PREMIER MINISTRE

Secrétariat général
de la défense
nationale

Protection et
sécurité de l'Etat

Paris, le 25 août 2003

N° **1300** /SGDN/PSE/SSD

INSTRUCTION GÉNÉRALE

INTERMINISTÉRIELLE

SUR

LA PROTECTION DU SECRET

DE LA DÉFENSE NATIONALE

(Abroge et remplace l'instruction générale interministérielle sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'État n° 1300/SGDN/SSD du 12 mars 1982)

51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP - Tél 01.71.75.81.95 - Fax 01.71.75.82.00

MODIFICATIFS[1]

à l'instruction générale interministérielle N°1300 /SGDN/PSE/SSD sur la protection du secret de la défense nationale du 25 août 2003

Numéro des modificatifs	Date du modificatif	Pages concernées	Articles modifiés ou nouveaux

[1] Depuis la parution de l'instruction.

SOMMAIRE

INTRODUCTION

Le nouveau **code pénal (articles 413-9 et suivants)** et le **décret n° 98-608 du 17 juillet 1998** relatif à la protection des secrets de la défense nationale ont sensiblement modifié les fondements législatifs et réglementaires de la protection du secret de la défense nationale. Il est donc apparu nécessaire de réviser l'instruction générale interministérielle n° 1300 du 12 mars 1982 sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'État.

Il convient de rappeler aux destinataires de la présente instruction qu'en dehors des niveaux de classification au titre du secret de la défense nationale, tels qu'ils résultent du décret n° 98-608 précité, les autres notions ou mentions telles de « secret », « confidentiel », « confidentiel officiers », « diffusion restreinte », etc., ne bénéficient pas du fondement de l'article 413-9 du code pénal ni, par conséquent, d'une protection équivalente.

Article 1er

LES ENJEUX DE LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE

L'accès aux secrets de la défense nationale est une **préoccupation constante des services étrangers, de groupements divers ou d'individus isolés**, qui vise en permanence tous les domaines d'activité intéressant la défense nationale : politique, militaire, diplomatique, scientifique, économique, … L'action de ces organisations est souvent facilitée par l'ignorance, l'inattention ou la négligence de certains détenteurs d'informations, qui ne prennent pas les précautions suffisantes pour en assurer la protection.

Toutes les **personnes traitant d'informations présentant un caractère de secret de la défense nationale** doivent être **sensibilisées sur leurs responsabilités.** En cas de manquement, elles peuvent encourir des **sanctions pénales graves** en application des dispositions des **articles 413-9 et suivants du code pénal,** y compris en cas d'imprudence ou de négligence de leur part**.**

Cela est également vrai pour les personnes auxquelles est confié, dans le cadre de contrats, un secret de la défense nationale, qu'il s'agisse de personnes physiques ou morales, de droit public (autres que l'État) ou de droit privé. (articles 121-2 et 414-7 du code pénal)

La protection du secret de la défense nationale doit, en particulier, être assurée :

- ***dans toutes les administrations centrales,***
- ***dans les services déconcentrés de l'État,***
- ***dans les établissements publics nationaux placés sous l'autorité d'un ministre,***
- ***et d'une façon générale dans tous les organismes publics ou privés et par toutes les personnes dépositaires, soit par état ou profession, soit en raison d'une fonction ou d'une mission temporaire ou permanente, de secrets de la défense nationale.***

Les prescriptions de la présente instruction doivent être prises en compte par des **clauses particulières dans les marchés** et **autres contrats** comportant de telles informations, et soumis par ailleurs aux dispositions de l'instruction interministérielle n° 2000 /SGDN/SSD/DR du 1er octobre 1986 sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'État dans les marchés et autres contrats.

Article 2

LES FONDEMENTS LÉGISLATIFS ET RÉGLEMENTAIRES DE LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE

Présentent un caractère de secret de la défense nationale au sens des articles 413-9 et suivants du code pénal **les *renseignements, procédés, objets, documents, données informatisées ou fichiers :***

- ***intéressant la défense nationale qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion ;***
- ***dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.***

Pris en application des dispositions du dernier alinéa de l'article 413-9 du code pénal, **le décret n° 98-608 du 17 juillet 1998** :

- définit **trois niveaux** de classification **: Très Secret-Défense, Secret-Défense, Confidentiel-Défense ;**
- prévoit que les informations ou supports protégés portent la mention de leur niveau de classification ;
- détermine les **responsabilités respectives du Premier ministre et des ministres** relatives aux modalités d'organisation de la protection des informations ou supports protégés ;
- subordonne l'**accès** aux informations classifiées à **deux conditions** :
  - avoir fait l'objet d'une **décision d'habilitation préalable** intervenant à la suite d'une procédure définie par le Premier ministre ;
  - avoir **besoin de les connaître** pour l'accomplissement de sa fonction ou de sa mission.

Les informations ou supports protégés émis par des États étrangers ou dans le cadre d'organisations internationales, quand un accord de sécurité existe, ne bénéficient des mesures de protection que dans la mesure où elles portent une mention de classification nationale correspondant à l'un des trois niveaux définis par le décret du 17 juillet 1998, ou une mention équivalente de l'UE (circulaire du 5 mai 2002), de l'OTAN, de l'UEO, d'Euratom. (en application de l'arrêté du 25 février 1994 paru au JO du 1er mars 1994)

Article 3

LA TERMINOLOGIE

La présente instruction utilisera, comme le décret n° 98-608 du 17 juillet 1998, l'expression **"informations ou supports protégés"** pour désigner les renseignements, procédés, objets, documents, données informatisées ou fichiers présentant un caractère de secret de la défense nationale.

Article 4

L'OBJET DE LA PRÉSENTE INSTRUCTION

La présente instruction a pour objet, conformément aux dispositions des articles 5, 6 et 8 du décret du 17 juillet 1998,
- d'une part de préciser les conditions dans lesquelles chaque ministre, pour le département dont il a la charge, détermine les modalités de protection des informations ou supports protégés,
- et d'autre part de définir la procédure préalable à la décision d'habilitation aux secrets de la défense nationale.

Conformément à la volonté exprimée par le législateur lors de l'élaboration du nouveau code pénal, elle vise à **responsabiliser les détenteurs des informations ou supports protégés** et à prévenir tout excès de classification.

Retour au sommaire

TITRE PREMIER

L'ORGANISATION GÉNÉRALE DE LA PROTECTION ET LA RÉPARTITION DES COMPÉTENCES

Article 5

LE PREMIER MINISTRE

En vertu de l'article 21 de la Constitution, le Premier ministre est responsable de la défense nationale.

Conformément aux dispositions du décret n° 98-608 du 17 juillet 1998,

● **en ce qui concerne le Très Secret-Défense :**

- il détermine les critères et les modalités d'organisation de sa protection,
- il définit des classifications spéciales correspondant aux différentes priorités gouvernementales,
- il fixe les conditions dans lesquelles chaque ministre, pour le département dont il a la charge, détermine les informations et supports protégés qu'il y a lieu de classifier à ce niveau. (art. 5 du décret)

● **en ce qui concerne les niveaux Secret-Défense et Confidentiel-Défense :**

- il fixe les conditions dans lesquelles chaque ministre, pour le département dont il a la charge, détermine les informations et supports protégés qu'il y a lieu de classifier, et les modalités de leur protection. (art. 6 du décret)

● **en ce qui concerne les habilitations :**

- il définit la procédure à la suite de laquelle intervient la décision d'habilitation,
- il prend la décision d'habilitation pour le niveau Très Secret-Défense et indique la ou les classifications spéciales auxquelles la personne habilitée a accès. (art. 8 du décret)

Article 6

LE SECRÉTAIRE GÉNÉRAL DE LA DÉFENSE NATIONALE

En application du décret n° 78-78 du 25 janvier 1978 fixant ses attributions, le secrétaire général de la défense nationale **propose, diffuse, fait appliquer et contrôler les mesures nécessaires à la protection du secret de la défense nationale.** (art. 7 du décret)

Il dispose, à cette fin, conformément aux dispositions du décret du 11 mars 1963 portant organisation de la sécurité de défense, du **Service de Sécurité de Défense (SSD)** rattaché à la Direction Protection et Sécurité de l'État.

Dans le cadre des délégations de signature que lui accorde le Premier ministre, il prend la **décision d'habilitation** pour le **niveau Très Secret-Défense**.

Il désigne pour chacune des classifications spéciales du niveau Très Secret-Défense un agent central de sécurité, membre du service de sécurité de défense du Secrétariat Général de la Défense Nationale (SGDN), dont les missions sont définies par instruction particulière.

Il suit l'application, dans chaque département ministériel, des conditions de protection des autres niveaux de secret de la défense nationale (Secret-Défense et Confidentiel-Défense)

Dans le cadre des accords de sécurité internationaux, il assure les fonctions d'**autorité nationale de sécurité** (ANS)[2] et, au titre de la coordination interministérielle, il est l'interlocuteur des ANS étrangères.

Article 7

LES MINISTRES

Conformément aux dispositions du décret n° 98-608 du 17 juillet 1998, chaque ministre, pour le département dont il a la charge,

- détermine, dans les conditions fixées par le Premier ministre, les informations ou supports protégés qu'il y a lieu de classifier à l'un des trois niveaux, et les modalités d'organisation de leur protection pour les niveaux Secret-Défense et Confidentiel-Défense,
- prend les décisions d'habilitation pour les niveaux Secret-Défense et Confidentiel-Défense.

Article 8

LES HAUTS FONCTIONNAIRES DE DÉFENSE

Chaque ministre, à l'exception du ministre de la défense qui dispose d'une organisation spécifique faisant l'objet de directives particulières, est assisté par un ou exceptionnellement, si les structures du département l'exigent, plusieurs **hauts fonctionnaires de défense** (HFD) dont les attributions sont fixées par le décret n° 80-243 du 3 avril 1980 modifié. En application des dispositions de ce décret, le HFD est **responsable de l'application des dispositions relatives à la sécurité de défense et à la protection du secret** ; il relève directement du ministre et, pour l'exercice de ses missions, a autorité sur l'ensemble des directions et services du département ministériel.

Dans le cadre des délégations **de signature accordées** par le ministre, le HFD prend les **décisions d'habilitation** pour les niveaux Secret-Défense et Confidentiel-Défense**.**

Il assure **les liaisons nécessaires avec le SGDN pour les habilitations au niveau Très Secret-Défense**.

Il veille au bon fonctionnement des services qui gèrent les informations et supports protégés, vérifie l'exactitude des inventaires et procède aux contrôles et inspections nécessaires dans l'ensemble de son département ministériel.

