Le Premier Ministre

Paris, le 28 avril 2025

à

Mesdames et Messieurs

La ministre de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche,

Le ministre de la Justice,

Le ministre de l'Intérieur,

La ministre du Travail, de la Santé, des Solidarités et des Familles,

Le ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique,

Le ministre des Armées,

Le ministre de l'Europe et des Affaires étrangères,

La ministre de la Transition écologique, de la Biodiversité, de la Forêt, de la Mer et de la Pêche,

La ministre de l'Agriculture et de la Souveraineté alimentaire,

Objet : **Instruction interministérielle relative à la mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation**

INTRODUCTION

Afin de soutenir les objectifs internationaux de lutte contre la prolifération des armes de destruction massive et de leurs vecteurs, de dissémination d'armements conventionnels et plus globalement de maintien de la paix et de la sécurité internationales, la France s'est engagée en signant et ratifiant plusieurs textes et traités internationaux : le traité sur la non-prolifération des armes nucléaires (TNP), la convention sur l'interdiction des armes chimiques (CIAC), la convention sur l'interdiction des armes biologiques et à toxines (CIABT) ou encore le traité sur le commerce des armes. La France s'engage également dans la mise en œuvre de la résolution 1540 du Conseil de sécurité des Nations unies qui vise la non-prolifération des armes de destruction massive et de leurs vecteurs et dans les actions du Conseil de sécurité en faveur de la lutte contre le terrorisme. À ce titre, la France est tenue de contrôler les flux de biens, technologies, savoirs et savoir-faire sensibles qui quittent son territoire national. Le dispositif de protection du potentiel scientifique et technique de la nation (PPST), qui vise à lutter contre les captations ou détournements de savoirs et savoir-faire sensibles, contribue donc directement au respect de ces engagements.

Au niveau national, le code pénal prévoit parmi les crimes et délits contre la nation, l'État et la paix publique, les atteintes aux intérêts fondamentaux de la nation. Ces intérêts fondamentaux sont définis à l'article 410-1 de ce code et comprennent « les éléments essentiels du potentiel scientifique et économique de la nation ». La PPST est donc un dispositif situé au cœur de la protection de ces intérêts.

La protection des intérêts fondamentaux de la nation par le dispositif de PPST repose plus précisément sur l'existence de zones protégées intéressant la défense nationale[1]. Sur ce fondement, le décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation[2] crée la notion de « zones à régime restrictif » (ZRR). Les ZRR se définissent comme des lieux et espaces clos dont le besoin de protection tient à l'impératif qui s'attache à empêcher que des éléments essentiels du potentiel scientifique ou technique de la nation fassent l'objet d'une captation de nature à affaiblir ses moyens de défense, à compromettre sa sécurité ou à porter préjudice à ses autres intérêts fondamentaux, ou soient détournés à des fins de terrorisme, de prolifération d'armes de destruction massive et de leurs vecteurs ou de contribution à l'accroissement d'arsenaux militaires.

En complément, le décret n° 2024-430 du 14 mai 2024 portant diverses dispositions relatives à la protection du potentiel scientifique et technique de la nation[3] et l'arrêté du 3 juillet 2012 modifié[4] précisent le rôle des différents acteurs de la PPST, organisent les conditions d'accès et de circulation au sein des zones concernées et le suivi des activités des services, établissements ou entreprises exerçant au sein de secteurs scientifiques et techniques dits « protégés » et pour lesquelles la captation de savoirs, savoir-faire et technologies sensibles pourrait porter atteinte au potentiel scientifique et technique de la nation. Cette règlementation est applicable aux services de l'État et aux établissements publics mais sert également de guide pour la conclusion de conventions avec des entités privées.

Ce corpus juridique structure le dispositif de PPST afin qu'il puisse contribuer à prévenir toute forme de captation ou détournement de savoirs et savoir-faire sensibles qui pourrait se produire par le biais d'un accès physique ou au moyen d'un système d'information aux éléments constitutifs du potentiel à protéger, ou par la transmission indue de ces éléments dans le cadre

[1] Article 413-7 du code pénal.

[2] Crée l'article R. 413-5-1 du code pénal.

[3] Modifie l'article R. 413-5-1 du code pénal et crée l'article R. 413-5-2 du code pénal.

[4] Modifié par l'arrêté du 24 octobre 2024.

d'un projet de coopération avec une entité étrangère. La PPST permet ainsi, d'une part, de créer des zones à régime restrictif au sein de services, établissements ou entreprises dont les activités sont évaluées comme sensibles et, d'autre part, d'examiner certains projets de coopération internationale.

Le dispositif permet de s'adapter aux besoins et aux capacités d'exécution des services, établissements ou entreprises concernés, en proposant des mesures graduelles et adaptées issues d'un processus de concertation avec les autorités de l'État.

Enfin, le dispositif de PPST intervient en complémentarité avec d'autres dispositifs de protection (protection du secret de la défense nationale, sécurité des activités d'importance vitale, règlementation sur les micro-organismes et toxines, cybersécurité, mesures de conditionnalité des aides publiques, loi de blocage) ou de contrôle (contrôle des investissements étrangers en France, contrôle des exportations de biens et technologies à double usage, contrôle des exportations de matériels de guerre).

La présente instruction remplace la circulaire interministérielle n° 3415/SGDSN/AIST/PST et l'instruction interministérielle n° 11155/SGDSN/AIST/PST/CD-SF du 7 novembre 2012. Elle vise à détailler la structure et les modalités d'application du dispositif. Elle sera transposée par les différents ministères concourant au dispositif au sein d'instructions ministérielles. La présente instruction est organisée en quatre titres, qui présentent (I) les principes généraux et la gouvernance du dispositif, (II) les mesures de protection applicables aux secteurs scientifiques et techniques protégés, (III) les zones à régime restrictif et (IV) l'articulation avec les autres dispositifs et outils de protection.

TITRE I. Principes généraux et gouvernance du dispositif

Chapitre 1. Les grands principes

Section 1. Le potentiel scientifique et technique de la nation

Le potentiel scientifique et technique de la nation est constitué de l'ensemble des biens matériels et immatériels propres à l'activité scientifique fondamentale et appliquée et au développement technologique. Ce potentiel constitue l'un des éléments des intérêts fondamentaux de la nation définis par l'article 410-1 du code pénal.

Dans un contexte de diversification et d'accroissement du nombre d'opérations étrangères visant à capter des savoirs et savoir-faire scientifiques et techniques, en particulier dans le milieu de la recherche et de l'innovation, l'État est responsable d'identifier et de protéger, en concertation avec les acteurs concernés, les activités scientifiques et techniques les plus sensibles de recherche, de production, d'essais ou de développement.

L'objectif de la politique publique de protection du potentiel scientifique et technique de la nation (PPST) est de préserver les échanges et coopérations scientifiques, nécessaires à la recherche scientifique et au progrès technologique, tout en protégeant les intérêts fondamentaux de la nation. Elle vise ainsi à empêcher que les personnes qui pourraient accéder à certaines unités de recherche et/ou développement publiques ou privées sur le territoire national, ou qui se trouvent en contact avec le personnel qui y travaille, acquièrent de manière indue des savoirs ou savoir-faire qui pourraient être utilisés à des fins malveillantes ou défavorables aux intérêts de la France.

Cette politique publique est portée en concertation entre les autorités de l'État et repose sur des échanges d'informations entre les services, établissements ou entreprises concernées et les autorités compétentes de l'État (voir Chapitre 3 du présent titre). Elle doit favoriser l'émergence, au sein des unités de recherche et/ou développement, d'une culture de la protection du potentiel scientifique et technique qui y est hébergé, en sensibilisant les acteurs à la sécurisation de leurs travaux et en diffusant des bonnes pratiques et des outils adaptés.

À ce titre, le dispositif de la PPST est déployé au sein de secteurs scientifiques et techniques identifiés comme protégés et se manifeste par :

- l'identification et l'évaluation d'unités protégées dont les activités relèvent de secteurs scientifiques et techniques protégés en raison de l'intérêt qu'ils présentent pour la nation ou pour ceux qui les convoitent. La protection et la circulation des informations y sont organisées (voir le TITRE II de la présente instruction) ;
- l'examen de certains projets de coopérations scientifiques internationales formalisées par les établissements français et qui opèrent au sein des secteurs scientifiques et techniques protégés. L'examen est effectué avant signature de l'accord afin de limiter le transfert indu de savoirs et savoir-faire sensibles ;
- la création de zones à régime restrictif (ZRR), au sein des unités protégées les plus sensibles, définies à l'article R. 413-5-1 du code pénal et par les règles qui y régissent la circulation. Ces zones constituent des lieux et espaces clos à l'intérieur desquels des mesures de protection sont instaurées en raison des risques élevés de détournement ou de captation des informations, données, technologies et matériels qui s'y trouvent ;
- l'adoption d'une politique de sécurité des systèmes d'information adaptée à la protection des données sensibles hébergées dans les unités protégées, en cohérence avec la sécurité des systèmes d'information du service, de l'établissement ou de l'entreprise dans lequel ces unités se situent.

Le régime juridique créé pour protéger ce potentiel permet ainsi de contrôler des flux de savoirs et savoir-faire portés par :

- d'une part, des individus : il s'agit alors de réguler la circulation des personnes et les accès virtuels au sein d'une ZRR ainsi que celle des informations sensibles qui s'y rapportent (voir à ce sujet le TITRE III de la présente instruction) ;
- d'autre part, des accords de coopération : il s'agit alors de veiller avant signature à ce qu'ils ne comportent pas d'éléments ou clauses problématiques, ou d'inclure des clauses protectrices (voir à ce sujet le Chapitre 1 du TITRE II de la présente instruction).

Le régime permet de façon corollaire (voir le Chapitre 5 du TITRE III de la présente instruction) :

- de sanctionner, *via* l'article 413-7 du code pénal, l'intrusion sans autorisation en ZRR ;
- de sanctionner, *via* l'article R. 413-5-2 du code pénal, les personnes qui font entrave à l'accomplissement de la PPST, ou qui ne s'assurent pas du respect des obligations réglementaires qui leur incombent.

Ces mesures ne dispensent pas d'appliquer d'autres dispositions légales ou réglementaires, complémentaires (voir le TITRE IV de la présente instruction), en particulier celles relatives :

- à la protection du secret de la défense nationale ;
- à la sécurité des activités d'importance vitale ;
- à la résilience des infrastructures critiques et à la cybersécurité ;
- aux transferts et exportations de matériels et technologies contrôlés au titre des matériels de guerre ;
- au contrôle des exportations des biens et technologies à double usage ;
- au régime d'autorisation préalable pour les opérations réalisées sur le matériel biologique de la liste des micro-organismes et toxines (MOT).

Section 2. Les quatre risques au titre de la PPST

L'article R. 413-5-1 du code pénal vise à prévenir la captation et le détournement des savoirs et savoir-faire sensibles en organisant la PPST au regard des quatre risques suivants :

- le risque 1 (**R1**), « intérêts économiques de la nation », concerne les atteintes au potentiel scientifique et technique susceptibles de porter préjudice aux intérêts et à la compétitivité économiques et scientifiques de la France ;
- le risque 2 (**R2**), « arsenal militaire », concerne le détournement du potentiel scientifique et technique susceptible de renforcer les capacités militaires (conventionnelles) d'un autre pays ou d'affaiblir les capacités de défense françaises ;
- le risque 3 (**R3**), « prolifération », concerne le détournement de savoirs et savoir-faire susceptibles de contribuer à la prolifération des armes de destruction massive et de leurs vecteurs, dans les domaines nucléaire, balistique, chimique ou biologique ;
- le risque 4 (**R4**), « terrorisme », concerne le détournement de savoirs et savoir-faire susceptibles d'être utilisés pour commettre des actes terroristes, sur le territoire national ou à l'étranger (ce risque comprend également le risque radiologique).

Section 3. Les notions principales

A. *Secteurs scientifiques et techniques protégés et spécialités sensibles*

La protection des savoirs et des savoir-faire repose en premier lieu sur la notion de secteurs scientifiques et techniques protégés, qui permet de circonscrire la protection à certains domaines, identifiés comme potentiellement sensibles au regard des risques de la PPST. Ces secteurs, généraux par nature, sont définis en fonction de l'intérêt qu'ils suscitent pour la nation

ou pour ceux qui les convoitent. La liste des secteurs scientifiques et techniques protégés est publiée à l'annexe I de l'arrêté du 3 juillet 2012 modifié.

Au sein de ces secteurs protégés, certaines spécialités dites « sensibles » impliquent des savoir-faire susceptibles d'être détournés à des fins de terrorisme ou de prolifération d'armes de destruction massive et de leurs vecteurs (risques R3 et R4 mentionnés *supra*). La liste de ces spécialités sensibles figure en annexe de l'arrêté classifié non publié au Journal officiel du 3 juillet 2012 relatif aux spécialités dont les savoir-faire sont susceptibles d'être détournés à des fins de terrorisme ou de prolifération d'armes de destruction massive et de leurs vecteurs. Cette annexe a été modifiée par l'arrêté du 2 mars 2018, arrêté classifié non publié au Journal officiel.

Ces notions sont précisées au Chapitre 2 Section 1 du présent titre.

B. *Échange d'informations*

La PPST est assurée par concertation entre les pouvoirs publics et les chefs des services, établissements ou entreprises qui abritent une activité relevant d'un secteur protégé. Cette concertation se traduit par un échange d'informations qui permet aux autorités de l'État de prendre en compte les spécificités de chaque entité et d'envisager une protection adaptée au cas par cas, selon les risques, et en fonction des moyens et besoins de l'entité.

Les informations échangées entre un service, établissement ou entreprise et l'État permettent d'alimenter l'évaluation du besoin de protection au titre de la PPST. Si ce besoin est avéré, le service, établissement ou entreprise et l'État échangeront de nouveau des informations pour l'application du dispositif suivant les modalités présentées dans la présente instruction.

Ces notions sont précisées au Chapitre 2 Section 1 du présent titre.

C. *Unités protégées*

Une unité de recherche et/ou développement est une entité publique ou privée, aménagée pour effectuer des activités de recherche scientifique ou de développement et rattachée à un service, un établissement ou une entreprise. Si une unité qui relève d'un ou plusieurs secteurs scientifiques et techniques protégés a fait l'objet d'une détermination de son besoin de protection au titre de la PPST et a été évaluée comme étant exposée à un ou plusieurs risques visés par le dispositif (si la somme de la cotation des risques R1 à R4 est strictement supérieure à zéro), alors elle est considérée comme « unité protégée ».

Les unités protégées doivent faire l'objet de mesures de protection renforcées, détaillées au TITRE II de la présente instruction, par rapport aux unités qui ne le sont pas. Au sein de ces unités protégées, la création de ZRR peut être envisagée lorsque le besoin le justifie.

À l'exception des unités qui appartenaient à l'ancien dispositif des établissements à régime restrictif, une unité dont la sensibilité n'a pas encore été évaluée n'est pas une unité protégée.

Cette notion est précisée au Chapitre 2 Section 3 du présent titre.

D. *Coopérations internationales*

Une coopération internationale est entendue comme une coopération formalisée par un accord, quelle qu'en soit sa forme, portant sur un secteur scientifique et technique protégé et impliquant d'un côté, un ou plusieurs établissement(s) d'enseignement supérieur et de recherche ou établissement(s) privé(s) français, et de l'autre, un ou plusieurs établissement(s) étranger(s), ou sous contrôle étranger, ou une organisation internationale, publics comme privés.

Cette notion est précisée au Chapitre 1 du TITRE II de la présente instruction.

E. *Zones à régime restrictif*

Une ZRR est une catégorie de zone protégée définie à l'article R. 413-5-1 du code pénal. Ces zones constituent des locaux et terrains clos à l'intérieur desquels des mesures de protection et des règles de circulation sont instaurées en raison des risques de détournement ou de captation des informations, données, technologies et matériels qui s'y trouvent. Ces zones sont créées par arrêté ministériel, non publié au Journal officiel ou au Bulletin officiel. La création d'une ou plusieurs ZRR au sein d'une ne peut être envisagée que dans les unités évaluées comme unités protégées.

La notion de ZRR est détaillée au TITRE III de la présente instruction.

Section 4. La concertation

La PPST est une politique publique dont l'objectif est de garantir un dialogue permanent et structuré entre d'une part le milieu de la recherche et de l'innovation scientifique publique comme privée et d'autre part les autorités de l'État en charge de la protection des intérêts fondamentaux de la nation.

Cette concertation est, comme indiqué ci-avant, intimement liée aux échanges d'informations entre les services, établissements et entreprises concernées et les autorités compétentes de l'État. Les premiers possèdent l'information à protéger, les secondes possèdent les informations permettant de compléter l'évaluation des risques et menaces.

Chapitre 2. Les secteurs scientifiques et techniques protégés et les unités protégées

Section 1. Les principes généraux

Cette section détaille l'article 5 de l'arrêté du 3 juillet 2012 modifié.

A. *Secteurs scientifiques et techniques protégés et spécialités sensibles*

La protection des savoirs et savoir-faire sensibles repose sur l'identification précise des activités de recherche et développement les plus exposées aux quatre risques de la PPST. L'évaluation de sensibilité et du besoin de protection conduit à l'identification des unités dites protégées et à la création de ZRR au sein de ces unités les plus sensibles. Pour ce faire, il importe de définir la liste des secteurs scientifiques et techniques au sein desquels les captations ou détournements visés par l'article R. 413-5-1 du code pénal sont les plus à même de se produire. Ces secteurs sont ceux qui revêtent un potentiel scientifique ou économique majeur ou qui pourraient être détournés à des fins malveillantes, c'est-à-dire qui :

- sont indispensables pour pourvoir aux moyens de la défense nationale (notamment la base industrielle et technologique de défense) ;
- sont susceptibles de déboucher sur des biens, technologies et logiciels susceptibles d'avoir une utilisation militaire ;
- contribuent à la souveraineté économique et industrielle ;
- sont soutenus par une stratégie nationale ou européenne de recherche et/ou d'innovation (notamment les programmes de soutien du Secrétariat général pour l'investissement, ou du Conseil européen de la recherche) ;
- font l'objet d'intérêts de puissances étrangères (États ou organisations paraétatiques ou non gouvernementales) ;
- recouvrent des activités au sein des secteurs d'activité identifiés comme d'importance vitale ou critiques pour la nation ;

- recouvrent des activités mentionnées dans le code monétaire et financier au titre du contrôle des investissements étrangers en France ;
- font l'objet de recherches d'excellence, y compris de recherche fondamentale.

