moins de 10 personnes) ;
- les mainteneurs matériels du ministère pour tout sujet relatif à la maintenance des équipements centraux ;
- les éditeurs de logiciels de base et de middleware pour tout sujet relatif au bon fonctionnement ou aux mises à jour ;
- les titulaires fournissant au ministère d'autres services d'exploitation (comme par exemple le titulaire du marché MOSAIC) ;
- l'opérateur de supervision du WAN du ministère pour tout sujet relatif au VMAN ;

3.2.2. INFRASTRUCTURES

3.2.2.1. Infrastructures d'hébergement

Actuellement, le centre serveur principal et le centre serveur de secours sont situés respectivement sur les sites de Dutot et de Descartes.

La sécurité des infrastructures et des accès aux ressources du SI de l'administration centrale du ministère est obtenue en isolant les flux internes des sites des ministères, des flux d'accès à Internet par l'utilisation d'une plate-forme présente à la fois sur les sites de Dutot et Descartes.

Cette plate-forme est aujourd'hui infogérée par la société titulaire (Orange) et couvre les besoins fonctionnels liés :

- à la répartition de charge multi sites et interne, et à la redondance applicative ;
- à l'accélération et le déchiffrement SSL ;
- au filtrage Web ;
- au filtrage antivirus et codes malicieux ;
- à la détection et à la prévention d'intrusions ;
- au cloisonnement des zones applicatives ;
- à la consolidation des logs ;
- au contrôle d'accès à des fins d'administration.

Elle est constituée de :

- routeurs d'accès à Internet ;
- commutateurs (de niveau 2 et de niveau 3) ;
- deux paires de pare-feu en cluster avec DMZ ;
- répartiteurs de charges ;
- proxies Web ;
- reverses Proxies ;
- boîtiers filtrants applicatifs ;
- serveurs DNS et DHCP.

La liste des équipements de l'infrastructure est fournie en annexe 1 « Systèmes et éléments actifs du périmètre ».

L'architecture permet une redondance d'accès à Internet pour l'ensemble des sites des ministères.

3.2.2.2. Architecture d'ensemble, réseaux étendus

MOSAIC est un marché d'infogérance des environnements matériel et logiciel associés à la téléphonie, à la bureautique et aux réseaux, intégrant la fourniture, la mise en œuvre et l'administration d'une solution d'architecture de téléphonie sur IP (ToIP) pour l'administration centrale du ministère.

Le marché RISAC fournit le V-MAN Ethernet qui relie les sites de l'administration centrale entre eux et vers les deux points de sortie Internet (Dutot et Descartes).

Les deux principaux sites sont raccordés à Renater à 1 GB. Un mécanisme automatique de bascule (BGP) permet de diriger tous les flux sur l'autre site en cas de panne d'un des deux liens grâce au lien direct 10 GB entre ces sites (également via Renater).

Ces accès sont gérés dans le cadre du présent marché.

3.2.2.3. Télécommunications entre le titulaire et le ministère

Le ministère ne fournit pas les télécommunications entre le titulaire et son propre système d'information (supervision, intervention à distance, tous transferts de données).

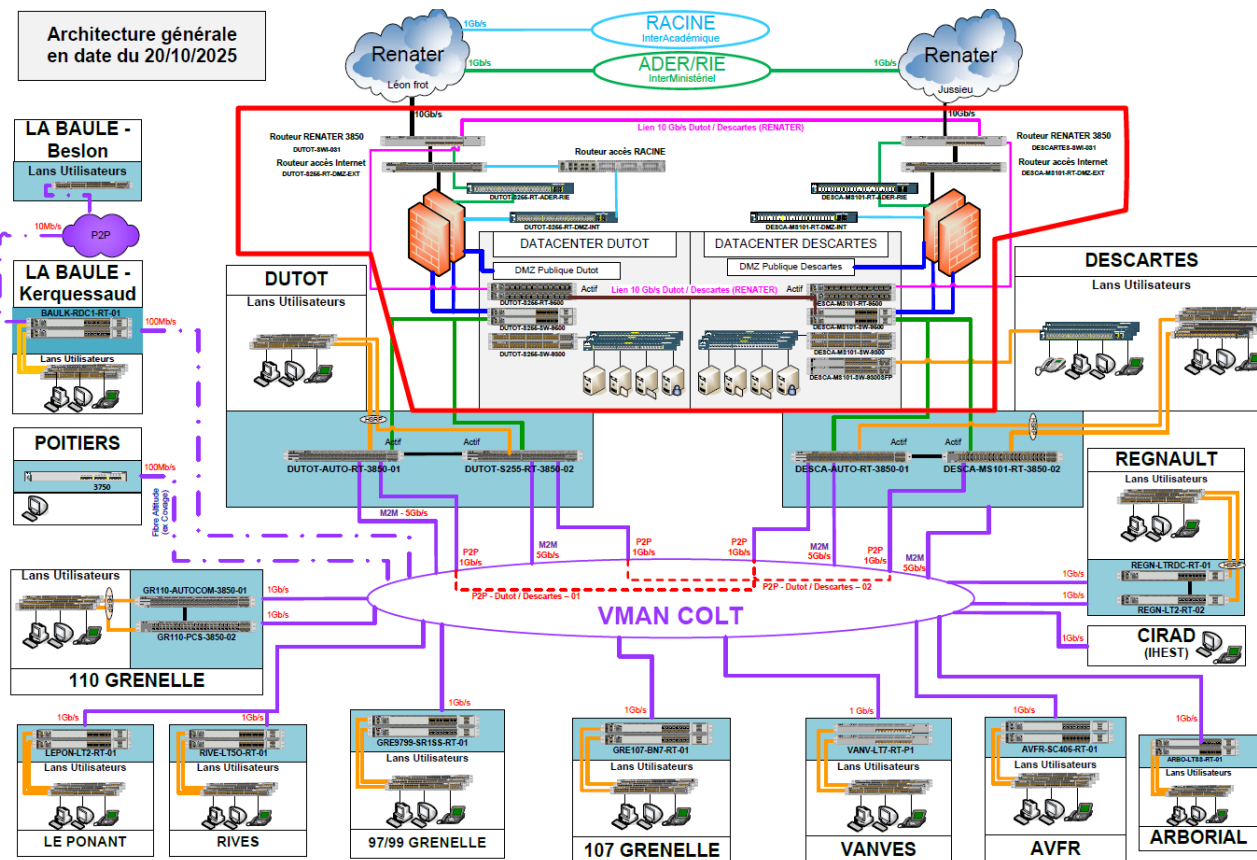
3.2.2.4. Environnement d'exécution des prestations

Les infrastructures comprises dans le périmètre objet du présent marché sont décrites en détail en annexe 1 « Systèmes et éléments actifs du périmètre » du présent CCTP.

3.2.2.5. Périmètre infogéré

Le schéma suivant illustre le périmètre principal des équipements infogérés (en encadré rouge). Les datacenters des sites de Dutot et de Descartes sont redondés avec, pour chacun :

- un proxy
- un répartiteur de charge interne
- un répartiteur de charge externe
- une infrastructure DNS/DHCP
- Cœurs de réseau
- Un cluster de 2 firewall



ARTICLE 4. OBJECTIFS

Le ministère a comme objectif d'assurer le maintien en conditions opérationnelles des équipements qui participent à l'infrastructure vitale de l'administration centrale, au travers de prestations de supervision, exploitation, administration et maintenance des composants matériels et logiciels la constituant.

Les orientations stratégiques relatives aux infrastructures de l'administration centrale peuvent se décliner autour des axes majeurs suivants :

- l'appui d'un NOC (Network Operation Center) et d'un SOC (Sécurité Opération Center) de la part du titulaire auprès des équipes du ministère ;
- disposer d'une gestion de configuration maîtrisée ;
- poursuivre les travaux d'élaboration du plan de continuité d'activité ;
- continuer à organiser les services en alignement avec l'organisation ITIL ;
- accompagner l'orientation stratégique technologique en particulier autour des produits Microsoft.

Dans ce cadre, le principal objectif assigné au titulaire est de garantir la sécurité, la disponibilité et la continuité des services de messagerie, des outils collaboratifs, des services DHCP, DNS et de l'accès à Internet, sur la base d'un mode redondé actif.

À ce titre et conformément à son offre, le titulaire propose une vision proactive des organismes vitaux de l'infrastructure centrale. Il propose un dispositif de SIEM (Security Information and Event Management), se doit d'accompagner le ministère et est force de proposition concernant la corrélation de logs et les actions de prévention à réaliser, ainsi que toute action du SOC.

ARTICLE 5. CADRE GENERAL D'EXECUTION DES PRESTATIONS

5.1. NATURE ET ETENDUE DES PRESTATIONS

Dans le cadre du présent marché, le titulaire s'engage à exécuter, conformément à son offre, les missions suivantes :

- **Mission 1** : Initialisation et prise en charge du marché
- **Mission 2** : Pilotage de l'infogérance
- **Mission 3** : Infogérance des infrastructures du ministère
- **Mission 4** : Fourniture de solutions de maintien en condition opérationnelle et d'évolutions des infrastructures et services
- **Mission 5** : Services constructeur
- **Mission 6** : Réversibilité

L'ensemble de ces missions est à réaliser sous la conduite du bureau DNE – AC1.

Une mission (ou une prestation d'une mission) regroupe une ou plusieurs unités d'œuvre (UO).

Les missions (ou les prestations des missions) sont présentées sous la forme suivante :

- **Objet de la mission** (ou de la prestation) : décrit l'objet de la mission, à quel(s) type(s) de prestation(s) elle correspond et sa finalité.
- **Description des services attendus** : précise les tâches principales à réaliser par le titulaire au titre de la mission (ou de la prestation).
- **Niveaux de services attendus** : précise le niveau de service attendu pour la mission (ou la prestation) décrite.
- **Unités d'œuvre (UO)** : liste des unités d'œuvre associées à la mission.
Un niveau de complexité peut être associé à chaque UO. Ce niveau de complexité définit la difficulté ou le volume de la prestation à réaliser. Le niveau de complexité peut être simple, moyen ou complexe.
Les niveaux de complexité sont définis pour chaque mission concernée
- **Livrables** : liste les livrables associés à la mission (ou à la prestation).
- **Délais d'exécution et recette** : précise les délais dans lesquels les livrables de chaque unité d'œuvre sont transmis au ministère. Les délais sont indiqués en **jours ouvrés**.

5.2. CONTRAINTES ET EXIGENCES

5.2.1. *RESPECT DES REFERENTIELS*

Le ministère applique les règles de sécurité étatiques et interministérielles en vigueur et notamment les recommandations de l'agence nationale de la sécurité des systèmes d'information (ANSSI).

Le titulaire s'engage à prendre connaissance et mettre en œuvre les consignes des référentiels d'exigences « Maîtriser les risques de l'infogérance, externalisation des systèmes d'information » (Décembre 2010) et « Prestataires d'audit de la sécurité des systèmes d'information » (version 2.1 du 06 octobre 2015) édités par l'ANSSI.

Le titulaire s'engage également à appliquer les référentiels interministériels (RGS, PSSIE, etc.) et leurs déclinaisons ministérielles communiquées par le ministère.

Dans le cas où, pendant l'exécution du marché, certaines exigences ne seraient pas vérifiées par le titulaire, celui-ci s'engage à en informer le bureau DNE AC1 sans délai et, en tout état de cause, préalablement à toute nouvelle commande.

5.2.2. RESPECT DES PREREQUIS MINISTERIELS

Dans le cadre du marché qui lui est confié le titulaire met en œuvre le référentiel ITIL.

Dans le cadre du marché qui lui est confié, le titulaire s'interdit strictement les actes suivants :

- l'utilisation de comptes génériques d'administrateur sur les actifs en écriture du ministère ;
- le Telnet sur les actifs du ministère. Le cas échéant, proposer la migration sur SSH ;
- la mise en place d'un réseau d'administration de type VPN, sans le passage obligatoire par une console préalablement identifiée et validée par le ministère,
- toute modification de configuration sans log systèmes (l'ensemble des dates, intervenants, actions réalisées doivent être tracés) ;
- la non répudiation des logs (les logs doivent être parfaitement fiables et non modifiables).

Ces interdictions spécifiques du ministère précisent et complètent les prérequis de sécurité de l'ANSSI.

5.2.3. QUALIFICATION DES INTERVENANTS

Conformément à son offre, le titulaire propose, *a minima*, dans le cadre du présent marché :

- une équipe commerciale dirigée par un commercial senior disposant de 5 ans d'expérience minimum dans le domaine de l'infogérance.
- une équipe technique composée de profils de différents niveaux disposant des compétences et certifications nécessaires à la gestion du contrat d'infogérance. Cette équipe technique doit être dirigée par un responsable opérationnel senior disposant de 5 ans d'expérience minimum dans l'infogérance informatique et sécurité.

Dans tous les cas, pour chaque personne composant l'équipe (par exemple les référents techniques) un remplaçant est nommé.

5.2.4. ÉVOLUTIONS PREVUES ET PREVISIBLES DU PERIMETRE DU MARCHE

Le périmètre des infrastructures de l'administration centrale est relativement stabilisé, néanmoins des projets de renouvellement d'équipements et de refonte de système peuvent intervenir durant la durée du marché. Ceci n'exclut pas l'obligation pour le titulaire de maintenir le périmètre qui lui est confié conforme à l'état de l'art et de la technologie existante.

5.3. PILOTAGE ET CONDUITE DES PRESTATIONS

Le pilotage et la conduite du marché s'applique à l'ensemble des prestations décrites dans le présent CCTP et regroupe, outre les réunions des instances de pilotage, les activités liées aux réunions de travail, au suivi et au bilan d'exécution.

Conformément à l'article 11.1.2 du CCAP, le titulaire désigne au sein de son équipe un chef de projet qui est l'interlocuteur privilégié du ministère. Ce chef de projet, qui a notamment pour mission d'assurer le suivi de l'exécution du marché et de veiller à la bonne exécution des prestations, participe aux différentes instances de pilotage et de conduite des prestations, ainsi qu'aux différentes réunions de travail que le ministère planifie.

5.3.1 MODALITES DES ECHANGES ENTRE LE TITULAIRE ET LE MINISTERE

Le ministère met à la disposition du titulaire les informations en sa possession, nécessaires pour mener à bien les prestations demandées.

Le titulaire organise, en outre, les entretiens, échanges et/ou demandes d'information nécessaires pour mener à bien les prestations qui lui sont confiées.

Par dérogation à l'article 3.1 du [CCAG-TIC](#), les notifications de décisions, d'informations ou d'observations faisant courir un délai sont exclusivement réalisées par des moyens dématérialisés permettant de déterminer de façon certaine la date et, le cas échéant, l'heure de leur réception, via le profil d'acheteur ou tout autre moyen de communication électronique (courriel avec accusé de

réception accompagné, le cas échéant, par un dépôt de pièces sur le serveur documentaire du ministère.

En l'absence d'un horodatage permettant de donner une heure certaine à la réception d'un courriel, le destinataire en accuse réception dès qu'il en a connaissance, par retour d'un courriel. La date et l'heure à prendre en compte pour le décompte des délais de réponse ou de traitement des informations est la date de notification (date de réception) ou celle figurant sur le courriel d'accusé de réception.

En cas d'échange par téléphone, le titulaire adresse au ministère, au plus tard dans les 48 heures ouvrées suivant l'appel, soit un courriel reprenant les éléments échangés, soit un compte-rendu d'appel téléphonique.

À cette fin, dans le cadre de la réunion de lancement, le titulaire communique au ministère l'adresse électronique dédiée aux échanges. En cas de modification de ces coordonnées, le titulaire en informe le ministère dans un délai maximum de 24 heures.

Dans le cas où le titulaire se présente sous la forme d'un groupement momentané d'entreprises, la notification de ces informations se fait au mandataire pour l'ensemble des cotraitants.

D'une manière générale, tous les documents transmis au ministère doivent permettre d'identifier sans ambiguïté leur auteur, leur objet, la date de leur réalisation conformément aux dispositions de qualité que le ministère entend voir respecter pour tout élément de documentation et de réalisation concernant le domaine informatique, et sont téléchargeables dans un format exploitable.

- Les formats « Open document Format ». odt, .ods ou .odp doivent être privilégiés pour les documents modifiables. Les formats .docx, .xlsx, .pptx, .csv, .txt et .pdf sont acceptés.
- Le format pdf visualisable et imprimable pour les documents en lecture seule (factures, documentations, etc.).

5.3.2 MOYENS TECHNIQUES

5.3.2.1. Moyens mis à la disposition du titulaire

5.3.2.1.1. Logiciels

Au-delà des équipements du périmètre, le ministère ne met aucun outil spécifique à disposition du titulaire.

5.3.2.1.2. Interventions sur sites

Le ministère octroie au titulaire tous les droits d'accès nécessaires à tous les sites aussi bien en heures ouvrées et non ouvrées en fonction des modalités en vigueur au ministère.

Conformément à l'article 7.1 du CCAP, les frais de transport, repas et hébergement sont à la charge du titulaire pour son personnel.

5.3.2.1.3 Gestion documentaire

Le ministère met à disposition du titulaire un espace dédié sur un site collaboratif permettant le dépôt des livrables et des pièces contractuelles du marché selon le calendrier défini dans le PAQ.

5.3.2.2. Moyens mis à la disposition du ministère par le titulaire

5.3.2.2.1. Outil de supervision

Conformément à son offre, le titulaire met à la disposition du ministère un outil de supervision dans le cadre de la prestation de supervision prévue au titre de la mission 3 (cf. article [6.3.2.1.1.1](#) du présent CCTP).

Cet outil doit permettre au ministère de consulter les alarmes signalant un défaut ainsi que les journaux des incidents survenus sur les infrastructures objet du présent marché.

L'hébergement chez le titulaire, le fonctionnement et le droit d'usage de cet outil pour le ministère sont inclus dans le montant des prestations du marché.

Cet outil est uniquement accessible aux personnes identifiées par le ministère à savoir les représentants du ministère du bureau DNE AC1 (profil administrateur – 7 comptes nominatifs).

5.3.2.2.2. Outil de gestion des tickets et de suivi des incidents

Conformément à son offre, le titulaire met à la disposition du ministère un outil de gestion des tickets et de suivi des incidents dans le cadre de la prestation d'exploitation et d'administration prévue au titre de la mission 3 (cf. article [6.3.2.1.1.2](#) du présent CCTP).

Cet outil doit permettre au ministère de réaliser par lui-même un suivi des demandes d'intervention, signalements et de leur statut (traité, en cours de traitement, non traité) par l'extraction d'une liste récapitulative sur une période donnée.

L'hébergement chez le titulaire, le fonctionnement et le droit d'usage de cet outil pour le ministère sont inclus dans le montant des prestations du marché.

Cet outil est uniquement accessible aux personnes identifiées par le ministère à savoir les représentants du ministère du bureau DNE AC1 (profil administrateur – 7 comptes nominatifs).

Le ministère se réserve la possibilité de refuser la solution proposée par le titulaire et d'en proposer une autre, qu'elle lui soit propre ou non.

5.3.2.2.3. Outil de gestion des configurations

Conformément à son offre, le titulaire met à la disposition du ministère un outil de gestion des configurations, dans le cadre de la prestation de gestion des configurations prévue au titre de la mission 3 (cf. article [6.3.2.1.2.1](#) du présent CCTP).

Cet outil doit permettre au ministère de consulter les enregistrements réalisés par le titulaire.

L'hébergement chez le titulaire, le fonctionnement et le droit d'usage de cet outil pour le ministère sont inclus dans le montant des prestations du marché.

Cet outil est uniquement accessible aux personnes identifiées par le ministère à savoir les représentants du ministère du bureau DNE AC1 (profil administrateur – 7 comptes nominatifs).

5.3.3 MOYENS ORGANISATIONNELS DE PILOTAGE

5.3.3.1. Réunions de travail

Le titulaire participe, pour mener à bien les prestations dont il a la charge, à des réunions de travail qu'il planifie avec le ministère.

Ces réunions se déroulent dans les locaux du ministère à Paris. Des conférences téléphoniques peuvent également être organisées après accord du ministère.

Le titulaire assure la rédaction des documents préparatoires et des comptes rendus de ces réunions.

Les comptes rendus prennent la forme de relevés d'information décision action (RIDA) et sont adressés par courrier électronique ou sur le serveur documentaire du ministère (cf. article [0](#) du présent CCTP) aux représentants concernés du ministère dans un délai de trois (3) jours ouvrés suivant la réunion de travail. Ces comptes rendus sont accompagnés, le cas échéant, de toutes les pièces utiles (ex : supports de présentation, dernières versions, etc.).

Les différentes versions de travail des documents sont notamment identifiées par un numéro, par la date de mise à jour et la désignation du(des) rédacteur(s).

Les services du ministère apportent leur concours et toute la documentation utile au titulaire. Celui-ci peut demander des compléments, apporter ses propres éléments d'éclairage et en effectuer la synthèse.