Conformément aux dispositions de l'article 5 du décret n° 80-243 du 3 avril 1980, chaque ministre met à disposition du HFD les moyens en personnel qui lui sont nécessaires. Il convient de désigner à cet effet un ou plusieurs **fonctionnaires de sécurité de défense** rattachés au HFD, pour contrôler, sous sa direction, l'exécution des mesures de protection et proposer toutes dispositions en vue d'en renforcer l'efficacité. En fonction des structures propres à chaque ministère et de leur format, il convient par ailleurs de désigner des fonctionnaires de sécurité dans les organismes rattachés, les établissements publics sous tutelle et, si nécessaire, dans les entreprises publiques.

Pour les départements ministériels utilisant des systèmes d'information nécessitant une protection, le ministre désigne un **fonctionnaire de sécurité des systèmes d'information (FSSI)**, placé sous l'autorité du HFD.

Dans la suite de l'instruction, l'expression haut fonctionnaire de défense désigne soit le haut fonctionnaire de défense, soit l'autorité déléguée par le ministre de la défense.

[2] Décret du 13 février 1969 relatif à la protection du secret dans les rapports entre la France et les États étrangers.

Article 9

L'ORGANISATION FONCTIONNELLE

Dans les armées et dans les différents départements ministériels, les autorités hiérarchiques civiles ou militaires ayant reçu délégation du ministre dont elles dépendent assurent, chacune à son échelon et dans le cadre de ses attributions, la responsabilité des mesures de sécurité.

Ces autorités, lorsqu'elles utilisent des **informations ou supports protégés classifiés au niveau Très Secret-Défense**, doivent être assistées d'un **agent de sécurité** et créer des **«antennes d'utilisation»** dans les conditions fixées par une instruction particulière du Premier ministre (cf. art. 49). Pour la gestion, l'enregistrement et la conservation des informations ou supports protégés classifiés au niveau Secret-Défense, des **bureaux Secret-Défense** sont créés en **zone réservée**.

Les **entreprises publiques ou privées dépositaires de secrets de la défense nationale, notamment parce qu'elles sont titulaires de marchés classés** de défense nationale ou à clause de sécurité, doivent désigner, avec l'agrément de l'autorité contractante ou de l'autorité de décision compétente en matière d'habilitation de la personne morale de l'entreprise, un **agent de sécurité** chargé d'assurer le contrôle permanent des informations ou supports protégés.

Retour au sommaire

TITRE II

L'HABILITATION DES PERSONNES

Article 10

LA PORTÉE DE L'HABILITATION

Aux termes de l'article 7 du décret n° 98-608 du 17 juillet 1998, «*nul n'est qualifié pour connaître des informations ou supports protégés s'il n'a fait au préalable l'objet d'une décision d'habilitation et s'il n'a besoin de les connaître pour l'accomplissement de sa fonction ou de sa mission*».

Le besoin d'en connaître, lié aux fonctions exercées, ne constitue pas un droit personnel à prendre connaissance d'informations. L'appréciation de ce besoin relève de l'autorité hiérarchique compétente.

Lorsqu'une personne présente une **vulnérabilité**, il est préférable de ne pas lui donner accès à des informations ou supports protégés, dans son intérêt et afin d'assurer la protection du secret de la défense nationale. L'évaluation des vulnérabilités de la personne se fonde sur l'existence ou l'absence de risques objectifs. Cette mesure n'affecte en rien l'honorabilité de la personne et ne remet pas en question son appartenance au service de l'État, à l'organisme ou à l'entreprise qui possède un lien juridique avec elle.

Article 11

LES CATALOGUES DES EMPLOIS

Les hauts fonctionnaires de défense élaborent les instructions nécessaires pour faire établir, par les administrations de l'État ou les organismes publics ou privés traitant des informations ou supports protégés et relevant de leur département ministériel, les **catalogues des emplois pouvant nécessiter l'accès aux informations ou supports protégés classifiés Secret-Défense ou Très Secret-Défense.** En ce qui concerne le niveau Confidentiel-Défense, l'élaboration d'un catalogue des emplois est fortement recommandée. Pour les entreprises mentionnées à l'article 9 le répertoire des personnels habilités tiendra lieu de catalogue des emplois.

Ces catalogues des emplois peuvent être établis par directions, par services, ou au niveau des administrations déconcentrées de l'Etat, notamment dans les administrations ou les organismes, publics ou privés, aux effectifs importants. Ils doivent tenir compte des besoins réels et des flux d'informations ou de supports protégés.

Afin de permettre au SGDN de maîtriser le nombre de personnes ayant accès aux informations ou supports protégés, le HFD lui rend compte annuellement du dispositif retenu.

Article 12

LE CAS DES RESSORTISSANTS ÉTRANGERS

Les ressortissants étrangers peuvent, **dans certains cas limités au strict (fonctionnel et géographique) besoin d'en connaître**, et dans la mesure où ils sont affectés dans un emploi nécessitant l'accès à des informations ou supports protégés, **être habilités aux niveaux Confidentiel-Défense** et **Secret-Défense**. (cf. art. 22)

Article 13

LE CAS DES PERSONNELS CONVOYEURS DE SUPPORTS PROTÉGÉS

Le transport de supports protégés par des personnels convoyeurs, qui n'ont pas à en prendre connaissance, doit être subordonné à la délivrance d'une décision de «sécurité convoyeur» (Mle 05/IGI 1300). Cette décision intervient après un contrôle élémentaire demandé (Mle 03/IGI 1300) aux services spécialisés. Le convoyage des supports classifiés Très Secret-Défense est organisé selon des dispositions particulières[3].

Article 14

LA DÉCISION D'AGRÉMENT

Certaines personnes, dans le cadre de leurs fonctions, peuvent être amenées à **prendre connaissance de façon occasionnelle seulement**, d'informations ou de supports protégés au **niveau Très Secret-Défense,** de différentes classifications spéciales, ou d'informations ou de supports protégés aux **niveaux Secret-Défense et Confidentiel-Défense.**

Dans ce cas, les intéressés feront l'objet d'une décision d'agrément prise à l'issue d'une procédure d'habilitation ordinaire. Néanmoins, l'agrément ne doit pas être considéré comme une habilitation de réserve, accordée par précaution à un nombre variable de personnes pour satisfaire des besoins mal définis.

[3] Directives d'application pratique n° 02/SGDN/SSD/CD du 3 février 1986 sur l'organisation et le fonctionnement des classifications spéciales Très Secret-Défense.

CHAPITRE PREMIER

LA PROCÉDURE PRÉALABLE A LA DÉCISION D'HABILITATION

Article 15

L'OBJET DE LA PROCÉDURE

La procédure d'habilitation a pour objet de vérifier qu'une personne peut, sans risque pour la défense nationale ou pour sa propre sécurité, connaître des informations ou supports protégés dans l'exercice de ses fonctions.

Article 16

LE DÉCLENCHEMENT DE LA PROCÉDURE

La procédure préalable à la décision d'habilitation des personnes est une opération coûteuse en temps et en personnel. Il convient donc d'éviter toute surcharge inutile des services chargés de cette mission.

C'est pourquoi, **lorsqu'un poste à pourvoir exige une habilitation aux niveaux Secret-Défense ou Confidentiel-Défense**, une procédure sera engagée au seul profit de la personne effectivement nommée dans l'emploi. Toute mesure d'anticipation reste possible si nécessaire.

Toutefois, **lorsque l'habilitation requise est du niveau Très Secret-Défense**, il revient à l'autorité d'emploi d'apprécier la nécessité d'une enquête concernant chacun des candidats au poste concerné.

Article 17

LE DÉROULEMENT NORMAL DE LA PROCÉDURE

La procédure préalable à la décision d'habilitation comporte normalement les phases suivantes.

- La constitution du dossier d'habilitation, comprenant :

- la **demande d'habilitation** formulée par le chef du service employeur attestant le besoin de connaître des informations ou supports protégés à un niveau donné, pour une personne nommément désignée ;
- la **notice individuelle de sécurité,** renseignée intégralement par l'intéressé et vérifiée par l'officier de sécurité ou agent de sécurité du service ou de l'organisme dont dépend l'intéressé.

- **L'instruction du dossier d'habilitation** effectuée par :

- les **services compétents du ministère de l'intérieur** pour les personnels civils employés dans les ministères civils ou les organismes travaillant à leur profit ;
- le **service compétent du ministère de la défense**[4] pour les personnels militaires et civils du ministère de la défense ou employés dans les organismes et entreprises travaillant au profit du ministère de la défense.

[4] La Direction Générale de la Sécurité Extérieure (DGSE) effectue l'instruction du dossier d'habilitation pour son personnel et celui des organismes et entreprises travaillant à son profit.

Article 18

LE CAS DE L'HABILITATION DES AGENTS DE L'ÉTAT AU NIVEAU CONFIDENTIEL-DÉFENSE HORS MINISTÈRE DE LA DÉFENSE

Les agents de l'État (fonctionnaires et contractuels) hors ministère de la défense, seront habilités ès qualité au niveau Confidentiel-Défense, sauf demande expresse d'enquête de l'autorité hiérarchique, sous réserve **:**

- d'occuper un poste figurant au catalogue des emplois (cf art. 11) établi sous la responsabilité du HFD ;
- de remplir la notice individuelle de sécurité, attestant sur l'honneur l'exactitude des informations mentionnées (ces renseignements sont exploités par l'autorité hiérarchique qui peut demander expressément une enquête des services spécialisés) ;
- d'avoir signé l'engagement de responsabilité défini à l'article 27 ci-après.

Article 19

LA CONSTITUTION DU DOSSIER D'HABILITATION

La seule finalité du dossier est de réunir les éléments en vue de délivrer la décision d'habilitation. En effet, aux termes des dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, le recueil d'informations nominatives est subordonné à des conditions strictes. Le dossier comprend :

- la **demande d'habilitation** Mle 02/IGI 1300 ;
- la **notice individuelle de sécurité** Mle 01/IGI 1300 établie par l'intéressé en trois exemplaires (un original et deux photocopies) ;
- **trois photographies d'identité**, identiques et récentes.

Article 20

L'INSTRUCTION DU DOSSIER D'HABILITATION : L'AVIS DE SÉCURITÉ

Le dossier d'habilitation est adressé par le chef du service employeur[5], au HFD qui le vérifie et le transmet :

- pour le niveau Très Secret-Défense au SGDN (SSD) qui fait déclencher l'enquête par les services compétents,
- pour les niveaux Secret-Défense et Confidentiel-Défense directement aux services compétents.

Au terme de la procédure, le service spécialisé ayant instruit les dossiers fait connaître ses conclusions techniques par l'émission d'un avis de sécurité à la seule autorité compétente pour prendre la décision d'habilitation : Premier ministre (SGDN/SSD) ou ministre (HFD) selon le niveau d'habilitation.