La liste de ces secteurs dits « protégés », conçue comme une nomenclature nationale, est publiée en annexe I de l'arrêté du 3 juillet 2012 modifié relatif à la protection du potentiel scientifique et technique de la nation.

Une unité de recherche et/ou développement relève d'un secteur scientifique et technique protégé si sa discipline scientifique principale ou l'une de ses disciplines secondaires fait partie de cette liste, arrêtée par le Premier ministre.

Cette liste est volontairement généraliste afin de ne pas exclure *ex ante* des activités sensibles. Elle n'implique pour autant aucune automaticité de sensibilité pour les unités dont les activités en relèvent. Elle confie uniquement à l'État la mission de réaliser des évaluations de sensibilité.

Parmi ces secteurs protégés, les savoir-faire de certaines spécialités scientifiques et techniques sont particulièrement susceptibles d'être détournés à des fins de terrorisme ou de prolifération des armes de destruction massive et de leurs vecteurs. Ce sont les spécialités dites « sensibles ». Ces spécialités sont listées par arrêté classifié du Premier ministre, non publié au Journal officiel.

Ces deux listes (secteurs protégés et spécialités sensibles) sont actualisées par le Secrétaire général de la défense et de la sécurité nationale, en concertation avec les ministres intéressés.

B. *Échanges d'informations*

L'article 2 du décret n° 2011-1425 du 2 novembre 2011 dispose que la protection est assurée par concertation entre les pouvoirs publics et les chefs des services, établissements ou entreprises qui abritent une activité relevant d'un secteur protégé. Cette concertation se traduit par un échange régulier d'informations qui permet aux autorités de l'État de prendre ou recommander des mesures de protection les plus en adéquation avec les besoins évalués. Cette transmission d'informations est obligatoire pour les services, établissements ou entreprises sur lesquels l'État exerce une autorité ou une tutelle, et précisée aux termes d'une convention dans les autres cas. Les hauts fonctionnaires de défense et de sécurité (HFDS) des ministères (dont le rôle est précisé à la Section 2 du Chapitre 3 du présent titre) disposent de conventions-type. Ainsi, les chefs de services, établissements ou entreprises qui abritent une activité relevant des secteurs scientifiques et techniques protégés et qui sont placés sous l'autorité ou la tutelle d'un ministre fournissent à ce dernier les informations figurant en annexe II de l'arrêté du 3 juillet 2012 modifié. Sinon, la transmission de ces informations est fixée par convention entre le chef de service, d'établissement ou d'entreprise et le ministre compétent.

La liste complète des catégories d'informations nécessaires à la PPST et leurs modalités de transmission est publiée en annexe II de l'arrêté du 3 juillet 2012 modifié relatif à la PPST.

Le HFDS, selon les risques particuliers qu'il évalue à son niveau, informe le chef de service, d'établissement ou d'entreprise des mesures spécifiques de protection qu'il estime nécessaires.

Section 2. La détermination du besoin de protection

Le ministre compétent pour déterminer le besoin de protection est celui qui a la charge des éléments essentiels du potentiel scientifique et technique à protéger. En pratique, le ministre avec lequel le dialogue PPST doit se faire est celui qui est le plus à même d'apprécier la sensibilité des activités en cause : soit par son lien de tutelle (pour les unités hébergées dans des laboratoires publics sous tutelle du ministre chargé de la recherche par exemple), soit par son expertise sectorielle (pour les entreprises du secteur de l'énergie par exemple), soit par un lien contractuel (pour les entreprises de la base industrielle et technologique de défense par exemple). Le ministre compétent pour déterminer le besoin de protection de l'unité fait toutes diligences pour informer

les autres ministres co-tutelles (ou en convention avec) de l'unité de son intention de déterminer son besoin de protection. Au besoin, le secrétariat général de la défense et de la sécurité nationale (SGDSN) pourra trancher sur le choix du ministre compétent pour déterminer le besoin de protection.

Sur la base des informations fournies selon les modalités exposées dans la section précédente, le ministre compétent évalue le besoin de protection des unités qui abritent une activité relevant des secteurs scientifiques et techniques protégés. Cette évaluation du besoin de protection est réalisée à l'initiative de ce ministre ou sur demande du service, établissement ou entreprise. Il convient d'examiner le besoin de protection de la manière la plus objective possible.

A. *L'évaluation de la sensibilité*

La sensibilité d'une unité dont l'activité fait partie d'un secteur scientifique et technique protégé fait l'objet d'une cotation de 0 à 3 pour chacun des risques R1 à R4 (voir le Chapitre 1 Section 2 du présent titre).

La cotation sur chaque risque répond aux critères suivants :

- 0 = non concerné : absence de risque ou absence d'intérêt ;
- 1 = préjudice limité : le risque de captation ou détournement des travaux ne peut pas être écarté mais son impact resterait limité (travaux d'intérêts mais non cruciaux par exemple) ;
- 2 = préjudice moyen : le risque de captation ou détournement des travaux est avéré et son impact serait important (travaux de qualité et/ou au cœur du risque associé) ;
- 3 = préjudice fort : le risque de captation ou détournement des travaux est très élevé et son impact serait majeur (travaux d'excellence, intérêt stratégique, importance vitale).

Dès lors que la somme des cotations est strictement supérieure à zéro, l'unité est qualifiée d'unité protégée et les mesures de protection relatives à ces unités s'appliquent (voir Section 3 du présent chapitre et TITRE II de la présente instruction). En complément, la création d'une ou plusieurs ZRR peut être envisagée (voir TITRE III de la présente instruction) selon des modalités qui seront définies par chaque ministère. Quand les travaux relèvent de spécialités sensibles, la cotation retenue pour le R3 ou le R4 ne peut être nulle.

Pour réaliser cette évaluation, les ministères s'appuient entre autres sur la documentation produite par le SGDSN. Ces documents d'aide à la décision sont rassemblés sur un espace informatique commun sécurisé. Chaque ministère est responsable de l'évaluation qu'il réalise des services, établissements ou entreprises dont il a la charge.

B. *Un exemple de processus d'évaluation : le « collège des experts » de la PPST*

Le ministère chargé de la recherche pilote, en concertation avec le SGDSN, un collège d'experts dont le mandat est de procéder à l'évaluation de sensibilité des unités de recherche placés sous sa tutelle. Ce collège, réparti en sous-comités thématiques correspondants aux catégories de secteurs scientifiques et techniques protégés, est composé de scientifiques reconnus dans leur discipline, issus des universités et établissements participant à la PPST, et de spécialistes des questions de défense et de sécurité représentant l'administration.

Le collège des experts est une enceinte mixte de dialogue entre le monde de la recherche et l'administration. L'association des chercheurs à ces travaux d'analyse permet de renforcer l'adhésion de la communauté scientifique au dispositif de la PPST et la bonne prise en compte dans le dispositif des enjeux de cette communauté.

Chaque année, une liste d'unités de recherche à évaluer pour la PPST est élaborée sur la base des vagues d'évaluations menées par le haut conseil de l'évaluation de la recherche et de l'enseignement supérieur. Les unités listées font l'objet d'une évaluation de sensibilité par les sous-comités du collège, qui déterminent de façon collégiale les cotations des quatre risques PPST,

s'expriment sur le besoin de protection et, le cas échéant, formulent des recommandations au ministre. Dans le cas d'unités mixtes de recherche, les HFDS des ministres concernés par la co-tutelle (ou par convention) de l'unité sont informés dès le stade de l'établissement de la liste des unités visées par l'évaluation. L'évaluation des sous-comités est quantifiée et argumentée sur le plan scientifique et technique. Elle est basée sur les informations relatives aux activités des unités ainsi que sur un questionnaire d'auto-évaluation rempli par les unités. La cotation de sensibilité de l'unité et le besoin de protection sont discutés entre les membres du sous-comité et, le cas échéant, sont confirmés après discussion bilatérale avec le directeur d'unité concerné. Les fonctionnaires de sécurité et de défense des établissements tutelles de l'unité concernée sont associés à ces discussions.

Le ministère chargé de l'enseignement supérieur et de la recherche poursuit le dialogue avec les établissements en vue de mettre en œuvre les mesures de protection pertinentes.

Au cas par cas, le collège peut évaluer la sensibilité des unités de recherche placées sous la tutelle principale d'un établissement relevant d'un autre ministère qui en ferait la demande.

Section 3. Les unités protégées

Cette section détaille l'article 6 de l'arrêté du 3 juillet 2012 modifié.

Une unité relevant d'un secteur protégé bénéficie d'un niveau de protection renforcé lorsque la somme de la cotation des risques R1 à R4 est strictement supérieure à zéro. Elle est alors désignée « unité protégée ». Le ministre qui a procédé à l'évaluation en informe le chef de service, d'établissement ou d'entreprise et lui présente les risques auxquels l'unité protégée fait face. Ce dernier est responsable, ou donne délégation au responsable de l'unité protégée pour ce faire, de mettre en œuvre les mesures de protection rappelées ci-après.

Conformément à l'article 6 de l'arrêté du 3 juillet 2012 modifié, le responsable d'une unité protégée au sein d'un service, établissement ou entreprise placée sous l'autorité ou la tutelle d'un ministre prend toute disposition utile pour assurer la protection des informations concernées :

- il veille à ce que les stagiaires exercent leurs activités au sein de l'unité sous le contrôle d'un personnel permanent nommément désigné ;
- il veille à ce que soit tenu un répertoire des visites, conservé pendant une durée de cinq ans ;
- il veille à ce que les coopérations internationales de nature scientifique ou technique impliquant l'unité protégée n'entrainent pas de transfert incontrôlé de ses savoirs ou savoir-faire. À ce titre, il transmet pour avis préalable au ministre chargé d'exercer la tutelle les projets de telles coopérations.

En complément, il est recommandé au responsable d'une unité protégée au sein d'un service, établissement ou entreprise placée sous l'autorité ou la tutelle d'un ministre d'adopter les mesures de protection renforcées prévues pour les ZRR à savoir notamment :

- mettre en place une politique de sécurité des systèmes d'information adaptée à la sensibilité des activités de son unité ;
- établir un circuit de notoriété pour les visites de délégations étrangères et informer le ministre ayant déterminé le besoin de protection de tout projet de telles visites .

Le responsable d'une unité protégée au sein d'un service, établissement ou entreprise organise ou fait organiser des sensibilisations au profit de ses collaborateurs sur les menaces de captation et les bonnes pratiques en matière de protection des informations sensibles.

Les formalités d'accès à une unité protégée sont précisées dans un règlement intérieur dont le contenu peut être défini le cas échéant par instruction ministérielle.

Dès lors qu'une unité de recherche et/ou développement acquiert le statut d'unité protégée, elle peut bénéficier d'une protection par ZRR si le besoin de protection le justifie. Dans ce cas, les accès sont soumis à des modalités spécifiques (voir le Chapitre 3 du TITRE III de la présente instruction). Les limites de la ou des ZRR peuvent se superposer partiellement ou totalement avec les limites de l'unité protégée.

Lorsque l'unité protégée ne relève pas d'un service, établissement ou entreprise placée sous l'autorité ou la tutelle d'un ministre, les dispositions utiles pour assurer la protection des informations concernées sont fixées par convention entre le chef de service, d'établissement ou d'entreprise et le ministre compétent pour déterminer le besoin de protection.

Le HFDS du ministre qui a déterminé le besoin de protection peut consulter sur demande l'ensemble des documents listés au II de l'annexe II de l'arrêté du 3 juillet 2012 modifié. Des instructions ministérielles précisent les modalités de transmission des éléments statistiques annuels concernant la PPST adressés par le chef de service, d'établissement ou d'entreprise.

Chaque ministre est responsable du suivi des unités protégées qu'il a évaluées.

Section 4. Les services, établissements et entreprises abritant une unité protégée

Le chef de service, d'établissement ou d'entreprise qui héberge une ou plusieurs unités protégées est le responsable et le garant de la bonne mise en œuvre de la PPST. Pour ce faire, il peut s'appuyer sur ou désigner un fonctionnaire de sécurité et de défense (FSD) au sein de son établissement. Exerçant sous son autorité, le FSD est l'interlocuteur privilégié du ou des gestionnaires de ZRR et le relai fonctionnel des HFDS.

Le chef de service, d'établissement ou d'entreprise prend toute disposition utile pour assurer la protection des informations relatives à la PPST dans une unité protégée. Il désigne le responsable PPST pour cette unité qui en exerce la gestion en lien étroit avec le FSD. En particulier :

- il assure la concertation sur la PPST entre l'ensemble des co-tutelles de l'unité et le ministre de tutelle ou celui compétent pour évaluer le besoin de protection ;
- il concourt, sur demande de ce ministre, à la détermination du besoin de protection de ses unités, ou à la création de ZRR ;
- il s'assure de la bonne transmission des projets d'accord de coopération internationale (voir le Chapitre 1 du TITRE II de la présente instruction) ;
- il définit dans le règlement intérieur les mesures nécessaires pour l'exécution des mesures de protection.

Il peut également déléguer, conformément aux règles de droit administratif sur la délégation de signature, au responsable de l'unité protégée concernée ou au responsable de la ZRR la faculté de signer en son nom les documents prévoyant les mesures de sécurité applicables ou les autorisations d'accès aux dites ZRR.

Dans le cas d'une unité protégée à tutelle multiple, l'établissement hébergeur est en règle générale responsable de la PPST. Les chefs de service ou d'établissement qui concourent à l'activité de cette unité, qu'ils relèvent d'un seul ou de plusieurs ministres, insèrent dans la convention qui en régit le fonctionnement un article spécifique à la PPST, qui prévoit notamment :

- les mesures à prendre et les moyens à mettre en œuvre en vue d'assurer la PPST ;
- la désignation d'un service ou établissement responsable de la gestion PPST pour l'unité considérée. Cette responsabilité en gestion n'excluant pas la responsabilité du ou des services ou établissements hébergeurs.

En cas de désaccord entre les chefs de service ou d'établissement, le HFDS du ministre qui a déterminé le besoin de protection désigne parmi les chefs de ces services ou établissements dont il exerce la tutelle, le responsable de la PPST des unités concernées.

Chapitre 3. Le rôle des autorités de l'État

Section 1. Le Premier ministre et le secrétaire général de la défense et de la sécurité nationale

Le Premier ministre est chargé de définir les orientations nationales en matière de protection du potentiel scientifique et technique de la nation, en tenant compte de l'évolution de la sensibilité des recherches et des technologies, de l'évaluation de la menace, de la situation internationale et des engagements internationaux et bilatéraux de la France.

Pour cela, il établit la liste des secteurs scientifiques et techniques protégés, ainsi que les catégories d'informations qui doivent être transmises, dans le cadre de la PPST, par les services, établissements ou entreprises, au SGDSN et aux ministres concourant au dispositif. Le Premier ministre établit également et met à jour la liste des spécialités sensibles dont les savoir-faire sont susceptibles d'être détournés à des fins de terrorisme ou de prolifération d'armes de destruction massive et de leurs vecteurs (risques R3 et R4).

Son action est déclinée par le SGDSN, service du Premier ministre. Le SGDSN anime le dispositif de PPST, coordonne l'action des ministères et veille au bon déploiement du dispositif de protection. Il établit et tient à jour les documents et outils qui permettent d'apprécier les risques encourus par le potentiel scientifique et technique de la nation. Il est garant du respect des procédures et arbitre les éventuels différends entre ministères.

A. *Pilotage du dispositif de protection*

Afin de pouvoir décliner les orientations nationales en matière de PPST, en lien avec les ministres concernés, et d'en contrôler l'exécution, le SGDSN anime le réseau interministériel de la PPST. Il anime pour cela les travaux d'un comité de direction et d'un comité de pilotage, ainsi que d'éventuels groupes de travail *ad hoc* sur des sujets spécifiques. Les travaux de ces comités et de ce réseau sont alimentés par les informations qui lui sont transmises par les ministres et les HFDS.

Le comité de direction est présidé par le Secrétaire général de la défense et de la sécurité nationale. Il est composé des HFDS des ministères concourant à la PPST, soit les ministères exerçant une tutelle ou ayant une attribution de compétences sur les services, établissements ou entreprises concernés, ainsi que les autres directeurs concernés au sein des ministères chargés des affaires étrangères, de la défense et de l'intérieur. Ce comité de direction se réunit une fois par an et valide les orientations nationales, le bilan annuel et les travaux de mise à jour des documents et outils d'aide à la décision permettant de faciliter l'application du dispositif.

Le comité de pilotage, présidé par la direction des affaires internationales, stratégiques et technologiques du SGDSN, réunit les représentants des services ministériels en charge de la PPST. Il permet de présenter les évolutions de la menace qui pèse sur le potentiel scientifique et technique de la nation et de l'application du dispositif pour chaque ministère, ainsi que de définir les priorités d'action et de préparer les travaux présentés au comité de direction. Il instruit les évolutions du dispositif et arbitre si besoin les différends entre les ministères. Ce comité de pilotage se réunit en tant que de besoin et a minima tous les semestres.

B. *Répertoire national des ZRR*

Le SGDSN crée et tient à jour un répertoire national des ZRR, non public. Il est diffusé aux HFDS et aux services de l'État ayant à en connaître.

C. *Gestion de la base de données interministérielle*

Conformément au décret n° 2022-368 du 15 mars 2022 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Base interministérielle PPST », le SGDSN tient une base de données interministérielle permettant de mutualiser les informations issues des demandes d'accès aux ZRR et des suites qui leur ont été données. Les

ministères concourant à la PPST transmettent régulièrement au SGDSN certaines informations relatives aux demandes d'accès qu'ils ont traitées et les avis rendus.

D. *Coordination de la protection des spécialités sensibles*

La liste des spécialités mentionnées au IV de l'article 2 du décret n° 2011-1425 du 2 novembre 2011 est précisée en annexe de l'arrêté non publié du 3 juillet 2012 modifiée par arrêté du 2 mars 2018 relatif aux spécialités dont les savoir-faire sont susceptibles d'être détournés à des fins de terrorisme ou de prolifération d'armes de destruction massive et de leurs vecteurs. Le SGDSN met à jour cette liste des spécialités sensibles et coordonne l'action des ministres pour leur protection.