Sans remarque du ministère dans les cinq (5) jours ouvrés suivant cette transmission, le compte rendu est considéré comme approuvé.

5.3.3.2. Instances de pilotage

Les instances de pilotages sont :

- le comité d'exploitation ;
- le comité de suivi ;
- le comité de pilotage ;
- le comité de projet.

La composition, les attributions et la périodicité des réunions de ces différents comités sont définies dans le cadre de la mission 2 (cf. article [6.2](#) du présent CCTP).

La participation aux instances est obligatoire et effective. Sauf accord du représentant du ministère qui préside l'instance, le représentant du titulaire ne peut pas se prévaloir d'un défaut d'information ou de préparation ou d'une délégation de pouvoir insuffisante pour ne pas prendre ou différer une décision.

5.3.4 INDICATEURS DE PERFORMANCE

Conformément à son offre, le titulaire établit mensuellement un tableau de bord qu'il transmet au comité d'exploitation, par courriel trois (3) jours ouvrés avant la tenue de ce dernier.

Le tableau de bord est un document de synthèse regroupant à la fois le recueil des indicateurs requis et les éléments d'accompagnement nécessaires à leur exploitation.

Le tableau de bord doit apporter une bonne visibilité sur la qualité des prestations.

À ce titre, la qualité de l'intervention et la contribution du titulaire s'expriment au regard des indicateurs suivants :

- La clarté, la lisibilité et la complétude de la documentation produite, ainsi que la gestion du référentiel documentaire ;
- La gestion des montées de niveaux avec la liste des matériels gérés, leur dénomination, version logicielle, le niveau de patch et la date de la dernière mise à jour ;
- La gestion des fins de licence ;
- La gestion des configurations ;
- Le strict respect du contenu, de la qualité et des délais dans la fourniture des livrables ;
- Le suivi des demandes de correction par niveau d'urgence (volumétrie) et la réactivité du titulaire (respect des délais de correction) ;
- La capacité à proposer des profils ayant les compétences et le degré d'expertise requis pour satisfaire à la production des livrables attendus ;
- Le respect des normes et processus en vigueur au sein du ministère.

Lorsque la qualité observée n'est pas dans la cible, des mesures correctives doivent être proposées par le titulaire.

5.3.5 PLAN DE PROGRES

Les parties s'inscrivent dans le cadre d'une démarche d'amélioration continue des prestations du marché.

Ce plan de progrès est intégré au référentiel documentaire du marché.

5.3.5.1. Contenu du plan de progrès

Le plan de progrès s'articule, *a minima*, autour des axes définis, ci-après :

- Axe 1 : l'amélioration de la qualité des prestations.
- Axe 2 : diminution des délais d'exécutions des changements.
- Axe 3 : l'amélioration de l'impact environnemental des prestations.

Ces axes de progrès peuvent être complétés conjointement par les parties dans le cadre du plan de progrès initial. Les axes de progrès sont mesurés à l'aide d'indicateurs de mesure lors des Comités de Pilotage.

5.3.5.2. Mise en œuvre du plan de progrès

5.3.5.2.1. Élaboration du plan de progrès

L'élaboration du plan de progrès est initiée par le titulaire du contrat dans le cadre du premier comité de pilotage.

Il présente des propositions d'amélioration sur les axes définis ci-dessus, conjointement avec le ministère, en tenant compte des retours d'expérience capitalisés à l'issue de la première année d'exécution.

Sur la base de cette proposition, les parties engagent des discussions afin d'élaborer le plan de progrès initial, lequel comprend *a minima*, pour chacun des axes définis, les points suivants :

1) les objectifs ;

- 2) les indicateurs de mesure ;
- 3) les actions à la charge du titulaire ;
- 4) les actions à la charge du ministère ;
- 5) les moyens et ressources mobilisés par chacune des parties ;
- 6) le calendrier prévisionnel de chacune des actions ;
- 7) les modalités de partage des éventuels gains financiers ou autres que financiers.

L'élaboration du plan de progrès est réalisée, par la suite, dans le cadre des réunions du comité d'exploitation afin d'affiner les axes d'amélioration en identifiant les objectifs et indicateurs associés et en déclinant les différentes propositions permettant l'atteinte de ces objectifs dans un plan d'actions.

Une fois finalisé, le plan de progrès est validé par les parties dans le cadre du comité de suivi et intégré aux documents contractuels du marché selon les modalités ci-après :

- Dans l'hypothèse où le plan de progrès conduirait à modifier les stipulations du marché, notamment les conditions d'exécution il donne lieu à la conclusion d'un acte modificatif dans le cadre de la clause de réexamen définie à l'article 23 du CCAP.
- Dans le cas où le plan de progrès n'entraîne aucune modification des stipulations du marché, le plan de progrès est formalisé par un simple échange de courrier entre les parties.

En cours d'exécution du marché, le titulaire est tenu d'exécuter les décisions arrêtées au titre du plan de progrès.

5.3.5.2.2. Suivi et pilotage du plan de progrès

Les parties conviennent d'opérer un suivi régulier des actions mises en œuvre et d'établir semestriellement, dans le cadre du comité de suivi, un bilan du plan de progrès élaboré conjointement.

Ce bilan détaille notamment les actions engagées, les résultats constatés, les difficultés rencontrées et le cas échéant propose des ajustements du plan de progrès initial.

5.4. LANGUE DE TRAVAIL

La langue de travail est exclusivement le français, à l'oral et à l'écrit. Toutefois, les anglicismes liés aux méthodes de travail ou techniques informatiques sont autorisés.

5.5. LIEUX D'EXECUTION DES PRESTATIONS

5.5.1. PRESTATIONS

La mission d'initialisation se déroule dans les locaux du ministère, à Paris ou en région parisienne. Exceptionnellement, cette réunion peut se dérouler dans le cadre d'une visioconférence organisée par le ministère.

Les autres prestations s'exécutent dans les locaux du ministère à Paris ou en région parisienne et dans ceux du titulaire.

5.5.2. REUNIONS

Les réunions pour lesquelles la présence du titulaire ou de son représentant est requise (ex : réunions des instances de pilotage, etc.) se déroulent en présentiel dans les locaux du ministère à Paris ou en région parisienne.

Les réunions en présentiel peuvent être remplacées par des réunions à distance selon les moyens techniques de téléconférence (audioconférence, visioconférence notamment) définis conjointement par les parties.

5.6. EXIGENCES LIEES AUX PERSONNELS DU TITULAIRE ET DE SES SOUS-TRAITANTS

Le personnel du titulaire ou de ses sous-traitants est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie.

Le personnel du titulaire ou de ses sous-traitants doit avertir le ministère, dans les meilleurs délais, de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, une infection de son poste, etc.

La connexion d'équipements non maîtrisés, non administrés ou non mis à jour par le ministère (qu'il s'agisse d'ordiphones, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles) en filaire ou en wifi sur les réseaux professionnels du ministère est autorisée uniquement sur les VLAN, mis en œuvre pour les invités.

Par ailleurs, le ministère rappelle qu'Internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'Internet (par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors du ministère.

5.7. STANDARDS ET NORMES – PLANS D'ASSURANCE QUALITE ET SECURITE

Il est attendu de la part du Titulaire qu'il veille, lors de l'exécution des travaux et de la production des livrables (documentaires et logiciels), à respecter scrupuleusement les standards et normes en vigueur pour le ministère, en particulier en matière de :

- Sécurité et confidentialité des données ;
- Ergonomie et accessibilité des applications ;
- Interopérabilité et performance des SI ;
- Dispositions environnementales.

L'ensemble des dispositifs mis en œuvre pour respecter et contrôler le respect de ces exigences est formalisé dans un plan d'assurance qualité (PAQ), une convention de service (CdS) et plan d'assurance sécurité (PAS) dont une première version est fournie au stade de l'offre, mise au point et complétée lors de la phase d'initialisation, puis mis à jour tout au long de l'exécution du marché.

5.8. LIVRAISON, VERIFICATION ET ADMISSION DES PRESTATIONS

5.8.1. CONDITIONS DE LIVRAISON

Si le ministère l'estime nécessaire, une livraison peut donner lieu à une réunion organisée par le ministère, dans ses locaux, le jour prévu de la livraison ou la veille de la livraison.

La livraison a lieu au plus tard le dernier jour du « délai maximum de production des livrables » ou sur demande du titulaire s'il souhaite avancer la date.

Les livrables sont remis sous une forme dématérialisée selon les modalités décrites à l'article [5.3.1](#) du présent CCTP.

Les livrables sont, sans que cette liste soit exhaustive, les documentations techniques, les comptes rendus d'ateliers, etc.

Les livrables doivent être pertinents et fonctionnellement vérifiables.

5.8.2. CONDITIONS DE VERIFICATION ET D'ADMISSION DES PRESTATIONS

Par dérogation à l'article 30.3 du [CCAG-TIC](#), le ministère n'est pas tenu d'aviser le titulaire des jour et heure fixés pour procéder aux opérations de vérification.

Les opérations de vérification quantitative, notamment pour ce qui concerne les prestations de la mission 4, ont pour objet de contrôler la conformité entre la quantité livrée ou le travail fait et la quantité ou le travail commandé par le ministère.

La mise en conformité quantitative ne fait pas obstacle à l'exécution des opérations de vérification qualitatives des matériels livrés.

Les opérations de vérification qualitative ont pour objet de permettre au ministère de contrôler que les moyens mis en œuvre par le titulaire et les prestations qu'il a réalisées sont conformes aux prescriptions des documents du marché, notamment au regard de sa politique de sécurité.

Par dérogation à l'article 32.1 du [CCAG-TIC](#), la vérification porte notamment sur le contenu, la forme et la qualité des produits livrés.

Par dérogation à l'article 30.1 du [CCAG-TIC](#), le point de départ des opérations de vérification est la date de la livraison ou de mise en service.

À l'issue de la phase de vérification qualitative qu'il organise, le ministère procède à l'admission formelle des prestations de chaque mission au fur et à mesure de la production des livrables et selon les délais d'admission définis pour les unités d'œuvre correspondantes.

Cette admission est matérialisée par un procès-verbal d'admission définitive, établi par le ministère lorsque l'ensemble de la prestation commandée est approuvé. Ce procès-verbal constate que le résultat des opérations réalisées par le titulaire est conforme aux attentes et que la qualité de sa prestation est approuvée.

Par dérogation à l'article 34 du [CCAG-TIC](#), pour chacune des missions un tableau figurant sous les articles « Délais et admission » précise les délais de production des livrables, d'admission et de correction applicables.

- Le titulaire dispose du nombre de jours prévus dans la colonne « Délai maximum de production des livrables » de ces tableaux pour remettre au ministère lesdits livrables.
- Par dérogation aux articles 34.1 et 34.2 du [CCAG-TIC](#), le ministère dispose, à compter de la livraison, du nombre de jours fixés dans la colonne « Délai maximum d'admission du ministère » de ces tableaux pour transmettre au titulaire des observations et/ou des demandes de correction.
- Par dérogation à l'article 34.2 du [CCAG-TIC](#), le titulaire dispose, à compter de la réception des observations du ministère, du nombre de jours prévus dans la colonne « Délai de correction éventuelle du titulaire » de ces tableaux pour intégrer les observations et/ou les demandes de correction et présenter les solutions susceptibles de mener à la bonne réalisation des prestations demandées. Il peut, notamment, proposer le remplacement d'un ou des collaborateur(s) désigné(s) pour la mise en œuvre des prestations objet du présent marché.

Après analyse de ces propositions, le ministère peut décider :

- soit d'ajourner une nouvelle fois l'admission des prestations : le titulaire dispose à nouveau du nombre de jours indiqué dans la colonne « délai de correction éventuelle » pour corriger les livrables et les transmettre de nouveau au ministère ;
- soit de résilier le marché, conformément à l'article 21 du CCAP.

Tout dépassement de délai est passible des pénalités de retard prévues à l'article 16.1 du CCAP.

ARTICLE 6. **NATURE DES PRESTATIONS ATTENDUES**

Le marché comprend les prestations suivantes :

- les prestations uniques, qui ne sont réalisées qu'une seule fois pendant la durée du marché.
- les prestations récurrentes, qui concernent toutes les tâches récurrentes réalisées par le titulaire, jusqu'à la fin du marché, dans le cadre de ses prestations d'infogérance, pour le maintien en conditions opérationnelles de l'infrastructure de sécurité du ministère.

La description des services récurrents attendus, comprend les services relatifs à la production en continu, le contrôle de ceux-ci et les changements induits ainsi que la sécurité de l'information (supervision, prévention, détection, alerte, remédiation et rapports).

Il est précisé que les mises à jour de correctifs, patches (mises en production majeures annuelles, service packs, hot packages, etc.) sont réalisés par le titulaire dans le cadre des services récurrents.

- les prestations à la demande, qui concernent des actions ponctuelles, réalisées par le titulaire dans le cadre du présent marché.

Conformément à son offre, le titulaire met en œuvre l'organisation et le fonctionnement lui permettant de garantir la continuité d'exploitation dans le respect des engagements de service définis et de contribuer, par leur exécution, à la réalisation des actions d'amélioration de service et d'industrialisation telles que définies dans le plan de progrès.

Mission	Réurrence des UO
M1 – Initialisation et prise en charge du marché	Commandée une seule fois
M2 – Pilotage de l'infogérance	Récurrentes
M3 – Infogérance des infrastructures du ministère	Récurrentes et à la demande
M4 – Fourniture de solutions de MCO et d'évolution des infrastructures et services	A la demande
M5 – Services constructeurs	Récurrentes
M6 - Réversibilité	Commandée une seule fois

6.1. MISSION 1 : INITIALISATION ET PRISE EN CHARGE DU MARCHE

6.1.1. OBJET DE LA MISSION 1

La mission 1 a pour objet de permettre au titulaire de prendre connaissance de l'existant, de mettre en place l'organisation et les outils permettant la réalisation des prestations de la mission 3 (Infogérance des infrastructures du ministère), de proposer et valider avec le ministère le référentiel documentaire, de mettre en place avec le ministère les modalités de gouvernance du marché.

La mission 1 est une prestation unique. La phase d'initialisation est de 43 jours ouvrés maximum, dont 30 jours ouvrés maximum entre la réunion de lancement et la réunion de clôture de cette phase.

6.1.2. DESCRIPTION DES SERVICES ATTENDUS

Conformément à son offre, le titulaire réalise, selon les modalités décrites ci-après, les prestations attendues au titre de la mission 1, à savoir :

- participation à la réunion de lancement (M1.1) ;
- prise de connaissance du contexte du marché (M1.2) ;
- mise en place de l'organisation et de la gouvernance du marché (M1.3) ;
- participation à la réunion de clôture de la phase de prise en charge (M1.4).

6.1.2.1. Réunion de lancement (M1.1)

Dans les dix (10) jours ouvrés suivants la réception du bon de commande le ministère initie avec le titulaire une réunion de lancement, soit dans les locaux du ministère à Paris ou en région parisienne, soit en distanciel par visio-conférence. Dans ce dernier cas, le ministère communique au titulaire les liens permettant d'installer les outils numériques du ministère.

Le titulaire rédige l'ordre du jour et les supports nécessaires à la tenue de la réunion de lancement, qu'il adresse au ministère trois (3) jours ouvrés avant la tenue de cette dernière.

Cette réunion de lancement permet aux deux parties de définir ensemble le dispositif à mettre en place pour l'exécution du marché, conformément aux dispositions des documents contractuels.

Au cours de cette réunion de lancement, le titulaire doit notamment :

- désigner le chef de projet, lequel est l'interlocuteur privilégié du ministère ou de son représentant désigné ;

- présenter les outils mis à la disposition du ministère et décrits à l'article [5.3.2.2](#) du présent CCTP (outil de gestion des tickets et de suivi des incidents, outil de gestion des configurations, outil de supervision, etc.) ;
- commenter le plan d'assurance qualité (PAQ) fourni dans son offre et collecter les remarques du ministère sur ce document en vue de sa finalisation (version V1), notamment en ce qui concerne :
 - l'équipe définitive en charge de la réalisation des prestations (pour chacun des intervenants présentation de leur(s) rôle(s), leur(s) responsabilité(s), leur(s) attribution(s). Les profils de cette équipe doivent être conformes à ceux présentés dans son offre ;
 - la méthodologie retenue pour préparer et réaliser les prestations du marché,
 - les processus de coordination et les modalités d'interaction retenus entre le titulaire et le ministère et l'organisation des différents comités prévus à la mission 2 ;
 - le calendrier prévisionnel de travail de la mission 1
 - la mise en place, conjointement avec le ministère, des indicateurs de suivi et de pilotage.
 - les modalités d'échange entre le titulaire et le ministère ;
- présenter le document récapitulatif des niveaux de services ;
- présenter l'organisation de la transition et le plan d'accompagnement au changement ;
- présenter le plan de réversibilité entrante ;
- présenter le plan de communication qu'il met en place a minima une fois par an à l'attention des usagers du ministère.

À l'issue de la réunion de lancement, le titulaire dispose d'un délai de cinq (5) jours ouvrés pour rédiger et transmettre au ministère un compte rendu comprenant a minima les modifications éventuelles à apporter aux documents qu'il a présentés.

Ce compte rendu est accompagné, le cas échéant, de toutes les pièces utiles (ex : supports de présentation, etc.).

Sans remarque du ministère dans les sept (7) jours ouvrés suivant sa transmission, le compte-rendu est considéré comme approuvé.

Dans le cas où le ministère formule des remarques sur ce compte-rendu, le chef de projet du titulaire dispose d'un délai de trois (3) jours ouvrés pour lui transmettre une version corrigée.

6.1.2.2. Prise de connaissance du contexte du marché (M1.2)

À ce titre, le ministère met à la disposition du titulaire toute documentation utile à la réalisation de cette prestation.

Pour mener à bien celle-ci, le titulaire étudie l'ensemble de la documentation mise à sa disposition et organise les ateliers et entretiens nécessaires à la prise de connaissance du contexte et des caractéristiques des infrastructures objet du présent marché. Dans ce cadre, le titulaire peut être amené à travailler avec le prestataire sortant.

À l'issue de cette phase, le titulaire rédige un bilan de prise de connaissance comportant notamment :

- une description de l'ensemble des conditions et prérequis nécessaires à la bonne exécution du marché ;
- une présentation détaillée de l'organisation et des moyens techniques et humains mis en place pour assurer l'ensemble des prestations objet de la mission 3 (phase opérationnelle) tenant compte des connaissances acquises. Cette présentation doit être prise en compte par le titulaire dans la finalisation de son PAQ ;
- un bilan, comportant :
 - une analyse de l'infrastructure de sécurité de l'administration centrale et des configurations existantes associées ;
 - une analyse de la documentation et des procédures existantes ;
 - un guide d'amélioration de la documentation et des procédures existantes ;
 - une évaluation du niveau actuel de sécurité des infrastructures du périmètre ;
 - une analyse des pistes d'amélioration de cette infrastructure de sécurité ;

- un document décrivant de manière exhaustive la liste initiale des licences et contrat de maintenance relatives aux infrastructures du marché.

Tous les intervenants du titulaire (responsable opérationnel, chef de projet, techniciens, consultants, etc.), ses éventuels sous-traitants et tous leurs intervenants sont réputés disposer du même niveau de connaissance du contexte du ministère pendant toute la durée du marché.

6.1.2.3. Mise en place de l'organisation et de la gouvernance du marché (M1.3)

Dans le cadre de cette prestation, le titulaire :

- élabore le référentiel documentaire du marché ;
- met en place les processus d'échanges et de suivi des prestations.

6.1.2.3.1. Élaboration du référentiel documentaire du marché

À l'issue de la réunion de lancement au cours de laquelle les modèles et processus ont été présentés, le titulaire finalise les différents documents à mettre en œuvre dans le cadre des différentes missions du marché et les soumet pour validation au ministère.

Ce référentiel comporte notamment, sans que cette liste soit exhaustive :

- le plan d'assurance qualité mis à jour (au minimum deux fois par an) ;
- le plan d'assurance sécurité mis à jour ;
- la convention de service ;
- le plan de réversibilité entrante mis à jour (au minimum deux fois par an) ;
- les trames des tableaux de bord fournis lors des comités de gestion des services ;
- les modèles de livrables ;
- le plan de progrès ;
- les pièces contractuelles du présent marché ;
- etc.

Ce référentiel documentaire est accessible par les représentants du ministère, à partir d'un espace partagé fourni par le ministère (cf. article [9](#) du présent CCTP).

Il appartient au titulaire de veiller à l'exhaustivité de ce référentiel et de le mettre à jour.

Cette gestion documentaire est assortie d'un indicateur contractuel pénalisable.

6.1.2.3.2. Finalisation du plan d'assurance qualité (PAQ)

Le PAQ est un document contractuel, mis à jour régulièrement par le titulaire et matérialisant la gestion de la qualité dans le cadre du présent marché.