Article 21

LA PROCÉDURE D'URGENCE

Diverses personnes peuvent être concernées par cette procédure et, en particulier, celles entrant dans les catégories ci-après :

- **hauts fonctionnaires, diplomates, officiers généraux ;**
- **personnes envoyées en mission dans le cadre d'opérations inopinées ;**
- **responsables de haut niveau affectés dans des conditions exceptionnelles.**

[5] Une organisation spécifique est en place au ministère de la défense.

Elles peuvent être appelées, en raison de leur désignation à une fonction, à prendre connaissance d'informations ou de supports protégés dans des délais très brefs.

Le chef du service employeur doit alors, dans la demande Mle 02/IGI 1300, préciser et motiver l'urgence de l'habilitation et l'impossibilité de procéder autrement. Le dossier est adressé :

- pour le niveau Très Secret-Défense, au SGDN (SSD), qui prend la décision d'engager ou non la procédure d'urgence et poursuit l'instruction du dossier ;
- pour les niveaux Secret-Défense et Confidentiel-Défense, au HFD, qui consulte les services spécialisés.

Dans les **quinze jours** suivant leur saisine, les services spécialisés émettent un **avis de sécurité provisoire**, au vu duquel l'autorité compétente peut prendre une **décision d'habilitation provisoire**.

Cette procédure d'urgence ne doit concerner qu'un **nombre très limité de personnes et rester exceptionnelle** pour le niveau Confidentiel-Défense**. Elle ne remplace ni n'interrompt la procédure normale**.

Article 22

L'HABILITATION DES RESSORTISSANTS ÉTRANGERS

Les ressortissants étrangers peuvent, **dans certains cas limités au strict (fonctionnel et géographique) besoin d'en connaître** et dans la mesure où ils sont affectés dans un emploi nécessitant l'accès à des informations ou supports protégés, **être habilités aux niveaux Confidentiel-Défense** et **Secret-Défense.**

La responsabilité du déclenchement de la procédure et de la décision d'habilitation est de la compétence du ministre (HFD). Conformément aux termes du décret du 13 février 1969 relatif à la protection du secret dans les rapports entre la France et les pays étrangers, **le SGDN assure les fonctions d'Autorité nationale de sécurité** (ANS). **La communication avec les ANS étrangères a donc lieu exclusivement par son intermédiaire**. Dans certains cas, après information et accord du SGDN, des échanges directs entre les Autorités de sécurité désignées (ASD) et leurs homologues étrangers pourront être autorisés.

Si l'habilitation intervient dans le **cadre d'une organisation multinationale** possédant une réglementation propre relative à la protection des informations ou supports protégés, ou dans le **cadre d'un accord multilatéral** comportant des dispositions particulières concernant la protection des informations ou supports protégés, il convient de **se référer aux textes** en question pour déterminer les conditions et les procédures d'habilitation à appliquer.

Si l'habilitation intervient dans le **cadre d'un accord bilatéral de sécurité**, il convient de s'en tenir à la **mise en œuvre de l'accord** en ce qui concerne les conditions d'habilitation.

En cas d'accord particulier le prévoyant **explicitement**, une habilitation accordée par une ANS étrangère peut être acceptée par les autorités compétentes (cf art. 24) quand le ressortissant étranger occupe un emploi en France nécessitant l'accès aux informations ou supports protégés. Cette acceptation se traduira de façon explicite par l'émission d'une décision d'habilitation aux informations ou supports protégés au vu du certificat de sécurité produit par l'ANS étrangère.

Lorsqu'il n'existe **aucun accord de sécurité entre la France et le pays dont la personne concernée détient la nationalité, aucune habilitation à aucun niveau ne doit, en principe, être délivrée par une autorité française**. Néanmoins, si l'habilitation de la personne considérée se révèle véritablement nécessaire, il demeure possible pour l'autorité requérante de **saisir le SGDN** qui émettra un avis sur l'opportunité de l'habilitation et déterminera éventuellement les modalités de la procédure à suivre.

Article 23

LA DURÉE DE VALIDITÉ DE L'AVIS DE SÉCURITÉ

La durée de validité de l'avis de sécurité rendu par les services enquêteurs varie en fonction du niveau d'habilitation demandé. Elle ne peut excéder :

- **trois ans** pour le niveau Très Secret-Défense et pour le contrôle préalable à la décision de « sécurité convoyeur » ;
- **cinq ans** pour le niveau Secret-Défense ;
- **dix ans** pour le niveau Confidentiel-Défense.

La **durée de validité de la décision d'habilitation** peut être **distincte de celle de l'avis de sécurité,** elle reste cependant toujours inférieure. En effet, l'habilitation est valable tant que la personne a besoin, par son emploi, de connaître des informations ou supports protégés, tandis que l'avis de sécurité est valide pendant les durées prévues ci-dessus et à concurrence d'un changement de situation nécessitant de nouvelles investigations.

L'attention de la personne habilitée doit être appelée sur l'obligation qu'elle a d'informer l'autorité qui a décidé son habilitation, **de toute modification intervenant dans sa situation** concernant l'un des quatre domaines suivants :

- situation maritale (mariage, remariage, conclusion d'un PACS, établissement d'un concubinage effectif, etc…),
- fonction professionnelle,
- lieu de résidence,
- établissement d'un contact suivi et fréquent avec un ou des ressortissants étrangers.

Cette information doit être donnée au plus vite et de préférence au moyen de la **notice individuelle de sécurité en faisant ressortir les éléments nouveaux.**

Retour au sommaire

CHAPITRE II

LA DÉCISION D'HABILITATION

Article 24

LES AUTORITÉS COMPÉTENTES

En application des dispositions de l'article 8 du décret n° 98-608 du 17 juillet 1998, les décisions d'habilitation au niveau **Très Secret-Défense** sont prises par le Premier ministre. Elles peuvent être également prises, en vertu de délégations de signatures données par celui-ci, par le **Secrétaire général de la défense nationale** et les **autres autorités déléguées**, qui les adressent aux ministères concernés.

Les décisions d'habilitation au **Secret-Défense** et au **Confidentiel-Défense sont prises**, en application des dispositions de l'article 8 du décret du 17 juillet 1998, **par chaque ministre** pour le département dont il a la charge. Elles peuvent être également prises par les autorités ayant reçu délégation à cet effet.

Article 25

LES CARACTÈRES DE LA DÉCISION D'HABILITATION[6]

La **décision d'habilitation** est une **autorisation explicite** qui permet à une personne, en fonction du besoin d'en connaître, d'avoir **accès aux informations ou supports protégés classifiés au niveau précisé** dans la décision et aux niveaux inférieurs.

Pour prendre cette décision, l'autorité compétente n'est pas liée par l'avis de sécurité formulé par le service spécialisé ayant instruit le dossier de demande d'habilitation. Cet avis n'est qu'une évaluation des vulnérabilités de la personne et ne peut être considéré comme une autorisation ou un refus implicite d'accès aux informations ou supports protégés. Il n'en est fait aucunement référence dans la décision d'habilitation. Compte tenu de la teneur de l'avis de sécurité, une **mise en garde de l'autorité d'emploi** et/ou une **mise en éveil de la personne concernée** peuvent être prévues au moment de la décision d'habilitation.

Pour le niveau Très Secret-Défense, si **une même personne** doit avoir **accès aux informations relevant de plusieurs classifications spéciales,** une décision d'habilitation est émise pour **chacune de ces classifications spéciales**. Ainsi, une seule personne peut faire éventuellement l'objet de plusieurs décisions d'habilitation au niveau Très Secret-Défense.

Article 26

LE REFUS D'HABILITATION

Le refus d'habiliter une personne ne donne pas lieu à une motivation explicite de la décision. Les **motifs de ce refus étant couverts par le secret de la défense nationale**, si la personne concernée demande à en avoir connaissance, l'autorité compétente se réfère aux dispositions du dernier alinéa de l'article 1er de la **loi n° 79-587 du 11 juillet 1979 modifiée relative à la motivation des actes administratifs,** combinées aux dispositions de l'article 6 de la loi n° 78-753 du 17 juillet 1978 modifiée, portant diverses mesures d'amélioration des relations entre l'Administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

[6] La décision d'accès à la sécurité des systèmes d'information est définie par l'instruction interministérielle N° 910/SGDN/DISSI/SCSSI/SSD/DR du 19 décembre 1994 sur les articles contrôlés de la sécurité des systèmes d'information.

Article 27

L'ENGAGEMENT DE RESPONSABILITÉ

Tout titulaire d'une décision d'habilitation dont le poste peut nécessiter l'accès à des informations ou supports protégés, doit avoir été informé des règles de protection du secret de la défense nationale, des obligations lui incombant, ainsi que, plus particulièrement, des dispositions des articles 411-6 à 411-8 et 413-9 à 413-12 du code pénal, avant de signer le premier volet d'un «engagement de responsabilité» dont le modèle figure en annexe (Mle 08/IGI 1300). Par cet engagement, il reconnaît avoir pris connaissance des obligations particulières imposées à toute personne dépositaire ou ayant eu connaissance d'une information ou d'un support protégé, ainsi que des sanctions prévues par les articles 413-10 à 413-12 du code pénal. Le deuxième volet de cet engagement est signé lors de la cessation de fonctions ou du retrait de l'habilitation.

La délivrance d'une décision d'habilitation ou d'une décision d'habilitation provisoire, selon la procédure d'urgence, doit avoir été précédée de la signature d'un engagement de responsabilité.

Article 28

LE RETRAIT DE L'HABILITATION

La décision d'habilitation ne confère pas à son titulaire un droit acquis à son maintien. Elle peut être retirée quand l'intéressé cesse de remplir les conditions nécessaires à sa délivrance. Il en est ainsi lorsque des **éléments de vulnérabilité** apparaissent, signalés notamment par :

- un avis défavorable ou restrictif des services spécialisés ;
- une demande motivée du supérieur hiérarchique ou de l'officier de sécurité du service ou de l'organisme auquel l'intéressé est rattaché, consécutive à un changement de situation ou de comportement de celui-ci présentant un risque pour la défense nationale.

Article 29

L'EXPIRATION DE LA DÉCISION D'HABILITATION PROVISOIRE PRISE EN URGENCE

La décision d'habilitation provisoire prise selon la procédure d'urgence décrite à l'article 21, n'interrompt pas la procédure normale, qui se poursuit après l'émission de l'avis de sécurité provisoire.

La décision d'habilitation provisoire prend fin, soit lors de la délivrance ou du refus de l'habilitation à l'issue de la procédure normale, soit au plus tard, six mois après sa date d'émission.

Article 30

LA DURÉE DE VALIDITÉ DES DÉCISIONS D'HABILITATION ET DES DÉCISIONS DE SÉCURITÉ CONVOYEUR

La décision d'habilitation précise sa durée de validité, dans la limite de la durée de validité de l'avis de sécurité au vu duquel elle a été prise. Il en est de même pour la décision de sécurité convoyeur.