E. *Agence nationale de la sécurité des systèmes d'information (ANSSI)*

L'ANSSI est l'autorité nationale en matière de sécurité et de défense des systèmes d'information. Elle assiste le SGDSN dans le respect de ses attributions en matière de sécurité des systèmes d'information prévues à l'article R* 1132-3 du code de la défense. Elle définit les mesures de protection des systèmes d'information, notamment celles adaptées aux enjeux de la PPST, et est informée des incidents affectant ces systèmes. Elle propose également des mesures destinées à répondre aux crises affectant ou menaçant la sécurité des systèmes d'information les plus sensibles pour la nation. Elle peut accompagner les services, établissements et entreprises concernés par le dispositif PPST.

Section 2. Le ministre et le haut fonctionnaire de défense et de sécurité

Conformément à l'article R. 413-5-1 du code pénal, le ministre qui a la charge des éléments essentiels du potentiel scientifique et technique à protéger détermine leur besoin de protection. Il fixe les orientations nationales relevant de la compétence de son ministère. Il signe les conventions avec les entreprises privées qui souhaitent adhérer au dispositif de PPST.

Dans chaque ministère, le HFDS agit au nom du ministre pour ce qui relève de la protection du potentiel scientifique et technique le concernant. Le service du HFDS participe à la définition des orientations nationales en matière de PPST. Il décline les orientations validées par le SGDSN et celles de son ministre dans une instruction ministérielle et s'assure de sa bonne exécution.

A. *Le rôle du HFDS dans le domaine de la protection du potentiel scientifique et technique*

Le HFDS dresse et actualise la cartographie des services, établissements et entreprises qui relèvent de son département ministériel, en distinguant :

- ceux avec lesquels un lien formel de tutelle existe ;
- ceux qui adhèrent par convention au dispositif de protection ;
- ceux dont les activités justifieraient qu'ils rejoignent le dispositif.

Le HFDS est chargé d'informer les opérateurs relevant de son département ministériel sur le dispositif de PPST, en soulignant sa complémentarité et son articulation avec les autres dispositifs de protection (voir le TITRE IV de la présente instruction).

Le HFDS reçoit et examine les projets d'accords de coopération internationale qui lui sont soumis pour avis préalable ou pour information (voir le Chapitre 1 du TITRE II de la présente instruction).

Le HFDS supervise les ZRR relevant de son ministère. Pour ce faire il :

- confirme le besoin de création des ZRR en validant la cotation des risques PPST ;
- apporte son aide à la définition des mesures de sécurité et des règlements intérieurs ;
- signe les arrêtés de création, de modification (et, le cas échéant, les abroge) de ZRR, s'il en a reçu délégation ;
- instruit les demandes d'avis ministériel pour les accès en ZRR, soumises sur le fondement de l'article R. 413-5-1 du code pénal ;

- informe en tant que de besoin les chefs de services, d'établissements ou d'entreprises des risques qui pèsent sur leur secteur d'activité ;
- tient à jour une base de données ministérielle et rapporte les informations relatives aux demandes d'accès en ZRR sur la base de données interministérielle dédiée, conformément au décret n° 2022-367 du 15 mars 2022 ;
- fait procéder en cas de besoin aux contrôles nécessaires par les services spécialisés (voir Section 3 du présent chapitre) ;
- participe à la mise en œuvre du régime contraventionnel prévu à l'article R. 413-5-2 du code pénal (voir Section 3 Chapitre 5 du TITRE III de la présente instruction).

Le HFDS évalue la mise en œuvre des mesures relatives à la PPST applicables aux services, établissements ou entreprises qui relèvent du périmètre de son ministère. À ce titre, et en liaison avec les services spécialisés (voir Section 3 du présent chapitre), il définit les critères et informations nécessaires à une telle évaluation et s'assure de sa conformité aux orientations nationales et générales susmentionnées. Autant que possible, il tient informé les responsables locaux de la PPST de l'évolution de la menace.

B. *Les bilans du haut fonctionnaire de défense et de sécurité*

Le HFDS adresse chaque année avant la fin du premier semestre de l'année N au SGDSN le bilan annuel des activités relevant de la PPST pour l'année N-1. La composition du bilan annuel est précisée chaque année par le SGDSN. Le bilan comporte notamment : (i) une appréciation synthétique du dispositif de PPST dans le périmètre relevant du ministère, en identifiant notamment ses points forts, ses difficultés principales et ses axes de progression, (ii) un état statistique commenté et (iii) les évolutions que le ministère propose d'apporter aux outils et documents d'aide à la décision.

Les bilans annuels sont archivés sur un espace informatique commun sécurisé. Ces bilans peuvent être complétés de bilans particuliers demandés en comité de pilotage.

Pour mener à bien ses activités, le HFDS s'appuie sur ses relais dans les services, établissements ou entreprises (officiers de sécurité ou fonctionnaires de sécurité et de défense par exemple). Le HFDS est chargé d'animer ce réseau de correspondants. L'articulation entre les missions du HFDS et celles de ces relais est précisée par les ministères dans leurs instructions ministérielles.

Section 3. Les services spécialisés concourant à la PPST

Au titre de leur mission de protection économique et scientifique, de contre-prolifération et de lutte contre l'ingérence étrangère, la Direction générale de la sécurité intérieure (DGSI) et la Direction du renseignement et de la sécurité de la défense (DRSD) assurent, dans leurs périmètres de compétence respectifs et sur l'ensemble du territoire national, le suivi des services, établissements ou entreprises abritant des ZRR.

La DGSI et la DRSD sont des interlocuteurs privilégiés des responsables de ZRR. Elles les sensibilisent aux risques liés à la captation de leurs savoirs et savoir-faire et sont informées des incidents ou problèmes de sûreté affectant leurs ZRR. Elles le font en lien avec la gouvernance des établissements hébergeurs, notamment les FSD. La DGSI et la DRSD informent également les HFDS de ces incidents et conviennent avec eux des mesures de remédiation à apporter.

À la demande des HFDS des ministères de tutelle, la DGSI et la DRSD peuvent procéder à des enquêtes de sécurité sur les personnes sollicitant un accès aux ZRR ainsi qu'à des vérifications portant sur l'application des mesures de protection imposées aux ZRR. Au titre de ses compétences nationales et interministérielles, le Service national des enquêtes administratives et de sécurité (SNEAS) peut également être sollicité pour procéder à ces enquêtes.

TITRE II. Les mesures de protection applicables aux secteurs scientifiques et techniques protégés

Les mesures de protection détaillées dans ce titre sont prévues de façon générale dans les services, établissements ou entreprises dont les activités relèvent d'un ou plusieurs secteurs scientifiques et techniques protégés. C'est en particulier le cas pour ceux qui hébergent des unités protégées, et *a fortiori* ceux disposant, au sein de ces unités protégées, d'une ou plusieurs zones à régime restrictif (ZRR).

Chapitre 1. L'examen des coopérations internationales

Les articles L. 123-7-1 et D. 123-19 du code de l'éducation et les articles L. 810-1 et L. 812-1 du code rural et de la pêche maritime pris ensemble créent une obligation légale d'avis ministériel préalable sur l'ensemble des projets de coopération internationale de certains établissements publics. Cet avis est rendu à l'issue d'un examen conjoint du projet entre le ministère chargé de l'enseignement supérieur, le ministère chargé des affaires étrangères et les autorités de tutelle.

Aux termes de l'article 6 de l'arrêté du 3 juillet 2012 modifié, le responsable d'une unité protégée veille à ce que les coopérations internationales impliquant l'unité n'entrainent pas de transfert incontrôlé de ses savoirs ou savoir-faire. À ce titre, il transmet pour avis préalable au ministre chargé d'exercer la tutelle les seuls projets de coopérations qui intéressent la protection du potentiel scientifique et technique de la nation (PPST).

Enfin, conformément à l'article 5 de l'arrêté du 3 juillet 2012 modifié et à son annexe II, les services, établissements ou entreprises qui abritent une activité relevant des secteurs scientifiques et techniques protégés et qui sont placés sous l'autorité ou la tutelle d'un ministre informent le haut fonctionnaire de défense et de sécurité (HFDS) de leurs projets de coopérations internationales de nature scientifique ou technique.

Le présent chapitre vient préciser comment l'examen des coopérations scientifiques internationales au titre de la PPST se décline pour ces entités.

Section 1. Établissements et coopérations concernés

Les dispositions suivantes s'adressent aux établissements visés par l'article 6 de l'arrêté du 3 juillet 2012 modifié, à savoir ceux pour lesquels un projet de coopération implique des activités en unité protégée. Un tel établissement soumet un projet d'accord de coopération pour avis ministériel préalable au titre de la PPST, quelle que soit sa forme juridique, à son ministère de tutelle ou celui ayant déterminé le besoin de protection, lorsque les trois critères suivants sont réunis :

1° - l'établissement français exerce une activité rattachée à un secteur scientifique et technique protégé ;

2° - le projet de coopération est conclu avec un établissement étranger ou sous contrôle étranger ou une organisation internationale, public comme privé ;

3° - la coopération entre les établissements visés en 1° et en 2° intègre au moins un des critères suivants :

- une activité de recherche et/ou développement exercée en ZRR ;
- un financement reçu d'une entité extra-européenne ;
- un budget unilatéral de mobilité entrante ou sortante pour un ou plusieurs chercheurs ;
- un mécanisme de transfert explicite de technologie et/ou de savoirs (cession de propriété intellectuelle, transfert de compétences, joint-ventures notamment) ;

- une activité de recherche ou développement concernant ou incluant une technologie dite « critique » de l'Union européenne ;
- une activité de recherche ou développement concernant ou incluant un bien ou technologie à double usage ;
- une activité de recherche ou développement sur des agents pathogènes visés par la règlementation sur les micro-organismes et toxines ;
- la participation d'un pays visé par un régime de sanctions (international ou européen) ou d'un établissement lié à une entité sous sanctions ;
- la participation d'une entité liée à une organisation militaire étrangère.

Sont exclues de cette procédure de demande d'examen certaines coopérations internationales faisant déjà l'objet d'un examen spécifique à savoir :

- les licences de transfert ou d'exportation de matériels de guerre et assimilés ;
- les projets ayant obtenus une licence d'exportation au titre de contrôle des exportations des biens et technologies à double usage ;
- les arrangements de coopération et groupes de travail internationaux validés par le Délégué général pour l'armement.

Des instructions ministérielles pourront préciser les coopérations prioritairement visées par cette procédure et, le cas échéant, celles qui peuvent en être explicitement exclues. Elles pourront également préciser les modalités de transmission des informations concernant les autres activités de coopération qui ne sont pas forcément l'objet d'un accord.

Conformément aux dispositions de l'article 5 de l'arrêté du 3 juillet 2012 modifié, lorsque les projets d'accord n'impliquent pas d'activité en unité protégée, ils font seulement l'objet d'une information au HFDS du ministère de tutelle, dès lors que les trois critères présentés *supra* sont vérifiés. Cette obligation d'information s'applique également aux établissements publics sous tutelle n'hébergeant pas d'unité protégée. Un avis ministériel préalable à la conclusion d'un accord de coopération peut toutefois être demandé par l'établissement s'il l'estime utile.

Pour les établissements qui ne sont pas sous tutelle ministérielle et les entreprises privées, l'information ou la transmission des projets de coopération internationale est facultative. Ses modalités peuvent être inspirées des dispositions du présent chapitre et sont fixées dans les conventions qui les lient avec le ministre ayant déterminé le besoin de protection, conformément à l'article 2 du décret n° 2011-1425 du 2 novembre 2011.

Section 2. Procédure de saisine et d'examen des coopérations internationales

Les établissements soumis à un avis préalable ou souhaitant solliciter un avis ministériel sur un projet de coopération mené avec une entité étrangère soumettent le projet à leur ministre de tutelle ou au ministre ayant déterminé le besoin de protection. Ces projets de coopération font l'objet d'un examen puis d'un avis ministériel. Au regard de leurs compétences en matière de protection économique et de lutte contre les ingérences étrangères, les services spécialisés concourant à la PPST (DGSI et DRSD) peuvent être sollicités par les ministères dans le cadre de l'examen des projets.

A. *Transmission du projet d'accord au ministère compétent*

Dans le cas d'un établissement sous tutelle, le projet sera transmis au ministère de tutelle.

Dans le cas d'un établissement qui n'est pas sous tutelle ou qui est sous tutelle multiple, l'établissement s'adresse au ministère qui a déterminé le besoin de protection (celui qui a procédé à la cotation des quatre risques PPST pour l'unité de recherche et/ou développement concernée)

ou, à défaut, au ministère qui a la charge des éléments essentiels du potentiel à protéger dans le cadre de cette coopération.

En cas de doute, il revient à l'établissement hébergeur des activités visées par la coopération de trancher sur le ministère à contacter.

Dans le cas d'une coopération impliquant plusieurs établissements, un établissement coordinateur sera désigné par ces derniers afin de saisir son ministère de tutelle sur le projet de coopération envisagé.

Dans tous les cas, si l'établissement est soumis aux dispositions des articles L. 123-7-1 et D. 123-19 du code de l'éducation ou des articles L. 810-1 et L. 812-1 du code rural et de la pêche maritime, le projet est adressé au ministère identifié comme compétent selon les modalités exposées ci-dessus, avec en copie le ministère chargé de l'enseignement supérieur et le ministère chargé des affaires étrangères.

B. *Évaluation préliminaire au niveau de l'établissement*

L'établissement concerné par le projet d'accord peut s'appuyer sur les outils mis à sa disposition par le HFDS pour pré-évaluer la sensibilité du projet de coopération envisagé. Il transmet le projet d'accord, cette évaluation préliminaire et les informations nécessaires à l'analyse du projet, au ministère compétent identifié conformément aux dispositions du paragraphe *supra*.

C. *Avis ministériel*

L'avis ministériel rendu sur un projet de coopération internationale est uniquement un avis de sécurité au titre de la PPST. Il peut prendre plusieurs formes :

- avis favorable : la coopération peut être conclue ;
- avis réservé ou défavorable en l'état : le projet de coopération devrait a minima être modifié pour tenir compte des réserves émises ;
- avis défavorable : la coopération ne devrait pas être conclue, même amendée.

Le ministère compétent dispose d'un délai de deux mois à compter de la réception du projet pour rendre un avis consolidé à l'établissement. À l'expiration de ce délai, l'avis ministériel est réputé favorable.

L'avis ministériel étant préalable à la signature de l'accord, le projet doit être soumis au ministère compétent dès que les contours de la coopération sont suffisamment définis et avant sa finalisation, en anticipant le délai de deux mois nécessaire au traitement du dossier.

D. *Coopérations impliquant des activités en ZRR*

L'article R. 413-5-2 du code pénal prévoit que l'absence d'information par l'établissement aux autorités de tutelle, au ministre chargé de l'enseignement supérieur et au ministre chargé des affaires étrangères d'un projet de coopération internationale impliquant une activité en ZRR dans un établissement soumis aux dispositions des articles L. 123-7-1 et D. 123-19 du code de l'éducation ou des articles L. 810-1 et L. 812-1 du code rural et de la pêche maritime, constitue une contravention de la cinquième classe.

L'avis rendu par le ministre sur le projet d'accord impliquant une activité en ZRR ne dispense ni ne préjuge des avis qui seraient rendus pour l'accès à cette ou ces ZRR dans le cadre de la coopération.

E. *Registre des coopérations*

Les ministères en charge de l'examen de ces projets de coopération tiennent un registre des coopérations, qui précise notamment :

- le nom de l'établissement français concerné ;
- la présence ou non de ZRR ;
- le ministère de tutelle ;
- l'établissement(s) étranger(s) concerné(s) ;
- le(s) pays concerné(s) ;
- le secteur scientifique et technique protégé concerné ;
- le sujet de la coopération ;
- des observations éventuelles.

F. *Articulation avec les dispositions du code de l'éducation ou du code rural et de la pêche maritime*

La procédure d'examen au titre de la PPST décrite *supra* est compatible avec les dispositions du code de l'éducation et du code rural et de la pêche maritime. Néanmoins, dans le cas où les conditions de soumission au titre de la PPST (voir Section 1 du présent chapitre) ne sont pas réunies, l'établissement n'est pas dispensé de ses obligations générales au titre des articles L. 123-7-1 et D. 123-19 du code de l'éducation ou des articles L. 810-1 et L. 812-1 du code rural et de la pêche maritime.

Chapitre 2. La sécurité des systèmes d'information (SSI)

Section 1. Articulation de la PPST avec la politique de cyberrésilience et de SSI

Face à l'évolution des menaces et à l'interconnexion croissante des systèmes d'information (SI), ceux-ci représentent une voie d'accès privilégiée par les pirates informatiques pour accéder aux informations sensibles détenues dans les services, établissements ou entreprises entrant dans le champ de la PPST.

Les textes législatifs et règlementaires relatifs à la cyberrésilience et à la sécurité des SI, définis au niveau national et européen - tels que la *directive (UE) 2022/2555 du Parlement Européen et du Conseil du 14 décembre 2022, concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (« directive NIS2 »)* - précisent les objectifs et exigences applicables en la matière, et destinés à répondre à ces enjeux.

Ces textes peuvent s'appliquer aux services, établissements ou entreprises entrant dans le champ de la PPST. En effet, dans le contexte de la PPST, des objectifs et exigences de SSI contribuent à assurer la protection d'informations sensibles des différentes disciplines de recherche concernées et à préserver la sécurité des activités scientifiques et techniques essentielles pour la nation et sa souveraineté.

Section 2. Gouvernance de la SSI

La sécurisation des SI implique le déploiement d'une gouvernance SSI effective et d'une organisation de gestion des risques visant à assurer la cyberrésilience et l'amélioration continue du niveau de sécurité des SI.

Les établissements publics de l'État entrant dans le champ de la PPST sont soumis par ailleurs au cadre de gouvernance de l'État précisé dans l'instruction générale interministérielle (IGI)

n° 1337/SGDSN/ANSSI du 26 octobre 2022 sur l'organisation de la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics.

