**Descriptif du Projet**

**Marché public de fournitures courantes et services**

**Pouvoir adjudicateur contractant :**

**L’Etat - Services du Premier ministre
Secrétariat général de la défense et de la sécurité nationale (SGDSN)
51, bd de La Tour-Maubourg - 75700 Paris 07 SP**

**Objet du marché :**

**Prestations de** **mise en œuvre d’un service de lutte contre le cybersquattage.**

**Ce document ne constitue pas le cahier des charges des prestations à exécuter dans le cadre du futur marché à notifier au titulaire retenu.**

**Ce document a pour unique objectif d’informer sur les caractéristiques essentielles des futures prestations à réaliser et permettre ainsi aux éventuels candidats de se positionner vis-à-vis de ce projet.**

**Mise en œuvre d’un service de lutte contre le cybersquattage**

**Sommaire**

[1 Objectif 3](#_Toc74563764)

[2 Prestations attendues de la part du titulaire 3](#_Toc74563765)

# Objectif

Dans le cadre de ses missions, l’Agence Nationale de Sécurité des Systèmes d’Information (ANSSI) souhaite lutter contre le cybersquattage.

Le cybersquattage est une pratique malveillante consistant à accaparer, en le déposant, un nom de domaine reprenant ou évoquant une marque, un site Internet légitime, une personne physique ou morale bénéficiant d’une notoriété publique. Le typosquattage est une forme de cybersquattage consistant à déposer un nom de domaine très proche d'une marque ou d'un site Internet connu. Cette action malveillante repose sur l'utilisation d'une graphie ou d'une phonétique proche permettant de tromper l'utilisateur. Ces deux techniques ont principalement pour but d’obtenir des informations sensibles ou de tromper les usagers.

Le présent marché vise à faire établir par un prestataire un service de surveillance des noms de domaine en lien avec la sphère étatique. Il sera aussi demandé au prestataire une activité de conseil sur les méthodologies retenues et la définition du périmètre surveillé, ainsi qu’une expertise juridique pouvant lui permettre de soutenir l’Etat dans ses démarches en cas d’attaques avérées.

# Prestations attendues de la part du titulaire

Les principales prestations attendues de la part du titulaire sont :

Conseil

Le prestataire doit assurer une mission de conseil auprès des acteurs étatiques quant à la définition et la pertinence de la veille. Il doit notamment faire profiter de son expertise en termes de cybersquattage et de surveillance des noms de domaine ainsi que des procédures de réponses appropriées.

Cette activité de conseil comprend, en particulier, la définition des typologies de cybersquattage (typovariation, homoglyphe, etc.) ainsi que les méthodologies de détection et réaction adaptée au cadre étatique. Le prestataire doit être force de proposition quant à la définition du service de lutte contre le cybersquattage.

Veille et Analyse : Il convient de noter que cette veille s’appuiera sur la mise en œuvre par le titulaire d’un outil de veille adapté aux besoins de l’ANSSI.

Le prestataire doit mettre en œuvre une veille sur le périmètre défini de manière à détecter l'ensemble des actes de cybersquattage (potentiel ou avéré) quelle que soit la méthode employée. Ces détections doivent être traitées par le prestataire lors d'une analyse préliminaire afin de catégoriser ces différentes alertes. En particulier, mais sans être exhaustif, cette analyse préliminaire doit permettre de lever les faux positifs et distinguer les attaques avérées nécessitant une intervention rapide en raison de leur impact sur les Administrations de l'État ou les usagers. De plus, le prestataire doit avoir la capacité de placer les noms de domaine pouvant servir à des fins de cybersquattage sous surveillance afin de monitorer leur évolution de façon à pouvoir conduire les actions nécessaires le cas échéant.

Réponses en cas de cybersquattage avéré

Le prestataire doit être capable de fournir une capacité de réponse aux différentes alertes, selon le processus qui sera défini, afin de conduire à la résolution de l'incident, en collaboration avec les autorités concernées de l'État. Il doit notamment disposer des connaissances et du savoir-faire quant aux différentes procédures françaises et étrangères ou méthodes permettant de résoudre les cas de cybersquattage. Par ailleurs, le prestataire doit avoir la capacité d'accompagner les services juridiques compétents de l'État dans le cadre de cette prestation et ceci quelles que soient les procédures engagées.

Suivi de la prestation

Concernant le suivi de la prestation, le titulaire doit organiser, fournir les éléments (comptes rendus d'activité, indicateurs, etc.) et se rendre disponible (réunions de suivi, etc.) afin de permettre au responsable technique du pouvoir adjudicateur de suivre le bon fonctionnement de la prestation, ainsi que sa pertinence et son efficacité. Il doit également, au titre de ce suivi, proposer des axes d'améliorations du service de lutte contre le cybersquattage.

Suivi de l’activité de détection et de traitement

Quant au suivi de l'activité, le titulaire doit fournir et mettre en œuvre des moyens afin de permettre de suivre les activités de détection et de traitement. Ces moyens doivent être adaptables à l'organisation mise en place par l'État dans le cadre de la lutte contre le cybersquattage. Par ailleurs, ces moyens doivent permettre de faciliter la communication entre le titulaire et les autorités compétentes de l'État afin de fluidifier la prise en compte des alertes et le bon déroulement des traitements.