Les décisions d'habilitation restent valables au maximum six mois après leur date d'expiration, dans la mesure seulement où une demande de renouvellement a été formulée dans le délai prévu à l'article 31. Il en est de même pour les décisions de sécurité convoyeur.

Par ailleurs, la durée de validité de la décision d'habilitation est liée à la durée d'occupation du poste qui a justifié sa délivrance mais peut n'être limitée dans le temps que par la durée de validité de l'avis de sécurité ou le départ de l'intéressé de l'organisme ou de l'entreprise.

En cas de changement d'affectation d'une personne habilitée, l'officier de sécurité ou agent de sécurité de l'organisme quitté renvoie la décision d'habilitation et l'engagement de responsabilité de cette personne à l'autorité ayant pris la décision d'habilitation. Si le responsable du nouvel organisme d'affectation formule une demande d'habilitation, l'autorité compétente prend une nouvelle décision sur la base de l'avis de sécurité encore en cours de validité. Cette autorité de décision peut, si nécessaire, obtenir les éléments utiles à sa décision auprès de l'autorité de décision précédente.

Article 31

LE RENOUVELLEMENT DES DÉCISIONS D'HABILITATION ET DES DÉCISIONS DE SÉCURITÉ CONVOYEUR

La demande de renouvellement doit être effectuée dans les six mois qui précèdent la date de péremption de l'avis de sécurité. Elle doit comprendre une demande d'habilitation (Mle 02/IGI 1300) et trois exemplaires de la notice 94 A (Mle 01/IGI 1300), accompagnés de trois photographies récentes (datant de moins d'un an).

La décision d'habilitation initiale reste valable **au maximum six mois après la date d'expiration** de l'avis de sécurité, à la condition impérative qu'une demande de renouvellement ait été effectuée dans le délai prévu à l'alinéa précédent.

Article 32

LA CONSERVATION DES DÉCISIONS D'HABILITATION ET DES DÉCISIONS DE SÉCURITÉ CONVOYEUR

Pendant leur durée de validité, les décisions doivent être **conservées par le service employeur**. Ces documents ne doivent en aucun cas être remis aux intéressés ou reproduits sous quelque forme que ce soit. En cas de nécessité, les titulaires d'autorisation reçoivent un certificat de sécurité (Mle 07/IGI 1300) délivré pour une mission déterminée et une période limitée, par l'autorité ayant pris la décision. Celle ci peut déléguer la délivrance des certificats de sécurité.

Pour le niveau Très Secret-Défense, lorsque l'habilitation est devenue sans objet par suite du retrait d'habilitation, du changement d'affectation ou du changement d'emploi répertorié sur le catalogue des emplois, l'autorité compétente en avise le SGDN/SSD en renvoyant sans délai la décision devenue sans objet ainsi que l'engagement de responsabilité dûment signé.

Article 33

LES RÉPERTOIRES DES HABILITATIONS

Le **SGDN** (SSD) tient à jour le **répertoire central** des **habilitations au Très Secret-Défense** ainsi que les habilitations dépendant des alliances.

Dans **chaque département ministériel**, il est tenu pour chaque niveau de classification un **répertoire** :

- *des dossiers d'habilitation en cours d'instruction ;*
- *des habilitations en cours de validité.*

Pour permettre au SGDN/SSD d'évaluer le nombre total d'habilitations délivrées et de personnes ayant accès aux informations ou supports protégés, le HFD lui adresse en fin d'année les états des personnes habilitées aux niveaux Secret Défense et Confidentiel Défense dans son département ministériel.

Article 34

LA PORTÉE D'UNE DÉCISION D'HABILITATION AU REGARD DES INFORMATIONS OU SUPPORTS PROTÉGÉS DES DOMAINES INTERALLIÉS

Toute **décision d'habilitation aux informations ou supports protégés du domaine national** peut, s'il en est besoin, donner **accès aux informations ou supports protégés du niveau correspondant et des niveaux inférieurs des domaines interalliés**, par application des dispositions de l'accord de sécurité conclu entre les États signataires du traité de l'Atlantique Nord, des dispositions juridiques mises en place dans le cadre de l'Union européenne, de l'accord conclu entre les États signataires du traité de Bruxelles modifié (Union de l'Europe occidentale) et des différents accords de sécurité signés par la France.

En revanche, **une décision d'habilitation aux informations ou supports protégés du domaine allié ne donne pas accès aux informations ou supports protégés correspondants du domaine national**[7]**,** sauf décision particulière se référant au catalogue des emplois. Cette décision qui ne s'applique pas au niveau Très Secret-Défense, est du ressort du SGDN, ce dernier gérant l'ensemble des réseaux interalliés.

Retour au sommaire

[7] Cf. instruction interministérielle n° 2100/SGDN/SSD du 1er décembre 1975 pour l'application en France du système de sécurité de l'organisation du traité de l'Atlantique nord et instruction interministérielle n° 2101/SGDN/SSD du 22 mai 1995 pour l'application en France du système de sécurité de l'Union de l'Europe occidentale.

TITRE III

LA PROTECTION DES INFORMATIONS OU SUPPORTS PROTÉGÉS

CHAPITRE PREMIER

LES PRINCIPES ET LES RÈGLES GÉNÉRALES DE PROTECTION

SECTION I

LES MESURES GÉNÉRALES

Article 35

LES PRINCIPES DE CLASSIFICATION

La décision de classifier une information ou un support au titre du secret de la défense nationale a pour conséquence de placer cette information ou ce support sous la protection des articles 413-9 et suivants du code pénal ; elle constitue le seul moyen d'assurer cette protection.

Une information dont la divulgation serait de nature à nuire à la défense nationale, mais qui n'aurait pas fait l'objet d'une décision de classification au titre du secret de la défense nationale, ne sera pas protégée par les dispositions des articles 413-9 et suivants du code pénal. Toute mention ou timbre destiné, dans l'esprit de son émetteur, à assurer la confidentialité d'une information ou d'un support, mais qui ne correspondrait pas aux marquages définis dans la présente instruction, n'assurera pas à cette information ou à ce support la protection prévue aux articles 413-9 et suivants du code pénal pour les secrets de la défense nationale.

Les infractions spécifiques prévues et réprimées par les articles 413-9 et suivants du code pénal ne couvrent que les faits relatifs à des informations ou supports protégés au titre du secret de la défense nationale.

L'article 3 du décret n° 98-608 du 17 juillet 1998 définit trois niveaux de classification :

- **Le niveau Très Secret-Défense est réservé aux informations ou supports protégés dont la divulgation est de nature à nuire très gravement à la défense nationale et qui concernent les priorités gouvernementales en matière de défense ;**
- **Le niveau Secret-Défense est réservé aux informations ou supports protégés dont la divulgation est de nature à nuire gravement à la défense nationale ;**
- **Le niveau Confidentiel-Défense est réservé aux informations ou supports protégés dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale classifié au niveau Très Secret-Défense ou Secret-Défense.**

La décision de classifier une information ou un support est un acte important, par les **contraintes qu'il induit** en matière de mesures de protection, et par les **conséquences judiciaires** qu'il peut entraîner, ainsi qu'il a été rappelé plus haut.

La décision de classification doit être prise au **niveau hiérarchique le plus apte à évaluer les enjeux**. En effet, une *sur classification* dévalorise la notion de secret de la défense nationale et

s’accompagne de surcoûts, tandis qu’une *sous classification* entraîne des mesures de protection insuffisantes.

L’autorité qui procède à la classification doit donc toujours être à même de justifier sa décision devant sa hiérarchie.

Article 36

OBLIGATIONS S’IMPOSANT A TOUTE PERSONNE DÉPOSITAIRE D’UN SECRET DE LA DÉFENSE NATIONALE

Tout détenteur d’une habilitation doit être informé de ses responsabilités à l’égard de la protection des informations classifiées. Il veille au respect des dispositions du Code Pénal relatives à la protection du secret de la Défense Nationale.

Aux risques de s’exposer aux peines prévues par l’article 413-10 du code pénal, la personne dépositaire d'un renseignement, procédé, objet, document, donnée informatisée ou fichier qui a un caractère de secret de la défense nationale a le devoir d’empêcher tant leur destruction, détournement, soustraction ou reproduction, que leur prise de connaissance par du public ou une personne non habilitée dans les conditions rappelées aux articles 10 à 34 ci-dessus, sauf à encourir les poursuites prévues par les dispositions pénales précitées.

Article 37

ACCÈS DES JURIDICTIONS FRANÇAISES À LA COMMUNICATION DES INFORMATIONS PROTÉGÉES AU TITRE DU SECRET DE LA DÉFENSE NATIONALE

1. L’accès d’une juridiction française à des documents classifiés au titre du secret de la défense nationale est régi par les dispositions de la loi n°98-567 du 8 juillet 1998 instituant une Commission consultative du secret de la défense nationale. Celle ci prévoit qu’une juridiction française, dans le cadre d’une procédure engagée devant elle, peut demander la déclassification et la communication d’informations protégées au titre du secret de la défense nationale à l’autorité administrative en charge de la classification. Cette dernière saisit sans délai la Commission consultative du secret de la défense nationale.

La mise en œuvre de la loi a fait l’objet de la circulaire 4776/SG du 13 février 2001 qui précise que la consultation de la Commission doit être effectuée, alors même que l’administration saisie serait décidée à déclassifier les informations et à les communiquer à la juridiction demanderesse.

Dans les deux mois de sa saisine, la Commission formule un avis, qui est transmis à l’autorité administrative ayant procédé à la classification.

L’autorité administrative notifie sa décision, assortie du sens de l’avis, à la juridiction demanderesse ayant demandé la déclassification et la communication d’informations classifiées dans un délai de quinze jours francs à compter de la réception de l’avis, ou, au plus tard, à l’expiration du délai de deux mois dont dispose la commission pour se prononcer.

Le sens de l’avis de la Commission est publié au Journal officiel.

2. Lorsqu’une juridiction française est amenée, soit à constater des infractions, soit à rechercher des personnes ou des objets relatifs à ces infractions dans des établissements militaires, elle doit adresser à l’autorité militaire des réquisitions tendant à obtenir l’entrée dans ces établissements. (art.698-3 du C.P.P.)

Elle veille, en liaison avec le représentant qualifié de l’autorité militaire, au respect des prescriptions relatives au secret militaire.