Le chef de service, d'établissement ou d'entreprise dont l'activité entre dans le champ de la PPST est responsable de l'organisation de la gouvernance SSI.

Il désigne un responsable de la sécurité des systèmes d'information (RSSI). Afin de réaliser ses missions de manière adéquate, le RSSI désigné a le droit d'en connaître sur le niveau de risque et les mesures de protection requises pour le service, l'établissement ou l'entreprise concernée, ainsi que sur toute information relative aux systèmes d'information des unités protégées et zones à régime restrictif. Il peut être amené à accéder aux ZRR dans les conditions prévues au TITRE III de la présente instruction. Un réseau de correspondants à la sécurité des systèmes d'information (CSSI) de proximité peut être mis en place pour l'application de la PSSI et des mesures de sécurisation des SI.

Les mesures de sécurisation des SI assurant la protection des informations sensibles au titre de la PPST sont mises en place dans le cadre de la gouvernance SSI. La concertation entre la gouvernance SSI et la gouvernance de la PPST doit être assurée par le chef de service, d'établissement ou d'entreprise. Les chaînes respectives de remontées et de gestion d'incident collaborent ensemble notamment en cas d'incident sur les SI.

Chaque ministère concerné tient à jour la liste des RSSI (avec leurs coordonnées) des services, établissements et entreprises dont il a déterminé le besoin de protection et la partage avec l'ANSSI.

Les services, établissements et entreprises tiennent à jour et mettent à disposition du ministre ayant déterminé le besoin de protection et de l'ANSSI la liste de leurs RSSI et CSSI (avec leurs coordonnées).

Section 3. Politique de sécurité des systèmes d'information (PSSI)

Les services, établissements ou entreprises hébergeant une ou plusieurs ZRR se dotent d'une politique de sécurité des systèmes d'information (PSSI) et la mettent en œuvre. La PSSI est approuvée par le chef de service, d'établissement ou d'entreprise.

La PSSI est applicable aux systèmes d'information traitant des informations sensibles relevant de la PPST. La PSSI du service, de l'établissement ou de l'entreprise entrant dans le champ de la PPST est conforme aux mesures prévues par l'instruction interministérielle n° 901/SGDSN/ANSSI (II 901) du 28 janvier 2015 relative à la protection des systèmes d'information sensibles.

En conséquence, le service, l'établissement ou l'entreprise est tenu de se conformer aux règles relatives aux systèmes d'informations sensibles prévues dans l'II 901. Dans les cas où il traiterait d'informations relatives aux spécialités dont les savoir-faire sont susceptibles d'être détournés à des fins de terrorisme ou de prolifération d'armes de destruction massive et de leurs vecteurs (risques R3 et R4), les règles qui s'appliquent sont celles relatives aux systèmes d'information « Diffusion Restreinte » prévues par l'II 901.

Les mesures de protection des SI déclinées dans la PSSI doivent répondre aux objectifs de confidentialité, de disponibilité et d'intégrité des données traitées dans ces SI. Elles sont d'ordre technique et organisationnel. Elles comprennent des mesures de base, appelées « mesures d'hygiène » et des mesures de défense en profondeur des SI. Le marquage des données contribue notamment pleinement aux mesures de sécurisation spécifiques à mettre en place. La PSSI rappelle que l'accès aux informations sensibles détenues dans une zone à régime restrictif, qu'il s'agisse d'accès physique ou à distance, doit faire l'objet d'une autorisation d'accès dans les conditions prévues au Chapitre 3 du TITRE III de la présente instruction.

La PSSI doit prévoir une politique de gestion des accès aux SI qui prenne en compte le recours à des prestataires informatiques et à l'externalisation de l'hébergement des informations (voir section suivante).

La PSSI s'articule de manière cohérente avec la politique de sécurité interne déclinant la PPST. Cette articulation relève de la responsabilité du chef de service, d'établissement ou d'entreprise.

Section 4. Recours à des prestations informatiques externalisées

Le service, l'établissement ou l'entreprise qui héberge une unité protégée doit être en mesure de garantir que les informations sensibles ne puissent être accessibles que par des personnes autorisées et ayant le besoin d'en connaître, y compris dans le cadre des prestations informatiques externalisées (notamment d'infogérance, d'hébergement et d'audit).

De façon générale, une analyse de risques et une analyse d'impact doivent être conduites préalablement au recours à de telles prestations d'externalisation ou d'hébergement, en vue de mettre en œuvre un ensemble de mesures de réduction des risques, conciliant les impératifs économiques et techniques des entités concernées, leurs méthodes de travail et les besoins de protection du potentiel scientifique et technique national.

Concernant les mesures SSI relatives à l'externalisation, le service, l'établissement ou l'entreprise porte une attention particulière dans le cadre du recours à un fournisseur de service informatique en nuage. À ce sujet, il s'appuie également sur l'ensemble des recommandations de l'ANSSI pour l'hébergement dans le *cloud* des systèmes d'information sensibles.

Le recours à une prestation informatique externalisée nécessite de prévoir des conditions contractuelles, offrant des garanties techniques, juridiques, et de sécurité appropriées, particulièrement dans le cas d'un prestataire établi ou opérant hors du territoire national ou soumis à une législation permettant un accès aux données par des autorités publiques d'États tiers non autorisé par le droit de l'Union européenne ou d'un État membre.

Section 5. Le dispositif de veille, de signalement et de coordination relatif aux incidents

La PSSI organise le signalement des incidents majeurs sur un SI par le service, l'établissement ou l'entreprise concerné, au ministre qui a déterminé le besoin de protection, aux services spécialisés (DGSI et DRSD), ainsi qu'à l'ANSSI. Le service, l'établissement ou l'entreprise fait ce signalement sans retard injustifié et en tout état de cause dans les 24 heures après avoir eu connaissance de l'incident.

Les services des HFDS des ministères concernés concourent aux échanges d'informations relatives aux diffusions d'alertes en cas d'incidents majeurs sur un SI. L'ANSSI et les services des HFDS des ministères se tiennent mutuellement informés des alertes et des incidents majeurs portés à leur connaissance.

Chapitre 3. La sécurité des documents

Si la protection du potentiel scientifique et technique de la nation vise à protéger certaines informations sensibles contre les captations et détournements, elle ne doit cependant pas empêcher le transfert dans le domaine public des travaux de recherche (par publication dans des revues scientifiques ou par dépôt de brevets par exemple).

Pour autant, dès lors qu'une unité de recherche et/ou développement est évaluée comme sensible, la protection des documents qu'elle détient implique une attention particulière. C'est l'objet du présent chapitre.

Par application de l'article 6 de l'arrêté du 3 juillet 2012 modifié, le responsable de l'unité protégée prend toute disposition utile pour assurer la protection des informations concernées. La première

de ces dispositions est d'effectuer une analyse de sensibilité des données et informations contenues et produites par son unité. Le marquage doit être explicite afin qu'une personne, en les manipulant, ne puisse en ignorer la sensibilité et qu'elle puisse se référer à une échelle précisant les précautions associées. Ainsi, le marquage doit être visible sur les documents hébergés sur le système d'information du service, de l'établissement ou de l'entreprise entrant dans le champ de la PPST.

En cas d'échange avec d'autres entités, l'échelle de sensibilité doit aussi être transmise afin que le receveur ait connaissance des précautions de manipulation associées au marquage et qu'il sache, par exemple, s'il peut la diffuser ou la retransmettre dans les limites fixées par le respect du besoin d'en connaître.

Le règlement intérieur de l'unité protégée ou de la ZRR précise les règles spécifiques encadrant la sécurité des documents relatifs aux travaux scientifiques qui y sont menés. Ces règles doivent concilier le besoin légitime d'ouverture de l'unité et le respect des impératifs de protection de certaines données.

Section 1. Le marquage des documents

A. Mention « Diffusion Restreinte »

Dans la plupart des cas, les unités protégées et zones à régime restrictif n'hébergent pas d'information classifiée au titre du secret de la défense nationale. Il est en revanche fortement recommandé d'utiliser, pour les données les plus sensibles de ces unités (par exemple lorsque les risques R3 ou R4 ont été évalués non nuls), la mention de protection « Diffusion Restreinte » qui apporte un niveau adapté de protection et de manipulation des documents sensibles. L'IGI 1300 en précise les modalités de mise en œuvre (en particulier dans son annexe 1). Cette mention est donc fortement recommandée pour les informations ayant trait à des spécialités sensibles.

La mention « Diffusion Restreinte » est une mention de protection. Elle vise à protéger des informations et supports qu'il n'y a pas lieu de classifier mais qui présentent une sensibilité particulière. Son objectif principal est de sensibiliser l'utilisateur à la nécessaire discrétion dont il doit faire preuve dans la manipulation des informations et supports couverts par cette mention. Ceux-ci ne peuvent être communiqués qu'aux personnes ayant besoin d'en connaître, c'est-à-dire pour qui il est nécessaire d'y accéder pour l'exercice de leurs fonctions ou l'accomplissement d'une mission, et dans le respect des mesures de protection associées.

La mention « Diffusion Restreinte » ne confère pas de protection pénale. Pour autant, la divulgation d'informations et supports portant la mention « Diffusion Restreinte » à des personnes physiques ou morales n'ayant pas le besoin d'en connaître est susceptible d'exposer son auteur à des sanctions disciplinaires, administratives, et éventuellement pénales, notamment au titre de la violation du secret professionnel.

B. Autres mentions

Au-delà des mentions décrites dans l'IGI 1300, il est recommandé de faire usage de mentions telles que par exemple les mentions Confidentiel Entreprise, Confidentiel Industrie, Confidentiel Recherche.

La divulgation d'informations et supports portant les mentions Confidentiel Entreprise, Confidentiel Industrie, Confidentiel Recherche à des personnes physiques ou morales n'ayant pas le besoin d'en connaître est susceptible d'exposer son auteur à des sanctions disciplinaires ou administratives. Il est recommandé à cet effet que la charte d'utilisation des systèmes d'information applicable dans l'organisme mentionne des sanctions disciplinaires.

Section 2. Les publications et brevets

De façon générale, aucun contrôle ni restriction de publication ou de dépôt de brevet n'est prévu par la PPST.

De façon exceptionnelle, justifiée par une sensibilité élevée et un besoin impérieux de protection de certaines informations issues des travaux scientifiques, le règlement intérieur peut prévoir des modalités spécifiques de revue interne des projets de publication ou de dépôt de brevet. L'ajout de cette mesure est de la responsabilité du chef de service, d'établissement ou d'entreprise.

À titre d'exemple, le Conseil national consultatif pour la biosécurité (décret n° 2015-1095 du 31 août 2015) peut être saisi pour avis par les responsables d'un projet de recherche ou les auteurs d'une publication, lorsque les résultats de ce projet ou la publication qui en fait état sont susceptibles de comporter des risques pour la biosécurité.

Section 3. Le rapport de stage

Au sein d'une unité protégée, le stagiaire exerce ses activités sous le contrôle d'un personnel de l'unité. Son stage doit être formalisé par une convention qui prévoit les relations entre cette personne, son établissement d'origine et l'unité protégée d'accueil. Cette convention de stage doit, le cas échéant, mentionner la durée de validité de l'autorisation qui lui est accordée pour pénétrer dans une ZRR. Le responsable de stage est rendu destinataire de tout projet de rapport de stage effectué dans l'unité. Il le transmet en tant que de besoin au responsable de l'unité protégée en appelant son attention sur les risques inhérents à la diffusion des informations contenues dans le rapport.

Afin de lui permettre de protéger les éléments constitutifs du potentiel scientifique et technique, le responsable de l'unité protégée, après avis éventuel du responsable de stage, peut exiger du stagiaire qu'il occulte les informations dont la diffusion présente un risque au sens du I de l'article R. 413-5-1 du code pénal. Il peut également lui imposer d'éventuelles restrictions concernant la diffusion du rapport en question. Ces éléments peuvent être précisés dans la convention de stage.

Le stagiaire qui diffuserait ces informations, nonobstant l'opposition du responsable de l'unité protégée, est susceptible de voir sa responsabilité pénale engagée, soit sur le fondement de l'article 413-10 du code pénal si les informations font l'objet d'une classification au titre de la protection du secret de la défense nationale, soit sur celui des articles 226-13 (secret professionnel) ou 314-1 (abus de confiance) du même code.

Section 4. Contrats d'externalisation ou de prestation de services

Par application de l'article 1er de l'arrêté du 3 juillet 2012 modifié, les contrats ou conventions d'externalisation ou de prestation de services, y compris pour le traitement des données, notamment l'infogérance, l'audit ou le conseil en propriété industrielle, mentionnent le caractère confidentiel des informations portant sur les techniques, les méthodes et les connaissances relatives aux travaux scientifiques et techniques menés dans les ZRR, et prévoient une clause spécifique relative aux obligations de protection de ces informations pendant et après la prestation.

De même, le service, l'établissement ou l'entreprise qui héberge une unité protégée devant être en mesure de garantir la protection des informations qu'elle détient, une vigilance particulière doit être apportée dans la conclusion de contrats d'externalisation et de prestation de service.

TITRE III. Les zones à régime restrictif

Les zones à régime restrictif (ZRR) sont définies aux articles 413-7 et R. 413-5-1 du code pénal. Il s'agit d'une catégorie de zone protégée constituée de locaux et de terrains clos dans lesquels l'accès et la circulation sont réglementés afin d'empêcher que des éléments essentiels du potentiel scientifique ou technique de la nation (PPST) :

- fassent l'objet d'une captation de nature à affaiblir ses moyens de défense, à compromettre sa sécurité ou à porter préjudice à ses autres intérêts fondamentaux ;
- soient détournés à des fins de terrorisme, de prolifération d'armes de destruction massive et de leurs vecteurs ou de contribution à l'accroissement d'arsenaux militaires.

Les espaces concernés par la ZRR sont clairement délimités au sein du bâtiment, du laboratoire, de l'étage, etc. (article R. 413-4 du code pénal) et font l'objet de mesures de protection adaptées aux éléments constitutifs du potentiel scientifique et technique concernés (article 1 de l'arrêté du 3 juillet 2012 modifié), décrites au présent titre. Les ZRR s'inscrivent au sein d'unités protégées qui elles-mêmes s'intègrent dans un ensemble plus vaste (département de recherche, entreprise, campus universitaire, par exemple).

Les mesures de protection spécifiques aux ZRR détaillées dans ce titre complètent les mesures de protection présentées dans le titre précédent.

Chapitre 1. La création, modification et suppression d'une ZRR

Les ZRR sont créées selon la procédure prévue aux articles R. 413-1 et suivants du code pénal. En particulier, l'article R. 413-5-1 de ce code dispose que le besoin de protection est déterminé par le ministre qui a la charge des éléments essentiels du potentiel scientifique et technique à protéger.

L'article 2 du décret n° 2011-1425 du 2 novembre 2011 précise que les informations nécessaires à la PPST sont fournies au ministre compétent pour déterminer le besoin de protection dans des conditions fixées, selon les caractéristiques du service, établissement ou entreprise intéressé par ce ministre ou par convention entre ce ministre et les organes compétents du service, établissement ou entreprise intéressé. Pour autant, la décision de création des ZRR relève de la seule autorité administrative et s'impose au chef de service, établissement ou entreprise concerné via un arrêté ministériel de création. Cette compétence se rattache à l'exigence constitutionnelle de protection des intérêts fondamentaux de la nation par le pouvoir exécutif.

Le statut d'une ZRR et les informations spécifiques permettant de caractériser sa sensibilité (en particulier ses cotations sur les quatre risques de la PPST) constituent une information de niveau « Diffusion Restreinte ».

Section 1. Préalables à la création d'une ZRR

La décision de créer une ZRR doit répondre à un besoin qu'il convient d'examiner de la manière la plus objective possible. C'est tout l'objet de l'évaluation du besoin de protection explicitée au Chapitre 2 Section 2 du TITRE I de la présente instruction, préalable systématique à toute création de ZRR. Dès lors que la somme des cotations de l'unité évaluée est strictement supérieure à zéro, la création d'une ou plusieurs ZRR peut être envisagée. Le ministre qui a déterminé le besoin de protection devra veiller :

- à ce que la réglementation de la circulation au sein de ces zones n'ait pas pour objet ou pour effet de remettre en cause, le cas échéant, le principe d'enrichissement de l'enseignement par la recherche ;
- à fixer un périmètre pour la ZRR, qui corresponde au strict besoin de protection. Le choix de l'emprise d'une ZRR résulte en effet d'un compromis entre les contraintes liées à la

protection de la confidentialité des activités de recherche et le besoin de fonctionnement de l'unité. Les limites de la ou des ZRR peuvent se superposer totalement ou partiellement aux limites de l'unité protégée ;

- à une cohérence au sein de l'unité protégée. Ceci est notamment le cas lorsqu'il est envisagé la création de plusieurs ZRR au sein d'une même unité, ZRR relevant parfois de périmètres ministériels différents.

L'emprise d'une ZRR et les modalités d'organisation qui en découlent résultent donc d'un équilibre entre :

- le besoin de protection relatif à la PPST ;
- le fonctionnement et les contraintes spécifiques de l'unité protégée concernée ;
- les principes du processus de Bologne[5] sur l'enseignement supérieur et la recherche.

La création d'une ZRR peut découler d'engagements pris par le service, établissement ou entreprise au titre de :

- une lettre d'engagements signée dans le cadre d'une autorisation sous conditions d'un investissement étranger en France ;
- une convention ou un contrat de financement (subvention notamment) public portant des clauses spécifiques de sécurité ;
- un engagement contractuel spécifique au titre de la sécurité.

Le ministre qui prend l'initiative de la création d'une ou plusieurs ZRR dans une unité protégée qu'il a évaluée et qui est sous tutelle de (ou en convention avec) plusieurs ministres fait toute diligence pour en informer les autres ministres. Tout différend entre ministres sur la création de cette ou ces ZRR sera tranché par le secrétariat général de la défense et de la sécurité nationale.

Section 2. La procédure de création d'une ZRR

Lorsqu'au sein d'une unité protégée, il existe un risque avéré lié à la captation ou au détournement d'informations susceptibles d'affaiblir le potentiel scientifique et technique de la nation, le ministre qui a déterminé le besoin de protection se rapproche du chef de service, d'établissement ou d'entreprise afin de créer une ou plusieurs ZRR.