Le PAQ s'applique à l'ensemble des équipes du titulaire, y compris ses sous-traitants éventuels.

Le titulaire fournit une version finalisée V1 du PAQ (la version V0 figurant dans l'offre du titulaire) en conformité avec les exigences de qualité minimum formulées par le ministère au cours de la réunion de lancement.

Ce PAQ doit au minimum contenir les éléments suivants :

- la présentation du document (objet du PAQ, procédure d'approbation, procédure d'évolution, modalités de diffusion, etc.) ;
- la présentation et l'organisation du marché, comprenant notamment :
 - l'objet du marché (contexte, objectifs et contraintes, attentes spécifiques, et conditions de réalisation) ;
 - l'organisation du ministère (organigramme, principaux contacts, etc.) ;
 - l'organisation du titulaire et des éventuels sous-traitants (organisation, organigramme, rôles et responsabilités, ainsi que, le cas échéant, le service d'assistance, etc.) ;
- la présentation de la méthodologie de réalisation des prestations, décrivant notamment :
 - les différentes phases de réalisation des prestations ;
 - la description du processus de réalisation de chacune des prestations avec l'ensemble des actions à mener. Pour chaque action, sont définis les objectifs, les tâches, les responsabilités, les conditions de vérification avant le passage à l'action suivante. Le cas échéant, la description d'une action peut renvoyer à la description des modalités de

sécurité mises en œuvre dans le cadre du présent marché dans le cadre du plan d'assurance sécurité (PAS) ;

- la phase de livraison ;
- les modalités d'admission conformément aux exigences de délais et d'organisation indiqués dans le présent CCTP ;
- la stratégie de recette et de plan de tests du paramétrage des outils de mesure et validation des niveaux de services contractuels ;
- la maîtrise des livrables (format, modalités de remise des livrables, circuit d'approbation, traitement des remarques, diffusion, etc.) ;
- la traçabilité des opérations de vérification avant livraison, les contrôles/revues, les dérogations spécifiques, l'amélioration continue ;
- la description des principes et des modalités de gestion des risques, des modifications, des non-conformités, des ressources, qui sont partie prenante dans la réalisation des prestations ;
- les modalités des échanges avec le ministère ;
- la gestion des sous-traitants ;
- la présentation du pilotage du marché décrivant notamment :
 - les modalités de réunions de travail et de gouvernance ;
 - les instances de communication externe (avec le ministère) et interne (entre l'équipe projet du titulaire) ;
 - les modalités de suivi des commandes et de la facturation ;
 - les outils de suivi (modèles de tableaux de bord, etc.) et de pilotage ainsi que les indicateurs servant à mesurer l'atteinte des objectifs. Pour chaque indicateur, une valeur de référence doit être donnée ;
 - les modalités de propositions d'amélioration du marché.
- La présentation de la procédure de mise à jour du référentiel documentaire incluant le PAQ.

En cas de non-respect des dispositions du PAQ en vigueur, une pénalité peut être prononcée en application de l'article 16 du CCAP.

De même, si la cause du non-respect des dispositions du PAQ n'est pas corrigée dans un délai de cinq (5) jours ouvrés, une pénalité de retard peut être prononcée en application de l'article 16 du CCAP.

6.1.2.3.3. Finalisation du plan d'assurance sécurité (PAS)

Le titulaire s'engage à exécuter ses obligations concernant la sécurité selon le plan d'assurance sécurité, dénommé PAS défini ci-après.

Le PAS est un document contractuel matérialisant la gestion de la sécurité par le titulaire dans le cadre du présent marché.

Le PAS s'applique à l'ensemble des équipes du titulaire, y compris ses sous-traitants éventuels.

Le titulaire est responsable de la rédaction initiale du PAS ainsi que de ses évolutions nécessaires pour satisfaire aux exigences de sécurité du ministère pendant toute la durée du marché.

Le titulaire fournit une version finalisée V1 du plan d'assurance sécurité (PAS) (la version V0 figurant dans son offre) en conformité avec les minimums d'exigences de sécurité minimum formulées par le ministère.

Ce PAS doit, au minimum, contenir les éléments suivants :

- La présentation de l'organisation générale mise en place par le titulaire en matière de sécurité par l'établissement des rôles et responsabilités de chacun des intervenants, des principales tâches associées, des modalités de contact (identification des contacts technique et décisionnel), les modalités de remplacement des personnels, etc. ;
- L'identification des risques associés à la réalisation des prestations du marché ;
- La méthodologie (mesures techniques, organisationnelles et procédurales) mise en œuvre pour gérer la sécurité (chaîne des responsabilités, sensibilisation et formation des personnels, contrôle

des accès, modalités d'authentification, règles de gestion des droits d'accès, sécurisation des communications, etc.) ;

- La matrice de couverture des exigences de sécurité ;
- Les modalités d'application du PAS, l'étendue de sa diffusion et les conditions de son évolution, notamment en ce qui concerne le circuit d'approbation des modifications ;
- La description de la documentation concernant la sécurité, fournie au titre du présent marché ;
- Les modalités d'hébergement des outils (gestion des incidents, supervision, etc.), en particulier la répartition géographique des Datacenter du titulaire, le cas échéant le prestataire en charge de ces derniers ;
- Les modalités de plans de reprise informatique prévus en cas de sinistre d'un ou plusieurs Datacenter, ainsi que les délais de rétablissement du service ;
- Les mesures prises contre les attaques pouvant conduire à une indisponibilité du service (ex : DDOS, etc.).

En cas de non-respect des dispositions du PAS en vigueur, une pénalité peut être prononcée en application de l'article 16 du CCAP.

De même, si la cause du non-respect des dispositions du PAS n'est pas corrigée dans un délai de cinq (5) jours ouvrés, une pénalité de retard peut être prononcée en application de l'article 16 du CCAP.

6.1.2.3.4.Finalisation de la convention de service

La convention de service contient impérativement pour chaque groupe de services :

- le rappel du périmètre concerné (inclus/exclu) et les horaires de service ;
- la présentation complète des services fournis ;
- un tableau reprenant par service les rôles et responsabilités réciproques du ministère et du titulaire (matrices de responsabilité) ;
- un tableau précisant les indicateurs qui sont fournis et les niveaux de service contractuels ;
- le mode de calcul des principaux indicateurs ;
- la description de l'ensemble des conditions et prérequis nécessaires au démarrage de la mission 3 (Infogérance des infrastructures du ministère) ;
- le document de récapitulation des niveaux de services ;
- les processus de coordination et les modalités d'interaction retenus entre le titulaire et le ministère ;
- l'organisation des différents comités de gestion des services prévus ;
- les schémas détaillés de l'infrastructure de sécurité du périmètre ;
- les procédures et modes opératoires pour réaliser les prestations ;
- les procédures d'escalade ;
- commentaires éventuels.

La convention de service est un document contractuel. Elle est mise à jour régulièrement. Elle matérialise le catalogue des services disponibles.

La non atteinte des niveaux de services contractuels est pénalisable selon les modalités prévues au cahier des clauses administratives particulières.

6.1.2.3.5.Mise en place du processus d'échanges et de suivi des prestations

Conformément à son offre, le titulaire s'engage à mettre en œuvre les procédures de coordination et d'échange avec le ministère, les consignes, les formulaires et documentations associés aux prestations récurrentes de la mission 3 et aux prestations à la demande des missions 4 et 5, tels que décrits dans le PAQ et le PAS et couvrant notamment :

- les différents niveaux d'intervention ;
- les modalités de validation des demandes ;
- les outils mis en place ;

- les modalités de catégorisation, de gestion et d'archivage des événements détectés dans le cadre des prestations ;
- les procédures et modes opératoires pour réaliser les prestations ;
- les procédures d'escalade ;
- la mise à disposition d'un extranet permettant au ministère de consulter l'ensemble des rapports demandés ;
- la mise à disposition de la console déportée de supervision dans les locaux du ministère lui permettant uniquement de consulter en temps réel les événements du périmètre ;
- la présentation et l'initialisation de l'outil de CMDB (Configuration Management Database au sens ITIL du terme) ;
- la stratégie de recette et de plan de tests du paramétrage des outils de mesure et validation des niveaux de services contractuels ;

Le titulaire établit une liaison permanente entre son point de supervision et le point d'accès au réseau du ministère. En cas d'incident sur cette liaison, un accès de secours est prévu par le titulaire pour permettre aux services de supervision de continuer à fonctionner. Le point d'accès devra être assez performant et redondé pour recevoir tous les logs des équipements sans impacter sur la performance de la supervision et des actions d'exploitation.

6.1.2.4. Réunion de clôture de la phase de prise en charge (M1.4)

Le titulaire organise et anime, dans les 30 jours ouvrés suivant la réunion de lancement, une réunion de clôture de la phase de prise en charge, soit dans les locaux du ministère à Paris ou en région parisienne, soit en distanciel par visio-conférence. Dans ce dernier cas, le ministère communique au titulaire les liens permettant d'installer les outils numériques du ministère. Cette réunion de clôture marque la bascule de responsabilité entre le titulaire sortant et le titulaire entrant.

Le titulaire rédige les supports nécessaires à la tenue de cette réunion de clôture, qu'il adresse au ministère cinq (5) jours ouvrés avant la tenue de cette dernière.

Au cours de cette réunion de clôture, le titulaire doit notamment :

- déclinier opérationnellement les enjeux de cette phase de transition et de démarrage des prestations ainsi que les objectifs du ministère énoncés à l'article 4 ci-dessus, de la manière suivante :
 - organisation du traitement sans rupture des incidents ;
 - mise en place d'une incidentologie outillée ;
 - industrialisation du niveau 1, notamment en y ramenant des incidents traités au niveau 2 ;
 - réalisation d'une détection proactive des incidents ;
 - dépersonnalisation du service rendu au moyen de modes opératoires (tous les actes élémentaires de supervision, d'administration et d'exploitation).
- fournir les versions mises à jour et validées des documents suivants :
 - la convention de services (cf. 6.1.2.3.4 « Convention de service » du présent CCTP) ;
 - le plan d'assurance qualité ;
 - le plan d'assurance sécurité ;
 - les trames des tableaux de bord fournis lors des comités de gestion des services ;
 - les configurations des infrastructures du périmètre ;
 - les schémas détaillés de l'infrastructure de sécurité du périmètre ;
 - la description du processus inhérent à la CMDB permettant d'assurer le suivi et la maintenance relatifs aux infrastructures du périmètre.

À l'issue de la réunion de clôture, le titulaire dispose d'un délai de trois (3) jours ouvrés pour rédiger et transmettre au ministère un compte rendu accompagné, le cas échéant, de toutes les pièces utiles (ex : supports de présentation, etc.).

Sans remarque du ministère dans les sept (7) jours ouvrés suivant sa transmission, le compte-rendu est considéré comme approuvé.

Dans le cas où le ministère formule des remarques sur ce compte-rendu, le chef de projet du titulaire dispose d'un délai de trois (3) jours ouvrés pour lui transmettre une version corrigée.

6.1.3. ROLES ET RESPONSABILITES

Le tableau précise les principales responsabilités entre, d'une part, le titulaire et d'autre part, le ministère.

(R = Réalise ; A = Approuve ; C = Contribue ; I = est Informé)

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Réunion de lancement (M1.1)		
Préparer et transmettre au ministère l'ordre du jour et les supports de présentation	R	CA
Animer la réunion de lancement	R	CA
Préparer et transmettre au ministère le compte rendu de réunion	R	A
Prise de connaissance (M1.2)		
Mise à disposition de la documentation nécessaire		R
Organise les ateliers nécessaires à la prise de connaissance	R	C
Rédige et présente un bilan de prise de connaissance	R	A
Mise en place de l'organisation et de la gouvernance du marché (M1.3)		
Élaboration du référentiel documentaire	R	A
Mise en place du processus d'échanges et de suivi des prestations	R	A
Réunion de clôture (M1.4)		
Préparer et transmettre au ministère l'ordre du jour et les supports de présentation	R	CA
Animer la réunion de clôture	R	CA
Préparer et transmettre au ministère le compte rendu de réunion	R	A

6.1.4. NIVEAUX DE SERVICE

Sans objet.

6.1.5. UNITES D'ŒUVRE

Les prestations uniques de la mission 1 correspondent à l'unité d'œuvre suivante :

Code UO	UO
M1-PU01	Initialisation et prise en charge du marché

6.1.6. LIVRABLES

Le titulaire remet au ministère les livrables suivants :

- Au titre de la réunion de lancement (M1.1)
 - l'ordre du jour et les supports de la réunion de lancement ;
 - le compte-rendu et les supports de présentation de la réunion de lancement ;
 - la liste nominative des personnes constituant son équipe projet, accompagnée des curriculums vitae, et les rôles et attributions de chacun (correspondant aux profils prévus dans son offre) ;
 - le calendrier prévisionnel de travail de la mission 1.

- Au titre de la prise de connaissance (M1.2)
 - le bilan de prise de connaissance défini à l'article [6.1.2.2](#) du présent CCTP.

- Au titre de la mise en place de l'organisation et de la gouvernance du marché (M1.3)
 - le plan d'assurance qualité mis à jour (au minimum deux fois par an) ;
 - le plan d'assurance sécurité mis à jour ;
 - la convention de service ;
 - le plan de réversibilité entrante mis à jour (au minimum deux fois par an) ;
 - les trames des tableaux de bord fournis lors des comités de gestion des services ;
 - le PV de transfert de contrat de maintenance.

- Au titre de la réunion de clôture (M1.4)
 - le support de présentation de la réunion de clôture ;
 - le compte-rendu de la réunion de clôture ;
 - le document actualisé précisant les configurations des infrastructures du périmètre ;
 - les schémas détaillés actualisés de l'infrastructure de sécurité du périmètre ;
 - le processus inhérent à l'outil de gestion des configurations (cf. article [6.3.2.1.2.1](#) du présent CCTP), permettant d'assurer le suivi et la maintenance relatifs aux infrastructures du périmètre ;
 - Le PV de bascule de responsabilité signé.

6.1.7. DELAIS D'EXECUTION ET D'ADMISSION

La mission 1 n'a lieu qu'une seule fois pour toute la durée du marché. Elle débute à la réception par le titulaire du bon de commande établi par le ministère et s'achève au plus tard dans un délai de quarante-trois (43) jours ouvrés (hors délais de recette et de correction) à compter de cette date.

Le titulaire doit organiser une réunion de lancement avec les représentants du ministère, selon les modalités décrites à l'article 6.1.2.1 du présent CCTP, dans un délai maximum de dix (10) jours ouvrés suivant la réception du bon de commande.

Les prestations de la mission 1 doivent être réalisées dans les délais mentionnés dans le tableau ci-dessous :

M1 / UO	Livrables	Délai maximum de production des livrables (*)	Délais d'admission du ministère (*)	Délais de correction éventuelle du titulaire (*)
M1-PU01	Ordre du jour et supports de la réunion de lancement (M1.1).	3 jours avant la tenue de la réunion de lancement	7 jours	3 jours
	Liste nominative des intervenants du titulaire et leurs curriculum vitae correspondant aux profils prévus dans l'offre du titulaire (M1.1).	5 jours à l'issue de la réunion de lancement	7 jours	3 jours

M1 / UO	Livrables	Délai maximum de production des livrables (*)	Délais d'admission du ministère (*)	Délais de correction éventuelle du titulaire (*)
	Méthodologie définitive retenue pour réaliser les différentes missions (M1.1).			
	Compte-rendu de la réunion de lancement et supports de présentation (M1.1).			
	Bilan de prise de connaissance (M1.2)	5 jours avant la réunion de clôture	7 jours	3 jours
	Référentiel documentaire (M1.3)	5 jours Avant la réunion de clôture	7 jours	3 jours
	Support de présentation de la réunion de clôture (M1.4)	5 jours Avant la réunion de clôture	7 jours	7 jours
	Compte-rendu de la réunion de clôture et supports de présentation (M1.4)	3 jours Après la réunion de clôture	7 jours	3 jours
	Document actualisé précisant les configurations des infrastructures du périmètre (M1.4)	5 jours après la réunion de clôture	7 jours	3 jours
	Schémas détaillés actualisés de l'infrastructure de sécurité du périmètre (M1.4)	5 jours après la réunion de clôture	7 jours	3 jours
	Processus inhérent à l'outil de gestion des configurations (M1.4)	5 jours après la réunion de clôture	7 jours	3 jours
	PV de bascule de responsabilité signé (M1.4)	5 jours après la réunion de clôture	7 jours	3 jours

(*) Les délais s'expriment en jours ouvrés.

L'admission a pour objet de valider le contenu, la forme et la qualité des produits livrés. Elle est constatée de manière expresse par le ministère et matérialisée par un procès-verbal d'admission définitive selon les conditions d'admission précisées à l'article 5.8 du présent CCTP.

En cas de dépassement des délais, des pénalités de retard sont appliquées conformément à l'article 16 du CCAP.

6.2. MISSION 2 : PILOTAGE DE L'INFOGERANCE

6.2.1. OBJET DE LA MISSION 2

La mission 2 a pour objet de définir les conditions dans lesquelles le titulaire réalise les opérations de pilotage de l'infogérance des infrastructures du ministère.

Cette mission est constituée de prestations récurrentes.

6.2.2. DESCRIPTION DES SERVICES ATTENDUS

Le titulaire assure la direction, le contrôle et la coordination de l'exécution du contrat d'infogérance.

Le responsable opérationnel du titulaire réalise les prestations suivantes :

- définition et mise en œuvre des processus et solutions nécessaires pour réaliser les prestations ;
- réalisation des choix techniques à mettre en œuvre pour assurer l'adéquation de ses prestations au présent marché ;
- garantie du niveau de qualité tel que convenu par les parties dans la convention de services ;
- vérification du respect du planning et des délais ;
- pilotage et coordination de ses différentes équipes, de celles de ses sous-traitants éventuels ou prestataires tiers intervenant dans l'exécution du marché (mainteneurs matériels du ministère, éditeurs du ministère), en cohérence avec le planning et les niveaux de services contractuels ;
- maintien d'un état permanent de réversibilité des prestations ;
- création et maintien à jour de la documentation nécessaire à la bonne exécution des prestations, notamment le plan de réversibilité ;
- information rapide du ministère de tout événement et/ou fait de nature à compromettre la bonne exécution des prestations et prise des mesures nécessaires pour y remédier ;
- rendre compte régulièrement lors des comités définis de l'exécution des services d'infogérance et des éventuelles difficultés rencontrées ;
- mise en œuvre d'une solution de présentation en ligne sécurisée des informations opérationnelles et de pilotage des prestations ;
- proposition et fourniture une fois par an d'une étude basée sur une veille technologique et les actualités des sujets SSI.

6.2.2.1. Synthèse de la gouvernance attendue

Comité	Fréquence	Rapports présentés	Niveaux de service
COMEX	Mensuelle (sauf si COSUI)	Rapport mensuel Retours d'expérience Documentation	MOE1 - Fourniture du rapport mensuel complet MOE4- Fourniture d'un état exhaustif et à jour de la documentation MOE5 – Fourniture d'un état exhaustif et à jour de gestion de parc MOE7 – Fourniture d'un état de prévision des évolutions du parc (capacity planning) USE1 – Taux de prise d'appel USE2 - Temps de décrocher USE3 - Temps de réponse des demandes émises via le portail USE4 – Pertinence de la catégorisation des tickets USE5 - Dossiers résolus lors du premier contact USE6 - Temps de résolution USE7 - Temps de résolution des dossiers bloquants USE8 - Délai de transmission au support approprié SUP1 - Délai de prise en compte d'un incident et délai de transfert au service concerné SUP2 – Détection des incidents SUP3- Taux de traitement des incidents dans les délais SUP4- Fourniture des tableaux de bord relatifs aux incidents RES1 - Taux de disponibilité des infrastructures de Sécurité RES2 – Fourniture des rapports d'incidents mineurs RES3 – Fourniture des rapports d'incidents majeurs RES5 – Fourniture d'un état à jour sur la gestion des montées de niveaux MEP1 - Délai de mise en production sur l'ensemble des sites ADM1 – Disponibilité des infrastructures ADM2 - Taux d'incidents traités dans les délais ADM3 – Taux d'incidents évités grâce à des actions d'administration préventives ADM4 – Taux d'incidents ayant une valeur capitalisable ADM5 – Taux de demandes traitées dans les délais IMA1 - Délais de réalisation des IMACs mineurs critiques IMA1 - Délais de réalisation des IMACs mineurs non critiques IMA1 - Délais de réalisation des IMACs majeurs critiques
COSUI	Trimestriel	Documentation	Consolidation des indicateurs présentés en COMEX MOE3 - Fourniture d'un état à jour des fins de licence
COPIL	Annuel	Rapport semestriel Documentation	Consolidation des indicateurs présentés en COSUI
Comités de projet	En tant que de besoin	Rapport de crise Rapport continu Documentation	MOE2- Fourniture du rapport de gestion de crise MOE6 - Délai de mise à jour de l'inventaire du parc après un mouvement en mode projet

6.2.2.2. Comités

Le titulaire organise et anime les réunions du comité d'exploitation, du comité de suivi, du comité de pilotage et du comité de projet et plus généralement, participe à toute réunion de travail organisée à l'initiative du ministère en fonction des besoins.