Article 38

LES RÈGLES DE CLASSIFICATION

L'attribution d'un niveau de classification tient compte des règles suivantes :

- **le niveau de classification est déterminé en fonction de la nature de l'information ou du support protégé, mais sa source** (sensibilité et besoin de protection) peut également influer. La source de l'information est définie au sens de la présente instruction comme étant le ou les système(s) de renseignement ayant permis, à un degré quelconque, de produire une information. Le niveau de classification n'est pas attribué uniquement par référence au niveau donné aux informations du même domaine ;
- **tout ensemble comprenant une ou plusieurs informations ou supports protégés (dossier, document relié…) est classifié au minimum au niveau de celui de l'information ou du support de niveau le plus élevé qui y est contenu** ; un ensemble d'informations ou de supports peut par ailleurs être classifié si le regroupement des informations ou supports qui le composent l'exige, alors même qu'aucun de ses éléments n'est classifié ;
- tout extrait d'information ou de support protégé relève pour sa classification de la première règle énoncée ci-dessus : protection en raison de sa nature, et éventuellement de sa source.

Article 39

LES ATTRIBUTIONS DES AUTORITÉS

En vertu des dispositions du décret n° 98-608 du 17 juillet 1998, chaque ministre, pour le département dont il a la charge, détermine, dans les conditions fixées par le Premier ministre, les informations ou supports protégés qu'il y a lieu de classifier à l'un des trois niveaux, et les modalités d'organisation de leur protection pour les niveaux Secret-Défense et Confidentiel-Défense.

Conformément à ces dispositions, chaque ministre définit, pour ce qui relève de ses attributions, et dans les conditions fixées par la présente instruction :

a - les conditions d'emploi des niveaux de classification Secret-Défense et Confidentiel-Défense afin de :

- déterminer le champ d'application de chacun de ces deux niveaux et dresser la nomenclature des informations ou des catégories d'informations qui devront être couvertes par le secret de la défense nationale ;
- fixer les critères objectifs à prendre en compte pour apprécier le caractère secret de l'information (par exemple : importance dans l'organisation et la politique de la défense nationale, domaine concerné, nature de la source; etc …) ;
- préciser les autorités responsables de la classification.

b - les informations ou catégories d'informations protégées qui doivent être classifiées au niveau Très Secret-Défense :

- soit dans les classifications spéciales qui cloisonnent ce niveau ;
- soit dans une nouvelle catégorie à l'intérieur d'une des classifications spéciales existantes, ou dans une nouvelle classification spéciale, après demande exceptionnelle de création au Premier ministre.

Article 40

LA DURÉE DE VIE DES CLASSIFICATIONS

La sensibilité d'une information ou d'un support protégé au regard de la défense nationale évolue en fonction du temps ou des circonstances. Le niveau de classification qui lui a été initialement attribué peut donc être modifié (déclassement ou reclassement) ou supprimé (déclassification) pour maintenir un niveau de protection adapté et le cas échéant alléger les charges de travail et les coûts de gestion de la documentation.

L'article 4 du décret n° 98-608 du 17 juillet 1998 relatif à la protection des secrets de la défense nationale prévoit que les modifications ou suppressions des mentions de classification sont décidées par les autorités qui ont procédé à la classification. Seule l'autorité classificatrice (ou encore autorité émettrice) peut déclassifier ou déclasser un document à tout moment.

Toute décision de modification ou de suppression de classification doit être notifiée aux destinataires de l'information ou du support par l'autorité émettrice.

Il appartient à l'autorité classificatrice, chaque fois que possible, de **mentionner sur le document le délai** au terme duquel l'information ou le support sera déclassé au niveau inférieur, ou déclassifié. Elle peut aussi éventuellement préciser l'événement (début de production d'un matériel, retrait de service d'un matériel, fin d'un exercice, etc...) à l'issue duquel le document sera déclassé ou déclassifié.

La révision du niveau de protection des informations ou supports protégés doit être effectuée périodiquement.

A titre indicatif, une durée de **vingt ans** est conseillée pour les niveaux Secret-Défense et Confidentiel-Défense.

L'autorité émettrice conserve bien entendu la possibilité de prolonger à tout moment le délai de validité qu'elle a éventuellement fixé a priori à une classification. Sans indication de durée, les informations ou supports protégés seront déclassifiés après les délais suivants à compter de leur date d'émission :

- 30 ans pour le Confidentiel Défense
- 60 ans pour le Secret Défense et le Très Secret Défense

Article 41

LE VERSEMENT AUX ARCHIVES DES INFORMATIONS OU SUPPORTS PROTÉGÉS A L'EXPIRATION DE LEUR PÉRIODE D'UTILISATION COURANTE

La **loi n° 79-18 du 3 janvier 1979 relative aux archives prévoit** que les documents procédant de l'activité de l'État, des collectivités locales, des établissements et entreprises publics, de l'activité des organismes chargés de la gestion de services publics ou d'une mission de service public, font, **à l'expiration de leur période d'utilisation courante**, l'objet d'un **tri** pour séparer les documents à conserver et les documents dépourvus d'intérêt administratif et historique, destinés à l'élimination.

En ce qui concerne les informations ou supports protégés, ce tri doit être l'occasion de procéder, chaque fois que nécessaire, à la révision de leur niveau de classification.

Les dispositions suivantes s'appliquent aux informations ou supports protégés qui, à l'expiration de leur période d'utilisation courante, restent protégés :

1. Leur **destruction**

La destruction d'informations ou de supports protégés s'opère dans les conditions prévues aux articles 50, 64 et 68, et en conformité avec les dispositions de l'article 4 de la loi relative aux archives (en liaison avec l'administration des archives).

2. Leur **versement aux services d'archives**

Les services d'archives ne sont équipés et habilités que pour recevoir des informations ou supports protégés classifiés jusqu'au niveau Secret-Défense inclus. **Aucune information ni aucun support protégé classifié au niveau Très-Secret ne peut donc être versé à un service d'archives**. Pour faire l'objet d'une telle mesure, l'information ou le support doit préalablement être déclassé ou déclassifié.

En ce qui concerne la communication au public des informations ou supports protégés versés aux services d'archives, il convient de se référer aux dispositions de la loi n° 79-18 du 3 janvier 1979 (articles 6 et 7 notamment), de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal (articles 2 et 6), du **décret n° 79-1038 du 3 décembre 1979 relatif à la communicabilité des documents d'archives publiques** et du **décret n° 79-1035 du 3 décembre 1979 relatif aux archives de défense**. Au-delà d'un délai de trente ans pour les documents Confidentiel-Défense et de soixante ans pour les documents Secret-Défense à compter de la date d'émission du document, celui-ci devient, a priori, en application de la combinaison de ces dispositions, librement consultable. En deçà de ce délai, le statut du document reste déterminé par les règles relatives à la protection du secret de la défense nationale et à l'accès aux documents administratifs. L'autorité saisie d'une demande de communication d'archive classifiée doit s'interroger sur une éventuelle déclassification du document ; si sa classification est toujours justifiée, sa communication est refusée, sous réserve de la possibilité de dérogation prévue aux articles 2 du décret n° 79-1038 du 3 décembre 1979 et 7 du décret n° 79-1035 du 3 décembre 1979.

Article 42

LE MARQUAGE

En vertu de l'article 413-9 du code pénal, les renseignements, procédés, objets, documents, données informatisées ou fichiers acquièrent officiellement un caractère de secret de la défense nationale à partir du moment où ils font l'objet de "mesures de protection destinées à limiter leur diffusion".

Conformément aux dispositions de l'article 4 du décret du 17 juillet 1998, **la mention du niveau de classification**, par laquelle est matérialisée extérieurement la qualité de secret de la défense nationale, **doit être portée sur le support de l'information**.

Le marquage permet de vérifier **l'authenticité** et **l'intégrité** du support. Il comporte le **timbrage** et l'**identification du support**. Le timbre indiquant le niveau de classification a pour but, par sa position, sa taille et sa couleur, d'attirer immédiatement l'attention sur le caractère secret de l'information ou du support. L'identification est constituée par les références du support.

Article 43

LA REPRODUCTION D'INFORMATIONS OU SUPPORTS PROTÉGÉS

La généralisation des moyens de reproduction accroît les risques de diffusion incontrôlée des informations ou supports protégés.

Aussi, et sans préjudice des dispositions particulières prévues aux articles 50 pour les informations ou supports protégés classifiés au niveau Très Secret Défense et 57 pour les informations ou supports protégés classifiés au niveau Secret Défense, des consignes précises sont à établir, fixant :

- les autorités habilitées à accorder les autorisations de reproduction ;
- leur désignation par les directeurs ou chefs de service ;
- les procédures de contrôle de la reproduction ;
- la nécessité de consigner sur un système d'enregistrement le nombre et les détenteurs des pièces reproduites.

Article 44

L'ÉVACUATION D'URGENCE – LA DESTRUCTION D'URGENCE

Pour faire face à des circonstances exceptionnelles nécessitant l'évacuation des bâtiments par le personnel ou la destruction d'urgence des informations ou supports protégés, un **plan d'évacuation d'urgence** et un **plan de destruction d'urgence** sont établis par chaque service ou organisme détenteur d'informations ou supports protégés.

Les modalités d'exécution pratique de ces plans figurent sur des fiches disponibles en permanence dans chaque service ou organisme détenteur d'informations ou supports protégés. Elles précisent :

- *la liste des informations ou supports protégés à détruire ou à évacuer ;*
- *la localisation des informations ou supports protégés à détruire ou à évacuer ;*
- *les mesures applicables aux systèmes d'information ;*
- *la liste et la localisation des moyens de destruction et d'évacuation à utiliser ;*
- *les autorités qualifiées pour donner les ordres de destruction ou d'évacuation.*

Pour que ces plans puissent être exécutés rapidement et à tout moment, il est nécessaire de prévoir les conditions et modalités d'accès aux locaux ainsi qu'aux clefs et combinaisons des coffres, quels que soient le jour et l'heure.

Retour au sommaire

SECTION II

LES MESURES SPÉCIFIQUES A L'USAGE DES SYSTÈMES D'INFORMATION

Article 45

LES PRINCIPES DE L'USAGE DES SYSTÈMES D'INFORMATION

Les règles de gestion des informations ou supports protégés s'appliquent aussi quand cette information est traitée dans des systèmes d'information. Ces systèmes doivent donc permettre de marquer l'information, de garantir son authenticité, son intégrité, sa confidentialité, et sa disponibilité, de contrôler sa circulation, et d'assurer sa conservation et sa destruction.

Les systèmes d'information doivent donc être sécurisés conformément à une politique de sécurité définie en fonction du niveau de protection requis, en particulier du niveau de classification des informations traitées et sur la base d'une analyse des risques. Leur emploi doit faire l'objet d'une décision formalisée.

Le système d'information doit être conçu de telle sorte que tout utilisateur qui traite une information ou un support protégé ait le niveau d'habilitation requis pour le niveau de classification de l'information ou du support et le besoin reconnu d'en connaître.