Le chef de service, d'établissement ou d'entreprise adresse au ministre une demande de création de ZRR (incluant notamment un formulaire d'enregistrement de ZRR dont un modèle type est fourni en ANNEXE 2), dont les modalités sont précisées par des instructions ministérielles. En l'absence d'une telle transmission et si les relances du ministre à ce sujet s'avéraient infructueuses, ce dernier pourra procéder directement à la création de ZRR.

Pour éclairer sa décision, le ministre ou le haut fonctionnaire de défense et de sécurité (HFDS) sollicite au besoin les services spécialisés concourant à la PPST (DGSI et DRSD) sur l'opportunité d'une telle création. Les services du HFDS, accompagnés en tant que de besoin par des agents des services spécialisés mais également par des agents des réseaux territoriaux relevant de l'autorité du ministre, peuvent effectuer une visite du site. Lorsque cette visite s'effectue dans les locaux d'une entité privée, elle doit préalablement être autorisée par son représentant légal. À l'issue, le HFDS propose au ministre la création d'une ou plusieurs ZRR.

Le dossier de demande de création d'une ZRR comprend le compte-rendu de la visite et les avis recueillis, le projet d'arrêté (voir ANNEXE 4 de la présente instruction) ainsi que les renseignements nécessaires à la mise à jour du répertoire national des ZRR. Le formulaire d'enregistrement adressé par le service, établissement ou entreprise (dont un modèle est fourni en ANNEXE 2) est transmis par le ministre au secrétariat général de la défense et de la sécurité

[5] Ce processus est un mécanisme qui vise à renforcer la cohérence des systèmes d'enseignement supérieur en Europe.

nationale (SGDSN). Ce dernier vérifie au préalable que la zone ne fait pas déjà l'objet d'un arrêté pris par un autre ministre.

Le SGDSN attribue à la ZRR un numéro d'identifiant unique composé des informations suivantes accolées sans espaces : *numéro de département de la ZRR, code du ministère de tutelle*[6]*, quantième dans la liste des établissements sous tutelle de ce ministère hébergeant des ZRR, « ZRR », numéro de la ZRR*. Exemple : 75F25ZRR3.

Les numéros attribués à des services, établissements ou entreprises supprimés de l'inventaire ne sont pas réattribués.

Après avoir mis à jour le répertoire national, le SGDSN renvoie le dossier au ministre qui prend l'arrêté portant création de la ZRR, conformément au modèle proposé en ANNEXE 4 de la présente instruction. Conformément aux dispositions de l'article R. 413-3 du code pénal, l'arrêté de création de chaque ZRR est signé par le ministre ayant déterminé le besoin de protection et fixe l'implantation et les limites de la ZRR. De plus, lorsque l'activité principale du service, de l'établissement ou de l'entreprise concernée relève d'un autre ministre que celui ayant déterminé le besoin de protection, l'arrêté est pris conjointement par ces deux ministres.

L'arrêté portant création d'une ZRR est notifié, conformément aux dispositions de l'article R. 413-4 du code pénal, au chef de service, d'établissement ou d'entreprise par le ministre qui a déterminé le besoin de protection. Le ministre en adresse également une copie au SGDSN, aux services spécialisés (DGSI et DRSD) et au préfet de département concerné. Cet arrêté n'est pas publié au Journal officiel de la République française, ni dans les Bulletins officiels ministériels. Il fait l'objet d'une publication par affichage physique devant l'entrée principale de la ZRR, sur son périmètre extérieur. L'arrêté de création fait l'objet de la mention *Diffusion Restreinte*.

Dans tous les cas, une convention peut être conclue entre le ministre qui a déterminé le besoin de protection et les organes compétents du service, établissement ou entreprise intéressé pour fixer les mesures édictées par ce dernier en complément de celles qui résultent des dispositions législatives et réglementaires applicables pour assurer la protection des informations contenues dans les ZRR et les actions qui seront mises en œuvre par l'État pour accompagner le service, établissement ou entreprise dans le déploiement de ces mesures. Les HFDS des ministères disposent de conventions-type. Ces conventions concernent notamment la gestion des unités mixtes de recherche (voir le Chapitre 2 Section 4 du TITRE I de la présente instruction).

En parallèle, le chef de service, d'établissement ou d'entreprise fait toute diligence pour constituer la liste du personnel déjà en fonction dans le périmètre de la ZRR et transmettre pour avis au ministre ayant déterminé le besoin de protection les demandes d'autorisation d'accès en ZRR associées. Conformément aux dispositions de l'article R. 413-5-1 du code pénal, toute personne qui bénéficiait, antérieurement à la création ou à l'extension d'une ZRR, d'un accès aux lieux couverts par cette zone, est réputée, pour la première demande d'autorisation d'accès à cette zone qu'elle adresse au chef de service, d'établissement ou d'entreprise, avoir obtenu un avis ministériel favorable.

Section 3. Modification et suppression d'une ZRR

A. *Modifications d'une ZRR*

Toute modification d'une ZRR doit passer par un arrêté modificatif pris par le ou les ministres concernés. Le SGDSN est destinataire de cet arrêté modificatif.

[6] Code du ministre ayant déterminé le besoin de protection : A = ministre chargé de la défense, B = ministre chargé de l'écologie, C = ministre chargé de l'économie, D = ministre chargé de la santé, E = ministre chargé de l'agriculture, F = ministre chargé de l'enseignement supérieur et de la recherche.

Dès lors que les activités effectuées dans une ZRR sont déplacées hors de la zone pour toute raison légitime liée au fonctionnement de l'unité protégée (déménagement, transfert, rachat etc.), le chef de service, d'établissement ou d'entreprise adresse sans délai un dossier de modification précisant les évolutions à apporter à la ZRR existante.

Le ministre qui a déterminé le besoin de protection prend alors un arrêté de modification intégrant les modifications pertinentes à apporter à la ZRR concernée.

B. *Suppression d'une ZRR*

La suppression d'une ZRR est décidée par le ministre qui l'a créée. Il abroge l'arrêté portant création de la ZRR concernée. Le SGDSN est informé de cette abrogation. La proposition de suppression d'une ZRR est à l'initiative du HFDS ou du chef de service, d'établissement ou d'entreprise. En particulier, une attention sera portée aux ZRR devenues inactives (déménagement, restructurations, scissions). Toute demande de suppression de ZRR à l'initiative du service, établissement ou entreprise sera accompagnée d'un dossier indiquant les raisons de cette demande.

La décision de supprimer une ZRR peut être précédée d'une visite réalisée par le HFDS avec l'éventuelle assistance des services spécialisés (DGSI et DRSD) mais également celle des agents des réseaux territoriaux relevant de l'autorité du ministre afin de constater l'absence de nécessité de mesures de protection ou au contraire l'inadaptation de celles qui ont été prises.

En tant que de besoin, le SGDSN organise une concertation entre les ministères concernés par le projet de suppression. Cette concertation vise à assurer la bonne information des divers services des HFDS.

Toute liquidation, procédure collective ou fermeture qui entrainerait l'arrêt des activités d'une ZRR doit être suivie par le ministre qui a déterminé le besoin de protection afin de s'assurer que le potentiel à protéger est transféré en sécurité, le cas échéant en créant une nouvelle ZRR. Si les activités protégées ne sont pas arrêtées mais transférées à une autre entité juridique dans le cadre de la liquidation, ou d'une procédure collective, la ZRR doit être modifiée (voir paragraphe suivant) mais son existence n'est pas remise en cause par le changement de la personne morale qui l'héberge.

Chapitre 2. Le fonctionnement d'une ZRR

Section 1. Obligations minimales de protection

Chaque chef de service, d'établissement ou d'entreprise hébergeant une ou plusieurs ZRR doit se conformer, en plus des obligations relatives aux unités protégées, aux obligations de protection définies par les articles R. 413-4 et R. 413-5-1 du code pénal et par l'arrêté du 3 juillet 2012 modifié relatif à la protection du potentiel scientifique et technique de la nation qui prévoient :

- l'installation, sur le périmètre extérieur de la ZRR, d'une signalétique informant du statut de la zone et des restrictions de circulation associées (voir ANNEXE 1 pour un modèle de panneau, la version en français est obligatoire et peut être accompagnée, au besoin, de la version en anglais). À noter que cette signalétique doit rendre les limites de la zone apparentes au moyen de pancartes rectangulaires de 40cm par 30cm environ (format A3 minimum) placées aux endroits appropriés du périmètre extérieur (a minima sur toutes les entrées physiques). Ces pancartes doivent être en nombre suffisant pour être obligatoirement vues, même de nuit ;
- le déploiement d'un contrôle des accès à la ZRR. Des instructions ministérielles précisent les modalités de ces contrôles et de leur traçabilité ;

- l'application de mesures de sécurité applicables aux visites : notamment des « circuits de notoriété » définissant les itinéraires à emprunter et précisant les sujets qui ne doivent pas être abordés en présence de visiteurs ;
- la définition et l'application d'une politique de sécurité des systèmes d'information adaptée aux besoins de protection de l'unité protégée et la désignation d'un correspondant SSI chargé de l'unité protégée.

À ces fins, il établit un règlement intérieur de la ZRR (qui peut être intégré dans le règlement intérieur de l'unité protégée) et met en place une signalétique. Le règlement intérieur précise notamment :

- les modalités de recrutement et formalités administratives préalables à l'accueil des personnels au sein des unités comportant une ou plusieurs ZRR ;
- les formalités d'accès propres aux personnes qui travaillent de manière permanente au sein de la ZRR, ainsi que celles spécifiques aux personnes qui interviennent ponctuellement (stagiaires et visiteurs), étant rappelé que les autorisations d'accès sont limitées dans le temps ;
- les formalités de circulation pour chacune des catégories de personnes (circuits de notoriétés, encadrement des visites, stages, etc.) ;
- les formalités d'accès au SI hébergeant les données sensibles ou « Diffusion Restreinte » ;
- l'amplitude horaire d'ouverture des locaux ;
- les mesures de contrôle interne (port de badge, etc.) ;
- la conduite à tenir en cas d'incident, notamment sur les systèmes d'information ;
- les sanctions encourues en cas de non-respect de ces règles.

Une copie du règlement intérieur peut être envoyée au service du HFDS du ministre qui a déterminé le besoin de protection pour avis.

Il n'existe pas de normes techniques imposées pour la protection physique d'une ZRR. Chaque chef de service, d'établissement ou d'entreprise adapte le niveau de protection aux activités qu'il doit protéger. Des instructions ministérielles précisent les éléments propres aux services, établissements et entreprises de leur périmètre.

Section 2. Le rôle du chef de service, d'établissement ou d'entreprise

Le chef de service, d'établissement ou d'entreprise hébergeant une ou plusieurs ZRR est responsable de la PPST et de l'application des mesures de protection associées.

Conformément à l'article 1 de l'arrêté du 3 juillet 2012 modifié :

- il veille à maintenir ce niveau de protection lors de la conclusion et de l'exécution de contrats d'externalisation ou de prestation de services, y compris pour le traitement des données, notamment l'infogérance, l'audit ou le conseil en propriété industrielle ;
- il peut demander au HFDS du ministère qui a déterminé le besoin de protection de solliciter une enquête administrative de sécurité sur le prestataire auprès du ministère de la défense ou du ministère de l'intérieur ;
- il définit une politique de sécurité des systèmes d'information et en assure la mise en œuvre. Il prévoit en particulier la procédure par laquelle les incidents majeurs sont signalés au ministre qui a déterminé le besoin de protection et, le cas échéant, à l'autorité nationale en matière de sécurité des systèmes d'information.

De plus, conformément à l'article R. 413-5-2 du code pénal, il est responsable de :

- rendre apparentes les limites d'une zone à régime restrictif et les mesures d'interdiction dont elle est l'objet ;

- soumettre à autorisation l'accès d'une personne pénétrant dans une zone à régime restrictif ;
- autoriser l'accès à une zone à régime restrictif dans des conditions conformes aux exigences fixées par le II de l'article R. 413-5-1 du code pénal ;
- communiquer au ministre les informations qui lui sont transmises en application du V de l'article R. 413-5-1 du code pénal ;
- informer le ministre chargé de l'enseignement supérieur, les autorités de tutelle de l'établissement et le ministre chargé des affaires étrangères, d'un projet d'accord avec une institution étrangère ou internationale et impliquant des activités conduites dans une zone à régime restrictif, dans le cas où l'établissement relève des dispositions des articles L. 123-7-1 et D. 123-19 du code de l'éducation.

Dans le cas où la ou les ZRR se situent dans une unité à tutelle multiple (qui peuvent différer de celle dont relève le service, établissement ou entreprise qui l'héberge), il est possible de déroger au principe de responsabilité de l'hébergeur par une convention entre les parties afin de désigner le chef de service, d'établissement ou d'entreprise responsable de la gestion de la PPST pour cette ZRR. Dans ce cas, le chef de service, établissement ou entreprise désigné est indiqué comme tel dans l'arrêté de création de la ZRR (VI de l'article R. 413-5-1 du code pénal).

Le chef de service, d'établissement ou d'entreprise peut déléguer, conformément aux règles de droit administratif sur la délégation de signature, au responsable de la ZRR qu'il aura désigné, la faculté de signer en son nom les documents prévoyant les mesures de sécurité applicables ou les autorisations d'accès aux dites zones. Il rend compte au HFDS des accès dans les ZRR sous sa responsabilité et informe impérativement le ministre de sa décision lorsque le sens de l'avis ministériel n'est pas suivi.

Des instructions ministérielles précisent les données à transmettre au HFDS et en fixent les modalités de transmission.

Section 3. Le rôle du responsable de la ZRR

Le responsable de la ZRR veille à ce que les mesures de protection requises, y compris concernant la sécurité des systèmes d'information, soient effectives et efficaces en toutes circonstances. En cas de difficulté, il en réfère au chef de service, d'établissement ou d'entreprise qui demeure responsable de la PPST.

Afin d'aider le chef de service, d'établissement ou d'entreprise dans sa mission, il recueille toutes les informations permettant de réaliser les bilans de ce dernier.

S'il en a reçu délégation, il recueille les demandes d'accès à la ZRR et peut demander des informations complémentaires au demandeur (article 2 de l'arrêté du 3 juillet 2012 modifié) et reçoit les informations relatives à tout changement de situation d'un demandeur (article 4 de l'arrêté du 3 juillet 2012 modifié). Le cas échéant, il transmet ces informations au ministre compétent pour déterminer le besoin de protection de la ZRR.

Section 4. Le suivi d'une ZRR

Le suivi d'une ZRR relève des attributions des HFDS des ministères. Chacun précise dans des procédures internes ses modalités d'organisation.

Le suivi s'exerce de manière continue, notamment grâce aux informations figurant à l'annexe II de l'arrêté du 3 juillet 2012 modifié, transmises par le chef de service, d'établissement ou d'entreprise au ministre ayant déterminé le besoin de protection. Le chef de service, d'établissement ou d'entreprise signale toute modification liée à la structure ou à l'activité de l'unité protégée dans laquelle s'inscrit la ZRR.

Le changement de la structure juridique ou capitalistique d'une unité protégée n'a aucun effet sur le statut de la ZRR. Ce changement doit néanmoins être signalé en amont par le responsable au ministre ayant déterminé le besoin de protection. Doit également lui être signalée toute procédure collective susceptible de donner lieu à la fermeture ou à la cession, totale ou partielle d'une unité de recherche et/ou développement. Celui-ci évalue les risques découlant de cette nouvelle situation.

Le ministre ayant déterminé le besoin de protection peut, en cas de constat d'une faille de sécurité, demander au responsable de la ZRR de prendre les mesures de correction nécessaires. Il avise les partenaires de l'unité protégée qui héberge cette ZRR des risques qu'elle leur fait courir.

Le chef de service, d'établissement ou d'entreprise hébergeant une ZRR signale dans les plus brefs délais tout incident dans une ZRR au ministre qui a déterminé le besoin de protection ainsi qu'au service spécialisé concourant à la PPST (DGSI pour la sphère civile ou DRSD pour la sphère militaire). Le HFDS du ministre concerné peut, en lien et avec le soutien du service spécialisé concerné, apporter son expertise au responsable de la ZRR pour que l'incident ne se reproduise plus. Les incidents majeurs relatifs à un système d'information hébergé dans une ZRR doivent également être signalés à l'ANSSI, conformément aux dispositions de la Section 5 du Chapitre 2 du TITRE II de la présente instruction.

Chapitre 3. L'accès à une ZRR

Tout accès à une zone à régime restrictif doit faire l'objet d'une autorisation de la part du chef de service, d'établissement ou d'entreprise. L'autorisation d'accès à une ZRR est individuelle, nominative et limitée dans le temps. Dans les cas définis par l'article R. 413-5-1 du code pénal, cette autorisation ne peut intervenir qu'après avis favorable du ministre qui a déterminé le besoin de protection.

Cette autorisation renouvelable ne peut être délivrée pour plus de cinq ans.

Section 1. Terminologie

Au sens du II de l'article R. 413-5-1 du code pénal, le terme « accès » couvre l'ensemble des manières dont une personne peut avoir connaissance des informations détenues dans une ZRR :

- accès physique (la personne entre dans les locaux) ;
- accès à distance ou virtuel (la personne accède au réseau informatique de la ZRR à partir de l'extérieur ou se fait transmettre des informations par voie postale).

L'accès aux informations scientifiques et techniques détenues dans une ZRR peut être uniquement virtuel, sous la forme d'un accès à distance par voie électronique (prestation de service d'infogérance ou projet de recherche scientifique mené à distance sur un supercalculateur par exemple).

Tout accès, même virtuel, doit être autorisé par le chef de service, d'établissement ou d'entreprise, après avis ministériel favorable, conformément aux règles qui régissent l'accès physique. Cette autorisation doit par ailleurs être conforme à la politique de sécurité des systèmes d'information (PSSI) adoptée par le service, l'établissement ou l'entreprise entrant dans le champ de la PPST et aux procédures de sécurité appliquées dans la ZRR.