Le titulaire prépare l'ordre du jour et les supports de présentation de chaque comité qu'il transmet au ministère dans les délais fixés pour chacun des comités.

À l'issue de chaque réunion, le titulaire en rédige le compte-rendu et met à jour le relevé de décisions et le suivi des actions issues de ce comité.

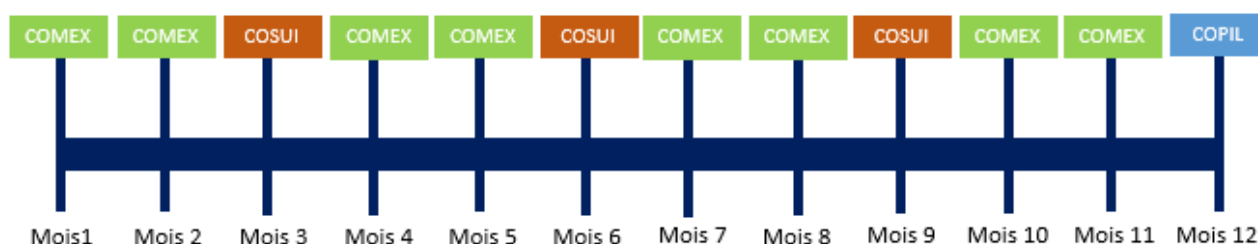
Ce compte rendu est transmis au ministère pour validation dans les deux (2) jours ouvrés suivant la réunion du comité.

Sans remarque du ministère dans les cinq (5) jours ouvrés suivants sa transmission, le compte-rendu est considéré comme approuvé.

Dans le cas où le ministère formule des remarques sur ce compte-rendu, le chef de projet du titulaire dispose d'un délai de deux (2) jours ouvrés pour lui transmettre une version corrigée.

L'organisation détaillée (composition, rôle, périodicité, lieu de réunion, etc.) des différents comités est formalisée dans le PAQ.

Les comités se déroulent selon la périodicité ci-dessous :



► Comité d'exploitation (COMEX)

Le comité d'exploitation se réunit selon une périodicité mensuelle.

Il a en charge le suivi et la coordination des actions prévues au marché, ainsi que des actions décidées conjointement par le titulaire et le ministère et placées sous la responsabilité du titulaire. Il permet une revue et un bilan mensuel des incidents d'exploitation et demandes ainsi que des risques et alertes sur la période écoulée dont il fait référence. Les tableaux de bords mensuels sont présentés par le titulaire et les différents indicateurs mis en œuvre expliqués.

L'ordre du jour, en coordination avec le ministère, est proposé par le titulaire au moins trois (3) jours à l'avance.

À l'occasion de ce comité d'exploitation, le titulaire présente un rapport mensuel d'activité, selon les modalités décrites à l'article [9](#) du présent CCTP.

► Comité de suivi (COSUI)

Le comité de suivi se réunit tous les trimestres.

C'est un comité d'exploitation amélioré, il se substitue donc à celui-ci. En plus des rapports d'activité sur le trimestre, il permet de suivre les aspects financiers et contractuels du marché. Il doit permettre de faire évoluer le marché en proposant, le cas échéant, des ajustements.

L'ordre du jour en coordination avec le ministère est proposé par le titulaire au moins sept (7) jours à l'avance.

► Comité de pilotage (COPIL)

Le comité de pilotage se réunit selon une périodicité annuelle.

Il permet de veiller au bon fonctionnement du marché et valide les choix stratégiques. Lors du COPIL, le titulaire présente un bilan chiffré de l'année écoulée ainsi que les axes d'amélioration et d'évolutions proposés pour la suite du marché.

L'ordre du jour en coordination avec le ministère est proposé par le titulaire au moins quinze (15) jours à l'avance.

► Comités de projet

Le ministère met en place des comités de projet à chaque fois que nécessaire.

Le ministère apporte son concours et toute documentation utile au titulaire. Celui-ci peut demander des compléments, apporter ses propres éléments d'éclairage et en effectuer la synthèse. Toutes les demandes d'information entre le titulaire et le ministère, question et réponse, se font par écrit, de préférence sous forme d'un message électronique ou dans le cadre de l'espace dédié du site collaboratif du ministère (cf. article [9](#) du présent CCTP).

6.2.2.3. Rapports

Le titulaire élabore et met à disposition du ministère les rapports suivants :

- Rapport de crise [sur demande et sur incident] ;
- Rapport mensuel ;
- Rapport semestriel ;
- Rapport continu ;
- Retours d'expérience ;
- Documentation.

6.2.2.3.1. Rapport de crise

Le rapport de crise a pour objet d'apporter un exposé précis, concis et explicatif sur un incident en cours impactant la production.

Ce rapport permet d'appréhender de façon simple, l'état des lieux et les actions en cours et planifiées, l'horaire prévisionnel de rétablissement du service à la date du rapport.

Ce rapport est destiné à être communiqué pour informer les utilisateurs sur un incident majeur. Le titulaire s'engage à fournir ce type de rapport à chaque fois que la gestion de crise est déclenchée sur impact majeur.

6.2.2.3.2. Rapport mensuel

Le rapport mensuel permet de présenter, de façon simple, l'état des lieux et les actions en cours à la date du rapport avec rappel des synthèses sur trois (3) mois glissants.

Il a pour objet de fournir une vision de management sur la situation à date, les actions à suivre et les décisions à prendre pour la période à venir.

Les points mentionnés sont :

- la vision sur les capacités disponibles et prévues, à date et en prévision ;
- la disponibilité des infrastructures et applicatifs, notamment la conformité avec les niveaux de services attendus ;
- les incidents en cours, avec indication de l'action en cours ;
- les incidents réglés depuis le dernier rapport mensuel, en mentionnant si les informations de retour d'expérience ont été saisies ;
- le volume de tickets en cours/fermés/restants au support titulaire ;
- les actions de changements terminées depuis le dernier rapport mensuel ;
- la liste, à date, des difficultés et événements passés mais devant être analysés au titre du Retour d'expérience trimestriel ;
- les relances ministère en attente ;
- une très courte synthèse rédigée.

Le titulaire doit, au titre de ce rapport, mentionner de manière rapidement lisible pour chaque point et systématiquement, la gravité, l'état d'avancement et l'ancienneté de l'incident.

Ce rapport doit faire ressortir, de manière non ambiguë et visuellement identifiable les points susceptibles de mettre en cause la qualité de service due aux utilisateurs (disponibilité, performance, etc.) ou l'avancement des actions majeures en cours.

Ce rapport mensuel, incluant d'éventuelles actions menées en tout début de mois, est mis à disposition des personnes désignées par le ministère chaque 5e jour ouvré du mois avant 12 heures (midi).

6.2.2.3.3. Rapport semestriel

Le rapport semestriel permet de visualiser la conformité des actions exécutées sur la période précédente avec les niveaux de service attendus, l'état des lieux et les actions en cours à la date du rapport avec rappel des synthèses sur les douze (12) mois glissants précédents.

Il a pour objet de fournir une vision de management sur la situation à date, les actions à suivre et les décisions à prendre pour la période à venir.

Les points mentionnés sont :

- un tableau de réalisation des engagements de service sur la période écoulée avec comparaison aux objectifs du SLA et mise en évidence des non-conformités ;
- un tableau de suivi des fins de licences et réabonnements constructeurs ;
- la liste des équipements du parc, regroupés par service avec le nombre d'incidents et le taux de disponibilité du service.
- la disponibilité des infrastructures et applicatifs, notamment la conformité avec les niveaux de services attendus ;
- les incidents en cours, avec indication de l'action en cours ;
- les incidents réglés depuis le dernier rapport, en mentionnant si les informations de retour d'expérience ont été saisies ;
- un état du parc complet avec la vision sur les capacités disponibles et prévues, à date et en prévision ;
- le volume de tickets en cours au support titulaire ;
- le nombre de tickets ouverts/en cours/gelés / fermé durant le mois et sur douze (12) mois glissants
- le nombre d'appels reçus par la cellule d'accueil du titulaire, et les statistiques d'appels présentant au minimum les nombres d'appels présentés, décrochés, abandonnés (non répondus), les temps d'attente, les temps de décroché, etc. ;
- un état des différentes règles et configurations non utilisées et obsolètes sur l'ensemble des équipements du ministère.
- une vision de la documentation et des actions effectuées dans la période passée, en cours, ou devant être démarrées dans la période à venir sur ce point ;
- une synthèse rédigée, comprenant notamment pour les non-conformités une analyse des causes et un plan d'action de remise en conformité.

Ce rapport semestriel est produit automatiquement par les outils du titulaire et mis à disposition du ministère en janvier et en juillet le 5e jour ouvré avant 12 heures (midi).

6.2.2.3.4. Rapport continu

L'outillage de rapport continu doit également permettre de fournir en ligne, à tout moment, une vision sur les points suivants :

- l'état de la supervision ;
- les plans d'actions en cours ;
- la disponibilité des infrastructures et applicatifs, notamment la conformité avec les niveaux de services attendus. L'information est disponible en vision à date et en glissant ;
- l'avancement des projets et actions de changements ;
- le volume des tickets ouverts ;
- les incidents majeurs non clos et les actions en cours.

6.2.2.4. Retours d'expérience

Le titulaire tient à jour une liste des événements et difficultés constatées, de tous ordres, dont l'importance, la fréquence de répétition ou l'impact sur la qualité de service délivrée ou perçue nécessite un traitement.

Le ministère peut faire inscrire les points qui lui semblent le mériter sur ce document.
 Les problèmes recensés dans le cadre ITIL sont d'office inscrits sur cette liste, au moins pour suivi.
 Lors des réunions des comités d'exploitation mensuels, le titulaire présente cette liste en effectuant une analyse de ces points ainsi que des propositions et préconisations de résolution.

6.2.2.5. Documentation

Le titulaire met à jour le référentiel documentaire prévu à l'article [6.1.2.3.1](#) du présent CCTP.
 À l'occasion de chaque comité, il fait un point sur l'exhaustivité des documents composant ce référentiel et les mises à jour effectuées.

6.2.3. ROLES ET RESPONSABILITES

Le tableau précise les principales responsabilités entre, d'une part, le titulaire et d'autre part, le ministère.

(R = Réalise ; A = Approuve ; C = Contribue ; I = est Informé)

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Gestion globale des services		
Proposer un ensemble de procédures de fonctionnement et de rapports vis-à-vis du ministère	R	CA
Préparer et faire appliquer les procédures internes	R	C
Analyser les services délivrés et proposer des améliorations	R	C
Définir / réviser les types de services	C	R
Fournir des prévisions globales sur l'évolution des besoins		R
Analyser l'ensemble des services, faire adapter les moyens et ressources en fonction de l'évolution de la charge et des besoins	R	I
Préparer les rapports et rendre compte au ministère	R	A
Préparer les réunions contractuelles et proposer l'ordre du jour	R	CA
Fournir un plan de progrès mis à jour pour le comité de pilotage	R	A
Préparer les comptes rendus des réunions contractuelles	R	A
Information des utilisateurs		
Informers le Support des situations de nature à affecter la qualité ou la continuité du service pour mettre à jour l'Intranet ou autres dispositifs	R	C
Informers les utilisateurs sur les situations affectant la qualité ou la continuité du service	C	IR
Diffuser aux utilisateurs les informations générales intéressant le système d'information local du ministère	C	IR
Gestion des niveaux de service		

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Mesurer les niveaux de service	R	A
Calculer les niveaux de service et les points d'alerte	R	A
Développer des plans pour l'amélioration du service et mettre en place les améliorations	R	C
Opérations d'exploitations		
Analyser régulièrement les configurations et préconiser les actions de mise en conformité par rapport aux spécifications de l'architecture technique	R	C
Gestion des problèmes		
Analyser les incidents récurrents, en rechercher les causes et proposer des plans d'action	R	C
Réaliser et suivre des plans d'action lorsqu'ils affectent le niveau de service ou le coût des prestations, ou la sécurité, ou supposent une participation du ministère	RC	AI
Documentation		
Maintenir à jour la documentation	R	A

6.2.4. NIVEAUX DE SERVICE ATTENDUS

Les principaux niveaux de service suivants sont attendus.

DEFINITION	MESURE	NIVEAU DE SERVICE
Gestion globale des services : Rapports		
MOE1 - Fourniture du rapport mensuel complet	Niveau attendu	Au plus tard le 5ème jour ouvré après la fin du mois
	Performances minimales	100%
	Intervalle de mesure	N/a
	Points d'alerte	N/a
MOE2- Fourniture du rapport de gestion de crise	Niveau attendu	Sous 30 minutes en cas d'incident majeur et déclenchement de l'état de crise
	Performances minimales	100%
	Intervalle de mesure	N/a
	Point d'alerte	N/a
MOE3 - Fourniture d'un état à jour des fins de licence	Niveau attendu	À chaque Comité d'Exploitation
	Performances minimales	100%
	Intervalle de mesure	N/a

DEFINITION	MESURE	NIVEAU DE SERVICE
	Points d'alerte	N/a
MOE4- Fourniture d'un état exhaustif et à jour de la documentation	Niveau attendu	À chaque Comité mensuel
	Performances minimales	100%
	Intervalle de mesure	N/a
	Point d'alerte	N/a
MOE5 – Fourniture d'un état exhaustif et à jour de gestion de parc	Niveau attendu	À chaque Comité mensuel
	Performances minimales	100%
	Intervalle de mesure	N/a
	Point d'alerte	N/a
MOE6 - Délai de mise à jour de l'inventaire du parc après un mouvement en mode projet	Niveau attendu	3 jours ouvrés après la fin du projet
	Performances minimales	99%
	Intervalle de mesure	N/a
	Points d'alerte	N/a
MOE7 – Fourniture d'un état de prévision des évolutions du parc (capacity planning)	Niveau attendu	À chaque Comité mensuel
	Performances minimales	100%
	Intervalle de mesure	N/a
	Point d'alerte	N/a

6.2.5. UNITES D'ŒUVRE

Les prestations récurrentes de la mission 2 correspondent à l'unité d'œuvre suivante :

Code UO	UO
M2-PR01	Pilotage de l'infogérance.

6.2.6. LIVRABLES

Le titulaire remet au ministère les livrables suivants :

- les comptes rendus et rapports des comités de suivi, d'exploitation, de pilotage et comités projet ;
- les rapports de gestion de crise, mensuels et continus en ligne ;
- les bilans de retour d'expérience.

6.2.7. DELAIS D'EXECUTION ET D'ADMISSION

La mission 2 débute à compter de la réception par le titulaire du bon de commande correspondant pour toute la durée prévue sur celui-ci.

Les prestations de la mission 2 doivent être réalisées dans les délais mentionnés dans le tableau ci-dessous :

M2 / UO	Livrables	Délai maximum de production des livrables (*)	Délais d'admission du ministère (*)	Délais de correction éventuelle du titulaire (*)
M2-PR01	Comptes rendus et rapports des comités de suivi, d'exploitation, de pilotage et de projet	A minima, délais prévus dans la description de la mission 2 ou, s'ils sont plus courts, ceux indiqués dans la convention de service	5 jours	3 jours
	Rapports de gestion de crise, mensuels et continus en ligne	Mensuel / continu	3 jours	3 jours
	Bilan de retour d'expérience	Délais prévus dans la convention de service	10 jours	3 jours

(*) Les délais s'expriment en jours ouvrés.

La validation des prestations effectuée durant le mois écoulé est réalisée à partir des états récapitulatifs mensuels fournis par le titulaire à l'occasion des comités d'exploitation.

L'admission a pour objet de valider le contenu, la forme et la qualité des produits livrés. Elle est constatée de manière expresse par le ministère et matérialisée par un procès-verbal d'admission définitive selon les conditions d'admission précisées à l'article 5.8 du présent CCTP.

En cas de correction des livrables par le titulaire, le ministère dispose d'un délai de trois (3) jours ouvrés, à compter de la réception des documents, pour examiner si la nouvelle version est conforme à l'ensemble des décisions prises lors des comités concernés. En cas de conformité, le ministère prononce l'admission mensuelle des prestations.

En cas de dépassement des délais, des pénalités de retard sont appliquées conformément à l'article 16 du CCAP.

6.3. MISSION 3 : INFOGERANCE DES INFRASTRUCTURES DU MINISTERE

6.3.1. OBJET DE LA MISSION 3

La mission 3 est constituée de prestations récurrentes et de prestations à la demande. Le titulaire s'engage à réaliser au titre de la mission 3 les prestations selon les modalités décrites ci-après.

6.3.2. DESCRIPTION DES SERVICES ATTENDUS

6.3.2.1. Prestations récurrentes mensuelles

Conformément à son offre, le titulaire réalise, selon les modalités décrites ci-après, les prestations récurrentes attendues au titre de la mission 3, sont :

- Le service de supervision, support et maintenance (M3 PR01) ;
- Le service d'administration et d'exploitation (M3 PR02) ;
- Les services du centre de sécurité opérationnel (SOC) (M3 PR03).

Ces prestations incluent :

- les actes élémentaires, dont notamment six (6) arrêts électriques planifiés annuels, prévus en HNO ;
- un exercice de simulation de sinistre majeur annuel, à une date définie d'un commun accord entre le ministère et le titulaire ;
- la contribution à un audit annuel, à une date définie d'un commun accord ;
- un test annuel à blanc de réversibilité, à une date définie d'un commun accord.

6.3.2.1.1. Service de supervision, support et maintenance (M3 PR01)

6.3.2.1.1.1. Services de supervision

6.3.2.1.1.1.1. Dispositions générales

Le système de supervision, proposé et mis en place par le titulaire, permet de vérifier en temps réel l'état de fonctionnement des infrastructures du ministère, de traiter les informations d'alerte et d'utiliser les outils paramétrés de manière *ad hoc* en vue d'assurer le diagnostic et le fonctionnement correct des systèmes et des applications, par les moyens appropriés (intervention, escalade vers les équipes de support).

Les alarmes signalant un défaut sont transmises aux opérateurs du ministère qui décident des actions à entreprendre en fonction de procédures d'identification, d'analyse et de traitement. Les alarmes ainsi que leur impact sur les services et/ou matériels sont enregistrés dans un journal de bord pour une analyse a posteriori et pour une diffusion dans le bilan d'exploitation mensuel.

La supervision, permanente, enregistre tous les incidents survenant sur les infrastructures entrant dans le périmètre du marché.

En cas d'incident escaladé vers un tiers (éditeur ou constructeur), le titulaire reste propriétaire du ticket et notamment est responsable du suivi et de la clôture.

Le titulaire assure la supervision des équipements et des services associés. Il exploite pour cela un ensemble d'indicateurs destinés à mettre en évidence les problèmes et anticiper sur les incidents.

La résolution d'incidents est réalisée par une mise en œuvre simultanée de supervision en temps réel, études des historiques et analyses de tendances à court, moyen et long terme, selon les processus qu'il décrit dans son offre et d'une application quasi mécanique des modes opératoires qu'il a documenté pour chaque type d'incident.

► Méthodologie

L'efficacité de la supervision des composants est étroitement liée à la pertinence des informations remontées. L'excès d'informations pour un événement donné peut nuire à la réactivité de prise en compte, de diagnostic et de traitement de l'événement.

Afin d'éviter cet écueil, et d'optimiser le traitement d'incidents, les scripts de supervision sont ordonnancés de façon à permettre une mise en corrélation des événements.

Par exemple, la perte d'une liaison est susceptible, sans cette corrélation d'événements, d'entraîner un flot d'alarmes à tous les niveaux de supervision (liaison, circuit, équipement, interface, niveau 3, peering, etc.).

Les scripts de supervision mis en œuvre par le titulaire doivent gérer une hiérarchisation des événements, permettant une identification rapide et précise de l'origine de l'incident.

► Journaux

Le titulaire conserve un historique des événements survenus sur les équipements sous forme de journaux génériques (tous les événements) ou spécifiques (erreurs, tentative de violation d'accès sur les équipements, access-list, syslog, etc.).

Leur analyse et l'extrait des données pertinentes sont diffusés au ministère. La période de rétention des événements demandée par le ministère est de douze (12) mois.

6.3.2.1.1.1.2. Spécificités

Spécificité réglementaire : Pour des contraintes réglementaires de sécurité imposées par l'État français à tous les ministères, le titulaire met à la disposition du ministère, dans les locaux de ce dernier, une réplique de la console de supervision. Un accès distant à la console de supervision du titulaire depuis les locaux du ministère est possible.

Spécificité incitative à la pro-activité : Le titulaire construit à sa guise son organisation pour atteindre les objectifs de niveaux de service fixés dans la convention de service. Cependant il s'engage à ce que sa solution de supervision détecte au moins 90% des incidents avant que les utilisateurs du ministère soient impactés.

