

## **Cahier des Clauses Techniques Particulières**

### **RELATIF AU RENOUVELLEMENT DE LA TIERCE MAINTENANCE APPLICATIVE DU**

**SI**



CCTP  
Renouvellement de la tierce maintenance  
applicative du SI Contentieux



| Edition | Date       | Nombre |
|---------|------------|--------|
| V0      | 08/01/2026 |        |

## TABLE DES MATIERES

|          |                                                                                                                  |           |
|----------|------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Généralités .....</b>                                                                                         | <b>4</b>  |
| 1.1      | Objet du document .....                                                                                          | 4         |
| 1.2      | Liste des annexes à ce document.....                                                                             | 4         |
| 1.3      | Textes réglementaires applicables & documentation de référence.....                                              | 4         |
| <b>2</b> | <b>Rappel du contexte.....</b>                                                                                   | <b>6</b>  |
| 2.1      | Système d'information SI Contentieux .....                                                                       | 6         |
| 2.2      | Organisation .....                                                                                               | 12        |
| <b>3</b> | <b>Prestations attendues .....</b>                                                                               | <b>13</b> |
| 3.1      | Généralités prestations .....                                                                                    | 13        |
| 3.2      | Prestation n°1 : Initialisation.....                                                                             | 13        |
| 3.3      | Prestation n°2 : Maintenance préventive, adaptative, corrective et Maintien en Condition de Sécurité (MCS) ..... | 15        |
| 3.4      | Prestation n°3 : Maintenance des licences.....                                                                   | 21        |
| 3.5      | Prestation n°4 : Etude et analyse d'impact.....                                                                  | 22        |
| 3.6      | Prestation n°5 : Mise en œuvre d'une évolution .....                                                             | 22        |
| 3.7      | Prestation n°6 : Formation des utilisateurs - optionnelle.....                                                   | 26        |
| 3.8      | Prestation n°7 : Réversibilité/Transférabilité.....                                                              | 27        |
| 3.9      | Prestation n°8 : Passage en C1DR.....                                                                            | 28        |
| <b>4</b> | <b>Pilotage opérationnel .....</b>                                                                               | <b>30</b> |
| 4.1      | Comitologie du SI .....                                                                                          | 30        |
| 4.2      | Suivi de prestations .....                                                                                       | 31        |
| 4.3      | Tableaux de bord des activités de maintenance .....                                                              | 31        |
| 4.4      | Dossier d'analyse des risques .....                                                                              | 32        |
| 4.5      | Gestion de la configuration .....                                                                                | 32        |
| 4.6      | Livrables & délais.....                                                                                          | 33        |
| <b>5</b> | <b>Exigences .....</b>                                                                                           | <b>34</b> |
| 5.1      | Exigences d'utilisabilité .....                                                                                  | 34        |
| 5.2      | Exigences techniques .....                                                                                       | 34        |
| 5.3      | Exigences de sécurité des systèmes d'information .....                                                           | 35        |

## 1 GENERALITES

Le présent document constitue le Cahier des Clauses Techniques Particulières (CCTP) pour le renouvellement de la tierce maintenance applicative et la mise à niveau technique du SI Contentieux, de la direction des affaires juridiques (DAJ), du centre interarmées de soutien juridique (CIJ) et des services locaux du contentieux (SLC) du SCA, et de la sous-direction des pensions (SDP) de la DRH-MD, que le Titulaire s'engage à respecter.

### 1.1 Objet du document

Ce document constitue le cahier des clauses techniques (CCTP) du nouveau marché qui a pour objet le renouvellement de la tierce maintenance applicative du SI Contentieux et la mise à niveau technique de ce SI avec les standards du ministère des armées et des anciens combattants.

Les prestations attendues dans le cadre de ce présent CCTP sont les suivantes :

- Prestation n°1 : Initialisation
- Prestation n°2 : Maintenance préventive, adaptative et corrective et maintien en condition de sécurité (MCS)
- Prestation n°3 : Maintenance des licences
- Prestation n°4 : Etude et Analyse impact
- Prestation n°5 : Mise en œuvre d'une évolution
- Prestation n°6 : Formation des utilisateurs
- Prestation n°7 : Réversibilité/transférabilité
- Prestation n°8 : Passage en C1DR

Le Titulaire aura le choix sur son mode de fonctionnement : en mode Agile ou en cycle en V.

Il devra motiver son choix et respecter les spécificités du mode choisi.

### 1.2 Liste des annexes à ce document

- Annexe 1 – Plan de management du produit SI Contentieux (PMP) établi par l'Administration ;
- Annexe 2 – CCT en vigueur en version NP + annexe contenant la pile logicielle générale
- Annexe 3 – Prérequis C1DR

### 1.3 Textes réglementaires applicables & documentation de référence

| Descriptif du document                                                     | Protection  | Origine | Validité             |
|----------------------------------------------------------------------------|-------------|---------|----------------------|
| <b>Généralités</b>                                                         |             |         |                      |
| <b>{R-01}</b> Référentiel Général d'Interopérabilité (RGI)                 | Non protégé | DINSIC  | 2.0 du 20/04/2016    |
| <b>{R-02}</b> Référentiel général d'amélioration de l'accessibilité (RGAA) | Non protégé | DINSIC  | V4.1.2 du 18/04/2023 |

| Descriptif du document                                                                                                                                          | Protection           | Origine             | Validité                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|---------------------|-------------------------------|
| <b>{R-03}</b> Charte internet de l'État (diffusée par circulaire du 1er Ministre n°5574/SG du 16 février 2012)                                                  | Non protégé          | DINSIC <sup>1</sup> | 16/02/2012                    |
| <b>Architecture technique</b>                                                                                                                                   |                      |                     |                               |
| <b>{R-04}</b> Cadre de cohérence technique des systèmes d'information et de communication du Ministère de la Défense                                            | Diffusion restreinte | DGNUM               | v.3.7 du 17/02/2026           |
| <b>Sécurité des systèmes d'information</b>                                                                                                                      |                      |                     |                               |
| <b>{R-05}</b> Instruction générale interministérielle n°1300/SGDN/PSE/PSD sur la protection du secret de la défense nationale                                   | Non protégé          | ANSSI <sup>2</sup>  | 09/08/2021                    |
| <b>{R-06}</b> Instruction ministérielle n°900/ARM/CAB/NP : protection de l'information et des données                                                           | Non protégé          |                     | 27/08/2025                    |
| <b>{R-07}</b> Instruction interministérielle n°901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles, dans ses dispositions du Titre II | Non protégé          | ANSSI               | 28/01/2015                    |
| <b>{R-08}</b> Référentiel général de sécurité (RGS)                                                                                                             | Non protégé          | ANSSI               | v.2.0 du 13/06/2014           |
| <b>{R-09}</b> Politique de sécurité des systèmes d'information de l'État (PSSIE) <sup>3</sup>                                                                   | Non protégé          | ANSSI               | Circ. N°5725/SG du 17/07/2014 |
| <b>{R-10}</b> Référentiel d'exigences applicables aux prestataires de services d'informatique en nuage (SecNumCloud)                                            | Non protégé          | ANSSI               | v3.2 du 08/02/2022            |
| <b>{R-11}</b> Directive n°29/DEF/DGSIC portant sur la gestion des traces et leur gestion au Ministère de la Défense                                             | Non protégé          | DGNUM               | 12/11/2013                    |

<sup>1</sup> <http://references.modernisation.gouv.fr>

<sup>2</sup> [https://www.sgdsn.gouv.fr/files/files/Nos\\_missions/igi-1300-20210809.pdf](https://www.sgdsn.gouv.fr/files/files/Nos_missions/igi-1300-20210809.pdf)

<sup>3</sup> [http://circulaire.legifrance.gouv.fr/pdf/2014/08/cir\\_38641.pdf](http://circulaire.legifrance.gouv.fr/pdf/2014/08/cir_38641.pdf)

## 2 RAPPEL DU CONTEXTE

### 2.1 Système d'information SI Contentieux

#### 2.1.1 Présentation générale

SI Contentieux est un système d'information mis en production en juin 2024. Il est destiné à être utilisé par les acteurs de la gestion du contentieux, soit la Sous-direction du contentieux de la Direction des Affaires Juridiques à Balard, le Service des Pensions et des Risques Professionnels à la Rochelle et la filière juridique du Service du commissariat des armées (Centre interarmées de soutien juridique, Services Locaux du Contentieux, DIRCOM et DICOM - Outre-mer). Le CIJ, les SLCs et les DIRCOM/DICOM sont implantés sur plusieurs sites déconcentrés sur l'ensemble du territoire national, y compris l'outre-mer.

SI contentieux sera le système unique pour le suivi du contentieux au Ministère des armées et des anciens combattants pour l'ensemble des juristes. Il a pour objectif d'harmoniser le processus de gestion et pilotage du contentieux.

Le système d'information SI Contentieux traite des informations de niveau Diffusion Restreinte (DR)

Les caractéristiques de ces données sont de niveau DR comptant des données à caractères personnels et des données de santé. La sensibilité des données est traitée dans le chapitre correspondant.

Legisway Enterprise est une solution progicielle de la société Wolters Kluwer, leader dans le domaine de la « Legaltech » et présente au sein de différents organismes (Thales, CNAM, INRIA, SNCF...).

Le terme « SI Contentieux » désigne le système informatique mis à disposition des utilisateurs du Ministère des armées et des anciens combattants. Le terme « Legisway » désigne la solution technique retenue pour outiller SI Contentieux.

Le renouvellement de la maintenance applicative du SI Contentieux doit tenir compte d'un enjeu clé : SI Contentieux remplacera à terme le SI SUDOCO, utilisé par la filière juridique du SCA, en reprenant les fonctionnalités et les données de ce système. A terme, 350 agents environ utiliseront au quotidien la solution.

Le système ne comprend qu'un volet INTRADEF (solution persistante).

#### 2.1.2 Périmètre du produit

On définit le « contentieux » par l'ensemble des affaires litigieuses dans lesquelles une entité du Ministère peut se trouver impliquée, tant comme responsable que comme victime. Le service juridique en charge du contentieux est alors amené à produire les éléments permettant de défendre la partie concernée devant les tribunaux ou via des transactions à l'amiable.

L'activité contentieuse du ministère des armées et des anciens combattants comprend plusieurs activités :

- Le « précontentieux » : phase « amiable » antérieure à la phase contentieuse. Durant cette phase, chacune des parties impliquées essaie de trouver un terrain d'entente sur lequel conclure un accord, pour éviter un éventuel contentieux. Le ministère des armées et des anciens combattants produit un « protocole transactionnel », document pouvant se définir comme « un contrat par lequel

les parties, par des concessions réciproques, terminent une contestation née, ou préviennent une contestation à naître ».