Article 46

LA SÉCURISATION D'UN SYSTÈME D'INFORMATION

Les règles à respecter pour protéger les informations ou supports au sein des systèmes d'information, lors de leur transmission notamment dans le cadre d'interconnexions, sont précisées dans *l'instruction générale interministérielle n° 900/SGDN/DISSI/SCSSI/SSD/DR du 20 juillet 1993*, et dans les instructions, directives et guides qui la complètent.

Dans le cadre international, le déploiement de systèmes d'information présente des enjeux de sécurité particuliers pour ce qui est de la protection des informations étrangères et nationales classifiées de

défense et de la mise en œuvre de solutions de sécurité interopérables. Ces questions doivent être traitées conformément aux accords de sécurité ou règlements en vigueur.

Les dispositions réglementaires applicables aux marchés d'étude, de réalisation, de fourniture, d'exploitation, de maintenance et de soutien des systèmes d'information traitant des informations ou supports protégés classifiés au niveau Secret-Défense ou Confidentiel-Défense sont précisées dans *l'instruction interministérielle n° 2000/SGDN/SSD/DR*.

Les prestations d'audit de sécurité des systèmes d'information traitant d'informations ou supports protégés classifiés au niveau Secret-Défense et Très Secret-Défense ne peuvent être confiées qu'à des personnels de l'administration dûment habilités.

Article 47

L'HOMOLOGATION DE SÉCURITÉ

Face à la complexité croissante et au niveau d'intégration et d'interconnexion élevé des systèmes d'information, il est nécessaire de mettre en œuvre une **gestion globale des risques de sécurité** pour l'ensemble du système d'information tout au long de son cycle de vie et impliquant les différents acteurs concernés. Une telle approche, dite « **démarche d'homologation de sécurité** » doit permettre d'identifier, d'atteindre puis de maintenir un niveau de risques de sécurité acceptable pour le système d'information considéré, compte tenu du niveau de protection requis.

Tout système d'information traitant des informations ou supports protégés doit faire l'objet d'une homologation, consistant en la déclaration par une autorité dite d'homologation, que le système d'information considéré est apte à traiter des informations ou supports protégés du niveau de classification retenu conformément aux objectifs de sécurité visés, et qu'elle accepte les risques de sécurité résiduels induits. Cette homologation de sécurité doit tenir compte des opérations de maintenance ou de télégestion du système d'information, en particulier lorsqu'elles relèvent de prestataires externes.

Chaque ministre définit, pour ce qui relève de ses attributions, la procédure de désignation de cette autorité d'homologation. Dans le cas de systèmes relevant de plusieurs ministères, l'autorité d'homologation peut être confiée à une autorité unique, interministérielle ou ministérielle, ou être déclarée conjointe. Dans un cadre international, l'autorité d'homologation de systèmes mis à disposition ou relevant de plusieurs autorités nationales sera désignée conformément aux accords de sécurité ou règlements en vigueur.

L'autorité d'homologation est chargée d'approuver la démarche d'homologation, les objectifs et la cible de sécurité ainsi que la politique de sécurité du système d'information.

Elle prononce l'homologation de sécurité du système d'information, en prenant en compte notamment que le système met en oeuvre des produits agréés (au sens de l'IGI 900) par le SGDN (DCSSI), fixe les conditions de maintien de l'homologation de sécurité au cours du cycle de vie du système d'information, et contrôle que le système opère effectivement selon les conditions qu'elle a approuvées, en particulier dans le maintien en conditions opérationnelles du système[8].

L'autorité d'homologation peut s'appuyer sur une commission d'homologation, dont elle fixe la composition et à laquelle elle peut inviter le SGDN à être représenté. La désignation de ces membres sera subordonnée à leur habilitation préalable au niveau nécessaire.

L'autorité d'homologation veille à ce que tous les acteurs concourant à la sécurisation du système d'information soient identifiés, désignés et habilités.

[8] Y compris les parties éventuellement assurées par des prestataires externes.

Article 48

LA DÉCISION D'EMPLOI D'UN SYSTÈME D'INFORMATION

Tout système d'information traitant des informations classifiées doit faire l'objet d'une décision d'emploi formelle. Cette décision d'emploi s'appuie sur l'homologation de sécurité du système d'information, et doit en respecter les conditions.

La décision d'emploi est prise par l'autorité responsable de l'utilisation du système d'information ; cette autorité peut être l'autorité d'homologation.

Lorsque l'urgence opérationnelle le requiert, l'homologation de sécurité pourra être prononcée postérieurement à la décision d'emploi. La décision d'emploi sera alors dite provisoire.

Retour au sommaire

CHAPITRE II

LES RÈGLES DE PROTECTION DES INFORMATIONS OU SUPPORTS PROTÉGÉS

SECTION I

LES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU TRÈS SECRET-DÉFENSE

Article 49

L'ORGANISATION DES RÉSEAUX DE SÉCURITÉ TRÈS SECRET-DÉFENSE

L'article 5 du décret n° 98-608 du 17 juillet 1998 relatif à la protection des secrets de la défense nationale stipule que : *« … Pour les informations ou supports protégés classifiés au niveau Très Secret-Défense, le Premier ministre définit les classifications spéciales dont ils font l'objet et qui correspondent aux différentes priorités gouvernementales".*

La protection de ces informations ou supports est organisée dans le cadre de la **réglementation particulière des classifications spéciales Très Secret-Défense**[9], qui complète les dispositions de caractère général de la présente instruction.

Aucun service ou organisme ne peut élaborer, traiter, stocker, acheminer, présenter ou détruire des informations ou supports protégés classifiés Très Secret-Défense, sans y avoir préalablement été autorisé par le Premier ministre (SGDN) sur proposition du ministre intéressé. Il doit **impérativement disposer d'une antenne d'utilisation** de la classification spéciale correspondante. Par application du principe de cloisonnement de l'information, des antennes distinctes sont prévues pour chacune des classifications spéciales. La décision de création de l'antenne est prise par le SGDN.

L'antenne d'utilisation est placée sous l'autorité d'un responsable choisi parmi les personnels d'autorité admis à la classification spéciale. Un **agent de sécurité** a pour mission d'appliquer les mesures de sécurité à l'intérieur de l'antenne, de veiller au respect des règles relatives à la protection des personnes et d'assurer la protection physique des informations classifiées.

---

[9] Directives d'application pratique N° 02 /SGDN/SSD/CD du 3 février 1986 sur l'organisation et le fonctionnement des classifications spéciales Très Secret-Défense.

La circulation des informations et supports protégés classifiés au niveau Très-Secret Défense emprunte obligatoirement, **entre ses différentes antennes d'utilisation,** le **réseau de sécurité constitué pour la protection de chaque classification spéciale.** Un **agent central de sécurité**, désigné par le Premier ministre (SGDN), exerce le contrôle centralisé de cette circulation.

Article 50

LA PROTECTION DES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU TRÈS SECRET-DÉFENSE

Les modalités de protection des informations ou supports protégés classifiés au niveau Très-Secret Défense sont déterminées par des instructions particulières, propres à chacune des classifications spéciales. **La reproduction totale ou partielle des informations ou supports protégés classifiés Très Secret-Défense est formellement interdite**. Ces informations ou supports ne peuvent être élaborés, reproduits, préparés en vue de leur circulation, conservés, archivés, ou détruits que dans les zones réservées comme définies à l'article 77 ci-après.

Retour au sommaire

SECTION II

LES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU SECRET-DÉFENSE

Article 51

LE BUREAU SECRET-DÉFENSE

Chaque ministre veille à l'installation (à l'échelon qu'il convient) **d'un ou de plusieurs bureaux Secret-Défense** au sein desquels s'effectuent l'élaboration, le traitement, le marquage, le stockage et le suivi de la destruction des informations ou supports protégés classifiés au niveau Secret-Défense.

Le bureau Secret-Défense est par ailleurs responsable de l'enregistrement, de l'expédition, de la réception et de la circulation des supports protégés classifiés au niveau Secret-Défense, à l'exclusion de ceux comportant la mention ACSSI[10]. Il a pour mission d'effectuer les formalités de contrôle et de sécurité de ces supports, qui ne peuvent transiter que par son intermédiaire. Il en dresse l'inventaire annuel.

Ce bureau doit être **situé en zone réservée définie à l'article 77 ci-après**, et composé exclusivement de personnes habilitées au niveau Secret-Défense.

Article 52

L'ÉLABORATION DES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU SECRET-DÉFENSE

Les **supports préparatoires** ayant servi à l'élaboration de l'information Secret-Défense (brouillons, impressions sur papier, disquettes…) doivent être détruits le plus rapidement possible et, en tout état de cause, au plus tard lorsque le support classifié est émis.

Article 53

[10] Instruction interministérielle n° 910 /SGDN/DISSI/SCSSI/SSD/DR du 19 décembre 1994 sur les articles contrôlés de la sécurité des systèmes d'information.

L'ENREGISTREMENT DES SUPPORTS D'INFORMATIONS PROTÉGÉES CLASSIFIÉES AU NIVEAU SECRET-DÉFENSE

Tout support contenant des informations protégées classifiées au niveau Secret-Défense est enregistré, dans l'ordre chronologique, par un système d'enregistrement (registre spécifique Secret-Défense coté et paraphé ou enregistrement de façon informatisée). Le nom des destinataires de l'information ou du support classifié est porté sur le système d'enregistrement.

L'enregistrement doit établir sans ambiguïté l'attribution du support à un détenteur/personne physique clairement identifié. Ce détenteur assume alors la responsabilité de sa protection. Cet enregistrement est la seule référence de l'attribution de la responsabilité.

Article 54

LE MARQUAGE DES SUPPORTS PAPIER D'INFORMATIONS PROTÉGÉES CLASSIFIÉES AU NIVEAU SECRET-DÉFENSE

Conformément aux dispositions de l'article 4 du décret n° 98-608 du 17 juillet 1998, chaque exemplaire d'un document classifié au niveau Secret-Défense porte la mention du niveau de classification des informations qu'il contient. Les paragraphes, alinéas, annexes, traitant d'informations qui ne relèvent pas du niveau Secret-Défense, sont, éventuellement, mis en évidence par la mention, dans la marge, de leur propre niveau de classification et par une mise en page qui les détache sans ambiguïté du contexte général du document. Une mention de déclassement ou de déclassification à terme est apposée le cas échéant (Mle 16/IGI 1300).

Le marquage des supports papier d'informations protégées classifiées au niveau Secret Défense comporte, outre la mention du niveau de classification (timbrage), des mentions d'identification et de pagination.

I. Timbrage.

Le timbre Secret-Défense est apposé avec une encre de couleur rouge au milieu du haut et du bas de chaque page. Pour les documents reliés, le timbre de même libellé et d'un modèle de dimensions supérieures est placé au milieu du bas de la couverture et de la page de garde (Mle 15/IGI 1300).