Spécificité incitative à l'industrialisation : Le ministère s'inscrit dans une démarche continue d'industrialisation des services rendus à ses utilisateurs. Aussi, le titulaire met en œuvre des processus et méthodes industriels (scripts, modes opératoires ou autres) pour diminuer le nombre d'incidents de niveau 2 en les traitant en niveau 1 sans rupture visible pour l'utilisateur final.

6.3.2.1.1.3. Types de supervision

► Supervision en temps réel

Les tâches effectuées dans le cadre de la supervision des services réseau et sécurité sont :

- surveillance de l'état des composants : équipements, liaisons et circuits, services ;
- analyse des journaux ;
- contrôle des indicateurs de performances ;
- traitement des alarmes.

La supervision en temps réel permet la détection des incidents. Elle se base principalement sur la scrutation régulière de l'état des composants et services et la réception d'événements.

Les incidents détectés sont transmis au personnel d'exploitation par alarmes sonores ou visuelles. Elles sont accompagnées d'une journalisation spécifique.

Lorsque cela est possible, la journalisation est associée à un pré-diagnostic par corrélation d'informations.

Les événements significatifs qui ne nécessitent pas d'intervention immédiate sont journalisés avec pré-diagnostic éventuel pour traitement ultérieur.

► Supervision en différé (ou pro-active)

L'analyse à posteriori est utilisée pour l'identification et la compréhension de problèmes n'ayant pas été détectés par la supervision en temps réel. Elle est réalisée principalement par l'analyse de traces d'événements et d'indicateurs, stockés au fil de l'eau, et en provenance du système d'administration ou des équipements.

► Supervision de l'accès au réseau et de l'accès au secours

L'accès au réseau et l'accès de secours doivent faire partie des équipements supervisés par le titulaire pour s'assurer de leur état. L'état de la disponibilité de ces lignes doit faire partie du rapport mensuel de disponibilité des équipements.

Les alertes et événements sont réacheminés sur les consoles de supervision au travers d'un lien unique et sécurisé entre le réseau du titulaire et le réseau du ministère.

Les services demandés sont notamment :

- réalisation des contrôles actifs (contrôle de l'ensemble des processus de bout en bout) ;
- surveillance des contrôles passifs ;
- prise en compte des alertes en provenance de la supervision ;
- diagnostic ;
- résolution 1er niveau ;
- transfert et suivi des incidents non résolus, le Titulaire restant « propriétaire » des incidents transférés ;
- enregistrement des incidents et des actions effectuées ;
- clôture des incidents réglés avec saisie des éléments d'information nécessaires ;
- fourniture des tableaux de bord : incidents, problèmes, qualité de service (Disponibilité, performances, etc.).

En tant que professionnel de l'infogérance de sécurité, le titulaire a l'obligation de mettre en place un outil de collecte et d'analyse de l'ensemble des logs des équipements appartenant au périmètre du marché. L'agrégation et la corrélation des logs collectées par le titulaire, ainsi que la transmission

de rapports est fournie au travers des prestations du SOC/SIEM (Security Information & Event Management).

Le ministère demande ce service pour ses besoins propres, soit l'ensemble des Logs des équipements appartenant au périmètre du marché.

6.3.2.1.1.2. Services de support

Le support est assuré exclusivement et obligatoirement en langue française.

Le service support est le point de concentration pour le suivi des incidents, en provenance des outils de supervision et des correspondants du ministère.

Le titulaire propose et met en place un outil de gestion des tickets de signalement des incidents, quelle qu'en soit l'origine. Un ticket d'incident doit impérativement être ouvert sur l'outil du titulaire et qualifié avant toute information ou demande de confirmation au ministère.

Le support qui est évoqué dans ce paragraphe est le support relatif aux incidents liés au fonctionnement des infrastructures infogérées. Il s'agit d'un support de niveau 2.

Il n'a pas vocation à être appelé par les utilisateurs finaux mais par des interlocuteurs appartenant à des fonctions identifiées (entre 5 et 10 personnes habilitées à ouvrir un ticket), notamment :

- collaborateurs habilités du ministère, désignés par celui-ci ;
- opérateur WAN ;
- autres opérateurs ou infogérants du ministère.

La volumétrie des appels est donc très inférieure à celle reçue par la fonction support utilisateur classique et représente annuellement, à titre informatif environ :

- 80 tickets d'incidents ;
- 100 demandes de changements (IMAC)
- 50 demandes d'information, problèmes et maintenances programmées.

Dans ce cadre restreint, conformément aux règles de l'art et au plan d'assurance qualité, le titulaire réalise les actions suivantes :

- accueil téléphonique ;
- création des tickets ;
- résolution ou transfert/suivi ;
- clôture et documentation ;
- rapport, sur demande, pour les incidents impactant.

Une attention particulière est apportée à la gestion par le titulaire des trois points suivants :

- l'organisation qu'il met en place pour un traitement sans rupture des incidents (alignement ITIL) ;
- le suivi jusqu'à résolution des tickets, y compris ceux transférés ou escaladés, par exemple, à un tiers (éditeur/constructeur) ;
- la documentation des tickets clos et la gestion des problèmes, au sens ITIL du terme.

6.3.2.1.1.3. Services de maintenance

Le titulaire s'engage à assurer la maintenance matérielle et logicielle des équipements du périmètre, *a minima* selon les délais de garantie du temps de rétablissement définis à l'article 6.3.2.1.4.2 du présent CCTP, ou s'ils sont plus courts, selon les délais fixés dans la convention de service.

► Intervention sur site

En cas d'incident, le titulaire intervient sur site pour réaliser la maintenance aussi souvent que nécessaire.

Au cours de ces dépannages, il est procédé à la réparation ou au remplacement des pièces devenues défectueuses à la suite de l'usage normal du matériel, ainsi qu'aux vérifications et réglages nécessaires.

Le remplacement des pièces ou équipements défectueux est effectué par des pièces neuves ou équivalentes, avec la même version logicielle, sans perturber l'environnement technique du ministère.

Les interventions/actions nécessitant une interruption des services sont planifiées en relation avec le ministère.

► Gestion des montées de niveaux et des correctifs logiciels

Le titulaire applique les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur tous les matériels dont il a la charge.

Le titulaire s'engage à déployer 100% des mises à niveau de firmwares et des logiciels des équipements et/ou leur appliquer les correctifs logiciels au plus tard trois (3) mois avant le délai d'expiration indiqué par l'éditeur ou le constructeur.

En cas d'alerte grave (attaque virale, faille critique) annoncée par le CERTA (centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques), le correctif doit être appliqué dans un délai de 24 heures sur les équipements du périmètre. Lorsqu'aucun correctif n'est disponible, le titulaire doit suivre les recommandations de l'éditeur ou du CERTA dans le cadre d'un contournement provisoire. Si le contournement nécessite la désactivation d'une fonctionnalité indispensable au système, le titulaire s'engage à proposer des mesures permettant d'éviter l'exploitation de la vulnérabilité.

Le titulaire doit mettre à jour l'état du parc avec la liste des correctifs de sécurité appliqués sur les équipements du ministère. Le titulaire présente à chaque comité de pilotage l'état du parc mis à jour des versions disponibles en rapport avec celles installées sur le parc du ministère.

Ces opérations ne doivent en aucun cas dégrader ou interrompre les services fournis aux utilisateurs.

Le titulaire a l'obligation de réaliser des tests sur maquette dans ses locaux avant tout changement. Le titulaire s'engage à tester, avant mise en production sur l'infrastructure du ministère, toute mise à jour fournie par le constructeur afin de s'assurer qu'il n'y ait pas d'effets de bord et qu'il y ait entière compatibilité avec l'environnement existant au ministère.

Chaque mois, le titulaire s'engage à fournir au ministère un état à jour sur la gestion des montées de niveaux avec la liste des matériels gérés, leur dénomination, version logicielle, le niveau de patch et la date de la dernière mise à jour. Cet indicateur est contractuel et pénalisable.

6.3.2.1.2. Service d'administration et d'exploitation (M3 PR02)

6.3.2.1.2.1. Services d'administration

► Gestion des configurations

Dans le cadre de la gestion des configurations, le titulaire est chargé d'identifier, de contrôler de maintenir et de vérifier les changements d'éléments de configuration.

Pour ce faire et en sa qualité de professionnel dans le domaine de l'administration d'infrastructures informatiques, le titulaire met impérativement en place un outil de suivi et de gestion des configurations de type CMBD (Configuration Management Database au sens ITIL du terme).

Cet outil fournit un état logique de l'infrastructure et des services. À ce titre, il doit permettre de :

- décrire tous les éléments informatiques et configurations du ministère et de ses services ;
- fournir des informations détaillées sur les configurations et leur documentation permettant de supporter tous les processus de gestion des services tels que défini à l'article [6.3.2.1.1](#) du présent CCTP ;
- fournir une base pour la gestion des incidents, la gestion des problèmes, la gestion des changements et la gestion des configurations ;
- comparer les éléments de configuration avec les infrastructures existantes afin de corriger tous les écarts ;
- définir les relations entre les éléments de configuration.

Conformément à son offre, le titulaire réalise les opérations nécessaires à la gestion de cette base (sauvegardes, mesures de sécurité, administration, maintenance, etc.).

Tous les mois, le titulaire transmet au comité d'exploitation un état exhaustif des éléments constitutif du périmètre de gestion des configurations accompagné d'un indicateur permettant d'en vérifier la conformité. Tout écart de conformité au regard de cet indicateur peut conduire à l'application des sanctions prévues à l'article 16 du CCAP.

Le ministère définit un changement comme toute installation, tout mouvement, ajout et/ou changement (IMAC) d'un équipement, d'un logiciel ou d'une configuration pouvant affecter le périmètre technique du présent marché.

Les IMAC se répartissent selon deux types, majeur et mineur, comme suit :

[illegible]

- 30 % d'IMAC mineurs critiques sont exécutées avec un temps d'exécution de 2 heures maximum.
- 70 % d'IMAC mineurs non critiques sont exécutées avec un temps d'exécution d'une journée.

[illegible]

- 25 % d'IMACS majeurs critiques sont exécutées avec un temps d'exécution ne dépassant pas une journée
- 75 % d'IMACS majeurs non critiques sont exécutées avec un temps d'exécution ne dépassant pas trois (3) jours.

Les IMAC ainsi définies sont comprises dans le prix du titulaire.

Conformément à son offre, le titulaire prévoit, dans le cadre de cette mission, la réalisation de 250 IMAC mineurs et de 80 IMAC majeurs. Une flexibilité de 15% est appliquée à ces nombres ainsi qu'un mécanisme de transformation d'IMAC mineurs<->majeurs dont le coefficient est fixé par le titulaire. Il prévoit également un maximum de 20 déplacements par an en horaire étendu (de 7h00 à 8h00 ou de 18h00 à 20h00) dans le cadre de cette prestation.

► Gestion des capacités et performances

La gestion de la capacité doit permettre au ministère de gérer plus efficacement les coûts associés à l'infrastructure de son SI, tout en minimisant les ruptures de services, grâce à la surveillance permanente de ses équipements informatiques.

Le titulaire doit tenir compte de la charge supplémentaire (trafic réseau, charge des matériels, etc.) induite par les services objet du présent marché pour s'assurer que l'infrastructure et les équipements possèdent une capacité suffisante en ce qui concerne les ressources (CPU, disque, mémoire, interfaces) et la bande passante. Dans le cadre de son obligation de conseil, le titulaire se doit également de faire au ministère les préconisations nécessaires pour en optimiser leur utilisation sans pour autant compromettre la disponibilité du système.

6.3.2.1.2.2. Services d'exploitation

Les opérations sont exécutées par le titulaire selon les procédures organisationnelles fixées dans le plan d'assurance qualité.

En qualité de professionnel de l'exploitation, le titulaire a l'obligation de mettre en place un outil de suivi et de gestion des incidents et des demandes.

► Gestion des incidents

➤ Dispositions générales

Le principal objectif du processus de gestion des incidents est de restaurer les services opérationnels le plus rapidement possible et de minimiser l'impact sur l'activité du ministère, et par la même de s'assurer que les meilleurs niveaux de service et de disponibilité sont maintenus.

La gestion des incidents consiste à prendre en charge chaque événement ne relevant pas du fonctionnement normal d'un service et provoquant, ou pouvant provoquer, une interruption ou une dégradation de la qualité de ce dernier.

Cette prestation, basée sur un service de gestion des incidents dédié doit permettre d'assurer au ministère le niveau de disponibilité maximum défini dans la convention de services. À cette fin, le service « Gestion des incidents » doit notamment :

- vérifier que les incidents sont pris en compte, traités et correctement résolus dans le respect des délais et des priorités fixées dans le PAQ ;
- gérer les incidents et leur documentation afin de réduire les temps de réponse (délai entre la détection et le diagnostic de l'incident).

Dans ce cadre, il est attendu du titulaire la réalisation, a minima, des actions suivantes :

- gestion des déclarations d'incident provenant du service support, des correspondants du bureau DNE AC1 du ministère, de l'équipe d'exploitation du titulaire ou d'une alerte issue de l'outil de supervision. Ces requêtes font l'objet d'une traçabilité allant de la détection du symptôme à sa résolution. Le cas échéant, l'utilisateur ayant signalé l'incident peut être contacté afin de compléter le diagnostic ;
- aussitôt l'incident déclaré, le type d'incident, son numéro, et les premières constatations sont envoyées aux correspondants du Bureau DNE AC1 ;
- information des correspondants du bureau DNE AC1 du ministère sur les suites données à la déclaration d'incident ;
- suivi des équipes chargées des corrections, escalade sur incidents majeurs ;
- suivi des indicateurs et vérification de leur compatibilité avec les engagements contractuels ;
- production des statistiques, rapports et comptes rendus (quotidiens, hebdomadaires et mensuels) liés à l'activité support aux correspondants ministère ;

- gestion d'une base de connaissances : afin de conserver une trace des corrections apportées, de permettre une résolution plus rapide et plus directe par le service support.

Les incidents sont qualifiés selon la typologie suivante :

- **Incident majeur** : constitué par une indisponibilité d'un élément de l'infrastructure conduisant à bloquer le travail de plusieurs utilisateurs du SI ou à diminuer significativement la capacité de traitement des services du ministère.
- **Incident mineur** : constitué par la perte d'un équipement ou d'un service dont la redondance complète implique que le service aux utilisateurs n'est pas affecté.

Sauf accord écrit du ministère, toute résolution d'incident par une méthode de contournement ne peut être que provisoire et limitée dans sa durée. Le retour à un mode nominal doit intervenir dans un délai inférieur à quinze (15) jours calendaires à compter de la mise en place de la solution de contournement ou de substitution.

Dans tous les cas, le titulaire informe le ministère par courriel, dans les 24 heures suivant la mise en place de la solution de contournement ou de substitution, du délai prévisible de retour en mode nominal.

Chaque incident fait l'objet d'un compte rendu d'incident.

Ce compte rendu contient a minima la cause, le diagnostic, le temps d'indisponibilité ainsi que les actions de résolutions qui ont été entreprises ainsi que les mesures prises afin que l'incident ne se reproduise pas.

Ce compte rendu est transmis au ministère par courriel ou sur le serveur documentaire du ministère :

- sous 24 heures ouvrées pour les incidents mineurs ;
- sous 48 heures ouvrées pour les incidents majeurs.

➤ Cycle de vie de l'incident

L'enregistrement des informations du ticket doit être à jour et consultable par le ministère en temps réel.

Tous les changements de statut doivent être tracés (date/heure, personne, statuts, action).

Les différents niveaux de supports doivent apparaître clairement ainsi que les différentes demandes d'escalades (fonctionnelles et hiérarchiques).

La priorité du ticket d'incident est fixée par le titulaire quand celui-ci déclenche le ticket. Cette priorité peut être remontée à tout moment par le ministère sur simple appel de ce dernier.

À la résolution de l'incident, il appartient au support du titulaire de :

- confirmer la résolution avec le demandeur ;
- compléter l'enregistrement de l'incident et catégoriser la solution apportée ;
- fermer le ticket en s'assurant que les détails de la solution sont clairs et que les temps passés sont bien enregistrés.

En cas de solution de contournement, le ticket peut être marqué comme résolu, mais le ticket ne peut être fermé tant que la solution provisoire est en place.

➤ Dispositif spécifique de communication sur incident majeur

Conformément à la convention de services, dans le cas d'un incident majeur, tel que défini ci-dessus, le titulaire réalise les actions nécessaires pour résoudre et, le cas échéant, contourner l'incident, tout en assurant une communication du ministère en temps réel.

Pour ce faire, le titulaire respecte, a minima, les étapes suivantes :

- communication initiale (courriel et appel simultanés) au ministère pour l'informer de la nature de l'incident, de la durée de l'indisponibilité estimée et des premières actions organisées pour contourner ou résoudre le l'incident ;

- communication ensuite toutes les quinze (15) minutes par sms (ou par téléphone, selon la demande du ministère) pour informer le ministère du résultat des actions engagées et actualiser le temps nécessaire pour la remise en service, et ce jusqu'à la résolution complète ou la mise en place d'une solution de contournement de l'incident ;
- 48 heures ouvrées après la résolution de l'incident ou la mise en place d'une solution de contournement, transmission au ministère, par courriel ou sur le serveur documentaire du ministère, d'un rapport précisant la méthode utilisée pour résoudre l'incident et, le cas échéant, le délai pour un retour en mode nominal.

Ce dispositif de communication est essentiel et a pour vocation principale d'informer en temps réel le ministère.

► Gestion des problèmes

L'objectif de cette prestation est, d'une part, de minimiser l'impact négatif des incidents causés par des erreurs des services informatiques du ministère sur la production et, d'autre part, de rechercher la cause première de ces incidents et de réaliser les actions nécessaires pour améliorer ou corriger la situation.

Cette gestion suppose de la part du titulaire de mettre en place un processus à la fois réactif (résolution des problèmes en réponse à un ou plusieurs incidents) et proactif (identification et résolution des problèmes ou erreurs connus avant la survenance d'un incident).

À ce titre, le titulaire réalise notamment les actions suivantes :

- le suivi des incidents (identification de l'origine et de la solution apportée à chaque incident) ;
- la gestion des tendances et l'identification des problèmes en identifiant les incidents récurrents et/ ou particuliers (top « dix » des incidents, temps de résolution élevé, etc.) ;
- l'analyse des solutions apportées aux incidents (préconisation de la solution pour résoudre l'incident ou, le cas échéant, mise en place d'une solution de contournement lorsque la résolution n'est pas applicable sans impact bloquant sur la production) ;
- le suivi des problèmes en cours (élaboration, contrôle et validation des solutions) ;
- l'amélioration de la connaissance des produits ;
- l'enrichissement de la base de connaissances ;
- la remontée des solutions validées vers l'outil de gestion des incidents.

Dans tous les cas, les mises à jour de correctifs, patchs sont effectuées sans impact sur les engagements de disponibilité et de performance définis dans le PAQ.

6.3.2.1.3. Services du centre de sécurité opérationnel (SOC)

Les opérations sont exécutées par le titulaire selon les procédures organisationnelles fixées dans le plan d'assurance sécurité soumis au ministère.

Le principal rôle du SOC est d'identifier les risques de sécurité afin de prévenir les incidents de sécurité en identifiant les risques.

Le SOC utilisera l'outil d'EDR du Ministère : Bit Defender. Un tenant en mode SAAS pour le périmètre de l'administration centrale est fourni par le ministère avec la création d'autant de compte que de besoin pour le ministère et ses partenaires. Le titulaire a à charge de déployer et mettre à jour l'EDR basé sur la solution BitDefender sur les serveurs et le parc bureautique de l'administration centrale. En cas de détection, sur le périmètre du marché d'un événement EDR à traiter, le Titulaire doit prendre en charge avec l'équipe DAC le déclenchement des actions ad hoc.

Un incident de sécurité est un événement qui porte atteinte à la disponibilité, à la confidentialité ou à l'intégrité d'un bien. Il peut s'agir par exemple de l'utilisation illégale d'un mot de passe, d'une intrusion non autorisée sur le réseau, une application ou un fichier.

Les principaux services attendus sont les suivants :

Le titulaire dans le cadre de ce marché met en place un service de SOC (Security Opération Center). Les principales missions du SOC sont :

- la prévention des incidents de sécurité ;
- la détection des incidents de sécurité ;
- l'assistance dans le traitement des incidents de sécurité.

- l'administration des équipements de détection.

En qualité de professionnel de l'exploitation, le titulaire a l'obligation de suivre toutes les demandes et les incidents déclarés dans l'outil de suivi et gestion mis en place pour l'exploitation.

6.3.2.1.3.1. Collecter et mettre à disposition l'ensemble des logs

Le principal objectif du processus de collecte de l'ensemble des logs est de fournir au ministère un espace et l'accès à un logiciel de SIEM (Security Information Event Management).