Le « contentieux » : phase qui débute lorsqu'une requête est déposée par un plaignant (le requérant) à l'encontre d'une autre partie. Durant cette phase, chacune des parties produit, devant le tribunal, les éléments (mémoires) nécessaires à sa défense.

- La « protection juridique » : désigne l'assistance juridique apportée par l'administration à un agent public en cas de préjudice subi dans le cadre de ses fonctions. Il s'agit donc des demandes formulées par des personnels de la défense, civils ou militaires, de protection juridique face à des faits survenus dans l'exercice de leurs « fonctions » (d'où le terme de protection « fonctionnelle »). En règle générale, la demande de protection juridique, dans le cas d'une décision d'octroi de protection, débouche sur une prise en charge des frais d'avocat associés. A ce titre, une convention de prise en charge des frais d'avocat est établie entre le ministère des armées et des anciens combattants et le cabinet d'avocat choisi par le personnel victime.

- Le conseil juridique : Les entités en charge du contentieux jouent également un rôle de conseil juridique. A ce titre, elles émettent des avis juridiques en réponse à des questions pouvant être posées par toute entité du ministère des armées et des anciens combattants, sur quelque question à caractère juridique que ce soit.

- Les "dons et legs" : vise à traiter l'ensemble des demandes de dons ou de legs du ministère des armées et des anciens combattants. Les acteurs internes sont le secrétariat de la DAJ/CX, qui reçoit les demandes de dons et legs par différents canaux (courriers, mails, ...) et les attribue au bureau BCG qui traite actuellement l'ensemble des dossiers de dons et legs. À noter que dans le futur, il est possible que d'autres services et bureau traitent ce type de dossiers. Le paramétrage a été pensé en conséquence.

- Les "expertises médicales" : dans le cadre du traitement d'un dossier Précontentieux ou Contentieux, et notamment en cas de préjudice physique subi par le demandeur, le responsable de l'élaboration du dossier pourra solliciter la cellule d'expertise médicale pour une demande d'avis médical ou d'une demande d'expertise via ce module dédié aux expertises médicales.

- L'exécution financière : l'exécution financière désigne les procédures d'indemnisation ou de recouvrement de sommes par le ministère des armées et des anciens combattants dans le cadre de l'exécution de décisions de justice, de protocoles transactionnels, de paiement de factures ou de l'exécution d'obligations légales. Le module couvre le contrôle interne par le Bureau Management Finances (BMF) des pièces justifiant l'indemnisation ou le recouvrement, la transmission dématérialisée de ces pièces justificatives au service exécutant, la gestion des éventuels rejets, oppositions ou admissions en non-valeur et le suivi de la bonne exécution des paiements et recouvrements.

### 2.1.3 Population ciblée

La cible d'utilisation est l'ensemble des agents de la Sous-direction du contentieux de la DAJ à Balard, le Service des Pensions et des Risques Professionnels à la Rochelle et la filière juridique du Service du Commissariat des Armées (centre interarmées de soutien juridique, les services locaux du contentieux, les directions du commissariat en OME (Outre-Mer étranger) et les directions du commissariat en opération), civils et militaires, du ministère des armées et des anciens combattants.

#### **2.1.4 Politique d'embarquement des agents**

Les agents de la Sous-direction du contentieux de la DAJ à Balard n'avaient pas d'outils avant la mise en place de SI Contentieux : l'embarquement a donc été immédiat.

Les agents du CIJ, des SLCs et des DIRCOM/DICOM ont, l'outil SUDOCO, du SCA. Le passage de l'ancien vers le nouveau système, SI Contentieux, s'est fait progressivement avec une reprise des données SUDOCO.

Les agents du SPRP n'ont pas d'outils pour traiter leurs dossiers : l'embarquement sera immédiat dès lors que le SI leur sera ouvert.

#### **2.1.5 Architecture technique**

SI Contentieux se base sur l'outil « legisway » de la société Wolters Kluwer, acquis « sur étagère » et dont les possibilités de paramétrage permettent de répondre aux besoins du ministère.

Le volet INTRADEF de SI Contentieux s'adresse à l'ensemble des agents du ministère pouvant être amené à suivre du contentieux, et comprend quatre instances : Intégration (PICSEL, en cours de création à date), Formation, Pré-production et Production.

##### Volet INTRADEF PICSEL - Plateforme (solution persistante)

Permet de réaliser les tests d'intégration avant la mise en pré-production, préalable au passage en C1DR. Elle est administrée par un agent du MINARM.

Première étape du parcours vers le cloud, la plateforme PICSEL fournit des outils de développement et de test modernes, conformes aux meilleures pratiques du secteur. La disponibilité de services représentatifs des différents environnements simplifie les phases de test. Par ailleurs, le contrôle qualité associé à une chaîne de livraison automatisée (CI/CD orientée GitOps) renforce la fiabilité et accélère la mise à disposition pour les utilisateurs.

##### Volet INTRADEF Formation :

L'environnement Formation est destiné exclusivement à l'acquisition et à la montée en compétence des utilisateurs.

Il permet :

- La mise à disposition d'un système identique, sur le plan fonctionnel, à celui de la production ;
- La réalisation de sessions de formation internes ou externes, avec un jeu de données adapté (anonymisé ou fictif) ;
- La simulation de scénarios métier sans impact sur les environnements de test ou de production.

Caractéristiques :

- Données représentatives et conformes aux normes de sécurité ;
- Paramétrage aligné sur la version en production ;
- Possibilité de réinitialisation régulière pour maintenir un contexte de formation optimal.

##### Volet INTRADEF Pré-production :

L'environnement Pré-production a pour objectif de valider les évolutions avant leur mise en service. Il sert d'espace de recette technique et fonctionnelle, au plus proche des conditions réelles d'exploitation.

Fonctions principales :

- ➔ Test et validation des correctifs, évolutions applicatives et mises à jour techniques ;
- ➔ Vérification des performances et de la compatibilité avec l'infrastructure existante ;
- ➔ Simulation des opérations de déploiement afin de limiter les risques en production.

Caractéristiques :

- Configuration matérielle et logicielle identique à la production ;
- Données représentatives et conformes aux normes de sécurité ;
- Accès restreint aux équipes de développement, de test et d'exploitation.

Volet INTRADEF Production :

L'environnement Production constitue le système opérationnel, en exploitation continue, accessible aux utilisateurs finaux.

Principes :

- Héberge les applications et services dans leur version stable et validée.
- Garantit un haut niveau de disponibilité, de performance et de sécurité.
- Soumis à une supervision en temps réel et à des procédures strictes de sauvegarde et de restauration.

Caractéristiques :

- Données réelles et critiques pour l'activité.
- Accès strictement contrôlé et journalisé.
- Changements soumis à un processus de validation préalable en pré-production.

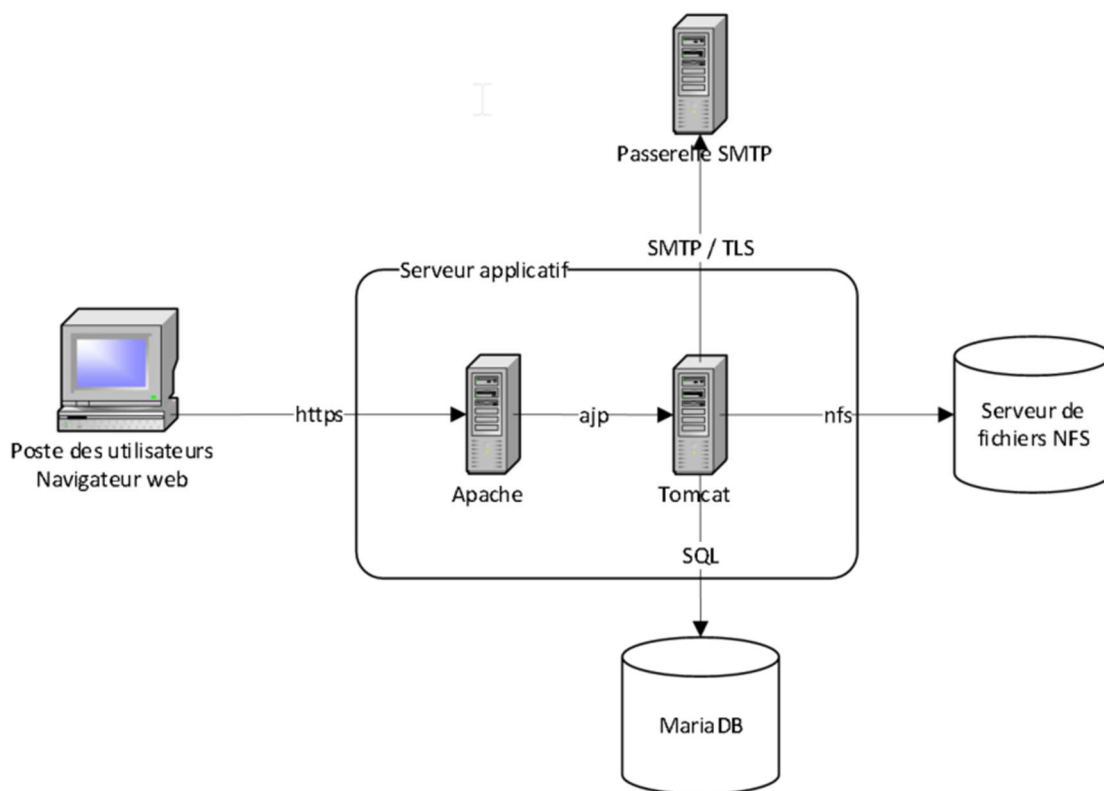
Authentification & accès :

La connexion à l'outil doit se faire par une double authentification via le composant Mindef Connect INTRADEF OpenID Connect et une vérification par mail.

**2.1.6 Architecture matérielle**

Le SI Contentieux est basé sur la solution legisway. Elle est hébergée sur un serveur d'applications. Le stockage des données est réalisé dans une base de données relationnelle. Les documents qui peuvent être rattachés à certains objets métier sont stockés dans un serveur de fichier (le lien étant stocké en base de données).

- Architecture INTRADEF :



**Figure 1 - Architecture technique**

Les serveurs sont fournis et installés par le CND.

Caractéristiques des plateformes de formation, pré-production, et production :

La pile logicielle n'est actuellement pas à jour ni conforme au CCT pour certains éléments, des travaux de modernisation sont en cours.