II. Identification.

Tout document classifié au niveau Secret-Défense est identifié dès sa première page, outre les références normales de toute pièce administrative (service émetteur et date) par :

- un numéro individualisant chaque exemplaire et faisant par ailleurs apparaître le nombre total d'exemplaires ;
- un numéro d'enregistrement émanant du bureau Secret-Défense compétent.

III. Pagination.

Chaque page du document est numérotée. Au bas de la première page est mentionné le nombre de pages, d'annexes ou de plans qui composent le document. Chaque annexe est également paginée et porte mention de son propre nombre de pages. Les pages blanches et les feuilles intercalaires doivent être numérotées et porter en leur centre la mention «PAS DE TEXTE».

Article 55

LE MARQUAGE DES AUTRES SUPPORTS D'INFORMATIONS PROTÉGÉES CLASSIFIÉES AU NIVEAU SECRET-DÉFENSE

Chaque support (non papier) d'informations protégées classifiées au niveau Secret-Défense ou chaque support classifié à ce niveau reçoit un **marquage adapté** au type de support, **définitif** et **toujours visible**. Ce marquage comporte le timbrage et l'identification.

I. Timbrage.

Le timbre spécifiant le niveau de classification peut avoir des dimensions adaptées à celles du support, mais il comporte l'indication de ce niveau en toutes lettres. Ces lettres sont de couleur rouge ou contrastant avec la couleur du support.

II. Identification.

En ce qui concerne les supports (non papier) d'informations protégées classifiées au niveau Secret-Défense, leur identification est assurée par l'inscription des références et, éventuellement, du volume de chacune des informations enregistrées. Lorsqu'il est impossible d'inscrire sur le support l'ensemble des références, celui-ci est identifié par son numéro d'enregistrement, délivré par le bureau Secret-Défense et, est éventuellement accompagné d'une fiche où sont inscrites les références réglementaires des informations contenues.

En raison de la possibilité technique de lire des informations théoriquement effacées, **un support** (non papier) d'informations protégées classifiées **conserve toujours le niveau de classification qui lui a été initialement attribué**. Il ne peut être déclassé ou déclassifié que dans le cas où les informations qu'il contient ou qu'il a contenues ont fait elles-mêmes l'objet de ce déclassement ou de cette déclassification.

Article 56

LA DIFFUSION DES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU SECRET-DÉFENSE

L'autorité qui doit diffuser des informations ou supports protégés classifiés au niveau Secret Défense en établit la **liste de diffusion**. Sur cette liste sont portés le nombre et le numéro des supports attribués à chaque destinataire ainsi que le numéro des exemplaires gardés par le service émetteur (deux au moins, dont un original destiné, à terme, aux archives).

La liste des destinataires, lorsqu'elle constitue en elle-même un secret de la défense nationale, n'est pas jointe à l'envoi de chacun des exemplaires de support.

Article 57

LA REPRODUCTION TOTALE D'INFORMATIONS OU DE SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU SECRET-DÉFENSE

Sans autorisation préalable de l'autorité émettrice, la reproduction totale d'informations ou de supports protégés classifiés au niveau Secret-Défense n'est possible qu'en cas d'urgence exceptionnelle. En dehors de ce cas d'urgence exceptionnelle, le dépositaire de l'information ou du support protégé classifié au niveau Secret-Défense adresse une demande motivée de reproduction à l'autorité ayant classifié. Si celle-ci accorde l'autorisation, elle doit spécifier les numéros à attribuer aux exemplaires supplémentaires et porter mention de cette reproduction sur l'exemplaire en sa possession.

En cas d'urgence exceptionnelle, le dépositaire peut s'affranchir de la procédure normale en prenant les dispositions suivantes :

- limiter au minimum indispensable le nombre des reproductions ;
- procéder au marquage réglementaire en attribuant à chaque exemplaire reproduit un numéro individuel composé de deux nombres fractionnaires :
  - le premier ayant en numérateur le numéro d'ordre de la copie dans la série des reproductions et en dénominateur le nombre total de reproductions ;
  - le deuxième étant le numéro individuel fractionnaire de l'exemplaire attribué par l'autorité émettrice du document.
- porter si nécessaire, sur l'exemplaire reproduit, la destination qui en est faite ou établir une liste séparée des destinataires ;
- rendre compte immédiatement à l'autorité en charge de la classification du nombre de reproductions, des numéros de reproductions, et de la destination des exemplaires. Celle-ci, après avoir accordé éventuellement l'autorisation (Mle 12/IGI 1300), porte mention de cette reproduction sur l'exemplaire en sa possession.

Article 58

LA REPRODUCTION
D'EXTRAITS DE DOCUMENTS DE SUPPORTS OU DE FICHIERS CONTENANT DES INFORMATIONS PROTÉGÉES CLASSIFIÉES AU NIVEAU SECRET-DÉFENSE

Les extraits de documents ou de supports contenant des informations classifiées au niveau Secret Défense sont classifiés au niveau approprié à leur contenu. S'ils ne justifient pas une classification, leur importance doit rester limitée de façon à ne pas compromettre, en cas de divulgation, l'information dont ils ont été extraits. La diffusion séquentielle d'extraits non classifiés par découpage de l'information classifiée est interdite.

Le dépositaire de documents ou de fichiers contenant des informations classifiées au niveau Secret Défense peut en reproduire des extraits en procédant comme indiqué à l'alinéa précédent.

Lors du transfert d'extraits de documents ou de fichiers contenant des informations classifiées au niveau Secret Défense sur un autre support, et dans l'hypothèse où ces extraits sont classifiés, le marquage est reporté sur le nouveau support selon les modalités précisées à l'article 54 ou 55.

Article 59

L'EXPÉDITION ET LA RÉCEPTION
DES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS SECRET-DÉFENSE

Les bureaux Secret-Défense compétents procèdent, après **marquage** et **enregistrement** de chaque support, aux opérations suivantes :

I.Modalités d'expédition :

- emploi d'un **bordereau d'envoi**, sans timbre de classification ni indication de l'objet des informations envoyées, portant le numéro de l'enveloppe de sécurité intérieure, et comprenant trois feuillets détachables A, B et B' (respectivement Mle 14, 14 bis et 14 ter/IGI 1300) signés par le chef du bureau Secret-Défense ou par ses représentants désignés :
  - les feuillets A et B sont adressés au destinataire, qui conserve le premier à titre d'élément de preuve et renvoie le deuxième à l'expéditeur, à titre d'accusé de réception ;
  - le feuillet B', de couleur différente, est conservé par l'expéditeur jusqu'à réception du feuillet B, qui lui est alors substitué ;

- **conditionnement** : tout support d'informations classifiées au niveau Secret-Défense ou tout support classifié à ce niveau est transmis sous double enveloppe, présentant des **conditions de solidité et de sécurité** de nature à assurer au maximum son intégrité physique :

- l'enveloppe extérieure, plastifiée et numérotée, porte l'indication du service expéditeur, l'adresse du service destinataire (sans mention trop explicite de nature à attirer l'attention sur le caractère protégé du contenu) et la mention du suivi ;

- l'enveloppe intérieure de sécurité de bonne qualité, si possible du modèle « toilé »ou « armé », interdisant son ouverture et sa refermeture discrètes, opaque et de dimensions adaptées, contient les feuillets A et B du bordereau d'envoi, porte le timbre "Secret-Défense", les références des supports transmis, le cachet de l'autorité d'origine, le nom et la fonction du destinataire, et l'indication du service ou de l'organisme où il est affecté.

II. Formalités de réception :

- **vérification de l'intégrité** de l'emballage, pour déceler une éventuelle compromission ;
- **enregistrement** conformément aux dispositions de l'article 53 ;
- **transmission par le bureau Secret-Défense au destinataire ;**
- **signature** et **renvoi** au bureau secret défense de l'autorité origine du **bordereau d'envoi** feuillet B, à titre d'accusé de réception.

Article 60

L'ACHEMINEMENT DES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU SECRET-DÉFENSE SUR LE TERRITOIRE NATIONAL

I. A l'intérieur d'un même immeuble.

Les informations ou supports protégés classifiés au niveau Secret-Défense sont acheminés **sur place** par le détenteur lui-même avec un compte rendu au **Bureau Secret-Défense**. Dans l'intérêt du service et sous réserve que la position des supports soit suivie sans discontinuité, cette règle peut être assouplie pour une **communication brève et temporaire, avec prise en compte**. Le détenteur des supports classifiés, responsable de leur acheminement, doit en contrôler la position et les faire réintégrer dès que les nécessités du service le permettent.

II. Avec changement d'immeuble et[/ou] de zone géographique [11]

L'acheminement peut s'opérer :

- par convoyeur autorisé ou toute personne habilitée au niveau Secret-Défense : les informations ou supports protégés sont placés dans une sacoche ou une valise fermant à clef, dépourvue d'indication extérieure ; le porteur ne peut en aucun cas s'en dessaisir jusqu'à la remise au bureau Secret-Défense du destinataire des informations ou supports protégés ;

- par voie postale militaire : dans les conditions fixées par les instructions du ministre de la défense ;

- par voie postale civile : sur le territoire national, à défaut de convoyeur et en cas d'urgence l'acheminement par voie postale est autorisé en ayant obligatoirement recours aux moyens protégés de la poste : envoi en pli chargé avec valeur déclarée. Le **bureau Secret-Défense** s'assure de la date et de l'heure prévues de livraison et en avise aussitôt le bureau Secret-Défense destinataire par télécopie banalisée, en indiquant le bureau de dépôt du courrier et les références des supports, à l'exclusion de leur objet et de leur caractère secret. Au reçu du courrier, le bureau Secret-Défense destinataire en accuse immédiatement réception. En cas de retard anormal, le bureau Secret-Défense destinataire met en œuvre les dispositions de l'article 88.

[11] A déterminer par le responsable de sécurité en fonction du niveau de protection des lieux.

Article 61

L'ACHEMINEMENT DES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU SECRET-DÉFENSE VERS L'ÉTRANGER

Les informations ou supports protégés classifiés au niveau Secret-Défense, envoyés à l'étranger ou transitant par des pays étrangers, doivent être protégés pour interdire en permanence leur compromission pendant toute la durée du transport, et notamment lors des escales. **Seuls les moyens suivants sont autorisés :**
Courrier militaire spécialisé – valise diplomatique – lettre de courrier

Les informations ou supports protégés **classifiés** au niveau **Secret-Défense** sont normalement acheminés par **valise diplomatique**, ou éventuellement par **courrier militaire spécialisé** ; pour les organismes militaires, le service convoyant est le BCAC (bureau du courrier de l'administration centrale). En cas d'urgence exceptionnelle, il est possible, sous certaines conditions, de bénéficier en dehors de la valise diplomatique d'une «lettre de courrier» délivrée par le ministère des Affaires étrangères (service de la valise).