Le titulaire prévoit le déploiement de l'outil de Collecte Bit Defender (fourni par le ministère) sur le périmètre SI des ministères comprenant :

- 600 serveurs (Microsoft et Linux)
- 6000 postes de travail (Essentiellement sous environnement Microsoft, MacOS et Linux)

À cette fin, le titulaire met en place un outil de collecte et de corrélation de logs permettant une consultation simultanée de 8 agents du ministère aux fins :

- d'accéder et de consulter immédiatement à l'ensemble des logs sur un mois glissant ;
- d'accéder et de consulter, sur demande écrite, à l'ensemble des logs sur un an glissant avec une mise à disposition de celui-ci dans les trois (3) jours suivant la réception de la demande.

6.3.2.1.3.2. Agrégation et corrélation de logs

Le SOC, au travers son outil de SIEM qu'il administre, analyse les logs afin de détecter d'éventuelles anomalies. De par son analyse, le SOC devra alerter, et devra remonter l'information au ministère afin d'avoir un délai le plus court possible entre la détection de l'anomalie et l'action mise en place pour y remédier.

Le titulaire, propose et met en place des procédures afin d'automatiser les actions préventives à mettre en place en cas d'anomalies et d'incidents avérés.

La gestion des anomalies de sécurités et des incidents de sécurité prend en charge chaque évènement qui cause, ou pourrait causer un danger pour l'intégrité de données, du système d'information ou une interruption ou une dégradation de la qualité de ce service.

Ce SOC doit contribuer à assurer une disponibilité maximum des services informatiques.

Une anomalie est détectée :

- par détection automatique du système de corrélation et d'analyse de l'outil de gestion des logs du titulaire ;
- par l'appel et la déclaration d'un incident par les correspondants du bureau DAC AC1 du ministère (campagne de méls, alerte opérateur, etc.).

Sauf accord écrit du ministère, toute résolution d'incident par une méthode de contournement ne peut être que provisoire et limitée dans sa durée. Le retour à un mode nominal doit intervenir dans un délai inférieur à quinze (15) jours ouvrés à compter de la mise en place de la solution de contournement ou de substitution.

Dans tous les cas, le titulaire informe le ministère par courriel, dans les 24 heures ouvrées suivant la mise en place de la solution de contournement ou de substitution, du délai prévisible de retour en mode nominal.

Chaque incident de sécurité fait l'objet d'un compte rendu formel d'incident.

Ce compte rendu contient *a minima* la cause, le diagnostic, le temps d'indisponibilité ainsi que les actions de résolutions qui ont été entreprises ainsi que les mesures prises afin que l'incident ne se reproduise pas.

Ce compte rendu est transmis au ministère par courriel ou sur le serveur documentaire du ministère :

- sous 24 heures ouvrées pour les incidents mineurs ;
- sous 48 heures ouvrées pour les incidents majeurs.

6.3.2.1.3.3. Déclenchement et vie de l'incident de sécurité

L'incident est déclenché dans la majorité des cas par la détection d'une anomalie de sécurité. Un ticket d'incident doit impérativement être ouvert sur l'outil du titulaire et qualifié avant toute information ou demande de confirmation au ministère. Le ticket d'incident suit alors le cycle de vie « normal » d'un incident d'exploitation.

À la résolution de l'incident, il appartient au support du titulaire de :

- confirmer la résolution avec le demandeur ;
- compléter l'enregistrement de l'incident et catégoriser la solution apportée ;
- fermer le ticket en s'assurant que les détails de la solution sont clairs et que les temps passés sont bien enregistrés.

En cas de solution de contournement, le ticket peut avoir le statut « résolu », mais ne peut être fermé tant que la solution provisoire est en place.

6.3.2.1.3.4. Rapport d'activité

Outre les rapports d'incidents de sécurité demandés, le titulaire émet un rapport mensuel qui reprend les principaux faits marquants, les actions en cours et finies. Dans ce rapport, le titulaire reprend et liste les indicateurs les plus pertinents concernant l'actualité, les menaces en cours ou passées.

6.3.2.1.3.5. Dispositif spécifique de communication sur incident de sécurité impactant la production

Dans le cas d'un incident de sécurité provoquant une indisponibilité majeure (bloquant le travail de plusieurs utilisateurs du SI) sur un élément de l'infrastructure, le titulaire s'organise pour traiter l'indisponibilité dans le respect de la convention de services et en maximisant la communication autour des actions qu'il réalise conjointement avec l'exploitation pour résoudre et, le cas échéant, contourner l'incident.

Ce dispositif de communication est essentiel et a pour vocation principale d'informer en temps réel le ministère.

6.3.2.1.4. Modalités d'exécution des services

6.3.2.1.4.1. Plages de couverture de service en 24/7

Le titulaire s'engage sur les plages de couvertures horaires des services en 24 heures sur 24 et 7 jours sur 7 comme décrit ci-après.

L'ensemble des services de déclenchement et de suivi des maintenances est délivré en 24/24, 7 jours sur 7.

Le titulaire garantit la disponibilité en 24/7 de tous les services et équipements qu'il a en charge et notamment ceux liés aux :

- services de messagerie ;
- services d'accès vers et depuis Internet / Intranet ;
- services de travail à distance (Direct Acces et/ou VPN).

Les sites du ministère qui doivent accéder en 24/7 aux services précédemment énumérés sont ceux qui hébergent un DataCenter et /ou un cabinet ministériel et/ou une direction sensible, donc à ce jour (Liste susceptible d'évoluer au cours du marché) :

- Dutot ;
- Descartes ;
- 110 Grenelle.
- Avenue de France.

Dès lors, les fonctionnalités sous-jacentes dont le titulaire doit assurer la disponibilité sont :

- le service DNS et DHCP ;

- le service d'accès à la messagerie électronique.
- le service d'accès au réseau internet.
- les services de travail à distance (Direct Acces et/ou VPN)

Le titulaire doit donc être à même de détecter une perte de service ou de capacité de redondance et d'assurer le service et le rapport correspondant (alerte notamment) pour garantir ces services sur ces sites.

Par exclusion et hors incidents, pour tout ce qui ne doit pas être couvert en 24 heures sur 24 et 7 jours sur 7 (24h/24 et 7j/7), le titulaire s'engage sur des plages horaires des services pour les changements, du lundi au vendredi de huit heures à dix-neuf heures (8h00 à 19h00).

En tant que de besoin, le titulaire prévoit une extension possible au samedi de neuf heures à dix-huit heures (9h00 à 18h00). Cette prestation à la demande peut être commandée ponctuellement par le ministère, à tout moment, moyennant un préavis minimum de cinq (5) jours ouvrés (UO L1-M3-PD07).

6.3.2.1.4.2. Criticité des services

Criticité niveau 1 (très critique) :

- le service d'accès à Internet ;
- le service d'accès et de synchronisation à la messagerie électronique ;
- le service DHCP pour la TOIP ;
- le service de fichiers en réseau.
- Le service de travail à distance (Direct Access et/ou VPN).

La criticité de niveau 1 correspond à la plage horaire de service en 24/7, une disponibilité de 99,4 % calculé mensuellement, une prise en compte des incidents sous trente (30) minutes et une garantie de temps de rétablissement (GTR) de deux (2) heures.

Criticité niveau 2 (peu critique) :

- le service de publication d'applications ;
- le service d'authentification ;
- le service d'accès aux académies ;
- le service de WI-FI.

La criticité de niveau 2 correspond à la plage horaire de couverture de services du lundi au vendredi de neuf heures à dix-huit heures (9h00 à 18h00), une disponibilité de 95 %, une prise en compte des incidents sous soixante (60) minutes et une garantie de temps de rétablissement (GTR) de six (6) heures.

Conformément à son offre, le titulaire peut proposer, dans les créneaux d'intervention définis ci-dessus, des plages pour effectuer la maintenance préventive. Ces modalités sont définies dans le plan d'assurance sécurité et font l'objet d'un accord du ministère dans le cadre de la réunion de lancement.

6.3.2.1.4.3. Briques techniques sous-jacente des services

Conformément à son offre, le titulaire, aux fins de réalisation des prestations décrites aux articles 6.3.2.1.1. et 6.3.2.1.2., garantit le fonctionnement des services redondés suivants :

- le service DNS et DHCP ;
- le service de pare-feu ;
- le service de filtrage web ;
- le service de frontal http / https ;
- le service d'échange de mél (MX) ;
- le service de filtrage de mél (antispam et antivirus) ;
- le service de routage et switching en data center ou sur le chemin (Renater, MOSAIC, etc.) ;
- Le service de répartiteur de charge :
 - le service d'accès aux applicatif (Intranet, etc.) ;

- le service d'accès à la messagerie électronique ;
- le service de reverse proxy.

6.3.2.1.5. Audit de la qualité des prestations

Conformément à l'article 14 du CCAP, le ministère se réserve le droit de demander que toute vérification qui lui paraîtrait utile pour constater le respect par le titulaire de ses obligations au titre du marché puisse être effectuée, notamment par le biais d'un audit de conformité aux référentiels PSSIE, RGS ET RGPD et au PAQ.

L'audit doit permettre une analyse du respect du présent marché et du RGPD, notamment :

- par la vérification de l'ensemble des règles de sécurité mises en œuvre par le titulaire pour protéger les données à caractère personnel ;
- par la vérification des journaux de localisation des données, de copie et de suppression des données ;
- par l'analyse des mesures mises en place pour supprimer les données ;
- par l'analyse des mesures prises pour prévenir toutes transmissions illégales de données à des juridictions non adéquates et à empêcher le transfert de données vers un pays non autorisé par le ministère.

L'audit doit enfin pouvoir permettre de s'assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié.

Le titulaire s'engage à contacter le ministère dans les plus brefs délais dès lors qu'un incident de sécurité numérique est détecté et risque de perturber le fonctionnement des infrastructures du ministère.

6.3.2.2. Prestations à la demande

Au-delà des prestations récurrentes, les prestations à la demande sont constituées :

- soit par des demandes du ministère pour la réalisation de modification du périmètre par l'ajout d'un équipement,
- soit par des demandes IMAC d'un équipement, d'un logiciel ou d'une configuration pouvant affecter l'état du périmètre technique du présent marché.

Le titulaire effectue l'ensemble des opérations nécessaires à la réalisation de ces prestations.

6.3.3. ROLES ET RESPONSABILITES

Les tableaux ci-après précisent les principales responsabilités entre, d'une part, le titulaire et d'autre part, le ministère.

(R = Réalise ; A = Approuve ; C = Contribue ; I = est Informé)

6.3.3.1. Services de supervision, de support et de maintenance

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Support		
Accueillir les appels.	R	
Qualifier / orienter les demandes.	R	
Transmettre à l'entité désignée les demandes de support hors du champ d'action du support.	R	
Suivre les demandes (changements) des utilisateurs jusqu'à la clôture.	R	

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Notifier les incidents aux responsables désignés au ministère.	R	
Déclencher les opérations d'installation / de modification.	R	
Administrer les utilisateurs sur les services d'infrastructure (services de fichiers, d'impression, de messagerie, etc.).	R	
Informer le support d'événements hors du périmètre du titulaire pouvant impacter son périmètre. (coupures électriques, par exemple).		R
Matériels, logiciels et applications du périmètre		
Fournir le support de 1 ^o niveau.	R	
Fournir le support de 2 ^o niveau.	R	
Déclencher les services IMACs selon la procédure.	R	
Fournir ou escalader au support de 3 ^o niveau.	R	
Documenter la résolution des tickets de demande et incidents et transmettre les informations au ministère.	R	
Créer, gérer une base de connaissance consultable par le ministère sur l'outil de gestion des tickets du titulaire.	R	C
Exploiter la base de connaissances	R	
Sécurité		
Réaliser un exercice de « crash recovery » suivant la périodicité établie entre le ministère et le titulaire compte-tenu de la situation validée durant la phase de mise en place. Le résultat de l'exercice donne lieu à un rapport fourni au ministère sous 5 jours ouvrés après l'exercice.	R	C

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Supervision		
Superviser et analyser le fonctionnement des infrastructures du périmètre sur la plage horaire contractuelle.	R	
Superviser et analyser le taux d'occupation des bandes passantes du périmètre.	R	
Détecter les incidents affectant les infrastructures du périmètre, les enregistrer et les suivre jusqu'à résolution.	R	
Suivre l'évolution des performances et des consommations de ressources pour anticiper les problèmes éventuels.	R	
Gestion des services relatifs aux Infrastructures du périmètre		
Proposer un ensemble de standards et procédures (escalade, notification, etc.) de fonctionnements et de rapports.	R	C

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Approuver / officialiser les procédures (escalade, notification, etc.) du titulaire vers le ministère.	C	R
Définir / réviser les types de services relatifs aux réseaux.	C	R
Adapter les moyens et ressources du titulaire en fonction de l'évolution de la charge et des besoins.	R	
Information des utilisateurs		
Informier le support des situations concernant les réseaux de nature à affecter la qualité ou la continuité des services.	R	
Informier le ministère des situations concernant les réseaux de nature à affecter la qualité ou la continuité des services.	R	
Planning et analyse		
Définir les besoins fonctionnels et service.	C	R
Effectuer des préconisations en ce qui concerne la capacité et la performance des infrastructures du ministère dans le cadre des rapports au comité de suivi.	R	A
Gérer les projets ainsi que les charges associées dans le cadre de nouvelle installation ou de changement d'équipement. (incluant la création des plans de projet et la documentation appropriée).	R	
Définir les scénarii de test de « disaster recovery ».	R	C
Planifier le test de « disaster recovery ».	R	
Exécuter la planification de la sécurité en accord avec la politique du ministère.	R	
Maintenance		
Appliquer les procédures de maintenance et de réparation.	R	C
Installer les "patches", les packs services, « firmware », les mises à jours etc. fournis par les fabricants / fournisseurs et mettre à jour la base de connaissance du constructeur / éditeur.	R	I
Déclencher le remplacement des pièces et des systèmes défectueux.	R	I
Exploitation des réseaux		
Résolution des incidents et des problèmes.	R	C
Détecter les incidents affectant les réseaux.	R	
Notifier au ministère les incidents d'un certain niveau de gravité ou dont la résolution tarde.	R	
Résoudre les incidents ayant leur cause dans le périmètre du marché et remettre les réseaux en condition opérationnelle.	R	
Escalader les incidents ayant une cause extérieure aux réseaux vers le support approprié (serveurs, applicatif, etc.).	R	I

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Effectuer les interventions de proximité sur les sites du périmètre.	R	AI
Analyser les incidents récurrents et gérer les processus de résolution de problèmes.	R	C
Planifier les interventions sur les réseaux entraînant un arrêt ou une perturbation.	R	A
Déclencher et suivre les appels à la maintenance pour les incidents affectant le matériel et les logiciels de base (routeurs, etc.).	R	I
Intégration et tests		
Exécuter les tests d'intégration et de sécurité, en collaboration avec le ministère, pour tout équipement, logiciel ou services, nouveau ou mis à jour, intégré par le titulaire.	R	IA
Exécuter et approuver toutes les recettes utilisateurs pour tout équipement, logiciel ou services, nouveau ou mis à jour.	C	R
Mettre en production des équipements nouveaux ou mettre à jour par étape pour assurer une transition sans perturbation du service offert.	R	
Exécuter la gestion des configurations et les activités de contrôle de changement.	R	A
Suivi et réglage des performances		
Suivre l'évolution des performances et des consommations de ressources pour anticiper les problèmes éventuels.	R	
Proposer les évolutions permettant le maintien des performances et la couverture des besoins.	R	
Décider les évolutions des ressources.		R

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Gestion des capacités		
Superviser l'évolution des consommations de ressources et proposer des évolutions en temps utile lorsque des insuffisances de capacité risquent d'apparaître	R	I
Fournir les informations sur l'évolution à moyen terme (6 mois) des principales métriques utilisateurs et sur les projets de développement du ministère	I	R
Gestion des changements		
Émettre et enregistrer les demandes de changement		R
Instruire les demandes de changement, en analyser l'impact et le coût éventuel, et en proposer la planification	R	C
Décider les changements et en fixer la priorité	C	R
Suivre l'exécution des changements	R	I

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Gestion du parc et des licences		
Proposer les outils et méthodes de gestion de parc et des licences, ainsi qu'une stratégie de mise en œuvre	R	A
Fournir, implémenter, administrer et exploiter les outils de gestion de parc et des licences, en incluant la reprise éventuelle des données existantes	R	
Créer et mettre à jour les données à chaque mouvement	R	
Fournir des rapports réguliers ou à la demande d'un tiers, sur l'état du parc et des licences	C	R
Réaliser les achats de licences et déclarer les installations		R
Gérer la distribution et les versions des licences	R	I
Suivre et communiquer au ministère les informations lui permettant de gérer les droits de licence acquis rendus disponibles par les désinstallations	R	I

6.3.3.2. Services d'administration et d'exploitation

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Administration		
Mettre à jour les PAQ et PAS et proposer un ensemble de procédures (escalade, notification, etc.) de fonctionnement et de rapports.	R	C
Approuver / officialiser les procédures (escalade, notification, etc.) du titulaire vers le ministère.	C	R
Administration		
Définir / réviser les types de services relatifs aux infrastructures.	C	R
Adapter les moyens et ressources en fonction de l'évolution de la charge et des besoins.	R	
En fonction des évolutions de l'environnement et des besoins (demandes explicites ou évolution des ressources consommées), mettre à jour les données et paramètres de configuration et de fonctionnement des infrastructures et des services qu'ils délivrent : des droits, etc.	R	
Effectuer les opérations d'administration sur les infrastructures selon les règles de sécurité préconisées par l'ANSSI.	R	
Enregistrer les interventions d'administration effectuées, pour rapport et traçabilité.	R	
Effectuer un rapport des opérations d'administration lors du comité d'exploitation.	R	
Définir la stratégie d'accès et les caractéristiques des profils utilisateurs.	C	R
Effectuer les opérations d'administration correspondant à la mise à jour des règles, des droits et des profils.	R	I

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Planifier la mise en validation puis en production nécessaire pour la correction du problème.	C	R
Planification des mises en production		
Fournir une planification prévisionnelle des mises en production à trois mois.		R
Fournir une planification définitive des mises en production pour le mois suivant.		R
Fixer les dates exactes des mises en production en fonction des demandes et contraintes du ministère, signaler les éventuels conflits au ministère.	R	C
Fixer les priorités en cas de conflit entre les différentes mises en production demandées.		R
Décider de la plage horaire exacte des mises en production.		R
Aviser les utilisateurs des mises en production prévues et de la non-disponibilité des applications.	C	R
Mise en production		
Installer la nouvelle application ou règle.	R	C
Réceptionner le service en production, consigner le résultat dans le compte-rendu de réception (le compte rendu de recette est rempli conjointement et fourni au ministère dans les 3 jours ouvrés suivant l'installation.	R	C
Planifier une nouvelle mise en validation puis en production en cas de problème.	R	C
Problèmes en production liés aux procédures d'installation		
Gérer et résoudre les incidents postérieurs à la mise en production.	R	C
Consulter si nécessaire le constructeur/éditeur de l'application sur les problèmes rencontrés en production dans le cas où le développement de l'application a été confié à un tiers.	C	R
Corriger au besoin la procédure d'installation (partie serveur ou ministère) et le dossier d'exploitation dans le cas où le développement de l'application a été confié à un tiers.	C	R
Corriger au besoin la procédure d'installation (partie serveur ou ministère) et le dossier d'exploitation.	R	A
Opérations d'exploitations		
Proposer des opérations d'exploitations (notamment via l'outil de gestion de tickets) ayant pour objet une amélioration des performances ou de la productivité.	R	
Accepter les opérations d'exploitation ayant un impact sur le fonctionnement des applications, la productivité des utilisateurs ou la performance des systèmes.		R
Décider les actions de mise en conformité.		R

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Effectuer les opérations d'administration sur les systèmes.	R	
Enregistrer les interventions d'administration effectuées pour rapport et traçabilité.	R	
Traiter les demandes et escalader selon les procédures établies.	R	
Sauvegarder les systèmes et stocker les médias selon les procédures établies.	R	A
Gérer les activités de configuration et de changement.	R	A

ROLES ET RESPONSABILITES	MINISTERE	TITULAIRE
IMACs		
Réceptionner des demandes, déclencher et suivre les procédures d'approbation.	R	
Exécuter les demandes après approbation du ministère.		R
Planifier les demandes en mode projet.	C	R
Planifier les autres demandes.	R	
Étudier l'impact de chaque changement.	I	R
Préparer, paramétrer, tester et déployer le nouvel élément actif.		R
Mettre à jour la gestion de parc relativement à l'IMAC.	I	R
Organiser la bascule en phase opérationnelle.		R
Procéder à la recette de l'installation et la constater par la signature du rapport d'installation / désinstallation.	R	