➔ Environnement de formation :

| Rôle ou fonction serveur         | OS                        | CPU                    | RAM (Go) | Stockage immédiat                 | Stockage dans 3 ans |
|----------------------------------|---------------------------|------------------------|----------|-----------------------------------|---------------------|
| <b>Serveur Applicatif</b>        | CentOS 7.8 avec OpenJDK 8 | 8 CPU 64 bits à 2 Ghz  | 12       | 500 Go disque SATA avec cache SSD | 1 To                |
| <b>Serveur Base de données</b>   | CentOS 7.8                | 20 CPU 64 bits à 2 Ghz | 12 (8)   | 1 To                              | 2 To                |
| <b>Serveur de fichiers (NFS)</b> | CentOS 7.8                | 4 CPU 64 bits à 2 Ghz  | 8        | 1 To (RAID 5)                     | 2 To (RAID 5)       |

→ Environnement de Pré-Production

| Rôle ou fonction serveur         | OS                        | CPU                    | RAM (Go) | Stockage immédiat                 | Stockage dans 3 ans |
|----------------------------------|---------------------------|------------------------|----------|-----------------------------------|---------------------|
| <b>Serveur Applicatif</b>        | CentOS 7.8 avec OpenJDK 8 | 8 CPU 64 bits à 2 Ghz  | 12       | 500 Go disque SATA avec cache SSD | 1 To                |
| <b>Serveur Base de données</b>   | CentOS 7.8                | 20 CPU 64 bits à 2 Ghz | 12       | 1 To                              | 2 To                |
| <b>Serveur de fichiers (NFS)</b> | CentOS 7.8                | 4 CPU 64 bits à 2 Ghz  | 8        | 1 To (RAID 5)                     | 2 To (RAID 5)       |

→ Environnement de Production

| Rôle ou fonction serveur         | OS                        | CPU                    | RAM (Go) | Stockage immédiat                 | Stockage dans 3 ans |
|----------------------------------|---------------------------|------------------------|----------|-----------------------------------|---------------------|
| <b>Serveur Applicatif</b>        | CentOS 7.8 avec OpenJDK 8 | 8 CPU 64 bits à 2 Ghz  | 12       | 500 Go disque SATA avec cache SSD | 1 To                |
| <b>Serveur Base de données</b>   | CentOS 7.8                | 20 CPU 64 bits à 2 Ghz | 12 (8)   | 1 To                              | 2 To                |
| <b>Serveur de fichiers (NFS)</b> | CentOS 7.8                | 4 CPU 64 bits à 2 Ghz  | 8        | 1 To (RAID 5)                     | 2 To (RAID 5)       |

→ Environnement PICSEL : à venir

### 2.1.7 Architecture logicielle

Serveur applicatif :

- Apache 2.4
- Tomcat 9
- Compte de service dédié
- Runtime Java 8 (JRE)

Serveur de base de données :

- MariaDB 10.4
- Compte de service dédié

Serveur de fichiers :

- NFSv4
- Compte de service dédié
- Partage uniquement vers le serveur applicatif

L'application propose le téléchargement de fichiers par les utilisateurs en tant que pièces jointes. Ces fichiers sont stockés directement dans le système de fichiers du serveur.

### 2.1.8 Conformité au cadre de cohérence technique (CCT) en vigueur

L'architecture SI Contentieux doit-être conforme aux préconisations du Cadre de Cohérence Technique (CCT) en vigueur. Il appartient au Titulaire de vérifier auprès de l'Administration qu'il détient la dernière version à jour du CCT.

### 2.1.9 Sensibilité des données

Le volet INTRADEF est hébergé sur les infrastructures techniques ministérielles.

SI Contentieux traite, manipule et expose sur l'INTRADEF des données dont la sensibilité peut aller jusqu'à « Diffusion restreinte » (DR).

Il contient des données à caractère personnel :

- ➔ Données administratives ;
- ➔ Données médicales
- ➔ Données de type identité, état civil, données d'identification (nom, prénoms, adresses, adresses mail, numéro INSEE...) ;
- ➔ Sanctions : données relatives aux condamnations pénales et aux infractions.

Il appartient à chaque utilisateur de s'assurer que les données insérées sont conformes aux limitations ci-dessus. Le Titulaire, lorsqu'il a connaissance du non-respect de ces limitations, alerte l'administrateur fonctionnel et le responsable technique de système.

## 2.2 Organisation

Le système SI Contentieux s'inscrit dans les procédures de gouvernance des systèmes d'administration et de gestion (SIAG), pilotées par la DSI transverse du SGA.

La Direction d'Application du système SI Contentieux est en charge du pilotage opérationnel, centrale et transverse, afin de garantir la cohérence d'ensemble des paramétrages réalisés, la cohabitation harmonieuse des autorités utilisatrices et l'interopérabilité de leurs données.

### 2.2.1 Principaux acteurs

| Acteur                                      | Organisme responsable                                                                    |
|---------------------------------------------|------------------------------------------------------------------------------------------|
| <b>Autorité cliente</b>                     | DAJ                                                                                      |
| <b>Autorités utilisatrices</b>              | Les autorités utilisatrices sont la DAJ, le SPRP et les CIJ/SLCs, (dont DICOM et DIRCOM) |
| <b>Responsable technique de système</b>     | DTPM (département systèmes d'information, pôle des applications et projets techniques)   |
| <b>Responsable fonctionnel d'ensemble</b>   | DAJ                                                                                      |
| <b>Représentant du pouvoir adjudicateur</b> | CND                                                                                      |

### 3 PRESTATIONS ATTENDUES

---

#### 3.1 Généralités prestations

Chaque prestation correspond à un ensemble d'actions à réaliser par le Titulaire et donne lieu à la fourniture d'un ou plusieurs livrables (logiciel et/ou documentation).

##### Méthode de tests, deux options

➔ Option 1 : Le Titulaire choisit de travailler en cycle en V

Pour chaque prestation, les délais de Vérification d'Aptitude (VA) et Vérification de Suivi Régulier (VSR) sont déterminés comme suit :

- VA : 2 mois maximum
- VSR : 3 mois maximum

➔ Option 2 : Le Titulaire choisit de travailler en mode Agile

Pour chaque prestation, trois itérations (sprint) pourront être réalisées. Une itération comprend : une mise en ordre de marche et une VA. A l'issue, une itération en PROD sera réalisée. Celle-ci comprend une Mise en production et une VSR.

##### Neutralisation

Pour des raisons d'organisation, les périodes suivantes sont neutralisées :

- Du 23 décembre au 02 janvier de chaque année ;
- Le mois d'août de chaque année.

Aucune neutralisation ne sera effectuée pour tenir compte d'une éventuelle fermeture des Établissements du titulaire (ou des co-traitants ou des sous-traitants).

#### 3.2 Prestation n°1 : Initialisation

Au cours de cette phase d'initialisation, le Titulaire s'approprie le contexte.

Cette prestation d'initialisation permet au Titulaire de :

- Prendre connaissance du contexte technique et organisationnel global, se familiariser avec les processus existants, cadrer les travaux avec les différents acteurs identifier par l'Administration et rédiger les livrables attendus ;
- Etablir un état des lieux de la documentation existante ;
- Mettre en place les ressources et l'outillage nécessaires pour assurer les prestations du marché.

##### **3.2.1 Phase de transférabilité/réversibilité de la TMA**

Le Titulaire sortant assure un transfert de connaissance complet vers l'équipe de reprise et permettant à cette dernière de reprendre la maintenance corrective et évolutive de l'applicatif et en particulier :

##### 1) Au début de la phase de transférabilité :

- l'organisation d'une réunion de revue de lancement, avec l'administration et le preneur,

##### 2) Durant la phase de transférabilité :

- une présentation de l'organisation de la tierce maintenance applicative d'une durée minimum de

1 jour ouvré,

**3) En fin de phase :**

- la participation à une réunion de clôture du transfert organisé par le preneur.

### **3.2.2 Plan de management et d'assurance qualité**

Le Titulaire rédige une première version du plan de management et d'assurance qualité qui sera ensuite mis à jour tout au long du marché.

Ce document décrit l'ensemble des tâches qu'il s'engage à réaliser pour mener à bien le projet et y précise les prérequis, le responsable, les contributeurs éventuels, les livrables attendus de l'Administration. Il le met à jour le cas échéant.

Le plan de management et d'assurance qualité comprend obligatoirement les éléments suivants :

- La décomposition des prestations ;
- L'échéancier global ;
- L'organisation du projet, incluant les acteurs et leurs responsabilités respectives ;
- La démarche de conduite du projet (organigramme des tâches, logique de déroulement du projet, moyens et ressources nécessaires, méthodologie) ;
- Les modalités de suivi du projet ;
- Le management des risques ;
- La gestion de la configuration ;
- Le dispositif d'assurance qualité.

Le dispositif d'assurance qualité est constitué par l'ensemble des dispositions de prévention et de contrôle jugées appropriées pour assurer, contrôler, vérifier, valider et qualifier l'obtention du niveau de qualité requis par le projet, ainsi que les objectifs qualité qu'il juge pertinents.

### **3.2.3 Plan d'assurance sécurité**

Le Titulaire rédige une première version du plan d'assurance sécurité décrivant les dispositions établies pour répondre aux exigences de sécurité pendant la durée du marché.

Il sera mis à jour à chaque évolution.

Ce document contient, *a minima*, les informations suivantes :

- Objet du document ;
- Documents de référence ;
- Description du système externalisé ;
- Rappel des exigences ;
- Organisation ;
- Responsabilités liées au PAS (dont relations avec les tiers contractants du prestataire, cybersécurité, sécurité des données RGPD et réversibilité) ;
- Procédure d'évolution du PAS ;
- Mesures de sécurité ;
- Matrice de couverture des exigences de sécurité ;
- Documentation de suivi.

Le plan d'assurance sécurité doit mentionner la réversibilité/transférabilité (Prestation N°7).

### 3.2.4 Réunion de lancement des prestations

Le Titulaire organise, à une date fixée par l'administration, une réunion de lancement dans un délai de 15 jours ouvrés à compter de la date de notification du bon de commande d'initialisation (ou de la date de début d'exécution ultérieure fixée par ce bon de commande). Cette réunion de lancement se déroule sur le site de l'Administration à Paris.

La date de cette réunion de lancement est définie comme le jalon T1 dans le calendrier du projet.

La réunion de lancement a pour objectifs :

- La présentation du contexte ;
- La présentation des membres de l'équipe du titulaire, ainsi que leurs rôles et leurs responsabilités ;
- Un état des lieux de la documentation ;
- L'initialisation des procédures de travail et du calendrier de la prestation ;
- Le rappel des résultats attendus et des démarches par prestation ;
- La présentation du plan de management et d'assurance qualité (version initiale) ;
- La présentation du plan d'assurance sécurité (version initiale) ;
- La présentation de la démarche mise en œuvre pour le déroulement des prestations.