Le terme « stage » au sens du II de l'article R. 413-5-1 du code pénal concerne le séjour temporaire d'une personne qui participe directement aux activités scientifiques et techniques menées au sein de la ZRR. Le stage est encadré par une convention.

Le terme « exercer une activité professionnelle » au sens du II de l'article R. 413-5-1 du code pénal s'entend :

- de l'exercice pérenne de l'activité au sein d'une ZRR ;

- de la collaboration professionnelle occasionnelle en lien avec le secteur scientifique et technique concerné, qui implique une présence dans la ZRR.

Section 2. Principes généraux

Le processus d'instruction d'une demande d'autorisation d'accès à une zone à régime restrictif se décline en quatre grandes étapes :

- tout demandeur formalise sa demande en fournissant les renseignements nécessaires au moyen d'un formulaire dédié, dont un modèle figure en ANNEXE 3 ;
- le chef de service, d'établissement ou d'entreprise, accuse réception du dossier, complète la partie du formulaire qui le concerne et le transmet sans délai au ministre qui a déterminé le besoin de protection ;
- le HFDS, qui agit par délégation de son ministre, rend un avis sur la demande d'accès ;
- le chef de service, établissement ou entreprise notifie par écrit au demandeur la décision individuelle qu'il prend à son endroit sur la demande d'autorisation d'accès, qu'elle soit acceptée ou refusée. Si l'avis du ministre est défavorable, la demande d'accès doit être refusée. En cas d'avis favorable du ministre, le chef de service, d'établissement ou d'entreprise peut refuser l'accès après appréciation des enjeux de sécurité posés par l'accès du demandeur à la ZRR. Dans tous les cas, le chef de service, d'établissement ou d'entreprise informe impérativement le ministre de sa décision lorsque le sens de l'avis ministériel n'est pas suivi.

Lorsque le demandeur sollicite l'accès à plusieurs ZRR, il le précise sur son dossier de demande d'accès (voir ANNEXE 3).

La délivrance de l'autorisation d'accès est un préalable, le cas échéant, à la signature du contrat de travail ou à l'inscription du demandeur à des travaux de recherche se déroulant dans une ZRR.

Section 3. L'instruction de la demande d'accès

A. *Rôle du service, établissement ou entreprise*

La demande d'accès à une ZRR est formalisée directement par l'intéressé au moyen d'un formulaire (dont un modèle figure en ANNEXE 3). La demande ne peut pas être formulée par un mandataire pour le compte de l'intéressé.

Le service, établissement ou entreprise attribue à chaque demande d'accès un numéro unique sous le format suivant : *année-mois-code ZRR-n° de demande dans le mois pour la ZRR*.

L'ensemble est ensuite adressé sans délai au ministre ayant déterminé le besoin de protection par l'intermédiaire du chef de service, d'établissement ou d'entreprise dans le but de recueillir son avis.

Le silence gardé par le ministre dans un délai de deux mois suivant la réception par celui-ci de la demande d'avis complète vaut avis défavorable.

Le silence gardé par le chef de service, d'établissement ou d'entreprise, à l'issue d'un délai de trois mois suivant l'accusé de réception par ce service, établissement ou entreprise du dossier complet de la demande d'autorisation d'accès vaut décision de rejet.

Conformément à l'article 2 de l'arrêté du 3 juillet 2012 modifié, si elles sont strictement nécessaires à l'instruction de la demande, le ministre chargé de délivrer l'avis peut solliciter des informations complémentaires sur le demandeur auprès du chef de service, d'établissement ou d'entreprise. Ces informations sont relatives à tout ou partie des éléments suivants :

1° son domicile précédent ;

2° sa résidence secondaire ou occasionnelle, y compris à l'étranger ;

3° ses voyages et séjours à l'étranger durant les cinq dernières années ;

4° les nom, prénom, nationalité et employeur actuel ou dernier employeur du conjoint, les nom, prénom et nationalité des parents.

Le chef de service, d'établissement ou d'entreprise ou le responsable de la ZRR invite le demandeur à lui communiquer les informations et documents sollicités par le ministre et lui fixe un délai, qui ne peut excéder quinze jours, pour la transmission de ces informations.

Conformément à l'article 4 de l'arrêté du 3 juillet 2012 modifié, en application du V de l'article R. 413-5-1 du code pénal, le bénéficiaire d'une autorisation d'accès à une zone à régime restrictif est tenu de signaler au chef de service, d'établissement ou d'entreprise ou au responsable de la ZRR placé sous son autorité, tout changement de situation concernant :

1° les informations relatives à son état civil ;

2° ses liens professionnels ou personnels avec un État étranger, une entreprise ou organisation étrangère ou sous contrôle étranger ou un ressortissant d'un État étranger (déplacements de longue durée ou réguliers vers cet État, contrats conclus avec une personne physique ou morale de cet État, avantages et rémunérations - incluant bourses et prix - octroyés par des organisations étrangères ou sous contrôle étranger) ;

3° ses activités professionnelles sur le territoire national en lien avec l'activité principale exercée au sein de la zone à régime restrictif.

Cette obligation est valable pendant toute la durée de l'autorisation d'accès. Le chef de service, d'établissement ou d'entreprise informe le ministre chargé de délivrer l'avis de ces éléments. L'avis du ministre est délivré conformément aux procédures définies *infra*.

Le service, établissement ou entreprise veille à ce que les demandes d'avis soient adressées dans un délai qui permette au ministre de les instruire en cohérence avec les délais de décision implicite mentionnés précédemment.

B. *Avis du ministre*

Le ministre émet un avis sur la demande qui lui est présentée. Celui-ci peut être :

- explicitement favorable, favorable sous conditions, ou défavorable, transmis au chef de service, établissement ou entreprise ;
- implicitement défavorable, à la suite du silence gardé par l'administration pendant deux mois, conformément aux dispositions du II de l'article R. 413-5-1 du code pénal ;
- implicitement favorable, dans les cas précisés *infra*.

En cas de doute sur l'opportunité de délivrer un avis favorable, le ministre peut interroger le service, établissement ou entreprise pour rechercher avec lui les moyens de concilier les impératifs de protection avec les besoins de la recherche et les projets du demandeur. Des ajustements pourront notamment être demandés sur le lieu (proposition d'un lieu moins sensible) ou sur le sujet de recherche. Des mesures d'encadrement pourront également être proposées par le ministre ayant déterminé le besoin de protection.

Le cas échéant, l'avis du ministre peut être assorti de ces conditions, il s'agit de l'avis favorable sous conditions. Le chef de service, d'établissement ou d'entreprise ne peut alors autoriser l'accès en ZRR que s'il peut garantir le respect des conditions. Par exemple, un avis favorable peut prévoir que l'autorisation d'accès soit délivrée pour une durée inférieure à cinq ans. Elle peut aussi prévoir que le demandeur ne puisse pas avoir accès à tous les équipements présents dans la ZRR.

Le ministre peut, de sa propre initiative et à tout moment, revenir sur le sens de son avis y compris dans les cas où celui-ci est réputé favorable.

En application de l'article L. 114-1 du code de la sécurité intérieure, le ministre chargé de délivrer l'avis peut solliciter une enquête administrative. Ces enquêtes peuvent donner lieu à la consultation de traitements automatisés de données à caractère personnel. Lorsqu'une telle enquête a été menée, les éléments qui en sont issus ne sont pas communicables au chef de service, d'établissement ou d'entreprise, à l'exception du sens des conclusions du service enquêteur.

Lorsqu'une même demande d'avis ministériel concerne plusieurs ZRR, d'un même service, établissement ou entreprise, nominativement identifiées, l'instruction du dossier est unique pour l'ensemble de la demande. L'avis est cependant émis pour chacune des zones : il peut être favorable pour certaines ZRR et défavorable pour d'autres.

N'étant pas considéré comme une décision finale, l'avis du ministre, qu'il soit favorable ou défavorable, n'a pas à faire l'objet d'un formalisme particulier. Il est toutefois recommandé, dans tous les cas, de communiquer cet avis au chef de service, d'établissement ou d'entreprise par écrit (quel que soit le format), afin de conserver une trace du sens de l'avis et de la date à laquelle il a été rendu.

Si tout accès à une ZRR doit nécessairement faire l'objet d'une autorisation préalable du chef de service, d'établissement ou d'entreprise, il existe trois hypothèses exposées ci-après pour lesquelles le ministre compétent est réputé avoir émis un avis favorable (III de l'article R. 413-5-1 du code pénal) :

- les personnes bénéficiant, au titre de leurs fonctions, d'une habilitation au secret de la défense nationale, sont réputées avoir obtenu, pour les ZRR dont l'accès est nécessaire à l'exercice de ces mêmes fonctions, un avis ministériel favorable ;
- les personnes bénéficiant d'un avis favorable pour l'accès à une ZRR afin d'y exercer des activités d'entretien des surfaces et des infrastructures, de maintien en condition des prestations d'effluents, de sécurité ou de sûreté, sans avoir un accès direct à l'information protégée par ce régime, sont réputées, sauf mention contraire de cet avis, bénéficier d'un avis favorable pour l'accès, aux même fins et dans les mêmes limites, aux autres ZRR relevant du même ministre ;
- les personnes bénéficiant antérieurement à la création d'une ZRR, d'un accès aux lieux couverts par cette zone sont également réputées, pour leur première demande d'autorisation d'accès à cette ZRR, avoir obtenu un avis ministériel favorable. Toutefois, dès la création de la ZRR, le chef de service, d'établissement ou d'entreprise formalise une demande d'autorisation d'accès au ministre et lui transmet les éléments d'information utiles à l'instruction de la demande.

Section 4. La décision du chef de service, d'établissement ou d'entreprise

La décision du chef de service, d'établissement ou d'entreprise est transmise, soit au responsable de la ZRR qui la notifie au demandeur, soit directement au demandeur. Le chef de service, d'établissement ou d'entreprise informe impérativement le ministre de sa décision relative à l'autorisation d'accès lorsque le sens de l'avis ministériel n'est pas suivi.

Lorsque le ministre a donné un avis défavorable, le chef de service, d'établissement ou d'entreprise doit refuser la demande d'accès qui lui est adressée, ou retirer l'autorisation délivrée. Lorsque l'avis est favorable, ou favorable sous conditions, le chef de service, établissement ou entreprise peut ou non faire droit à la demande.

Le dernier alinéa du II de l'article R. 413-5-1 du code pénal prévoit que, par dérogation aux dispositions de l'article L. 211-2 du code des relations entre le public et l'administration, les décisions individuelles défavorables (refus et retrait d'autorisation) n'ont pas à être motivées. La décision de refus est notifiée par écrit au demandeur, dès que possible par lettre recommandée

avec accusé de réception (ou un autre procédé électronique équivalent). Le courrier accompagnant la décision de refus mentionne la faculté qu'a le demandeur d'effectuer, soit un recours administratif (recours gracieux et/ou hiérarchique), soit un recours contentieux devant le juge administratif, dans le délai de droit commun de deux mois à l'encontre de la décision du chef de service, d'établissement ou d'entreprise (délai qui court à compter de la date de réception de la notification écrite de la décision).

Le chef de service, d'établissement ou d'entreprise informe le ministre lorsqu'un recours gracieux a été fait contre sa décision ou s'il a connaissance d'un recours contentieux. Dans l'hypothèse d'un recours hiérarchique dont le ministre est par nature seul informé, celui-ci sollicite du chef de service, d'établissement ou d'entreprise un nouvel examen de la demande.

Chapitre 4. Les visites

Les visites sont des accès à une ZRR ou une unité protégée qui se caractérisent par leur aspect temporaire et par l'absence de participation ou interaction directes avec les activités scientifiques et techniques sensibles, qui n'entrainent donc pas un accès aux savoirs et savoir-faire protégés. Elles se caractérisent également par l'absence de contrat, ce qui les différencient de la prestation de services. Ce chapitre détaille l'article 3 de l'arrêté du 3 juillet 2012 modifié.

Section 1. Dispositions générales applicables aux visites

Le chef de service, d'établissement ou d'entreprise hébergeant une ou plusieurs ZRR détermine les mesures de sécurité applicables aux visites dans ces zones. Ces mesures peuvent être précisées par instruction ministérielle. Elles concernent notamment la désignation des personnes pour contrôler, accompagner et surveiller les visiteurs et l'organisation des circuits de notoriété.

Le responsable de la ZRR veille, sous l'autorité du chef de service, d'établissement ou d'entreprise, à ce qu'un répertoire de visites soit tenu à jour de manière à pouvoir être consulté à la demande du HFDS. Il est conservé pour une durée de cinq ans. Il contient les informations suivantes :

- le numéro de ZRR ;
- l'identification du visiteur (nom, prénom, organisme d'appartenance) ;
- l'identification de l'accueillant ou du responsable de la visite (si différent) ;
- la date, l'heure d'arrivée et de départ et le motif de la visite.

Toute visite doit être autorisée par le chef de service, d'établissement ou d'entreprise. Elle fait l'objet d'une procédure de demande dont les conditions sont définies par chaque chef de service, d'établissement ou d'entreprise. Le responsable de la ZRR, s'il en a reçu délégation, peut signer ces autorisations d'entrée en ZRR au nom du chef de service, d'établissement ou d'entreprise. Les visites ne sont toutefois pas soumises à la procédure d'avis ministériel favorable préalable.

Pour autant, afin de pouvoir prendre certaines dispositions utiles, le chef de service, d'établissement ou d'entreprise informe le ministre ayant déterminé le besoin de protection de tout projet de visite de délégation étrangère dans la ZRR. Si nécessaire, les services spécialisés (DGSI et DRSD) adressent un avis d'alerte au responsable de la ZRR et au HFDS.

En vertu du II de l'article R. 413-5-1 du code pénal, les missions d'audit ou d'inspection réalisées par ou pour le compte d'un État tiers ne peuvent pas être considérées comme des visites et doivent être précédées d'une autorisation d'accès avec avis préalable du ministre.

Section 2. Cas particulier des enseignements dispensés dans une ZRR

D'une manière générale et sauf mention contraire dans les instructions ministérielles, les enseignements de formation initiale (formation universitaire jusqu'au niveau master inclus) se déroulant pour tout ou partie en ZRR sont exclus des dispositions du II de l'article R. 413-5-1 du

code pénal. Lorsque les enseignements de formation initiale ne concourent pas à la préparation d'une thèse (cours, travaux dirigés et pratiques non sensibles), les étudiants qui y prennent part sont considérés comme des visiteurs.

Les modalités d'encadrement de ces visites sont précisées par instruction ministérielle.

Chapitre 5. Sanctions applicables en cas d'infraction aux règles de la PPST

Section 1. Sanctions en cas d'accès non autorisé à une ZRR

La ZRR, régie par l'article R. 413-5-1 du code pénal, est une catégorie de zones protégées.

La protection légale associée est régie par l'article 413-7 du code pénal, qui concerne toutes les catégories de zones protégées. Il réprime le fait de s'introduire, sans autorisation, à l'intérieur de ces zones. Cette infraction est punie de six mois d'emprisonnement et de 7 500 euros d'amende.

Section 2. Sanctions en cas de captation ou divulgation de données hébergées dans une ZRR

Conformément aux dispositions de l'article 410-1 du code pénal, les éléments essentiels du potentiel scientifique et économique de la nation sont des éléments relevant des intérêts fondamentaux de la nation. Ainsi, le potentiel scientifique et technique de la nation en fait également partie. L'atteinte à ce potentiel peut donc faire l'objet des sanctions prévues aux articles 411-1 à 411-12 du code pénal.

L'atteinte aux intérêt fondamentaux de la nation est un crime, puni par 100 000 à 300 000 euros d'amende et sept à vingt ans de réclusion criminelle. Il existe plusieurs catégories d'atteintes à ces intérêts concernées par la PPST, chacune soumise à des peines différentes. Si l'atteinte aux éléments du potentiel scientifique et technique hébergés dans une ZRR est caractérisée pour l'une de ces catégories, la peine associée pourra être encourue.

Ces atteintes peuvent revêtir les qualifications suivantes.

A. *Intelligences avec une puissance étrangère (article 411-5 du code pénal)*

Le fait d'entretenir des intelligences avec une puissance étrangère, avec une entreprise ou organisation étrangère ou sous contrôle étranger ou avec leurs agents, lorsqu'il est de nature à porter atteinte aux intérêts fondamentaux de la nation, est puni de dix ans d'emprisonnement et de 150 000 euros d'amende.

B. *Livraison d'informations à une puissance étrangère (articles 411-6 à 411-8 du code pénal)*

Le fait de livrer ou de rendre accessibles à une puissance étrangère, à une entreprise ou organisation étrangère ou sous contrôle étranger ou à leurs agents, des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de quinze ans de détention criminelle et de 225 000 euros d'amende.

Le fait de recueillir ou de rassembler, en vue de les livrer à une puissance étrangère, des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de dix ans d'emprisonnement et de 150 000 euros d'amende.

Le fait d'exercer, pour le compte d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger ou de leurs agents, une activité ayant pour but l'obtention ou la livraison de dispositifs, renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de dix ans d'emprisonnement et de 150 000 euros d'amende.

C. *Sabotage (article 411-9 du code pénal)*

Le fait de détruire, détériorer ou détourner tout document, matériel, construction, équipement, installation, appareil, dispositif technique ou système de traitement automatisé d'informations ou d'y apporter des malfaçons, lorsque ce fait est de nature à porter atteinte aux intérêts fondamentaux de la nation, est puni de quinze ans de détention criminelle et de 225 000 euros d'amende.

Lorsqu'il est commis dans le but de servir les intérêts d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger, le même fait est puni de vingt ans de détention criminelle et de 300 000 euros d'amende.

D. *Fausses informations (article 411-10 du code pénal)*

Le fait de fournir, en vue de servir les intérêts d'une puissance étrangère, d'une entreprise ou d'une organisation étrangère ou sous contrôle étranger, aux autorités civiles ou militaires de la France des informations fausses de nature à les induire en erreur et à porter atteinte aux intérêts fondamentaux de la nation est puni de sept ans d'emprisonnement et de 100 000 euros d'amende.

E. *Provocation de ces crimes (article 411-11 du code pénal)*

Le fait, par promesses, offres, pressions, menaces ou voies de fait, de provoquer directement à commettre l'un des crimes prévus au présent chapitre, lorsque la provocation n'est pas suivie d'effet en raison de circonstances indépendantes de la volonté de son auteur, est puni de sept ans d'emprisonnement et de 100 000 euros d'amende.