6.3.3.3. Services du centre de sécurité opérationnel

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Collecte des logs		
Stock vivant de log d'un mois.	R	I/A
Conservation de log pendant 1 an.	R	I/A
Paramétrage des équipements pour envoyer les logs vers les outils du titulaire.	R	
Supervision du SI		

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Détection des anomalies et incidents de sécurité.	R	C
Alerter des incidents de sécurité.	R	C
Résoudre les incidents de sécurité.	R	C
procédures de résolution pro-active des incidents de sécurité		
Gérer et résoudre les incidents de sécurité.	R	C
Consulter si nécessaire le constructeur/éditeur de l'application sur les problèmes rencontrés en production dans le cas où le développement de l'application a été confié à un tiers.	C	R
Mettre à jour les bases de connaissances des différents outils de supervision et de détection.	C	R
Mettre en place les procédures simples de protection du SI.	R	A
Opérations d'exploitation		
Proposer des opérations d'exploitations ayant pour objet une amélioration des performances ou de la productivité de l'outil SIEM du titulaire.	R	
Accepter les opérations d'exploitation ayant un impact sur le fonctionnement des applications, la productivité des utilisateurs ou la performance des systèmes.		R
Analyser régulièrement les configurations et préconiser les actions de mise en conformité par rapport aux spécifications de l'architecture technique.	R	C
Décider les actions de mise en conformité.		R
Effectuer les opérations d'exploitation sur les systèmes.	R	
Enregistrer les interventions d'exploitation effectuées pour rapport et traçabilité.	R	
Traiter les demandes et escalader selon les procédures établies.	R	
Sauvegarder les systèmes et stocker les médias selon les procédures établies.	R	A
Gérer les activités de configuration et de changement.	R	A
Administration		
Proposer un ensemble de procédures (escalade, notification, etc.) de fonctionnement et de rapports.	R	C
Approuver / officialiser les procédures (escalade, notification, etc.) du titulaire vers le ministère.	C	R

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Adapter les moyens et ressources en fonction de l'évolution de la charge et des besoins.	R	
En fonction des évolutions de l'environnement et des besoins (demandes explicites ou évolution des ressources consommées), mettre à jour les données et paramètres de configuration et de fonctionnement des infrastructures et des services qu'ils délivrent : des droits, etc.	R	
Effectuer les opérations d'administration sur les infrastructures selon les règles de sécurité préconisées par l'ANSSI.	R	
Enregistrer les interventions d'administration effectuées, pour rapport et traçabilité.	R	
Effectuer un rapport des opérations d'administration lors du comité d'exploitation	R	

6.3.4. NIVEAUX DE SERVICE ATTENDUS

6.3.4.1. Services de supervision, de support et de maintenance

DEFINITION	MESURE	NIVEAU DE SERVICE
Support : Temps de réponse		
USE1 – Taux de prise d'appel	Cible	99%
	Performances minimales	> 98%
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	N/a
USE2 - Temps de décrocher	Cible	< 30 secondes
	Performances minimales	> 95%
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	93%
USE3 - Temps de réponse des demandes émises via le portail	Cible	< 1h pendant un jour ouvré normal ou le jour suivant en dehors des heures ouvrées normales
	Performances minimales	99% du temps
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	N/a
USE4 – Pertinence de la catégorisation des tickets	Cible	95%
	Performances minimales	> 90%

DEFINITION	MESURE	NIVEAU DE SERVICE
Support : Temps de réponse		
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	N/a

DEFINITION	MESURE	NIVEAU DE SERVICE
Résolution d'incidents		
USE5 - Dossiers résolus lors du premier contact	Cible	> 60%
	Performances minimales	
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	N/a
USE6 - Temps de résolution	Cible	< 8h pour 80% des dossiers < 16h pour 95% des dossiers
	Performances minimales	
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	50% du 1 ^{er} délai de résolution
USE7 - Temps de résolution des dossiers bloquants	Cible	< 4h pour 95% des dossiers
	Performances minimales	
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	50% du 1 ^{er} délai de résolution
USE8 - Délai de transmission au support approprié <i>Dossiers ne relevant pas du Titulaire</i>	Cible	< 15 minutes après la prise en charge
	Performances minimales	90%
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	N/a

DEFINITION	MESURE	NIVEAU DE SERVICE
Supervision		
SUP1 - Délai de prise en compte d'un incident et délai de transfert au service concerné à compter du déclenchement d'une alerte dans les heures d'ouverture des services de supervision	Niveau attendu	< 15 minutes
	Performances minimales	90%
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	N/a
SUP2 – Détection des incidents avant que les	Niveau attendu	> 95% des incidents
	Performances minimales	90%

DEFINITION	MESURE	NIVEAU DE SERVICE
utilisateurs ne soient impactés	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	N/a
SUP3- Taux de traitement des incidents dans les délais	Niveau attendu	99%
	Performances minimales	99%
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	N/a
SUP4- Fourniture des tableaux de bord relatifs aux incidents	Niveau attendu	100%
	Performances minimales	100%
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	N/a

6.3.4.2. Services d'exploitation et d'administration

DEFINITION	MESURE	NIVEAU DE SERVICE
Maintien en opération des réseaux		
RES1 - Taux de disponibilité des infrastructures de Sécurité	Performances minimales	99.40%
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	Information par mél au bout de 30 minutes d'incident non résolu
RES2 – Fourniture des rapports d'incidents mineurs	Niveau attendu	Sous 48 heures ouvrées
	Performance attendue	> 90 %
	Intervalle de mesure	Chaque mois en comité d'exploitation
	Point d'alerte	N/a
RES3 – Fourniture des rapports d'incidents majeurs	Niveau attendu	Sous 24 heures ouvrées
	Performance attendue	> 90 %
	Intervalle de mesure	Chaque mois en comité d'exploitation
	Point d'alerte	N/a
RES5 – Fourniture d'un état à jour sur la gestion des montées de niveaux	Niveau attendu	À chaque comité d'exploitation
	Performance attendue	
	Intervalle de mesure	
	Point d'alerte	

DEFINITION	MESURE	NIVEAU DE SERVICE
Mise en Production		
MEP1 - Délai de mise en production sur l'ensemble des sites (hors re planification liée à une mise en production urgente)	Niveau attendu	95% dans les délais planifiés
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	N/a
DEFINITION	MESURE	NIVEAU DE SERVICE
Administration		
ADM1 – Disponibilité des infrastructures (réponse au ping et réponse à la fonction demandée)	Performances minimales	> 99,4%
	Intervalle de mesure	Mesure automatique mensuelle
	Points d'alerte	
ADM2 - Taux d'incidents traités dans les délais	Performances minimales	> 98%
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	95%
ADM3 – Taux d'incidents évités grâce à des actions d'administration préventives	Niveau attendu	> 30%
	Performance attendue	> 25%
	Intervalle de mesure	Chaque mois en comité d'exploitation
	Point d'alerte	N/a
ADM4 – Taux d'incidents ayant une valeur capitalisable (permet de mettre en évidence une amélioration de l'infrastructure à mettre en place ou un défaut de paramétrage)	Niveau attendu	> 50%
	Performance attendue	
	Intervalle de mesure	Chaque mois en comité de pilotage
	Point d'alerte	N/a
ADM5 – Taux de demandes traitées dans les délais	Niveau attendu	> 98 %
	Performance attendue	
	Intervalle de mesure	Chaque mois en comité d'exploitation
	Point d'alerte	

DEFINITION	MESURE	NIVEAU DE SERVICE
Installation		
	Niveau attendu	< 2 heures

DEFINITION	MESURE	NIVEAU DE SERVICE
IMA1 - Délais de réalisation des IMACs mineurs critiques (après réception des produits)	Performances minimales	95%
	Intervalle de mesure	Mesure mensuelle
	Points d'alertes	Information par mél dès dépassement du délai de traitement théorique de la demande
IMA1 - Délais de réalisation des IMACs mineurs non critiques (après réception des produits)	Niveau attendu	< 1 jours
	Performances minimales	95%
	Intervalle de mesure	Mesure mensuelle
	Points d'alertes	Information par mél dès dépassement du délai de traitement théorique de la demande
IMA1 - Délais de réalisation des IMACs majeurs critiques (après réception des produits)	Niveau attendu	< 1 jours
	Performances minimales	95%
	Intervalle de mesure	Mesure mensuelle
	Points d'alertes	Information par mél dès dépassement du délai de traitement théorique de la demande

6.3.4.3.Services du SOC

DEFINITION	MESURE	NIVEAU DE SERVICE
Administration		
ADM1 – Disponibilité des infrastructures (réponse au ping et réponse à la fonction demandée)	Performances minimales	> 99,4%
	Intervalle de mesure	Mesure automatique mensuelle
	Points d'alerte	
ADM2 - Taux d'incidents traités dans les délais	Performances minimales	> 98%
	Intervalle de mesure	Mesure mensuelle
	Points d'alerte	95%
ADM3 – Taux d'incidents évités grâce à des actions d'administration préventives	Niveau attendu	> 30%
	Performance attendue	> 25%
	Intervalle de mesure	Chaque mois en comité d'exploitation
	Point d'alerte	N/a
ADM4 – Taux d'incidents ayant une valeur capitalisable (permet de mettre en évidence une	Niveau attendu	> 50%
	Performance attendue	
	Intervalle de mesure	Chaque mois en comité de pilotage

DEFINITION	MESURE	NIVEAU DE SERVICE
amélioration de l'infrastructure à mettre en place ou un défaut de paramétrage)	Point d'alerte	N/a
ADM5 – Taux de demandes traitées dans les délais	Niveau attendu	> 98 %
	Performance attendue	
	Intervalle de mesure	Chaque mois en comité d'exploitation
	Point d'alerte	

6.3.5. UNITES D'ŒUVRE

6.3.5.1. Unités d'œuvre des prestations récurrentes

Les prestations récurrentes de la mission 3 correspondent aux unités d'œuvre suivantes :

Code UO	UO
M3-PR01	Service de supervision, de support et de maintenance
M3-PR02	Service d'administration et d'exploitation
M3-PR03	Service du Centre de Sécurité Opérationnel (SOC).

6.3.5.2. Unités d'œuvre des prestations à la demande

Les prestations de modification du périmètre de la mission 3 correspondent aux unités d'œuvres suivantes :

Code UO	UO
Ajout d'un équipement de grande complexité au parc en gestion (Cœur de réseau, Firewall, partage de charge)	
M3-MP01	Service de supervision, de support et de maintenance
M3-MP02	Services d'administration et d'exploitation
M3-MP03	Services du centre de sécurité opérationnel (SOC).
Ajout d'un équipement de moyenne complexité au parc en gestion (Antivirus, DNS, proxy, corrélation de logs)	
M3-MP04	Service de supervision, de support et de maintenance
M3-MP05	Services d'administration et d'exploitation
M3-MP06	Services du centre de sécurité opérationnel (SOC).
Ajout d'un équipement de faible complexité au parc en gestion (Switch, routeur)	
M3-MP07	Service de supervision, de support et de maintenance
M3-MP08	Services d'administration et d'exploitation
M3-MP09	Services du centre de sécurité opérationnel (SOC).

Les prestations à la demande de la mission 3 correspondent aux unités d'œuvre suivantes :

Code UO	UO
M3-PD01	IMAC unitaire mineur critique
M3-PD02	IMAC unitaire mineur non critique
M3-PD03	IMAC unitaire majeur critique
M3-PD04	IMAC unitaire majeur non critique
M3-PD05	Déplacement sur site dans le cadre d'un changement de version majeure. Cette prestation forfaitaire comprend la prestation du titulaire pour effectuer la mise à jour majeure d'un équipement, la version logiciel étant acquise dans les « services constructeurs » non inclus dans cette prestation.
M3-PD06	Unité de 10 changements en horaires étendus (7h-8h ou 18h-20h) au-delà des 20 annuels prévus.
M3-PD07	Unité d'intervention en extension d'horaire le samedi de 9h à 18h

6.3.6. LIVRABLES

Dans le cadre de la mission 3, le titulaire remet au ministère les livrables suivants :

► dans le rapport de comité mensuel :

- Au titre de la supervision
 - le rapport d'activité du service de supervision ;
- Au titre du support :
 - le rapport d'activité du service support
 - le rapport d'activité du service de maintenance.
 - le rapport mensuel d'activité des opérations d'administration
- Au titre de l'exploitation
 - le calendrier prévisionnel de planification des mises en production ;
 - le calendrier définitif de planification des mises en production ;
 - les comptes rendus de réception suite à la mise en production d'une application ;
 - le rapport mensuel d'activité des opérations d'exploitation.
- Au titre des opérations d'IMAC
 - le rapport mensuel d'activité des opérations d'IMAC.
- Au titre du SOC :
 - le rapport mensuel d'activité des opérations du SOC.

► dans le cadre de la mise à jour du PAQ :

- Au titre de la supervision
 - les standards et procédures de fonctionnement ;
 - les standards et procédures de sécurité ;
 - le rapport sur les besoins fonctionnels et de service
 - le rapport annuel des séances de planification des standards, de l'architecture et des projets ;
 - les scénarii « disaster recovery » ;
 - la documentation suite à l'application de patch ou à la mise à jour par les fabricants / fournisseurs ;
- Au titre du support

- les coordonnées du support technique (si elles n'ont pas été données dans le cadre de la réunion de lancement) ;
 - la base de connaissance et ses mises à jour ;
 - les résultats de l'exercice de « crash recovery ».
- Au titre de l'administration
- les standards et procédures de fonctionnement.

6.3.7. DELAIS D'EXECUTION ET D'ADMISSION

Les prestations d'infogérance des infrastructures du ministère (Mission 3) ne peuvent pas être commandées avant l'admission de la phase d'initialisation et de prise en charge (Mission 1).

Les bons de commande des prestations de la mission 3 précisent le délai d'exécution des prestations et la période couverte.

Les prestations de la mission 3 doivent être réalisées dans les délais mentionnés dans le tableau ci-dessous :

M3 / UO	Livrables	Délai maximum de production des livrables (*)	Délais d'admission du ministère (*)	Délais de correction éventuelle du titulaire (*)
Prestations récurrentes				
M3-PR01	État récapitulatif	Mensuel	5 jours	3 jours
M3-PR02				
M3-PR03				
Prestations à la demande				
M3 MP01	Bilan des prestations d'ajout d'un équipement	Mensuel	5 jours	3 jours
M3 MP02				
M3 MP03				
M3 MP04				
M3 MP05				
M3 MP06				
M3 MP07				
M3 MP08				
M3 MP09				
M3-PD01	Bilan des prestations de type IMAC	Mensuel	5 jours	3 jours
M3-PD02				
M3-PD03				
M3-PD04				
M3-PD05	État récapitulatif	Mensuel	5 jours	3 jours

M3 / UO	Livrables	Délai maximum de production des livrables (*)	Délais d'admission du ministère (*)	Délais de correction éventuelle du titulaire (*)
M3-PD06				
M3-PD07				

(*) Les délais s'expriment en jours ouvrés.

La validation des prestations effectuée durant le mois écoulé est réalisée à partir des états récapitulatifs mensuels fournis par le titulaire à l'occasion des comités de gestion des services.

L'admission a pour objet de valider le contenu, la forme et la qualité des produits livrés. Elle est constatée de manière expresse par le ministère et matérialisée par un procès-verbal de recette définitive selon les conditions d'admission précisées à l'article 5.8 du présent CCTP.

En cas de correction des livrables par le titulaire, le ministère dispose d'un délai de cinq (5) jours ouvrés, à compter de la réception des documents, pour examiner si la nouvelle version est conforme à l'ensemble des décisions prises lors des comités d'exploitation. En cas de conformité, le ministère prononce l'admission mensuelle des prestations.

En cas de dépassement des délais, des pénalités de retard sont appliquées conformément à l'article 16 du CCAP.

6.4. MISSION 4 : FOURNITURE DE SOLUTIONS DE MAINTIEN EN CONDITION OPERATIONNELLE ET D'EVOLUTION DES INFRASTRUCTURES ET SERVICES

6.4.1. OBJET DE LA MISSION 4

La mission 4 est constituée de prestations à la demande. Elle a pour objet de fournir au ministère des solutions permettant de garantir le maintien en condition opérationnelle et les évolutions des infrastructures du ministère.

Le titulaire s'engage à réaliser les prestations de cette mission selon les modalités décrites ci-après.

6.4.2. DESCRIPTION DES SERVICES ATTENDUS

Les prestations attendues pour l'ensemble des éléments (infrastructure) acquis dans le cadre du marché sont :

- le paramétrage,
- l'installation,
- l'intégration dans l'architecture existante en mode projet

D'une manière générale quand la solution mise en œuvre vient en remplacement d'une brique fonctionnelle existante la migration de la brique fonctionnelle doit être réalisée en mode projet.

Conformément à son offre, le titulaire fournit les solutions de maintien en condition opérationnelle et d'évolution des infrastructures répondant aux besoins fonctionnels suivants :

- répartition de charge multi sites et interne, et à la redondance applicative ;
- accélération et le déchiffrement SSL ;
- filtrage Web ;
- filtrage antivirus et codes malicieux ;
- détection et à la prévention d'intrusions ;
- cloisonnement des zones applicatives ;
- consolidation des logs ;
- contrôle d'accès à des fins d'administration ;
- services DNS ;
- services DHCP ;

- routage IP de niveau 3 ;
- commutation de niveaux 2 et 3.

Ces solutions doivent en outre permettre et garantir la continuité de l'exploitation en place.

Dans le cadre de cette prestation, le titulaire réalise également :

- les opérations de paramétrage, d'installation et d'intégration de l'équipement concerné ;
- la prise en charge des opérations de migration ;
- le support et la maintenance annuelle des équipements considérés.

Le catalogue de matériel du titulaire permet de compléter, le cas échéant, les acquisitions ou location de matériels qui ne figureraient pas dans la liste de ceux répondant aux besoins fonctionnels définis ci-dessus.

Ces matériels du catalogue du titulaire appartiennent exclusivement aux familles de produits suivantes :

- solutions de sécurité informatique ;
- solutions de filtrage Web ;
- solutions d'équipement réseaux ;
- connectiques et petits outillages informatiques.

En cours d'exécution du présent marché, il est prévu l'acquisition de solutions de sécurité de type « Pare-feu », qui viendront en complément de l'infrastructure existante et placés entre les datacenters et le réseau local du ministère. Ces solutions pourront être acquises via d'autres marchés (interministériels, académique, etc.) et seront intégrées au parc du ministère, modifiant ainsi l'infrastructure existante.

À ce titre, le titulaire prévoit :

- l'étude de l'intégration de ces systèmes de Firewalling additionnels (M4-EVO-FW-ET) ;
- le paramétrage, l'installation et l'intégration de ces nouveaux équipements sur l'infrastructure existante (M4-EVO-FW-REA).

6.4.3. ROLES ET RESPONSABILITES

Sans objet.

6.4.4. NIVEAUX DE SERVICE

Sans objet.