### 3.2.5 Livrables & délais

| Livable                                             | Type de vérification | Délai de livraison              |
|-----------------------------------------------------|----------------------|---------------------------------|
| Support de la réunion de lancement                  | VQ                   | T1 - 3 jours ouvrés             |
| Plan de management et d'assurance qualité définitif | VQ                   | T1 + 15 jours ouvrés            |
| Plan d'assurance sécurité définitif                 | VQ                   | T1 + 15 jours ouvrés            |
| Compte rendu de la réunion                          | VQ                   | 5 jours ouvrés après la session |

### 3.3 Prestation n°2 : Maintenance préventive, adaptative, corrective et Maintien en Condition de Sécurité (MCS)

Le titulaire s'engage à assurer la maintenance du SI Contentieux et des licences logicielles de la solution Legisway, acquises dans le cadre du précédent marché (EJ n°1200067871), indispensables à l'utilisation de la solution fournie. Cette maintenance inclut notamment:

- L'accès à SI Contentieux continu et conforme aux conditions d'utilisation de l'éditeur ;
- Le support utilisateur de niveau 2 et de niveau 3 ;
- La maintenance préventive, adaptative et corrective ;
- Le maintien en condition de sécurité ;

Il est rappelé que :

- Le Titulaire est tenu à une obligation de résultat et de discrétion ;
- La télémaintenance depuis un poste extérieur à l'INTRADEF est proscrite. Le titulaire s'engage à se rendre sur un site du MINARM.

## **Support utilisateur**

Le titulaire s'engage à fournir un support technique de **niveau 2 et de niveau 3**, incluant les prestations suivantes :

- **Niveau 2** : analyse et résolution des incidents et des anomalies de fonctionnement courants, assistance fonctionnelle avancée ;
- **Niveau 3** : traitement des incidents nécessitant une expertise technique ou applicative approfondie (code source, architecture logicielle, base de données, etc.), correction des anomalies, et développement de correctifs ou de patches.

Le support est accessible, par téléphone (service et appel gratuit) ou par email, durant les horaires suivants du lundi au vendredi de 9h à 18h, hors jours fériés.

Le support de niveau 1 est assuré par les ressources de l'Administration.

## **Maintenance préventive, adaptative, corrective et maintien en condition de sécurité**

Par maintenance préventive, on entend les mesures d'entretien exécutées pour éviter la survenance d'anomalies. La mise en production d'une version mineure préventive de SI CONTENTIEUX au titre de la TMA est décidée par l'Administration.

Par maintenance adaptative, on entend les mesures d'entretien et de maintenance permettant d'absorber des modifications de l'environnement technique d'exécution, comme les mises à jour ou les changements de systèmes d'exploitation, de bases de données, d'interfaces d'échange ou plus généralement des composants techniques et bibliothèques logicielles.

Par maintenance corrective, on entend toute intervention consistant à corriger tout incident en production affectant SI Contentieux et entraînant la modification, le changement d'un composant, la montée en version mineure d'un élément portant aussi bien sur l'architecture que sur l'application :

- Suite à une anomalie, un défaut de l'application, une défaillance technique sans modification du périmètre fonctionnel ;
- Ou pour garantir le bon fonctionnement du système dans le temps :
  - Modification ou remplacement d'un composant dans le but de palier à une obsolescence ou d'augmenter les performances du système ;
  - Maintien de la compatibilité du système avec l'environnement d'exploitation sur les infrastructures de l'Administration.

SI Contentieux est considéré comme remis en état dès lors que son fonctionnement nominal est rétabli.

Dans le cadre de la maintenance corrective, sur constat d'anomalie réalisé par l'Administration ou par le Titulaire, l'Administration applique la typologie des anomalies décrites au paragraphe 3.3.1 - Qualification des faits techniques ainsi que les exigences de traitement correspondantes.

Toute anomalie nécessitant l'intervention du Titulaire doit faire l'objet d'une déclaration dans l'outil de gestion des anomalies de référence, précisant les conditions d'apparition de l'anomalie et son degré de criticité. Le Titulaire analyse l'impact de l'anomalie notamment sur les données, la sécurité, la disponibilité du service et les processus métier concerné. Il détermine avec l'Administration le scénario de correction le plus adapté, en tenant compte de ces éléments.

Après avoir effectué les actions correctives, le Titulaire procède à la livraison d'une nouvelle version applicative corrective, ou du paramétrage modifié, ou d'une solution de contournement provisoire permettant un usage nominal de SI Contentieux en attendant une correction définitive.

Une solution de contournement est une action temporaire visant à restaurer partiellement ou totalement l'usage d'un service ou d'une fonctionnalité en cas d'anomalie, dans l'attente d'une correction définitive. Elle permet de limiter l'impact fonctionnel, opérationnel ou technique du problème identifié, sans supprimer sa cause.

Dans le cadre de ses activités de maintenance, le titulaire met à jour la documentation fonctionnelle et technique.

Par maintien en condition de sécurité, on entend que le titulaire assure à l'Administration que SI Contentieux conserve un niveau de sécurité constant, adapté à l'évolution de la menace et des vulnérabilités. Elle intègre le suivi, la prise en compte et l'application des correctifs de sécurité.

### **3.3.1 Qualification des faits techniques**

Les faits techniques consistent en :

- Des anomalies, soit des défauts de conception qui causent des dysfonctionnements du système ;
- Des modes opératoires inadaptés/perfectibles pour une fonctionnalité ;
- Des questions sur le comportement d'une fonctionnalité lorsqu'on l'exploite à ses limites ;
- L'Identification de compléments à apporter à la documentation (technique ou fonctionnelle).
- Un problème ou une observation liée à l'infrastructure, à l'environnement ou à des contraintes techniques.

Il appartient à l'Administration de décider du niveau de criticité et de la caractérisation des faits techniques relevées.

Les faits techniques sont formalisés par l'Administration dans l'outil de gestion des incidents de référence, BRIDGE. La date de création du fait technique dans BRIDGE fera référence vis-à-vis du titulaire pour le traitement des faits techniques. Les tickets seront transmis par voie électronique au fil de l'eau, puis seront accessibles directement par le titulaire lorsque qu'il disposera d'un accès à Bridge.

Le fait technique est clos après validation par l'Administration des corrections apportées, cette validation étant enregistrée dans l'outil de gestion des incidents ou transmise par courriel.

Sur constat d'un fait technique réalisé par l'Administration ou par le Titulaire, l'Administration classe le fait technique selon une typologie qui déterminera les délais de prise en charge et de correction ainsi que le type de correction attendus.

Le Titulaire applique les modalités de qualification des faits techniques » ainsi que les exigences de traitement rappelées dans le tableau suivant :

| Type                           | Caractérisation                                                                                                                                                                                         | Délai de prise en charge                              | Type de correction attendue                                       | Délai maximum de correction attendu |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------|
| <b>Fait technique bloquant</b> | Empêche le déroulement d'un processus métier et devant faire l'objet d'une correction ou d'une solution de contournement dans un délai de 1 jour ouvré.                                                 | Dans les 2h suivant la déclaration du fait technique  | Correction définitive ou solution de contournement                | 1 jour ouvré                        |
|                                | Dans le cas de la mise en œuvre d'une solution de contournement, après accord de l'administration, le délai de correction du fait technique devient celui d'un fait technique majeure (7 jours ouvrés). |                                                       | Correction définitive dans le cas d'une solution de contournement | 7 jours ouvrés                      |
| <b>Fait technique majeur</b>   | Autorise le fonctionnement partiel d'une ou plusieurs fonctionnalités et qui peut être contourné par l'utilisateur, mais avec des performances dégradées.                                               | Dans les 24h suivant la déclaration du fait technique | Correction définitive                                             | 7 jours ouvrés                      |
| <b>Fait technique mineur</b>   | N'impacte pas ou très peu l'utilisateur.                                                                                                                                                                | Dans les 48h suivant la déclaration du fait technique | Correction définitive (*)                                         | 15 jours ouvrés                     |

(\*) : les corrections correspondantes peuvent être livrées dans le cadre de regroupements de plusieurs anomalies.

Les délais stipulés ci-dessus s'entendent à compter de la date et heure de réception par le Titulaire de la demande d'intervention émise suite au constat d'un fait technique.

### 3.3.2 Activités de maintien en condition de sécurité.

Pour chaque vulnérabilité identifiée, le Titulaire alerte l'Administration, propose et met en œuvre les mesures nécessaires au maintien en condition de sécurité de SI Contentieux. La prestation inclut la mise à niveau de la documentation lorsque la portée des mesures mises en œuvre le requiert.

En cas de régression ou d'anomalie engendrée par l'installation d'un correctif de sécurité, le Titulaire doit réaliser les modifications nécessaires à sa bonne intégration.

Le Titulaire propose un accompagnement d'une journée maximum aux administrateurs fonctionnels et techniques de SI Contentieux dans le cas où la version livrée au titre du MCS impacte les modalités d'exploitation ou d'administration de SI Contentieux.

Pour toute nouvelle version d'OS ou d'un composant, il pourra être demandé au Titulaire de réaliser une analyse d'impact, d'identifier l'intérêt que représente cette nouvelle version pour le système, de réaliser l'évaluation de cette version du composant (intégration du nouveau composant, et essais de non-régression, compatibilité ascendante des versions de logiciels, fourniture des kits de réaménagements, exécution des prestations).

Le Titulaire souscrit aux alertes des éditeurs et aux avis et alertes du CERT-France ou d'autres sites Internet spécialisés. Il doit assurer une veille active de ces différentes sources. Les patches ou procédures de correction doivent être appliqués de la manière suivante :

- Les patches corrigeant un risque critique (risque de compromettre le fonctionnement du système et l'accès aux informations, de rendre indisponible le service) doivent être appliqués au maximum 24h après leur diffusion sur le site du CERT-France (ce centre indiquant la procédure ou l'adresse du site à partir duquel le patch peut être téléchargé).
- Les patches corrigeant un risque gênant (risque de perturbation dans la disponibilité du service) doivent être appliqués au maximum 5 jours ouvrés après leur diffusion sur le site du CERT-France.
- Les patches corrigeant un risque mineur (risque qui n'affecte pas la disponibilité et le bon fonctionnement du service) doivent être appliqués au maximum 10 jours ouvrés après leur diffusion sur le site du CERT-France.