F. *La circonstance aggravante applicable aux infractions commises dans un contexte d'ingérence étrangère*

L'article 411-12 du code pénal érige en circonstance aggravante le fait de commettre certains crimes ou délits dans le but de servir les intérêts d'une puissance étrangère, d'une entreprise ou d'une organisation étrangère ou sous contrôle étranger. Cette circonstance est notamment applicable aux chapitres II et III du titre II du livre III du code pénal (articles 322-1 à 323-8), qui concernent d'une part les destructions, dégradations et détériorations et d'autre part les atteintes aux systèmes automatisés de traitement de données.

La circonstance prévue par l'article 411-12 du code pénal a pour conséquence d'élever d'un degré sur l'échelle des peines la peine privative de liberté encourue ou, pour les peines de trois ans d'emprisonnement ou moins, de doubler la peine encourue. En particulier, il convient de souligner que les délits punis de dix ans d'emprisonnement revêtent une qualification criminelle lorsqu'ils sont commis avec cette circonstance aggravante.

Peines initialement encourue	30 ans	20 ans	15 ans	10 ans	7 ans	5 ans	3 ans ou moins
Peines aggravées encourues	Réclusion criminelle à perpétuité	30 ans	20 ans	15 ans	10 ans	7 ans	Peine doublée

Section 3. Régime contraventionnel relatif aux obligations de protection associées à une ZRR

A. *Objectif du régime contraventionnel*

Une contravention de cinquième classe a été introduite par l'article 2 du décret n° 2024-430 du 14 mai 2024, et codifiée à l'article R. 413-5-2 du code pénal, afin de réprimer pénalement les manquements à l'accomplissement du dispositif de PPST autres que la seule intrusion non autorisée en ZRR. Ce régime contraventionnel vise en priorité les personnes qui feraient obstacle à la bonne application des mesures de protection. Il concerne également les personnes en charge de les mettre en œuvre.

Le régime contraventionnel s'applique aux manquements ou obstructions à l'accomplissement des mesures minimales de protection associées à l'existence d'une ZRR :

- ne pas rendre apparentes les limites d'une ZRR et les mesures d'interdiction dont elle est l'objet ;
- s'abstenir de soumettre à autorisation l'accès d'une personne pénétrant dans une ZRR (autorisation du chef de service, d'établissement ou d'entreprise) ;
- autoriser l'accès à une ZRR dans des conditions non conformes aux exigences fixées par le II de l'article R. 413-5-1 du code pénal ;
- s'abstenir de communiquer au ministre les informations nécessaires en cas de changement de situation pour le demandeur ou le bénéficiaire d'une demande d'accès, ou de changement relatif à l'activité qu'il exerce en ZRR (V de l'article R. 413-5-1 du code pénal) ;
- s'abstenir d'informer le ministre chargé de l'enseignement supérieur, les autorités de tutelle de l'établissement et le ministre chargé des affaires étrangères, d'un projet d'accord avec une institution étrangère ou internationale et impliquant des activités conduites dans une ZRR, pour les établissements relevant des dispositions des articles L. 123-7-1 et D. 123-19 du code de l'éducation.

Chaque manquement à une ou plusieurs de ces obligations est puni de l'amende encourue pour les contraventions de cinquième classe, soit au maximum 1 500 euros par manquement.

En outre, le fait de faire obstacle à l'accomplissement des missions des personnes qui sont chargés de la protection de la ZRR, au sein du service, de l'établissement ou de l'entreprise la comprenant, est puni de la même amende.

B. *Mise en œuvre du régime contraventionnel*

Les infractions pouvant donner lieu à l'application du régime contraventionnel prévu à l'article R. 413-5-2 du code pénal sont constatées et traitées de la manière suivante.

1. Le HFDS est informé d'une non-conformité de l'application du dispositif de PPST dans un service, établissement ou entreprise hébergeant une ou plusieurs ZRR.
2. À partir des informations recueillies, le HFDS demande à l'entité de se mettre en conformité avec le dispositif en fixant un délai qu'il juge pertinent.
3. À l'issue de ce délai, le HFDS vérifie, avec l'appui des services spécialisés (DGSI ou DRSD), que l'entité s'est bien mise en conformité.
4. Si le service, l'établissement ou l'entreprise concernée n'a manifestement pas progressé sur sa mise en conformité, le HFDS et les services spécialisés ci-dessus mentionnés se concertent sur l'opportunité de constater la ou les infractions. La saisine de l'autorité judiciaire ne doit être envisagée qu'en dernier recours, en cas d'échec du dialogue engagé avec l'entité concernée.
5. Le HFDS signale au parquet territorialement compétent les potentiels manquements ou obstructions à la mise en œuvre des mesures de protection associées à l'existence d'une ZRR, sur le fondement de l'article 40 alinéa 1 du code de procédure pénale.
6. Le procureur de la République saisit le service enquêteur territorialement compétent aux fins de constatation de l'infraction et poursuite des investigations, le cas échéant en s'appuyant sur l'expertise des services spécialisés.
7. Autant que possible, les services spécialisés informent le HFDS des suites contraventionnelles apportées à son signalement.

TITRE IV. L'articulation avec les autres dispositifs et outils de protection

Le dispositif de protection du potentiel scientifique et technique de la nation (PPST) s'intègre dans un ensemble de dispositifs de protection et de contrôle participant à la sécurité de la nation, complémentaires et non exclusifs les uns des autres. La portée respective des dispositifs ne permet pas de promouvoir l'un pour protéger les éléments d'un autre.

Une attention particulière doit être portée à l'articulation avec certains dispositifs nationaux de protection, notamment ceux relatifs à la protection du secret de la défense nationale, de la sécurité des activités d'importance vitale, etc. qui peuvent également viser à contrôler des accès physiques à des lieux protégés. C'est aussi le cas de la politique de sécurité économique, l'adhérence venant de la prise en compte du risque économique R1 dans le cadre de la PPST. Enfin, dans le cadre du contrôle des exportations, l'adhérence vient de la prise en compte des risques R2, R3 et R4 ainsi que du contrôle des flux « intangibles » de biens à double usage ou de matériels de guerre.

Chapitre 1. L'articulation avec les autres dispositifs nationaux de protection

Section 1. Protection du secret de la défense nationale

Le secret de la défense nationale a pour objet de protéger des informations et supports dont la divulgation ou auxquels l'accès est de nature à nuire à la défense et à la sécurité nationale. Il participe de la préservation des intérêts fondamentaux de la nation, comme la PPST.

Les dispositions de protection du secret de la défense nationale (PSDN) et de la PPST peuvent coexister au sein d'une entité et des informations (savoirs et savoir-faire scientifiques et techniques) liées la PPST peuvent être classifiées si leur sensibilité justifie qu'elles soient protégées par les dispositions de protection du secret de la défense nationale.

Pour autant, seules les informations relevant du dispositif de PSDN font l'objet des marquages « Secret » et « Très Secret », selon les dispositions des articles R. 2311-2 et suivants du code de la défense. L'instruction générale interministérielle n° 1300 du 9 août 2021 (IGI 1300) sur la protection du secret de la défense nationale en précise les modalités de mise en œuvre.

La PPST prévoit par ailleurs que toute personne bénéficiant, en raison de ses fonctions, d'une habilitation au titre de la protection du secret de la défense nationale, quel qu'en soit le niveau (*Secret* ou *Très Secret*), est réputée avoir obtenu, pour les zones à régime restrictif (ZRR) dont l'accès est nécessaire à l'exercice de ces mêmes fonctions, un avis ministériel favorable.

Ceci ne dispense toutefois pas cette personne de disposer d'une autorisation d'accès en ZRR délivrée par le chef de service, établissement ou entreprise et de remplir le formulaire de demande d'accès afférant.

Section 2. Sécurité des activités d'importance vitale

Le dispositif de sécurité des activités d'importance vitale (SAIV) constitue le cadre permettant d'associer les opérateurs d'importance vitale (OIV), publics ou privés, à la mise en œuvre de la stratégie de sécurité nationale en termes de protection et, avec la future transposition de la directive REC, de résilience des opérateurs face aux actes de malveillance (terrorisme, sabotage) et aux risques naturels, technologiques et sanitaires. Les opérateurs d'importance vitale sont désignés parmi ceux qui exploitent ou utilisent des installations indispensables à la vie de la nation et qui concourent à la production et à la distribution de biens ou de services indispensables à l'exercice de l'autorité de l'État, au fonctionnement de l'économie, au maintien du potentiel de défense ou à la sécurité de la nation.

Afin d'assurer la meilleure articulation entre les deux dispositifs dans les cas où ils se superposeraient dans une entité, il convient d'apporter une attention particulière au zonage de la ZRR. Celle-ci ne peut pas être pensée de façon automatique comme identique au point d'importance vitale (PIV). Les enquêtes administratives relatives aux accès aux PIV et celles relatives à la ZRR ne sont pas exclusives l'une de l'autre.

Section 3. Contrôle de la fusion thermonucléaire par confinement inertiel

Les activités d'études et de recherches dans le domaine de la fusion thermonucléaire par confinement inertiel (FCI) font l'objet d'un contrôle particulier, en application du décret n° 80-247 du 3 avril 1980. Ce contrôle est destiné à éviter que ces activités ne conduisent à rassembler des renseignements, des objets, des documents ou des procédés dont l'exploitation serait de nature à nuire à la défense nationale.

En application de ce décret, toute personne s'apprêtant à entreprendre ou à faire entreprendre des études et recherches dans le domaine de la FCI sont tenus d'en faire la déclaration auprès du SGDSN, tandis que les études et recherches bénéficiant d'une aide ou d'un financement public sont soumises à autorisation préalable du Premier ministre.

Le contrôle étatique exercé sur les études et les recherches dans le domaine de la FCI ne dispense pas de la mise en œuvre des autres dispositifs de protection et en particulier de la PPST. Au contraire, il convient de compléter ce régime par le déploiement de ZRR dans les entités concernées.

Section 4. Agents pathogènes

Les agents pathogènes humains (micro-organismes et toxines hautement pathogènes (MOT)), utilisés à des fins de diagnostic, recherche, développement et enseignement, présentent un risque réel pour la santé et la sécurité humaine, en raison d'un éventuel rejet, soit accidentel (notion de sécurité biologique), soit intentionnel (notion de sûreté biologique). Une règlementation dédiée à ces micro-organismes et toxines a été adoptée dès 2001 (articles L. 5139-1 à L. 5139-3 du code de la santé publique).

Ces textes définissent les conditions et un régime d'autorisation pour toute opération de production, fabrication, transport, importation, exportation, détention, offre, cession, acquisition et emploi de tout ou partie des micro-organismes et toxines pathogènes.

De la même manière que pour les autres dispositifs, la PPST peut utilement compléter ce régime de protection. Il convient cependant de bien définir le zonage des ZRR dans les établissements concernés par la réglementation MOT afin de rechercher la meilleure complémentarité.

Section 5. Instances nationales de référence

Les instances nationales de référence comprennent les laboratoires nationaux de référence, sous tutelle du ministre chargé de l'agriculture, et les centres nationaux de référence, sous tutelle du ministre chargé de la santé. Ils ont notamment pour mission d'apporter une expertise scientifique et technique destinée à éclairer la prise de décision des pouvoirs publics au plus haut niveau.

Les résultats et méthodes des expertises conduites par les instances nationales de référence doivent impérativement présenter des garanties de confidentialité, d'impartialité et d'indépendance vis-à-vis de toute personne physique ou morale exerçant une activité de production, d'importation ou de commercialisation de produits ou de biens en rapport avec leur domaine de compétence.

Aussi, les instances nationales de référence peuvent être utilement protégées par l'application du dispositif de protection du potentiel scientifique et technique de la nation.

Chapitre 2. L'articulation avec la politique de sécurité économique

La sauvegarde de la compétitivité économique est l'un des enjeux de la protection du potentiel scientifique et technique, qui se matérialise en particulier à travers l'évaluation du risque R1. Ainsi, le dispositif participe pleinement à la politique de sécurité économique de la France dont la gouvernance est précisée dans le décret n° 2019-206 du 20 mars 2019 relatif à la gouvernance de la politique de sécurité économique. Ce chapitre vise à donner des lignes directrices quant à l'articulation du dispositif de PPST avec les outils participant à la politique de sécurité économique de l'État.

La PPST couvrant trois risques supplémentaires, en plus du risque économique, ce dispositif ne pourra se substituer aux outils ci-dessous. Le prisme de la sécurité économique ne saurait être le seul qui guide les efforts de déploiement du dispositif.

Section 1. Loi de blocage

La loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères, dite « loi de blocage », a été adoptée pour protéger les informations et données sensibles attentant aux intérêts de la nation, qui pourraient être communiquées comme preuves à l'occasion de procédures judiciaires à l'étranger. Il s'agit d'une opportunité souvent saisie par des sociétés étrangères afin d'obtenir des informations stratégiques sur leurs concurrents français.

La loi vise à s'assurer, d'une part, qu'aucune communication d'informations sensibles détenues par une société française à destination d'une autorité publique étrangère requérante ne puisse porter une atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public.

Le service de l'information stratégique et de la sécurité économiques (SISSE) est le guichet unique des établissements dans le cadre de l'application de la loi de blocage. Il publie des guides d'aide à l'identification des données potentiellement concernées par la loi auxquels il convient de se référer.

Le fait d'être protégé par la PPST doit inciter les entités concernées à explorer la possibilité de recourir à la loi de blocage en cas de sollicitations étrangères. Pour ce faire, l'entité informe le service du haut fonctionnaire de défense et de sécurité (SHFDS) du ministère de tutelle de ces sollicitations et prend l'attache du SISSE pour déterminer l'applicabilité de la loi de blocage.

Section 2. Contrôle des investissements étrangers en France

Le code monétaire et financier prévoit, au titre de la défense des intérêts nationaux, que soient soumis à autorisation préalable du ministre chargé de l'économie, les investissements étrangers dans une activité en France qui participe à l'exercice de l'autorité publique ou relève de certains domaines définis à l'article L. 151-3 du code monétaire et financier. Cette disposition concerne les activités de nature à porter atteinte à l'ordre public, à la sécurité publique, aux intérêts de la défense nationale ou aux activités de recherche, de production ou de commercialisation d'armes, de munitions, de poudres et substances explosives. Dans le cadre de la mise en œuvre du contrôle des investissements étrangers en France (IEF), le dispositif de PPST peut être mobilisé pour assurer la protection des savoirs et savoir-faire d'une entité française objet d'un investissement relevant de l'article L. 151-3 du code monétaire et financier.

Lorsqu'une entité ayant mis en place une ZRR fait l'objet d'une opération d'investissement étranger éligible à la procédure de contrôle des investissements étrangers en France, il convient de s'assurer auprès de la DG Trésor de la bonne articulation du dispositif de PPST avec le régime de contrôle des IEF, qui peut avoir pour objectif la protection des savoirs et savoir-faire.

Conformément au 2° de l'article R. 151-8 du code monétaire et financier, le dispositif de PPST peut être mobilisé pour les autorisations sous conditions d'un IEF afin d'assurer le maintien des savoirs et des savoir-faire de l'entité objet de l'investissement et faire obstacle à leur captation.

Section 3. Conditionnalité des aides publiques

L'apport de fonds publics pour soutenir l'innovation à travers de grands programmes tel que France2030 est un levier majeur pour inciter au développement d'une culture de sécurité de la recherche des établissements et entreprises concernés. Les institutions de financement (Agence nationale de la recherche et Bpifrance notamment) sont incitées à mobiliser la conditionnalité de leurs financements à la mise en place de mesures de protection.

Ces mesures peuvent être utilisées pour déployer la PPST. Les dispositions à mobiliser peuvent par exemple prendre la forme d'un avis PPST sur les recrutements dans le cadre du projet financé ou d'une évaluation du besoin de protection par le SHFDS qui assure la tutelle ou qui a une attribution de compétences sur les établissements et entreprises concernés.

Les SHFDS sont invités à se rapprocher des programmes soutenus par leurs ministères respectifs pour déployer au mieux cette gamme de conditionnalité des aides. De façon réciproque, l'identification des entités devant faire l'objet d'une évaluation du besoin de protection doit également s'appuyer sur ces programmes.

Chapitre 3. L'articulation avec le contrôle des exportations de matériels, biens et technologies sensibles

Section 1. Matériels de guerre

En France, la fabrication et le commerce des armes sont en principe prohibés, et soumis à autorisation de l'État (article L. 2332-1 du code de la défense). De la même manière, le fondement juridique du contrôle de l'exportation des matériels de guerre repose sur le principe général de prohibition des importations et des exportations d'armement (selon les articles L. 2335-1 et L. 2335-2 du code de la défense). Il conduit à soumettre l'ensemble des flux de matériels de guerre et assimilés au contrôle de l'État. Les autorisations sont délivrées par le Premier ministre après avis de la commission interministérielle pour l'étude des exportations de matériels de guerre (CIEEMG), présidée par le secrétaire général de la défense et de la sécurité nationale, et composée de représentants des ministères chargés de la défense, des affaires étrangères et de l'économie. Le contrôle du respect par les exportateurs des obligations qui leur incombent en application de ces dispositions est quant à lui assuré par des agents du ministère chargé de la défense.

Si le déploiement de la PPST au sein des entités ayant une activité de fabrication ou de commerce de matériels de guerre est pertinent compte tenu de la sensibilité des savoirs, savoir-faire et technologies qui peuvent y être manipulés, sa mise en œuvre ne se substitue pas aux obligations qui incombent à l'entité au titre du « régime des matériels de guerre ».

Un arrêté du 27 juin 2012 fixe la liste des matériels dont l'exportation est soumise à autorisation. Certaines technologies, savoir-faire et informations peuvent être contrôlés au même titre que les matériels physiques : une licence d'exportation ou de transfert est nécessaire avant de pouvoir les exporter ou les transférer et ce, quel qu'en soit le support. Il peut s'agir, par exemple, d'informations communiquées dans le cadre d'un prospect et qui seraient de nature à permettre ou à faciliter la fabrication ou la reproduction de matériels de guerre et matériels assimilés ou à compromettre leur efficacité. On parle alors « d'intangibles ». Dans ces cas-là, il convient de se référer au guide des bonnes pratiques en matière de communication, d'usage et de stockage d'informations, sans mouvement d'un support physique, susceptibles de relever du contrôle des exportations de matériels de guerre, édicté par le SGDSN.