6.4.5. UNITES D'ŒUVRE

Les prestations à la demande de la mission 4 correspondent aux unités d'œuvre suivantes :

Code UO	UO
Solution de pare-feu	
M4- FW-1	Fourniture, et livraison de solutions de sécurité de type Pare-feu
M4- FW-2	Paramétrage, installation, intégration et migration en mode projet de solutions de sécurité de type Pare-feu
M4-FW-3	Support et maintenance annuelle de solutions de sécurité de type pare-feu
M4-FW-4	Service constructeur : redevance annuelle de solutions de sécurité de type pare-feu

Code UO	UO
Solution de management de pare-feu	
M4-FW-MNG-1	Fourniture et livraison de solutions de management de service sécurité de type pare-feu.
M4- FW-MNG-2	Paramétrage, installation, intégration et migration en mode projet de solutions de management de service sécurité de type Pare-feu.
M4-FW-MNG-3	Support et maintenance annuelle de la solution de management de service sécurité de type pare-feu
M4-FW-MNG-4	Service constructeur : redevance annuelle pour la solution de management du service sécurité de type pare-feu
M4-FW-MNG-5	Service constructeur : redevance annuelle pour la solution SmartEvent
Solution de proxy et filtrage web	
M4- PROXY-1	Fourniture, et livraison de solutions de type Proxy et filtrage web
M4- PROXY-2	Paramétrage, installation, intégration et migration en mode projet de solution de type Proxy et filtrage web
M4-PROXY-3	Support et maintenance annuelle de solutions de type Proxy et filtrage web
M4-PROXY-4	Service constructeur : redevance annuelle pour Proxy et filtrage web
Solution de système de sécurité DHCP	
M4-DHCP-1	Fourniture, et livraison de système de sécurité de type DHCP
M4-DHCP-1-MNG	Fourniture, et livraison de système de management de type DHCP
M4- DHCP-2	Paramétrage, installation, intégration et migration d'équipement de sécurité de type DHCP en mode projet
M4-DHCP-3	Support et maintenance annuelle pour DHCP
M4-DHCP-4	Service constructeur : redevance annuelle pour DHCP
Solution de système de sécurité de type DNS	
M4- DNS-1	Fourniture, et livraison de système de sécurité de type DNS
M4- DNS-1-MNG	Fourniture, et livraison de système de management de type DNS
M4- DNS-2	Paramétrage, installation, intégration et migration d'équipement de sécurité de type DNS en mode projet
M4-DNS-3	Support et maintenance annuelle pour DNS
M4-DNS-4	Service constructeur : redevance annuelle pour DNS
Solution de type répartition de charge	
M4-RP-1	Fourniture, et livraison de système de sécurité de type répartiteur de charge
M4-RP-2	Paramétrage, installation, intégration et migration d'équipement de sécurité de type répartiteur de charge
M4-RP-3	Support et maintenance annuelle pour répartiteur de charge
M4-RP-4	Service constructeur : redevance annuelle pour répartiteur de charge

Code UO	UO
Solution de type anti-virus et code malicieux	
M4-AV-1	Fourniture, et livraison de système de sécurité de type Filtrage antivirus et codes malicieux
M4-AV-2	Paramétrage, installation, intégration et migration d'équipement de sécurité de type Filtrage antivirus et codes malicieux
M4-AV-3	Support et maintenance annuelle pour Filtrage antivirus et codes malicieux
M4-AV-4	Service constructeur : redevance annuelle pour Filtrage antivirus et codes malicieux
Solution de type collecte et consolidation de LOG	
M4- LOG-1	Fourniture, et livraison de système de sécurité de Consolidation des logs
M4- LOG-2	Paramétrage, installation et intégration d'équipement de sécurité de type Consolidation des logs
M4-LOG-3	Support et maintenance annuelle pour Consolidation des logs
M4-LOG-4	Service constructeur : redevance annuelle pour Consolidation des logs
M4-LOG-5	Redevance annuelle pour 50 licences supplémentaires pour l'outil de collecte SIEM (Security Information Event Management)
Solution de commutation de niveau 3 (routeur)	
M4- ROUT-1	Fourniture, et livraison de système de sécurité de type commutateur de niveau 3
M4- ROUT-2	Paramétrage, installation, intégration et migration d'équipement de sécurité de type commutateur de niveau 3
M4-ROUT-3	Support et maintenance annuelle pour commutateur de niveau 3
M4-ROUT-4	Service constructeur : redevance annuelle pour commutateur de niveau 3
Solution de commutation de niveau 2 (switch)	
M4- SWI-1	Fourniture, et livraison de système de sécurité de type commutateur de niveau 2
M4- SWI-2	Paramétrage, installation et intégration d'équipement de sécurité de type commutateur de niveau 2
M4-SWI-3	Support et maintenance annuelle pour commutateur de niveau 2
M4-SWI-4	Service constructeur : redevance annuelle pour commutateur de niveau 2
Service d'assistance à paramétrage de solution technologiques	
M4-ASS-1	Service d'assistance au paramétrage de solution technologique de faible complexité nécessitant une expertise de niveau 1.
M4-ASS-2	Service d'assistance au paramétrage de solution technologique de moyenne complexité nécessitant une expertise de niveau 2.
M4-ASS-3	Service d'assistance au paramétrage de solution technologique de forte complexité nécessitant une expertise de niveau 3 pouvant aller jusqu'à l'escalade au constructeur.
M4-COM-SSI	Service d'assistance à la tenue d'un comité SSI

Code UO	UO
Assistance à la tenue d'un comité SSI	
M4-TRANS-COMP	Transfert de compétence technique d'une journée sur un équipement du périmètre du marché, dans le cadre de montée en compétence d'un collaborateur du ministère.
Intégration dans le parc du ministère	
M4-EVO-FW-ET	Étude de l'intégration des nouvelles solutions additionnelle de sécurité de type pare-feu.
M4-EVO-FW-REA	Paramétrage, installation, intégration des nouvelles solutions de sécurité de type pare-feu sur l'infrastructure existante.

6.4.6. LIVRABLES

Au titre de la mission 4, le titulaire remet au ministère les livrables suivants :

- l'équipement concerné ;
- le bon de livraison ;
- la documentation technique ;
- le bilan des opérations de migration, paramétrage, installation et intégration des équipements considérés ;
- l'étude de l'intégration des nouvelles solutions additionnelles de sécurité de type pare-feu ;
- le rapport d'activité concernant le paramétrage, l'installation, l'intégration des nouvelles solutions de sécurité de type pare-feu sur l'infrastructure existante.

6.4.7. DELAIS D'EXECUTION ET D'ADMISSION

La mission 4 débute à compter de la réception du bon de commande établi par le ministère.

Les prestations de la mission 4 doivent être réalisées dans les délais mentionnés dans le tableau ci-dessous :

M4 / UO	Livrables	Délai maximum de production des livrables (*)	Délais d'admission du ministère (*)	Délais de correction éventuelle du titulaire (*)
M4- FW-1 à M4-SWI-5	Le bon de livraison	15 jours	5 jours	3 jours
	La documentation technique	15 jours		
	Le bilan de l'installation de l'équipement	30 jours		
M4-EVO-FW-ET	Étude de l'intégration des nouvelles solutions additionnelles de sécurité de type pare-feu	30 jours après la commande	10 jours	5 jours
M4-EVO-FW-REA	Rapport d'activité concernant le paramétrage, l'installation, l'intégration des nouvelles solutions de sécurité de type pare-feu sur l'infrastructure existante	10 jours après la mise en service	5 jours	3

(*) Les délais s'expriment en jours ouvrés.

L'admission a pour objet de valider le contenu, la forme et la qualité des produits livrés. Elle est constatée de manière expresse par le ministère et matérialisée par un procès-verbal de recette définitive selon les conditions d'admission précisées à l'article 5.8 du présent CCTP.

En cas de dépassement des délais, des pénalités de retard sont appliquées conformément à l'article 16 du CCAP.

6.5. MISSION 5 : SERVICES CONSTRUCTEURS

6.5.1. OBJET DE LA MISSION 5

La mission 5 est constituée de prestations récurrentes. Elle a pour objet la souscription auprès des constructeurs et/ou éditeurs de matériel et/ou logiciel de « services constructeurs ».

6.5.2. DESCRIPTIONS DES SERVICES ATTENDUS

Dans le cadre de cette mission, le terme « services constructeurs » désigne :

- la (ré)assurance constructeur ;
- le (ré)abonnement constructeur ;
- la redevance/honoraires constructeur ;
- le re-licencing.

Le titulaire assure la gestion complète des abonnements, réassurances, et redevances auprès des constructeurs sur les équipements présents et à venir du parc du ministère.

À cette fin, le ministère délègue au titulaire la gestion en son nom et pour son compte des contrats de licences et de maintenance logicielles qu'il détient auprès du constructeur, aux fins de faire assurer par ce dernier la gestion des renouvellements et la mise à jour des versions logicielles, des équipements et des bases de sécurité des infrastructures du ministère.

Les services constructeurs souscrits par le titulaire au nom du ministère comprennent :

- l'accès au support constructeur par le titulaire pour les équipements du ministère, notamment pour escalade ;
- la mise à disposition par le constructeur auprès du titulaire de toutes les versions logicielles et mises à jour majeures des équipements ;
- le référencement des équipements du ministère auprès du constructeur ;
- Les réassurances/redevances « constructeurs ».

Chaque mois, le titulaire s'engage à fournir au ministère un état à jour sur la gestion des fins de licence. Cet indicateur est contractuel et pénalisable.

Le titulaire tient informé mensuellement le ministère des contrats de services et des dates de renouvellements des « services constructeurs ».

À cet égard, le titulaire s'engage notamment à :

- définir et mettre en œuvre auprès des constructeurs les niveaux de service requis ;
- vérifier le respect du calendrier et des délais ;
- alerter et transmettre au ministère, au minimum deux mois avant la fin de la période couverte, les unités d'œuvres nécessaires aux commandes des « services constructeurs ».
- commander au nom du ministère, après validation par ce dernier, les « services constructeurs » nécessaires ;
- Fournir au ministère mensuellement un état complet, équipement par équipement, des « services constructeurs » liés au parc.

En outre, le titulaire s'engage à fournir au ministère dès qu'il en a connaissance, les dates de fin de support et de fin de vie des matériels en place, ainsi que les versions logicielles de chacun des équipements du parc en production sur le ministère.

6.5.3. ROLES ET RESPONSABILITES

Le tableau ci-après précise les principales responsabilités entre, d’une part, le titulaire et d’autre part, le ministère.

(R = Réalise ; A = Approuve ; C = Contribue ; I = est Informé)

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Réalise la souscription du ministère aux « services constructeurs »	R	AI
Assure la gestion et le suivi des « services constructeurs »	R	AI
Présenter un état récapitulatif des « services constructeurs »	R	A

6.5.4. NIVEAUX DE SERVICE.

Sans objet.

6.5.5. UNITES D’ŒUVRE

Les prestations récurrentes de la mission 5 correspondent aux unités d’œuvre suivantes :

Code UO	UO	NB
L1-M5-FW-MNG	Checkpoint Management	2
L1-M5-FW-PRI	Checkpoint Appliance 4807	2
L1-M5-FW-SEC	Checkpoint Appliance 4807 HA	2
L1-M5-PROX-AV	McAfee Webgateway 5500C	2
L1-M5-DNS-DHCP-MNG	Efficient IP Solid Server-1000	2
L1-M5-DNSINT	Efficient IP Solid Server-1000	2
L1-M5-DNSEXT	Efficient IP Solid Server-260	2
L1-M5-DHCP	Efficient IP Solid Server-250	6
L1-M5-CŒUR-RT	Cisco C9500-24Q	4
L1-M5-CŒUR-SW-CU	Cisco C9300-48T	4
L1-M5-CŒUR-SW-FI	Cisco C9300-24S	2
L1-M5-CŒUR-SW	Cisco C9500-16X	4
L1-M5-LB	F5 BIGIP-LTM-I2800	4
L1-M5-RT-DMZ-48p	Cisco WS-C3560G-48TS	4
L1-M5-RT-ADER-24p	Cisco WS-C3560G-24TS	2

6.5.6. LIVRABLES

Le titulaire remet au ministère les livrables suivants :

- le bon de livraison et l'accusé réception par le constructeur et/ou éditeur du « service constructeur » concerné ;
- l'état complet, équipement par équipement, des « services constructeurs » liés au parc du ministère.

6.5.7. DELAIS D'EXECUTION ET D'ADMISSION

La mission 5 débute à compter de la réception du bon de commande établi par le ministère.

Les prestations de la mission 5 doivent être réalisées dans les délais mentionnés dans le tableau ci-dessous :

M5 / UO	Livrables	Délai maximum de production des livrables (*)	Délais d'admission du ministère (*)	Délais de correction éventuelle du titulaire (*)
M5-FW-MNG à M5-ADER-24p	Bon de livraison et accusé réception du « service constructeur »	10 jours	5 jours	3 jours
	État récapitulatif des « services constructeurs »	Mensuel	5 jours	3 jours

(*) Les délais s'expriment en jours ouvrés.

L'admission a pour objet de valider le contenu, la forme et la qualité des produits livrés. Elle est constatée de manière expresse par le ministère et matérialisée par un procès-verbal de recette définitive selon les conditions d'admission précisées à l'article 5.8 du présent CCTP.

En cas de dépassement des délais, des pénalités de retard sont appliquées conformément à l'article 16 du CCAP.

6.6. MISSION 6 : REVERSIBILITE

6.6.1. OBJET DE LA MISSION 6

La mission 6 est une prestation unique. Elle a pour objet la réalisation des opérations de réversibilité en fin de marché.

6.6.2. SERVICES ATTENDUS

La réversibilité doit permettre au ministère de reprendre la gestion de la fonction externalisée, soit pour l'exploiter directement, soit pour en confier l'exploitation à un tiers de son choix.

La phase de réversibilité peut être commandée à tout moment en cas de fin du marché, quelle que soit la cause de cette fin.

Les opérations liées à la préparation et la mise en œuvre de la phase de réversibilité sont décrites dans le plan de réversibilité, dont une version 1 est livrée dans le cadre de la mission 1 et périodiquement mise à jour, tout au long de la durée du marché afin de garantir au ministère un état permanent de réversibilité des prestations dans le cadre de la mission 2.

Conformément à son offre, le titulaire s'engage à apporter l'assistance nécessaire durant la période de migration afin de faciliter le transfert des moyens matériels et logiciels de sécurité, et la reprise de leur exploitation par le ministère ou tout tiers désigné par lui.

Le titulaire garantit la sécurité des données et des applications qui lui ont été confiées, conformément à ses obligations, lors de leur transfert.

En tout état de cause, la mise en œuvre du projet de réversibilité ne modifie en rien la qualité, les termes et les conditions des services fournis durant le marché et définis dans les documents contractuels.

Au titre de la phase de réversibilité, le titulaire est notamment tenu :

- de transférer à l'équipe du ministère ou du tiers désigné par celui-ci les informations sur le contexte fonctionnel et technique de l'ensemble du périmètre ainsi que sur les aspects de suivi du projet ;
- de préparer un support informatique défini par le ministère contenant tous les éléments (documentations, programmes, chaînes de compilation, etc.) qu'il gère et qui seront, à l'issue de cette prestation, placés sous la responsabilité du ministère ou du tiers désigné par lui. Cette mise à disposition doit être faite sous un format pouvant permettre au ministère d'installer ou de faire installer, le cas échéant, l'ensemble de ces éléments sur la plate-forme de son choix pour un examen approfondi par celui-ci ;
- d'assurer une formation fonctionnelle approfondie (du type formation utilisateur et administrateur) aux personnels désignés par le ministère, avec travaux pratiques sur poste de travail, en présence de représentants du ministère. Cette formation doit s'appuyer sur les documentations utilisateurs et techniques rédigées par le titulaire.

En particulier, au titre de cette prestation, le titulaire :

- débute la prestation avec le ministère ou le tiers désigné par lui et les représentants du ministère. Il s'agit, au plus, de deux jours de réunion en vue de valider le calendrier et les modalités pratiques de cette phase ;
- met à disposition tous les éléments et documents produits pendant le marché ;
- présente l'ensemble des composants techniques ou fonctionnels du projet ;
- répond aux questions du ministère ou du tiers désigné par lui concernant l'organisation pratique des configurations et des documentations techniques sous 48 heures ;
- présente l'organisation de la maintenance corrective actuelle et l'environnement de développement et d'exploitation (répertoires, installation, procédures mises en œuvre, périodicité et ordonnancement des opérations d'exploitation, etc.) ;
- accueille, durant deux semaines, deux ou trois personnes désignées par le ministère afin de leur permettre d'observer l'activité assurée par l'équipe projet en place (assistance téléphonique, l'exploitation des infrastructures du périmètre, etc.) ;
- communique au ministère ou au tiers désigné par lui, les réponses apportées aux demandes d'assistance téléphonique traitées pendant toute la durée du marché.

En sus des comités de gestion des services de la mission 2, le titulaire organise et anime a minima :

- Une réunion de lancement de la phase de réversibilité au cours de laquelle il fournit au ministère *a minima* les éléments suivants :
 - le calendrier détaillé de la phase de réversibilité ;
 - la description de l'ensemble des conditions et prérequis nécessaires à la bonne exécution de la phase de réversibilité ;
 - la présentation détaillée de l'organisation et des moyens techniques et humains mis en place pour assurer le parfait déroulement du projet de réversibilité ;
 - les processus de coordination et les modalités d'interaction retenus entre le titulaire et le ministère ou le tiers désigné par lui ;
 - les supports de formation.
- une réunion de clôture de la phase de réversibilité au cours de laquelle il fournit au ministère en particulier les éléments suivants :
 - la convention de services mise à jour ;
 - le plan d'assurance qualité mis à jour ;
 - le plan d'assurance sécurité mis à jour ;
 - les configurations des infrastructures du périmètre mises à jour ;
 - les schémas détaillés de l'infrastructure de sécurité du périmètre mis à jour ;
 - le document exhaustif des licences et maintenances relatives aux infrastructures du périmètre à jour ;

- les procédures et modes opératoires pour réaliser les prestations mis à jour
- les procédures d'escalade mises à jour ;
- les feuilles de présence aux formations émargées par les participants ;
- le PV de bascule de responsabilité
- le PV attestant du transfert des contrats de maintenance

À l'issue de cette mission et à la demande du ministère, le titulaire procède à la destruction de l'ensemble des données et documentation du ministère se trouvant dans son système, sous sa possession ou son contrôle.

6.6.3. ROLES ET RESPONSABILITES

Le tableau ci-après précise les principales responsabilités entre, d'une part, le titulaire et d'autre part, le ministère.

(R = Réalise ; A = Approuve ; C = Contribue ; I = est Informé)

ROLES ET RESPONSABILITES	TITULAIRE	MINISTERE
Assistance à la migration	R	A
Restitution au ministère de l'ensemble des matériels, logiciels et documentations qui lui ont été confiés durant le marché	R	A
Transfert au repreneur du contexte fonctionnel et technique de l'ensemble du périmètre	R	A
Réalisation d'un support informatique contenant tous les éléments (documentations, programmes, chaînes de compilation, etc....) qu'il gère	C	R
Assurer une formation fonctionnelle approfondie (du type formation utilisateur et administrateur) au repreneur	R	AI
Participe à la réunion de lancement de la phase de réversibilité et prépare les supports associés	R	CA
Participe à la réunion de clôture de la phase de réversibilité et prépare les supports associés.	R	A
Destruction de l'ensemble des données et documentation du ministère se trouvant dans son système, sous sa possession ou son contrôle	R	I

6.6.4. NIVEAUX DE SERVICE

Sans objet.

6.6.5. UNITES D'ŒUVRE

Les prestations uniques de la mission 4 correspondent aux unités d'œuvre suivantes :

Code UO	UO
M6-PU01	Réversibilité

6.6.6. LIVRABLES

Le titulaire remet les livrables attendus pour chaque réunion. Ils sont *a minima* ceux listés au 6.6.2 ci-dessus.

Le titulaire remet au ministère les livrables suivants :

- plan de réversibilité mis à jour ;
- support informatique contenant tous les éléments (documentations, programmes, chaînes de compilation, etc.) qu'il gère ;
- supports de formation fonctionnelle ;
- supports et compte rendu de la réunion de lancement de la phase de réversibilité ;
- supports et compte rendu de la réunion de clôture de la phase de réversibilité ;
- l'attestation de la destruction de l'ensemble des données et documentation du ministère se trouvant dans son système, sous sa possession ou son contrôle ;
- le PV de bascule de responsabilité ;
- le PV attestant du transfert des contrats de maintenance.

6.6.7. DELAIS D'EXECUTION ET D'ADMISSION

La mission 6 débute à compter de la réception du bon de commande correspondant. Sa durée d'exécution maximale est de 40 jours ouvrés.

Les prestations de la mission 6 doivent être réalisées dans les délais mentionnés dans le tableau ci-dessous :

M6 / UO	Livrables	Délai maximum de production des livrables (*)	Délais d'admission du ministère (*)	Délais de correction éventuelle du titulaire (*)
M6-PU01	Plan de réversibilité mis à jour	2 jours suivant la réunion de lancement de la phase de réversibilité	10 jours	3 jours
	Support informatique contenant tous les éléments (documentations, programmes, chaînes de compilation, etc.) qu'il gère			
	Supports de formation fonctionnelle			
	Supports et compte rendu de la réunion de lancement de la phase de réversibilité			
	Supports et compte rendu de la réunion de clôture de la phase de réversibilité.	2 jours suivant la réunion de clôture de la phase de réversibilité	10 jours	3 jours
	Attestation de la destruction de l'ensemble des données et documentation du ministère se trouvant dans son système, sous sa possession ou son contrôle	2 jours suivant la réunion de clôture de la phase de réversibilité		
	PV de bascule de responsabilité	2 jours suivant la réunion de clôture de la phase de réversibilité		

M6 / UO	Livrables	Délai maximum de production des livrables (*)	Délais d'admission du ministère (*)	Délais de correction éventuelle du titulaire (*)
	PV attestant du transfert des contrats de maintenance	2 jours suivant la réunion de clôture de la phase de réversibilité	10 jours	3 jours

(*) Les délais s'expriment en jours ouvrés.

L'admission a pour objet de valider le contenu, la forme et la qualité des produits livrés. Elle est constatée de manière expresse par le ministère et matérialisée par un procès-verbal de recette définitive selon les conditions d'admission précisées à l'article 5.8 du présent CCTP.

En cas de dépassement des délais, des pénalités de retard sont appliquées conformément à l'article 16 du CCAP.

ARTICLE 7. **GLOSSAIRE**

SIGLE	Désignation
MOEn	Maîtrise d'œuvre
USEn	Services de support
SUPn	Services de supervision et d'exploitation - Supervision
RESn	Services de supervision et d'exploitation – Maintien en opération des réseaux
MEPn	Services de supervision et d'exploitation – Mise en production
ADMn	Services d'administration - Administration
IMAn	Services d'administration - Installation