En concertation avec la direction de projet et l'opérateur ministériel, le Titulaire doit vérifier que ces correctifs n'impliquent pas de régression vis-à-vis du système ou des fonctionnalités offertes aux utilisateurs. En cas d'incompatibilité avérée entre un correctif et le système existant, le Titulaire devra immédiatement avertir par courrier électronique la direction de projet et l'opérateur ministériel de l'incompatibilité rencontrée et des risques engendrés. Dans ce cas, le Titulaire devra proposer une solution pour rendre le système compatible avec le patch de sécurité concerné, dans les délais définis pour la maintenance applicative corrective.

À chaque application d'un nouveau patch, le Titulaire envoie un message aux correspondants indiqués (responsable du système, officier de sécurité des systèmes d'information, etc.) par l'Administration afin de les en informer. Les points de contact seront communiqués lors de la réunion de lancement

### 3.3.3 Prise en compte des vulnérabilités

Dans le cadre de la veille de vulnérabilités, le titulaire doit utiliser plusieurs sources distinctes.

Le titulaire doit, à la demande de l'Administration, prendre en compte les alertes de sécurité diffusées par le CALID.

Le titulaire doit utiliser un système de notation de type CVSS 3.0 pour attribuer une cotation à chaque vulnérabilité identifiée par l'activité de veille.

Le titulaire doit utiliser l'échelle de cotation des vulnérabilités suivante :

- Les vulnérabilités dont la note environnementale CVSS v3 est supérieure à 7 sont considérées comme majeures,
- Les autres sont considérées comme mineures. "

Lorsque le titulaire identifie une vulnérabilité classée comme majeure, le titulaire doit transmettre à l'Administration un bulletin d'alerte spécifique selon les délais définis par l'Administration en GT SSI. Le titulaire doit traiter l'ensemble des vulnérabilités au titre du MCS annuel récurrent en respectant le plan de sécurité.

Pour permettre le déploiement des correctifs de sécurité et des nouvelles versions logicielles, le titulaire doit présenter à l'Administration ces nouvelles versions sur la plateforme de référence (plateforme de test ou d'intégration industrielle) pour validation.

Le titulaire doit mettre à jour annuellement, lorsque c'est nécessaire, l'ensemble des documents fournis au titre du contrat.

### 3.3.4 Intervention sur site de l'Administration

Un déplacement du Titulaire sur l'un des sites de l'Administration doit être organisé dans l'un des cas suivants :

- Une intervention sur site peut être nécessaire dans le cas d'une mise à jour de version applicative ;
- Une intervention peut être nécessaire, à la demande de l'administration, dans le cadre de résolution d'un incident pour des opérations d'investigation, d'analyse et de correction ;
- Une intervention sur site peut être organisée pour préparer des futures interventions (mise à jour de version...).

Les interventions sur site sont effectuées à des dates fixées d'un commun accord entre l'Administration et le Titulaire.

Dans le cadre d'une opération de mise à jour ayant un impact sur l'utilisation normale du système SI Contentieux, le planning doit être validé entre le Titulaire et l'Administration pour minimiser l'impact de ses opérations sur le service aux utilisateurs.

Il est de la responsabilité du Titulaire de s'assurer des capacités de ses intervenants à réaliser les opérations nécessaires dans le cadre de l'intervention.

A l'issue de l'intervention sur site, le Titulaire fournit à l'Administration un rapport détaillé de son intervention en précisant :

- L'objet de l'intervention ;
- Les modalités de l'intervention : nom(s) du(es) intervenant(s), date, durée ;
- La description détaillée des opérations réalisées sur site ;
- Les conclusions de l'intervention et l'état du système en fin d'intervention ;
- Les recommandations d'actions à réaliser pour garantir le bon fonctionnement du système.

Ces interventions sur site sont comprises dans le forfait de maintenance préventive, adaptative et corrective.

### 3.3.5 Maintenance de la documentation SSI

Dans le cadre de cette prestation, le Titulaire met à jour la documentation SSI. Cette mise à jour peut intervenir après la mise en œuvre de patchs correctifs ou d'évolutions majeures ou dans le cadre de procédure de ré-homologation SSI du système.

Le dossier SSI est composé des documents suivants :

- Fiche d'expression rationnelle des objectifs de sécurité (FEROS), établie par l'Administration ;
- Procédures d'exploitation de la sécurité (PES et fiches réflexes) ;
- Politique de sécurité du système (PDS) ;
- Plan de maintien en condition de sécurité (PMCS) ;
- Plan d'actions SSI établi par l'autorité d'homologation.

### 3.3.6 Livrables & délais

| Livrable                                                              | Type de vérification | Délai maximal de livraison                   |
|-----------------------------------------------------------------------|----------------------|----------------------------------------------|
| Patch correctif ou nouvelle version (mineure) de composant applicatif | VA/VS                | A l'issue du délai de correction contractuel |
| Spécifications fonctionnelles de la solution                          | VQ                   | A l'issue du délai de correction contractuel |
| Dossier d'architecture technique                                      | VQ                   | A l'issue du délai de correction contractuel |
| Manuel d'utilisation et d'administration fonctionnelle                | VQ                   | Installation du correctif + 3 jours ouvrés   |
| Suivi des faits techniques actualisé                                  | VQ                   | Installation du correctif + 3 jours ouvrés   |
| Patch correctif SSI ou nouvelle version de composant applicatif       | VA/VS                | A l'issue du délai de correction contractuel |
| Manuel d'utilisation et d'administration fonctionnelle mis à jour     | VQ                   | A l'issue du délai de correction contractuel |
| Procédures d'exploitation de la sécurité mis à jour                   | VQ                   | A l'entrée en VS                             |
| Politique de sécurité du système mis à jour                           | VQ                   | A l'entrée en VS                             |
| Plan de maintien en condition de sécurité mis à jour                  | VQ                   | A l'entrée en VS                             |
| Plan d'actions SSI mis à jour                                         | VQ                   | A l'entrée en VS                             |

### 3.4 Prestation n°3 : Maintenance des licences

Cette prestation vise à renouveler les licences libératoires maintenue pour permettre une continuité de service pour les utilisateurs qui accèdent à SI Contentieux.

L'Administration se réserve le droit d'acquérir les licences nécessaires pour ses plateformes par ses propres moyens si celles-ci entrent dans l'un des accords-cadres en vigueur au sein du ministère.

#### 3.4.1 Activités à mener par le Titulaire

Le Titulaire est responsable de la mise en place d'une structure de gestion adaptée pour assurer une acquisition efficiente et de qualité des licences nécessaires. Une gestion centralisée doit garantir la bonne acquisition et le suivi des licences tout au long de la durée du marché.

À ce titre, l'architecture technique et administrative du dispositif, pour les licences, doit être compatible avec les prérequis établis pour garantir une intégration harmonieuse et une utilisation optimale des licences au sein du parc applicatif existant.

#### 3.4.2 Hypothèses de dimensionnement

Deux hypothèses sont à prendre en compte.

→ **Acquisition de licences unitaires**

Le Titulaire du marché aura distingué les éléments financiers suivants :

- Le coût d'acquisition de nouveaux droits d'usage pour les utilisateurs supplémentaires selon les tranches définies.
- Le coût annuel de maintenance associé aux droits d'usage déjà acquis exprimé en pourcentage du coût d'acquisition ;

➔ **Maintien de la licence libératoire**

Le coût annuel de maintenance permettant de conserver les droits d'usage attachés à la licence libératoire est précisé par le titulaire dans l'annexe financière.

### 3.5 Prestation n°4 : Etude et analyse d'impact

La commande de cette prestation n'implique pas nécessairement la commande, par la Personne publique, d'une évolution. Réciproquement, une commande d'évolution n'est pas systématiquement précédée d'une commande d'analyse d'impact.

Une analyse d'impact se réalise par itérations successives, chacune d'entre elles allant de plus en plus en profondeur dans le système pour confirmer ou affiner les conclusions de la précédente.

Dès la première itération, le Titulaire fournit à l'Administration une analyse de l'impact de chaque besoin fonctionnel et/ou technique, incluant le chiffrage de la charge de travail en jours/homme ainsi que les hypothèses associées.

Les niveaux de complexité d'une analyse d'impact sont les suivants :

- **Très simple** : l'analyse d'impact ne concerne qu'un composant technique du système ;
- **Simple** : l'analyse d'impact concerne deux composants techniques ;
- **Moyenne** : l'analyse d'impact concerne plus de deux composants techniques et les implications du besoin d'évolution se ramifient sur cinq composants ;
- **Complexe** : l'analyse d'impact concerne finalement un besoin d'évolution dont les implications sont multiples d'une part techniquement parce qu'elles se ramifient au sein du système au travers de plus de cinq composants et d'autre part parce que des implications et des choix fonctionnels sont à arbitrer.

En réponse à la demande d'étude et analyse d'impact de l'Administration, le Titulaire fournit un dossier d'analyse d'impact comprenant *a minima* :

- Un rapport de situation ;
- Les actions menées ;
- Les conséquences et risques éventuels induits par l'évolution envisagée ;
- Une proposition de solutions possibles au regard du besoin exprimé et pour parer aux conséquences et risques identifiés ;
- Le cas échéant, les éléments permettant de caractériser la prestation de réalisation de l'évolution analysée (complexité, délai et coût) ;
- Un devis détaillé faisant état des actions à mener et du montant associé.

Le Titulaire soumettra à l'administration des profils techniques et/ou fonctionnels à même de réaliser ces études et analyses d'impacts. L'administration validera le profil avant de lancer la prestation.

### 3.6 Prestation n°5 : Mise en œuvre d'une évolution

Par évolution, on entend les mesures visant à faire évoluer le système, afin d'intégrer de nouvelles fonctions, d'en améliorer le fonctionnement et l'ergonomie ou de prendre en compte de nouvelles

dispositions législatives ou réglementaires et les montées de version majeure de l'outil « legisway ». La mise en œuvre d'une évolution recouvre toute création de nouvelle(s) fonctionnalité(s) ou modification de fonctionnalités existantes.

Le Titulaire pourra combiner correctifs et évolution sous couvert de l'accord de l'Administration.

Les niveaux de complexité fonctionnelle des évolutions sont les suivants :

- **Très Simple** : la fonctionnalité est installée sur un processus déjà existant ou en cours de création dans l'applicatif concerné. Sa mise en œuvre ne nécessite aucune intervention sur les processus voisins. Son installation peut nécessiter une mise à jour du référentiel déjà existant.
- **Simple** : la fonctionnalité est installée sur un processus déjà existant ou en cours de création dans l'applicatif concerné. Le réglementaire peut nécessiter une mise à jour. Les processus voisins peuvent être modifiés à la suite de l'installation du composant.
- **Moyenne** : la fonctionnalité est installée sur un processus déjà existant ou en cours de création dans l'applicatif concerné et son installation entraîne des modifications sur les processus voisins et/ou sur le réglementaire.
- **Complexe** : l'installation de la fonctionnalité, soit comme partie d'un processus déjà existant, soit comme base d'un nouveau processus, nécessite une revue en profondeur d'une partie du réglementaire et des processus existants.