Section 2. Biens à double usage

Le règlement européen 2021/821, instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (BDU), précise que l'« on entend par biens à double usage les produits, y compris les logiciels et les technologies, susceptibles d'avoir une utilisation tant civile que militaire. Ils incluent les biens susceptibles d'être utilisés aux fins de la conception, de la mise au point, de la fabrication ou de l'utilisation d'armes nucléaires, chimiques ou biologiques ou de leurs vecteurs, y compris tous les biens qui peuvent à la fois être utilisés à des fins non explosives et intervenir de quelque manière que ce soit dans la fabrication d'armes nucléaires ou d'autres dispositifs nucléaires explosifs ». Le contrôle des exportations des biens et technologies à double usage est un outil indispensable, d'une part, de lutte contre la prolifération des armes de destruction massive, ainsi que de leurs vecteurs et, d'autre part, de lutte contre le renforcement des capacités militaires étrangères, notamment des pays soumis à des régimes de sanctions.

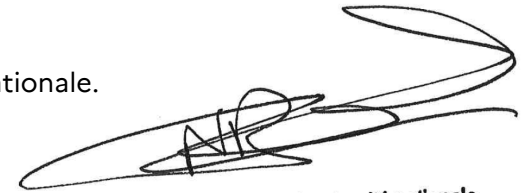
Le contrôle des exportations prévu par le règlement s'exerce également sur les exportations de biens à double usage intangibles, c'est-à-dire sur la transmission de logiciels ou de technologies, par voie électronique, y compris par télécopieur, téléphone, courrier électronique ou tout autre moyen électronique, vers une destination à l'extérieur du territoire douanier de l'Union européenne. Cela comprend la mise à disposition sous forme électronique des logiciels et des technologies à l'intention de personnes physiques ou morales ou des partenariats à l'extérieur du territoire douanier de l'Union européenne (à l'exception des BDU intangibles les plus sensibles pour lesquels il existe un contrôle intracommunautaire). Cela comprend également la transmission orale d'éléments relatifs à des technologies, lorsque ces dernières sont décrites via un support de transmission vocale.

En cohérence avec la maîtrise des exportations des matériels de guerre et équipements assimilés, la circulation des biens et technologies à double usage est encadrée par un système d'autorisations préalables d'exportation, délivrées par le service des biens à double usage (SBDU). Cette autorisation est délivrée après avis, lorsqu'elle est saisie par l'un de ses membres, de la commission interministérielle des biens à double usage (CIBDU), présidée par le secrétaire général de la défense et de la sécurité nationale.

Lors de l'évaluation du besoin de protection d'une entité au titre de la PPST, il est indispensable de prendre en compte la présence de BDU au sein de l'établissement, ou la tenue de recherches susceptibles de contribuer au développement de ces biens ou technologies. Cette vigilance doit également s'opérer dans le cadre de l'examen des projets de coopérations internationales qui sont susceptibles de nécessiter le dépôt d'une demande de licence d'exportation. Ce régime est également susceptible de s'appliquer dans le cas de l'accueil de ressortissants étrangers dans un établissement dont l'activité implique des BDU.

Enfin, il convient de noter que certaines législations étrangères relatives aux contrôles des exportations de matériels de guerre ou de biens à double usage peuvent impliquer des contraintes de sécurité pour des acteurs français. La PPST peut être mise en avant afin d'attester auprès des autorités étrangères d'un mécanisme de contrôle d'accès permettant de répondre à certaines exigences de leurs réglementations.

Fait le 28 avril 2025.
Par délégation du Premier ministre,
le secrétaire général de la défense et de la sécurité nationale.



Le secrétaire général de la défense et de la sécurité nationale

Nicolas ROCHE

ANNEXES

ANNEXE 1 - Modèle de signalétique de ZRR

ZONE À RÉGIME RESTRICTIF

INTERDICTION DE PÉNÉTRER SANS AUTORISATION
(ARTICLE R. 413-5-1 DU CODE PÉNAL)

TOUT CONTREVENANT S'EXPOSE AUX PEINES PRÉVUES
PAR L'ARTICLE 413-7 DU CODE PÉNAL

RESTRICTED ACCESS AREA

AUTHORIZED PERSONNEL ONLY
(ARTICLE R. 413-5-1 OF FRENCH PENAL CODE)

ANY OFFENDER IS LIABLE TO THE PENALTIES PROVIDED FOR
IN ARTICLE 413-7 OF FRENCH PENAL CODE

ANNEXE 2- Formulaire type d'enregistrement de ZRR

A - Rattachement administratif de la ZRR					
A01 **Ministère de tutelle ou de rattachement**					
A02 **Nom de l'établissement de rattachement**					
A03 **Nom de l'entité hébergeant la ZRR**					
A04 **Adresse de l'entité hébergeant la ZRR**					
A05 **Code postal de l'entité hébergeant la ZRR**		A06 **Ville**		A07 **Région**	
A10 **Code unité de recherche et/ou développement**		A09 **N° SIRET**		A08 **Zone de défense et de sécurité**	
A11 **Établissement éligible au contrôle des investissements étrangers en France**		A12 **Autre(s) dispositif(s) national(aux) de protection appliqué(s) par l'établissement**			

B - Informations relatives à la ZRR				
B01 **Nom de la ZRR**				
B02 **Numéro de ZRR au sein de l'établissement**		B03 **Localisation précise de la ZRR au sein de l'établissement**		
B04 **Nature de l'activité principale de la ZRR**				
B06 **Secteur scientifique et technique protégé principal**		B07 **Secteur scientifique et technique protégé secondaire**		
B08 **Référence(s) de(s) spécialité(s) sensible(s)**				
B09 **Effectif total**				
Évaluation de la sensibilité de la ZRR au regard des 4 risques (cotation de 0 à 3)	B10 **R1 (potentiel économique)**	0	B12 **R3 (prolifération nucléaire)**	0
	B11 **R2 (arsenal militaire)**	0	B13 **R3 (prolifération biologique)**	0
			B14 **R3 (prolifération chimique)**	0
	B16 **R4 (terrorisme)**	0	B15 **R3 (prolifération balistique)**	0

C – Contacts					
C01 **Nom du chef de service, d'établissement ou d'entreprise**		C02 **Téléphone**		C03 **E-mail**	
C04 **Nom du responsable de la ZRR**		C05 **Téléphone**		C06 **E-mail**	

D – Observations	
D01 **Observations**	

ANNEXE 3- Formulaire type de demande d'accès à une ZRR

A. Informations personnelles *(personal information)*

Nom de naissance *(birth name)**		**Nom d'usage** *(last name)**		**Prénom(s)** *(first names, separated by commas)**		**Sexe** *(gender)*	
Type de pièce d'identité *(type of ID)**		**Numéro de pièce d'identité** *(ID number)**		**Date de naissance** *(birthdate)** AAAA-MM-JJ		**Ville de naissance** *(birthplace)**	
				Pays de naissance *(country of birth)**		**Code postal** *(zip code)**	
Nationalité (pays) *(nationality)* *		**Autre nationalité** *(other nationality)**		**Date d'obtention de la nationalité française, le cas échéant** AAAA-MM-JJ		**Téléphone** *(phone number)**	
Adresse principale actuelle *(current main address)**		**Ville** *(city)**		**Code postal** *(zip code)**		**Pays** *(country)**	
Adresse électronique *(e-mail)**	-	**Situation professionnelle actuelle** *(current professional situation)**		**Organisme employeur actuel** *(name of the current employer)**			
Adresse de l'organisme employeur *(address of employer)**		**Ville** *(city)**		**Code postal** *(zip code)**		**Pays** *(country)**	

B. Activités au sein de la ZRR *(job to be pursued in the restricted access area)*

Statut au sein de la ZRR *(your status within the ZRR)* *		**Origine du financement de la mission** *(funding source for the job)**		**Montant du financement en euros** *(funding amount in euros)**	
Type d'accès *(access type)**		**Date de début de mission dans la ZRR** *(starting date of the job in the ZRR)*(AAAA-MM-JJ)*		**Date de fin de mission dans la ZRR** *(end date of the job in the ZRR)*(AAAA-MM-JJ)*	
Domaine scientifique principal *(main scientific field)**		**Discipline scientifique principale** *(main scientific discipline)**			
Intitulé du poste *(job title)**					
Résumé de la mission et de l'activité (sujet, thème) prévue au sein de la ZRR *(short description of the future position in the ZRR and the activities that you will carry out)**					

C. Informations complémentaires *(additional information)*

Si vous faites d'autres demandes d'accès simultanément à celle-ci indiquez les codes ZRR, séparés d'une virgule *(if you submit other access applications simultaneously indicate the ZRR code(s), separated by a comma)*		**Avez-vous déjà reçu une autorisation d'accès à une ZRR ?** *(have you already received a ZRR access clearance ?)**		**Si oui, indiquer la ZRR concernée** *(if so, indicate the relevant ZRR)**		**Si oui, indiquer la référence de l'autorisation** *(if so, indicate the reference of the clearance)**	
Êtes-vous habilité au secret de la défense nationale ? *(do you have an accreditation for French classified information ?)**		**Si oui, indiquer l'autorité d'habilitation** *(if so, indicate the enabling authority)**		**Si oui, indiquer la date d'expiration** *(if so, indicate the expiry date)**			
Intérêts et affiliations avec des organisations étrangères ou sous contrôle étranger, comprenant les avantages reçus d'organisations, publiques privées, étrangères ou sous contrôle étranger, y compris les bourses d'études et de recherche *(interests in and affiliations with foreign or foreign-controlled organizations, including benefits received from foreign or foreign-controlled public or private organizations, including scholarships and fellowships)*		**date de début d'affiliation/intérêt : nom de l'organisme et nationalité, séparés d'une virgule** *start date of affiliation/interest: name of organization and nationality, separated by a comma*					

IMPORTANT

Joindre à ce formulaire un descriptif complet et détaillé du sujet de la mission, une copie de la pièce d'identité (carte nationale d'identité ou passeport), un CV numérique complet sans rupture de date faisant apparaître les diplômes, titres, travaux et l'expérience professionnelle, ainsi que les documents relatifs au financement. Uniquement en format pdf. ***(Please attach a full and detailed description of the subject of the mission, a copy of the ID or passport, a full resume including degrees, certificates, accreditations and work experience, as well as any document related to the financing. Only pdf files.)****

*** = champ obligatoire /** ***required field***

Les données collectées dans le formulaire font l'objet d'un traitement de données à caractère personnel, conformément aux articles 39 et 40 de la Loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés. *(The data collected by this information sheet are subject for processing personal data, in accordance with articles 39 and 40 instituted by amended act n°78-17 of 6th january 1978 concerning data processing, files and freedoms).*

En remplissant ce formulaire je :
a) reconnais être informé(e) :
- du caractère obligatoire des réponses qui me sont demandées ;
- qu'en l'absence de réponse, aucune autorisation d'accès ne pourra m'être accordée ;
- que les données à caractère personnel et les informations recueillies font l'objet d'un traitement automatisé de donnée à caractère personnel dénommé « Base ministérielle PPST »/« SOPHIA » et d'un autre dénommé « Base interministérielle PPST » dont la finalité est de veiller à ce que des éléments essentiels du potentiel scientifique ou technique de la nation ne fassent pas l'objet d'une captation de nature à affaiblir ses moyens de défense, à compromettre sa sécurité ou à porter préjudice à ses autres intérêts fondamentaux, ou ne soient détournés à des fins de terrorisme, de prolifération d'armes de destruction massive et de leurs vecteurs ou de contribution à l'accroissement d'arsenaux militaires ;
- que le responsable de traitement ministériel est le service *** du ministère de *** et que le responsable du traitement interministériel est le Secrétariat général de la défense et de la sécurité nationale ;
- que je ne peux m'opposer au traitement de mes données, conformément à l'article 8 du décret n°2022-367 du 15 mars 2022 portant création de traitements automatisées de données à caractère personnel dénommés « Base ministérielle PPST » pris en application de l'article 117 de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
- que la durée de conservation et les destinataires des données à caractère personnel sont mentionnés aux articles 4 et 5 du décret n°2022-367 du 15 mars 2022 portant création de traitements automatisées de données à caractère personnel dénommés « Base ministérielle PPST » et du décret n°2022-368 du 15 mars 2022 portant création d'un traitement automatisé de données à caractère personnel dénommé « Base interministérielle PPST » ;
- que les traitements de données à caractère personnel ci-dessus mentionnés sont susceptibles de porter sur des données mentionnées au I de l'article 6 de la loi n°78-17 du 6 janvier 1978, dont la collecte et la communication seront limitées au strict nécessaire au regard des finalités du traitement ;
- que, conformément à l'article 2 de l'arrêté du 3 juillet 2012 modifié, des informations complémentaires sur ma situation peuvent être sollicitées afin de faciliter l'instruction de ma demande ;
- que je peux adresser des demandes tendant à l'exercice du droit d'accès, de rectification et d'effacement à la Commission nationale de l'informatique et des libertés, en application de l'article 118 de la loi du 6 janvier 1978 précitée ;
b) certifie l'exactitude des renseignements fournis à l'appui de ma demande et admets avoir été informé que je m'expose, en cas d'altération frauduleuse de la vérité, à une peine de 3 ans d'emprisonnement et de 45 000 euros d'amende, en application des dispositions de l'article 441-6 du code pénal.
c) m'engage, en cas de délivrance d'une autorisation d'accès à une zone à régime restrictif, à informer le chef de service, d'établissement ou d'entreprise dont relève cette zone à régime restrictif, de tout changement significatif de situation susceptible d'affecter l'appréciation portée sur mon droit d'accès.
Article 4 de l'arrêté du 3 juillet 2012 modifié : en application du V de l'article R. 413-5-1 du code pénal, le bénéficiaire d'une autorisation d'accès à une zone à régime restrictif est tenu de signaler au chef de service, d'établissement ou d'entreprise ou au responsable de la zone à régime restrictif placé sous son autorité, tout changement de situation concernant :
1° Les informations relatives à son état civil ;
2° Ses liens professionnels ou personnels avec un État étranger, une entreprise ou organisation étrangère ou sous contrôle étranger ou un ressortissant d'un État étranger ;
3° Ses activités professionnelles sur le territoire national en lien avec l'activité principale exercée au sein de la zone à régime restrictif.

D. Cadre réservé à l'établissement d'accueil
(DO NOT fill in this part)

Date de la demande (AAAA-MM-JJ) *	Numéro de la demande (année-mois-codeZRR-n° d'identifiant unique dans l'année ou le mois) *

Nom de l'établissement hébergeur de la ZRR *	
Nom du laboratoire	
Code de l'unité (si laboratoire de recherche) ex: UMR XXXX, EA XXXX*	
Code de la ZRR*	
Adresse de la ZRR*	
Ministère de rattachement*	
Nom et fonction du responsable de la ZRR *	
Téléphone*	
E-mail *	
Nom du responsable scientifique / de stage	
Avis motivé du responsable de la ZRR	
Avis du chef d'établissement ou délégué à la sécurité (FSD, officier de sécurité, etc.)	
Motif de la demande *	
Date de l'avis ministériel *	
Avis du ministère de tutelle *	
Commentaires, précisions sur poste/stage du demandeur	

DIFFUSION RESTREINTE

ANNEXE 4- Modèle d'arrêté portant création d'une ZRR

Arrêté du XX portant création d'une zone à régime restrictif à (… désignation)

La/Le ministre (… *désignation*),

Vu le code de la défense, et notamment l'article R. 2362-1 ;
Vu le code pénal, et notamment ses articles 413-7 et R. 413-1 à R. 413-5-2 ;
Vu le code des relations entre le public et l'administration ;
Vu l'arrêté du 3 juillet 2012 modifié relatif à la protection du potentiel scientifique et technique de la nation ;

Arrête :

Article 1

Sont classés « zone à régime restrictif » (ZRR) en application de l'article R. 413-5-1 du code pénal les locaux et espaces clos (… *désignation*), dont les limites sont précisées en annexe du présent arrêté, situés au sein de (… *établissement*) à (… *ville, département*). Cette ZRR est identifiée sous le numéro (…*numéro d'identifiant de la ZRR*).

Article 2

(… *désignation du chef de service*…) est responsable de la protection du potentiel scientifique et technique.
Il peut désigner un responsable de cette ZRR chargé, sous son autorité, de mettre en œuvre le dispositif de protection notamment en rendant apparentes les limites de cette zone et les mesures d'interdiction dont elle fait l'objet.

Article 3

Les limites de la zone à régime restrictif sont matérialisées de façon explicite par la mise en place de pancartes rectangulaires portant la mention « zone à régime restrictif ».

Les autorisations de pénétrer dans ladite zone sont délivrées dans les conditions fixées par l'article R. 413-5-1 du code pénal.

Article 4

Le haut fonctionnaire de défense et de sécurité est chargé de l'exécution du présent arrêté.

Article 5

Le présent arrêté fait l'objet d'une publication par affichage physique devant l'entrée principale de la ZRR, sur son périmètre extérieur.

DIFFUSION RESTREINTE

Annexe à l'arrêté de création de ZRR

Plan détaillé fixant les limites de la ZRR au sein de l'établissement.

Modèle de signalétique d'une ZRR

Les mesures d'interdiction sont rendues apparentes au moyen de pancartes rectangulaires de 40cm par 30cm environ (format A3 minimum) placées aux endroits appropriés du périmètre extérieur.
Elles doivent être en nombre suffisant pour être obligatoirement vues, même de nuit.

Elles portent de façon lisible l'inscription :

ZONE A RÉGIME RESTRICTIF

INTERDICTION DE PÉNÉTRER SANS AUTORISATION
(ARTICLE R. 413-5-1 DU CODE PÉNAL)

TOUT CONTREVENANT S'EXPOSE AUX PEINES PRÉVUES PAR L'ARTICLE 413-7 DU CODE PÉNAL

ANNEXE 5- Index