Les niveaux de complexité technique des évolutions sont les suivants :

- **Très simple** : l'évolution n'entraîne aucune modification sur les processus voisins de celui où elle est mise en œuvre et n'impacte pas les fonctionnalités standard ou spécifiques du produit.
- **Simple** : l'évolution entraîne des modifications sur les processus voisins de celui où elle est mise en œuvre mais n'impacte pas les fonctionnalités standard ou spécifiques du produit.
- **Moyenne** : l'évolution entraîne des modifications sur les processus voisins de celui où elle est mise en œuvre et impacte de façon modérée les fonctionnalités mises en œuvre de façon standard ou spécifique dans le produit.
- **Complexe** : l'évolution entraîne des modifications sur les processus voisins de celui où elle est mise en œuvre et impacte de façon importante les fonctionnalités mises en œuvre de façon standard ou spécifique dans le produit.

Une demande d'évolution peut survenir dans le cadre d'une évolution des besoins métiers couverts par le SI Contentieux, afin de répondre à des préconisations (suite au passage au C1DR par exemple) ou à toute autre obligation réglementaire impliquant des modifications.

Elles peuvent, pour exemple (liste non exhaustive), consister à :

- Adapter les applications aux évolutions des textes de lois ou règles édictées par une autorité de tutelle ;
- Modifier des fonctionnalités existantes, en ajouter de nouvelles ;
- Apporter des améliorations ergonomiques ;
- Modifier ou ajouter des interfaces vers ou en provenance d'autres systèmes d'information,
- Adapter des applications aux modifications techniques de l'environnement (par exemple : prise en compte des modifications induites sur SI Contentieux du système d'exploitation, des postes clients, des postes clients, évolution de l'infrastructure de socle technique, service d'authentification Mindef Connect, etc.);
- Optimiser SI Contentieux au niveau des performances ;

Dans le cadre de cette prestation, l'Administration transmet au Titulaire une expression de besoins, sous la forme d'un cahier des charges fixant le périmètre et le cadrage des besoins d'évolution.

En réponse au besoin de l'Administration, le Titulaire présente sa proposition de réalisation d'évolution, détaillant notamment :

- La compréhension du besoin ;
- Les choix d'architecture technique éventuels, ainsi que leur compatibilité avec la version en vigueur du CCT {R-04} ou l'explication de leur non compatibilité<sup>4</sup> ;
- La démarche proposée pour la mise en œuvre de la version ;
- Les conditions particulières d'exécution ;
- Une proposition de planning de réalisation et de mise en œuvre ;
- La charge de réalisation en jour/homme et son chiffrage financier ;
- Les profils techniques réalisant les différentes actions

Le Titulaire rédige et met à jour les spécifications fonctionnelles, en prenant en compte les exigences générales, d'utilisabilité et de sécurité détaillées dans le document, les textes réglementaires applicables et les conclusions des ateliers fonctionnels.

Si le titulaire choisit de travailler en mode agile, les spécifications devront être livrées en format « users stories ».

Les spécifications fonctionnelles comprennent obligatoirement, *a minima* :

- Une traçabilité entre exigences fonctionnelles et fonctionnalités de SI CONTENTIEUX ;
- L'enchaînement des écrans ;
- Une matrice des rôles et des droits associés.

Le Titulaire définit et actualise l'architecture technique de SI Contentieux et fournit le dossier d'architecture technique dans le respect des exigences techniques et de SSI définies aux chapitres afférents, des textes réglementaires applicables (y compris cadre de cohérence technique) et des conclusions des ateliers.

Le dossier d'architecture technique comprend obligatoirement, *a minima* :

- Le détail des différents composants logiciels utilisés ;
- Un schéma des flux inter modules ;
- Et pour chaque module ou serveur : la puissance de calcul, la consommation mémoire et les besoins réseau, en trois hypothèses (minimum, maximum, suffisant) ;
- Les avis, conseils et éventuels risques encourus pour le dimensionnement « suffisant » par rapport au dimensionnement « maximum » ;
- Schéma d'architecture technique & schéma d'architecture métier.

Le Titulaire assure la recette usine et garantit la qualité et la non-régression des versions réalisées. Il assure la mise à niveau de la documentation concernée lorsque la portée des nouvelles versions demandées le requiert.

---

<sup>4</sup> Le cas échéant, celle-ci fait l'objet d'une justification du Titulaire et devra être formellement acceptée par l'Administration.

Le cas échéant, le Titulaire présente à l'Administration les nouvelles fonctionnalités introduites par la version.

Le Titulaire garantit que toute évolution de SI Contentieux s'appuie sur des versions de COTS<sup>5</sup> à jour en termes de correctifs et annoncées maintenues pendant au moins la durée du marché.

Les délais de validation fonctionnelle des documents nécessaires au bon déroulement de la prestation pourront être ajustés lors de la réunion de lancement. Par défaut, ces documents devront être validés par l'Administration dans un délai de 10 jours ouvrés. L'Administration pourra formuler jusqu'à deux demandes de modification auprès du Titulaire.

### Spécificités Evolutions techniques C1DR

Selon les préconisations du MINARM, un passage dans l'infrastructure CLOUD C1DR est imposé d'ici 2029. Il est attendu de l'éditeur de se conformer aux préconisations techniques requis pour le passage en C1DR. Cette prestation fait l'objet du poste n°6.

#### **3.6.1 Livrables et Délais**

| Livrable                                                              | Type de vérification | Délai de livraison                                                     |
|-----------------------------------------------------------------------|----------------------|------------------------------------------------------------------------|
| <b>Dans le cas d'une analyse d'impact</b>                             |                      |                                                                        |
| Dossier d'analyse d'impact                                            | VQ                   |                                                                        |
| <b>Dans le cas de la mise en œuvre d'une évolution</b>                |                      |                                                                        |
| Spécifications fonctionnelles mises à jour                            | VQ                   | 15 jours ouvrés avant le début de la VA                                |
| Supports et CR d'ateliers et réunions                                 | VQ                   | Supports : 3 jours ouvrés minimum<br>CR : 2 jours ouvrés après maximum |
| Dossier d'architecture technique mis à jour                           | VQ                   | 10 jours ouvrés avant le début de la VA                                |
| Éléments constitutifs du dossier AGORA TECH                           | VQ                   | 10 jours ouvrés avant le début de la VA                                |
| Résultats des tests usine                                             | VQ                   | 5 jours ouvrés avant le début de la VA                                 |
| Solution incluant l'évolution et les nouvelles versions de composants | VA/VSR               | A l'issue du délai contractuel                                         |
| Dossier d'installation et de paramétrage mis à jour                   | VQ                   | A l'issue du délai contractuel                                         |
| Plan d'assurance sécurité mis à jour                                  | VQ                   | A l'entrée en VSR                                                      |

<sup>5</sup> « Commercial off the shelf », ou produit informatique standard.

Manuel d'utilisation et d'administration fonctionnelle mis à jour

VQ

A l'entrée en VSR

### 3.7 Prestation n°6 : Formation des utilisateurs - optionnelle

Cette prestation doit permettre d'organiser occasionnellement la formation de différents intervenants soit pour la prise en main d'éléments liés à l'application, soit des formations sur des méthodes ou technologies mobilisées dans le cadre du présent marché.

#### 3.7.1 Organisation des formations

Les objectifs pédagogiques visés par chaque formation seront fournis en amont.

Des sessions de formation seront organisées par le titulaire (maximum 10 personnes), de préférence en présentiel sur les différents sites « utilisateurs » en métropole, le cas échéant en distanciel pour les sites DIRCOM/DICOM.

Le titulaire s'assure d'obtenir la logistique nécessaire auprès de l'Administration, incluant la gestion des inscriptions et des convocations, ainsi que la mise à disposition d'une salle.

Le titulaire mettra en place diverses actions pédagogiques et organisationnelles pour atteindre les objectifs de formation, telles que l'évaluation des prérequis, l'adaptation des contenus, des exercices pratiques, des évaluations intermédiaires et un soutien pédagogique tout au long de la formation.

Le Titulaire sera autonome sur la réalisation des contenus de formation qui devront être adaptés au SI en place au sein du Ministère. Pour cela, le titulaire s'appuiera sur les spécifications « Ministère des armées et des anciens combattants » du SI, qui seront connues du Titulaire, le dossier d'architecture technique et le manuel d'utilisation.

Le Titulaire présentera les supports pour validation à l'Administration avant les formations.

A chaque montée de version applicative, le Titulaire remettra à jour le support de formation, qui doit ainsi pouvoir être utilisé par les utilisateurs.

Les formateurs disposent des compétences nécessaires pour utiliser l'ensemble des fonctionnalités courantes offertes par la solution, version « Ministère des armées et des anciens combattants », d'un plan de formation et des supports de formation nécessaires à l'animation des sessions qu'ils auront à dispenser. Ils définissent la démarche pédagogique.

Le bilan de la formation, fourni par le titulaire, comprendra les données de participation, les résultats des évaluations, une synthèse des retours des stagiaires, une comparaison entre les objectifs fixés et les résultats obtenus, ainsi que des propositions d'amélioration si nécessaire.

L'Administration se réserve le droit de faire procéder aux formations par un autre vecteur si celles-ci entrent dans l'un des accords-cadres en vigueur au sein du ministère.

| Les différents types d'utilisateurs       | Profils d'accès              | Rôle                                        |
|-------------------------------------------|------------------------------|---------------------------------------------|
| <b>Gestionnaire</b>                       | Utilisateur                  | Réaliser des rapports                       |
| <b>Administrateur fonctionnel délégué</b> | Administration référent      | Administration fonctionnelle de la solution |
| <b>Administrateur fonctionnel central</b> | Administration fonctionnelle | Administrer la plateforme au niveau global  |

### 3.7.2 Livrables & délais

| Livrable                                                       | Type de vérification | Délai de livraison                |
|----------------------------------------------------------------|----------------------|-----------------------------------|
| Support de formation et manuel utilisateur – version numérique | VQ                   | 5 jours ouvrés avant la formation |
| Bilan de la formation                                          | VQ                   | 5 jours ouvrés après la formation |

### 3.8 Prestation n°7 : Réversibilité/Transférabilité

Il est attendu du Titulaire la récupération des données du SI CONTENTIEUX dans une base de données relationnelle et/ou un format bureautique de type fichiers pivots permettant à l'administration d'être en capacité de pouvoir les injecter dans une autre solution.

Le Titulaire soutient l'administration et/ou le tiers reprenneur dans ses travaux de transformation des données, de chargement des données et de reprise des données durant toute la phase de réversibilité. Il fournit des scripts et répond à ses demandes pour l'aider efficacement.

Le Titulaire du marché n'ayant pas accès aux données du système d'information, celles qui devraient lui être communiquées devront être préalablement anonymisées.

Dans le cadre de cette prestation, le Titulaire est responsable de la mise en place d'un pilotage global couvrant toute la phase de réversibilité du marché, pour une durée de 3 mois.

Une fois la restitution effectuée, le Titulaire détruira les copies des Données détenues dans ses systèmes informatiques dans un délai de 3 mois et devra en apporter la preuve à l'Administration dans un délai raisonnable suivant la signature du procès-verbal de restitution.

À l'issue de la réversibilité du marché, le Titulaire rédige un bilan mentionnant les points d'attention sur les risques identifiés quant à la montée en compétences des entrants.

#### 3.8.1 Livrables & délais

| Livrable                                                                                                                                            | Type de vérification | Délai de livraison                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|---------------------------------------|
| Support de la réunion de lancement de la prestation de réversibilité                                                                                | VQ                   | 3 jours avant la réunion de lancement |
| Document technique de réversion des données                                                                                                         | VQ                   | A l'issue du délai contractuel        |
| Bilan de la phase de réversibilité (Recommandations, points de vigilance, indicateurs de suivi des risques de la réversibilité ou de la transition) | VQ                   | A l'issue du délai contractuel        |
| Compte rendu de la réunion de lancement                                                                                                             | VQ                   | 5 jours ouvrés après la session       |

|                                                       |    |                                               |
|-------------------------------------------------------|----|-----------------------------------------------|
| Dossier de réversion des données                      | VQ | 10 jours ouvrés avant la fin de la prestation |
| Attestation de suppression de l'ensembles des données | VQ | 10 jours ouvrés avant la fin de la prestation |

### 3.9 Prestation n°8 : Passage en C1DR

Le Ministère des armées et des anciens combattants a lancé un programme de transformation numérique où la migration vers le cloud est fondamentale. L'objectif étant d'apporter une offre d'hébergement basée sur les technologies Cloud notamment pour le domaine « Diffusion Restreinte ».

Les principaux prérequis au passage C1DR sont :

- Disposer d'une pile logicielle à jour et soutenue en MCO/MCS (condition d'homologation) ;
- Disposer de scripts de déploiements Ruche conformes (ceux de C1NP sont identiques à ceux d'Intradef, exigence précédemment en vigueur pour l'hébergement infogérance DR historique, étendue au VPS) ;
- S'adosser à l'authentification Mindef Connect de l'environnement support ;
- Respecter le format des journaux d'événement ;
- Exporter ses journaux d'évènements applicatifs dans le puits de log dès disponibilité (revient à produire des journaux d'évènements qui seront exportés ensuite automatiquement par un agent installé à cet effet) ;
- Instancier *a minima* l'API REST d'observabilité (l'instrumentation pourra être enrichie via développement mais c'est laissé à l'appréciation du projet de ses besoins en la matière) ;
- Gérer ses secrets et ses certificats via le service de socle Gestion des secrets (dès disponibilité du service dans cet environnement).

Les services offerts sur la plate-forme PICSEL ont été mis en place pour faciliter le développement et le test des quelques adaptations nécessaires et d'en contrôler la conformité avant déploiement sur C1DR.

Le titulaire s'engage à :

- Réaliser une analyse d'impact afin de vérifier que la solution Legisway respecte les exigences d'éligibilité au C1DR.
- Élaborer un plan d'actions et en assurer la mise en œuvre avant l'échéance de 2028 (échéance correspondant à la fermeture de l'infrastructure actuelle par le CND)
- Accompagner l'administration et ses partenaires industriels dans cette démarche en fournissant l'assistance et la documentation nécessaires à l'atteinte des objectifs fixés.

Il est précisé que le Cadre de Cohérence Technique ministériel (CCT), susceptible d'évoluer chaque année, peut inclure des composants dont l'utilisation est interdite et constitue un obstacle au passage en C1DR. L'éditeur sera informé de ces évolutions.

En cas de non-conformité aux exigences du CCT ou d'échec dans la mise en œuvre du plan d'actions, l'Administration se réserve le droit de résilier le contrat.

Le dossier technique relatif à la migration vers le C1DR est joint en annexe 3.

### 3.9.1 Livrables & délais

| Livrable                   | Type de vérification | Délai de livraison             |
|----------------------------|----------------------|--------------------------------|
| Rapport d'analyse d'impact | VQ                   | A l'issue du délai contractuel |
| Plan d'actions             | VQ                   | A l'issue du délai contractuel |
| Documentation technique    | VQ                   | A l'issue du délai contractuel |

## 4 PILOTAGE OPERATIONNEL

---

Le pilotage du système est réalisé par la Direction d'Application SI Contentieux.

Le Titulaire est responsable de la mise en place d'une structure de pilotage par prestation pour assurer une gestion efficiente et de qualité.

Ce pilotage par prestation doit garantir la bonne réalisation des prestations du marché et permettre un suivi simplifié

Le Titulaire fournit l'ensemble des éléments jugés nécessaires par l'Administration pour réaliser ses activités de pilotage des différentes prestations décrites dans ce présent CCTP.

### 4.1 Comitologie du SI

#### Comité de direction (CODIR)

Le Comité de direction (CODIR) représente le niveau de pilotage stratégique de l'ensemble des missions de la plate-forme de captation des idées et de pilotage de l'innovation. Il se réunit 1 fois par an au maximum.

La présence de l'éditeur n'est pas requise au CODIR, sauf demande exceptionnelle de l'administration, pour une présence partielle et à distance possible. L'éditeur sera informé 1 mois avant le CODIR et pourra répondre à des points technique précis et pourra contribuer au support si besoin.

#### Comité de pilotage (COPIL)

Le Comité de pilotage (COPIL) assure le pilotage et la conduite opérationnelle de la plate-forme. Il se réunit au minimum 1 fois par trimestre, en fonction du besoin et à la demande d'administration.

La participation du titulaire au COPIL est indispensable que ce soit en présentiel ou à distance sous réserve de l'autorisation de l'Administration.

L'éditeur sera informé 1 mois maximum avant le COPIL, pourra répondre à des points techniques précis et contribuer au support si besoin.

#### Comité de suivi (COSUI)

Le comité de suivi permet de s'assurer que le projet se déroule nominalement sans point de blocage particulier.

Il sera organisé une fois par mois minimum et jusqu'à 1 fois par semaine maximum en fonction des prestations en cours

La présence de l'éditeur est requise au COSUI avec une présence à distance ou en présentiel distance sous réserve de l'autorisation de l'Administration. Ce sera l'occasion de présenter les nouvelles fonctions de l'outil par l'Administration.

Lors du COSUI, les points suivants devront notamment être abordés :

- Avancement des prestations : état d'avancement de toutes les prestations du CCTP (initialisation, maintenance préventive/adaptative/corrective, maintenance évolutive, MCS, formations éventuelles, réversibilité, mise en œuvre d'une instance Internet temporaire, passage en C1DR) ;
- Points de blocage ou incidents critiques : identification, analyse et suivi des actions correctives ;

- État des actions en cours : suivi des actions décidées lors des COSUI précédents ;
- Planification des prochaines étapes : mise à jour du planning et des jalons.

### Comité des utilisateurs (COMU)

Le comité des utilisateurs n'est pas à proprement parler une instance de gouvernance du SI, dans la mesure où il ne prend aucune décision structurante mais il contribue à leur préparation.

Il a pour objet de réunir les administrateurs (centraux et locaux) et autres usagers « à droits étendus » pour :

- S'assurer que le SI soit toujours aligné avec les besoins métiers ;
- Echanger et partager les bonnes pratiques et astuces, émulation et entraide.

La présence de l'éditeur n'est pas requise au comité des utilisateurs.

### Comité de suivi contractuel.

Le comité de suivi contractuel a pour objectif d'échanger entre l'administration et le titulaire sur les conditions d'exécution du marché et les éventuels points de désaccord. Il se réunit exceptionnellement à la demande de l'une des parties. L'administration est représentée au minimum par le RPA.

## **4.2 Suivi de prestations**

Le suivi des activités du Titulaire sera effectué dans le cadre de plusieurs instances :

- Une réunion de lancement en début de marché (prestation d'initialisation) ;
- Une réunion de bilan en fin de marché (prestation de réversibilité) ;
- Des comités de suivi mensuels.

Le Titulaire fait bénéficier tout au long du marché l'Administration de son devoir de conseil.

## **4.3 Tableaux de bord des activités de maintenance**

Les tableaux de bord des activités de maintenance seront définis en phase d'initialisation, sur la base d'un socle minimal d'indicateurs exigés par le présent CCTP. Ces tableaux de bord seront intégrés aux supports du Comité de Pilotage. Ils contiendront des indicateurs synthétiques permettant un suivi consolidé de l'activité de tierce maintenance sur la période écoulée.

Le titulaire devra proposer, lors de la phase d'initialisation, des indicateurs complémentaires pertinents, en lien avec les spécificités du projet et les engagements contractuels.

Indicateurs minimaux exigés (liste impérative) :

### **1. Qualité / Taux d'anomalies :**

- Taux d'anomalies détectées par catégorie (mineures, majeures, bloquantes).
- Délai moyen de correction par catégorie d'anomalie.
- Taux d'anomalies récurrentes.

### **2. Respect des délais :**

- Taux de respect des jalons/plannings (livrables, réunions, correctifs).

### 3. Sécurité :

- Taux d'incidents de sécurité détectés (confidentialité, intégrité, disponibilité).
- Délai moyen de traitement d'un incident de sécurité.

### 4. Accessibilité numérique (conformité RGAA) :

- Taux de conformité RGAA (par composant ou version).
- Nombre d'écarts critiques identifiés lors des audits d'accessibilité.

Le titulaire pourra proposer des indicateurs complémentaires ou spécifiques à valeur ajoutée, qui seront validés conjointement avec le pouvoir adjudicateur en phase d'initialisation.

Ces indicateurs doivent être mesurés, tracés et analysés régulièrement (périodicité à préciser dans le plan avec un maximum de 1 an), et présentés dans les comités de pilotage avec leurs évolutions, commentaires, et le cas échéant les plans d'actions associés.

#### 4.4 Dossier d'analyse des risques

La Direction d'Application SI Contentieux effectue un suivi de l'ensemble des risques du système.

Le Titulaire communique à la Direction d'Application les risques qu'il identifie et évalue et qui relèvent du périmètre d'ensemble du système, dès qu'il en a connaissance.

Pour chaque risque, il fournit les éléments suivants :

- Description du risque ;
- Facteurs de risques ;
- Probabilité d'occurrence ;
- Criticité ;
- Evaluation de l'impact ;
- Proposition de plan d'actions de maîtrise du risque.

Ces risques font ensuite l'objet d'une analyse commune avec l'équipe ministériel avant intégration dans le portefeuille commun de suivi des risques du projet.

#### 4.5 Gestion de la configuration

La gestion de configuration doit permettre d'assurer la traçabilité des livraisons, notamment en regard des faits techniques résolus. Le titulaire décrit le processus de gestion de la configuration dans le plan management d'assurance qualité.

Le Titulaire met en œuvre une gestion de la configuration de SI Contentieux, afin d'assurer la traçabilité de ses différents composants (matériels, logiciels et documentaires) lors de chaque livraison.

Cette gestion de configuration comprend notamment :

- La gestion des différents environnements (production, pré production, formation, picseel) ;
- La gestion des versions du système d'information ;
- La gestion de tous les documents contractuels ;
- La composition de l'architecture matérielle (en particulier, plate-forme et contexte réseau) et logicielle (en particulier, versions et paramétrages, SGBD et systèmes d'exploitation utilisés).

L'ensemble de ces éléments est repris dans une annexe du dossier d'architecture technique, mis à jour le cas échéant.

#### 4.6 Livrables & délais

| Livrable                                                                                                                                                                                                                                                                           | Type de vérification | Délai de livraison                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|--------------------------------------------------------------------|
| Plan de management et d'assurance qualité                                                                                                                                                                                                                                          | VQ                   | Actualisé pour chaque comité de pilotage                           |
| Dossier d'analyse des risques                                                                                                                                                                                                                                                      | VQ                   | Actualisé pour chaque comité de pilotage                           |
| Tableaux de bord des activités de maintenance                                                                                                                                                                                                                                      | VQ                   | Actualisé pour chaque comité de pilotage                           |
| Dossier de suivi opérationnel de l'avancement, incluant :<br>1-pour une période de référence : <ul style="list-style-type: none"> <li>• Les activités réalisées ;</li> <li>• Les faits marquants ;</li> <li>• Les activités à venir ;</li> <li>• Le suivi des actions ;</li> </ul> | VQ                   | 10 jours ouvrés avant le comité de pilotage ou la réunion de suivi |
| 2-les éléments de suivi contractuel : <ul style="list-style-type: none"> <li>• La matrice de traçabilité des exigences ;</li> <li>• L'avancement de production des livrables et le reste à faire ;</li> <li>• Le suivi financier.</li> </ul>                                       |                      | 5 jours ouvrés avant le comité de pilotage ou la réunion de suivi  |
| Dossier de suivi de la configuration                                                                                                                                                                                                                                               | VQ                   | 1 mois avant chaque livraison de programme                         |

## 5 EXIGENCES

L'ensemble des exigences listées dans le présent document incombent au Titulaire.

Dans la suite du document, ces exigences sont cataloguées sous la forme suivante :

- Exigence d'utilisabilité
- Exigences techniques
- Exigences de sécurité

### 5.1 Exigences d'utilisabilité

#### 5.1.1 Accessibilité

L'accessibilité fait l'objet de la Charte internet de l'État {R-03} et surtout du Référentiel général d'amélioration de l'accessibilité (RGAA) {R-02}, référencés au 1.3. Des ressources tierces peuvent également faciliter la mise en œuvre et le contrôle de l'accessibilité de SI Contentieux, parmi lesquelles :

- <http://pidila.gitlab.io/checklist-pidila/>
- <http://pidila.gitlab.io/scampi/>

Ainsi que toute ressource que le Titulaire jugera pertinente et adaptée.

**{EU-1}** Le titulaire s'engage à respecter le Référentiel général d'amélioration de l'accessibilité (RGAA) en suivant un cycle d'amélioration continue.

**{EU-2}** Le Titulaire s'engage à ce qu'aucune intervention sur le SI, nécessaire à l'une des prestations détaillées au paragraphe 3, n'entraîne une régression du niveau de conformité au RGAA.

### 5.2 Exigences techniques

Les exigences techniques spécifiées ci-dessous visent à s'assurer de la conformité de SI Contentieux aux bonnes pratiques en général et aux normes de l'État en particulier. Elles ont pour objectif de disposer d'un logiciel qui soit à la fois :

- Compatible avec son environnement technique ;
- Compatible avec les API REST ;
- Capable d'assurer un certain niveau de sécurité d'utilisation et d'accès.

Ces exigences ont également un impact sur les processus liés à l'ingénierie et aux opérations techniques, particulièrement dans les domaines suivants :

- Intégration et recette de SI Contentieux ;
- Déploiement et support de SI Contentieux ;
- Interconnexion avec des systèmes tiers.

#### 5.2.1 Compatibilité avec l'infrastructure technique du ministère

- Cadre de cohérence technique ministériel

**{ET-1}** Le titulaire spécifie et maintient à jour un ensemble de règles et recommandations concernant les composants techniques (logiciels en particulier) recommandés dans le cadre des projets et systèmes mis en œuvre au sein du système d'information. Ces règles et recommandations sont rassemblées au sein du Cadre de cohérence technique des systèmes d'information et de communication du Ministère de la Défense (CCT) {R-04}. En particulier, le CCT indique de façon claire les composants logiciels soutenus et exploités par l'opérateur ministériel.

**{ET-2}** Le Titulaire respecte la dernière version du CCT en vigueur et détaille ses choix techniques et leur conformité avec la pile logicielle mise en œuvre par l'opérateur ministériel, en privilégiant les composants libres inscrits dans cette pile et en mentionnant, le cas échéant, les raisons qui lui font préférer un composant non libre ou réputé non soutenu. Dans le cas d'un composant non soutenu, le Titulaire expose, dans son dossier de réponse technique et de manière détaillée, les conditions de son maintien en condition opérationnelle et de sécurité, en précisant notamment les modalités de suivi, de correction des vulnérabilités, et de remplacement à terme le cas échéant

**{ET-3}** Le Titulaire respecte les exigences de migration vers le cloud du Ministère des armées et des anciens combattants C1DR.

**{ET-4}** Les montées de version applicative mineures et majeures sont proposées par le Titulaire. Le Titulaire soumet toute montée de version à la validation de l'Administration, qui se réserve le droit de la refuser.

Un tel refus n'exonère en rien le Titulaire de son obligation de maintenance de SI Contentieux pour la version exploitée par l'Administration, dans les limites des versions N (dernière version disponible de la solution legisway et N-1 – sauf dérogation convenue entre le titulaire et le Ministère des armées et des anciens combattants. En cas de dérogation, le maintien de la version antérieure aux versions N et N-1 exploitée par l'Administration ne peut donner lieu à aucune indemnisation ni facturation additionnelle.

En l'absence de dérogation convenue entre le titulaire et le Ministère pour maintenir la version exploitée au sein de l'Administration, le Titulaire n'est plus tenu d'assurer la maintenance. Dans ce cas, la facturation sera basée sur la durée réellement travaillée, dans les conditions définies à l'article 3.1 du CCAP.

Les modalités de mise en œuvre des montées de version applicative sont définies conjointement par le Titulaire et l'Administration, selon la complexité des travaux et les impacts identifiés sur le système SI Contentieux en exploitation. Ces modalités relèvent soit de la prestation de maintenance corrective (version mineure) ou, selon la nature des interventions, de la maintenance évolutive (version majeure). Pour toute montée de version, une documentation technique explique à l'infogérant les actions à mener.

### **5.3 Exigences de sécurité des systèmes d'information**

Les textes réglementaires applicables relatifs à la sécurité des systèmes d'information sont référencés plus haut. Les exigences portées par ces documents visent à minimiser l'occurrence et les conséquences d'incidents portant atteinte à la disponibilité, à l'intégrité et à la confidentialité de SI Contentieux.

### 5.3.1 Conception & réalisation

- Normes & pratiques de développement

- {ES-1}** Dans le cas d'échange de données avec des usagers ou d'autres entités externes, SI Contentieux devra s'appuyer sur les normes en vigueur, notamment le Référentiel général de sécurité (RGS) {R-08}.
- {ES-2}** Le Titulaire doit identifier, au sein de son équipe projet, un responsable de la sécurité du système d'information garant de la prise en compte de l'ensemble des besoins de sécurité pour le projet de développement.
- {ES-3}** Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité.
- {ES-4}** SI Contentieux doit être conçu pour enregistrer et restituer toutes les actions sur SI Contentieux sans que l'utilisateur et/ou un compte à privilège puisse modifier ces traces. La durée de conservation des traces doit être paramétrable et gérée de manière conviviale par un administrateur autorisé (consultation, purge, archivage, etc.).
- {ES-5}** Les informations de journalisation du système ne doivent être accessibles qu'aux administrateurs techniques de SI Contentieux, et paramétrables que par eux, notamment en termes de consultation, d'archivage, de modification et de suppression. Les informations de journalisation de ces fichiers doivent au minimum permettre pour chaque événement de sécurité, de l'horodater, de l'imputer à un compte de connexion au système, qu'il s'agisse d'un utilisateur physique (métier ou administrateur) ou technique (application tierce).
- {ES-6}** Les données en transit ne circulent pas en clair, le Titulaire doit utiliser des protocoles de chiffrement de flux réseau.
- {ES-7}** Le Titulaire n'utilise pas les données de SI Contentieux à des fins autres que celles spécifiées au marché. Il est interdit au Titulaire de communiquer toutes les données à des tiers n'intervenant pas au titre du marché, qu'il s'agisse de personnes physiques ou morales.
- {ES-8}** Sur demande écrite de l'Administration, le Titulaire cesse d'utiliser les données (transmises par l'Administration) et procède à leur destruction ainsi qu'à celle des copies éventuellement réalisées.
- {ES-9}** Le Titulaire installe et maintient toutes les ressources matérielles et logicielles dans les versions supportées par leurs fournisseurs ou leurs fabricants et aussi les mises à jour du point de vue de la sécurité après accord du RSSI de l'administration, sauf en cas de difficultés techniques
- {ES-10}** Le Titulaire est tenu, ainsi que l'ensemble de son personnel et, le cas échéant ses sous-traitants, cotraitants et fournisseurs, au secret professionnel et à l'obligation de discrétion pour tout ce qui concerne les faits, informations, études et décisions dont il aura connaissance durant l'exécution du marché. À ce titre, il s'engage à mettre en œuvre les mesures nécessaires à la protection des informations et documents recueillis au cours du marché.