Lors de la remise des envois, au plus tard la veille du départ de la valise, à la sous-direction du courrier et de la valise diplomatique du ministère des Affaires étrangères, un cachet apparent doit être apposé sur l'enveloppe extérieure ou sur une étiquette fixée au colis et comportant obligatoirement la mention **«Par valise accompagnée - sacoche»**.

Le **transport** est **obligatoirement assuré** par un **convoyeur autorisé** ou par une **personne habilitée** sous réserve que la «sacoche» ne dépasse pas 20 kilogrammes. Sinon, il y a lieu de prévoir des mesures particulières en fonction des instructions du département des Affaires étrangères. Une «lettre de courrier» accrédite sa qualité afin d'éviter l'examen du courrier par la douane ou le service de police compétent.

La **Convention de Vienne du 18 avril 1961 sur les relations diplomatiques** interdit toute mise en demeure par les autorités étrangères de leur soumettre le courrier, et stipule que «la valise diplomatique ne doit être ni ouverte, ni retenue». Le convoyeur doit seulement présenter sa «lettre de courrier» et faire appel, en cas de besoin, à l'assistance de l'agent diplomatique ou consulaire le plus proche. Si toutefois les autorités compétentes de l'État d'accueil demandent que la valise soit ouverte en leur présence, le convoyeur est en droit d'opposer un refus et de repartir avec la valise vers l'État d'origine.

Certificats de courrier : pour un seul ou plusieurs voyages

Pour les programmes en coopération, l'acheminement est possible par convoyeur autorisé, dans les conditions fixées à l'article 59. Le convoyeur est alors muni d'un certificat de courrier pour un seul ou plusieurs voyages (Mle 09/IGI/1300 et Mle 09bis/IGI/1300) délivré par les autorités de sécurité désignées (ASD).

Article 62

LA CONSERVATION DES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU SECRET-DÉFENSE

La responsabilité de la conservation des informations ou supports protégés classifiés Secret-Défense incombe à un détenteur responsable ou au chef du bureau Secret-Défense.

Les informations ou supports protégés classifiés au niveau Secret-Défense sont, en dehors des périodes d'utilisation, conservés dans des **coffres-forts** ou des **armoires fortes à combinaisons multiples**, si possible équipés d'un système d'alarme ou d'un compteur d'ouverture. Aucune indication quant à la nature des informations n'est visible à l'extérieur de l'armoire ou du coffre.

La combinaison des coffres-forts, suffisamment complexe pour être fiable, n'est connue que des seuls utilisateurs. Une copie de cette combinaison est conservée sous enveloppe opaque, fermée, dans le coffre-fort d'une autorité spécialement désignée, la clef correspondante étant placée dans un coffre distinct. **Les combinaisons sont changées au moins tous les six mois**, lors des mutations des personnels utilisateurs, et en cas de risque ou de présomption de compromission.

Les clefs sont impérativement mises en sécurité, notamment en dehors des heures ouvrables, suivant une procédure clairement définie par chaque autorité responsable (dépôt dans un coffre mural, sans clef, à combinaisons et à commande unique ou avec ouverture par lecteur de badge ; garde permanente avec système d'alarme). Il est formellement interdit d'emporter à l'extérieur des lieux de travail :

- des informations ou supports protégés classifiés au niveau Secret-Défense, sauf nécessités impérieuses de service ;
- les clefs des coffres ou armoires où sont conservés ces informations ou supports protégés.

Article 63

L'INVENTAIRE DES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU SECRET-DÉFENSE

Chaque ministre veille à faire procéder, **une fois par an** (courant décembre), à l'inventaire des informations ou supports protégés classifiés au niveau Secret-Défense détenus dans l'ensemble des services et organismes relevant de son département ministériel par les bureaux Secret-Défense afin de contrôler leur conservation et de s'assurer de leur présence non seulement comptable mais physique. Ces inventaires doivent être adressés au SGDN, par le HFD, au plus tard le 31mars de chaque année.

Le procès-verbal d'inventaire annuel dressé par chaque bureau Secret-Défense mentionne les références et l'identification de chaque support classifié Secret-Défense, et est accompagné, le cas échéant[14], de l'une ou l'autre des pièces administratives suivantes :

- un récépissé du nouveau détenteur ;
- un procès-verbal de destruction ;
- un procès-verbal de versement à un dépôt d'archives.

Un support classifié Secret-Défense est considéré comme inventorié, si le bureau secret défense s'est assuré que le destinataire initial est en mesure de le présenter ou, à défaut, de produire une des pièces justificatives énoncées ci-dessus. Le procès-verbal d'inventaire annuel est adressé aussitôt au HFD compétent. Il est présenté à l'occasion de toute inspection ou contrôle.

Les systèmes d'enregistrement de courrier départ et arrivée ne peuvent pas tenir lieu d'inventaire.

Un inventaire est effectué contradictoirement lors de toute mutation de personnel, chacun des détenteurs successifs - sortant et arrivant - apposant sa signature sur le procès-verbal d'inventaire.

La période d'inventaire est mise à profit pour alléger la gestion. Les dates de péremption sont vérifiées aux fins de déclassement ou de déclassification, la révision du niveau de protection des informations ou supports protégés et leur destruction, le cas échéant, doivent être réalisées.

[14] Ces pièces ne seront jointes à l'inventaire que si elles concernent des mouvements de documents ayant eu lieu depuis la production du procès-verbal d'inventaire de l'année précédente.

Article 64

LA DESTRUCTION DES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU SECRET-DÉFENSE

La destruction des informations ou supports protégés classifiés au niveau Secret-Défense, lorsqu'ils sont dépourvus d'indication de durée de vie et sont jugés périmés ou inutiles, peut être réalisée selon la procédure suivante :

L'autorité détentrice informe par écrit l'autorité émettrice en charge de sa classification que, sauf avis contraire de sa part, elle procèdera à la destruction du support. Sans réponse dans les deux mois, l'autorité détentrice, avec accord préalable de l'administration des archives procède à la destruction du support et en rend compte à l'autorité émettrice (en cas de dissolution du service dont relevait l'autorité ayant procédé à la classification, il convient de s'adresser au HFD du ministre compétent), en lui adressant copie du procès-verbal de destruction (Mle 13/IGI 1300).

La destruction des supports est réalisée par des **personnes habilitées** et une copie du procès-verbal de destruction est adressée au bureau Secret-Défense. Elle est effectuée dans des conditions telles qu'elle interdise toute reconstitution même partielle des informations contenues sur les supports. Outre le papier, les principaux supports d'information sont notamment de type magnétique, électronique, optique ou mécanographique. Les techniques de destruction sont choisies en fonction du type et du nombre de supports à détruire. Les principales sont : le brûlage, l'incinération, le broyage, le déchiquetage et la surtension électrique.

Les procès-verbaux de destruction portent la signature de l'autorité détentrice et celle d'un témoin qualifié. Les supports préparatoires devenus sans objet sont détruits sans formalité particulière.

Retour au sommaire

SECTION III

LES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU CONFIDENTIEL-DÉFENSE

Article 65

L'ÉLABORATION, LE MARQUAGE ET L'ENREGISTREMENT

Les informations ou supports protégés classifiés au niveau Confidentiel-Défense ne peuvent être traités que par des personnes habilitées au niveau requis, et dans des locaux sécurisés présentant les garanties de sécurité suffisantes pour éviter toute divulgation.

Les supports papier d'informations protégées classifiées au niveau Confidentiel-Défense, y compris leurs annexes, portent le marquage suivant :

- **sur la première page, les références** : service émetteur, date d'émission, **le numéro d'enregistrement et le timbre** Confidentiel-Défense avec, le cas échéant, la date de déclassification à terme ;
- **sur chaque page, le timbre Confidentiel-Défense** apposé avec une encre de couleur rouge au milieu du haut et du bas de chaque page ;
- **pour les dossiers reliés**, le timbre Confidentiel-Défense, placé au milieu du bas de la couverture et de la page de garde (Mle 15/IGI 1300).

Le marquage des supports autres que le papier et contenant des informations protégées classifiées Confidentiel-Défense est effectué conformément aux prescriptions de l'article 55.

L'enregistrement des informations ou supports protégés classifiés au niveau Confidentiel-Défense est réalisé sur un système d'enregistrement (registre spécifique Confidentiel Défense coté et paraphé ou enregistrement de façon informatisée) pour apporter la preuve de l'attribution d'un document à un détenteur responsable.

Article 66

L'EXPÉDITION ET LA RÉCEPTION DES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU CONFIDENTIEL-DÉFENSE

L'expédition a lieu selon un conditionnement réalisé sous **double enveloppe**, l'emballage présentant des **conditions de solidité** de nature à assurer son intégrité physique.

- emploi du type de bordereau d'envoi, à trois feuillets A, B, B', défini à l'article 59 ;
- enveloppe extérieure portant l'indication du service expéditeur, l'adresse du service destinataire (sans mention trop explicite de nature à attirer l'attention sur le caractère protégé du contenu) et la mention du suivi ;
- enveloppe intérieure de bonne qualité, opaque et de dimensions adaptées contenant les feuillets A et B du bordereau d'envoi, portant le timbre "Confidentiel-Défense", les références des supports transmis, le cachet de l'autorité d'origine, le nom et la fonction du destinataire, et l'indication de l'organisme où il est affecté.

Les formalités de réception, identiques à celles prévues à l'article 59, sont assurées par le destinataire.

Article 67

L'ACHEMINEMENT DES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU CONFIDENTIEL-DÉFENSE

Les supports classifiés Confidentiel-Défense sont transmis selon des procédés assurant la meilleure protection dans les délais compatibles avec le degré d'urgence et de la façon suivante :

a - sur le territoire national :

- à l'intérieur d'un même immeuble : par une personne habilitée ou, sous enveloppe, par un convoyeur autorisé, ou une personne du service de courrier interne autorisée ;
- avec changement d'immeuble et de zone géographique : sous double enveloppe en « recommandé » ou en « pli chargé » par appel à la Poste ou en ayant recours à des opérateurs postaux dûment habilités proposant des moyens de transport protégés, soit par voie postale militaire, soit par convoyeur autorisé.

b - vers les pays de l'Union européenne :

- par voie postale en **«service prioritaire recommandé international»** ;
- par convoyeur autorisé dans les conditions fixées à l'article 61, alinéa 4 ;
- par valise diplomatique ;
- par certificat de courrier pour les programmes en coopération.

c - vers l'étranger, hors des pays de l'Union européenne :

- par valise diplomatique ou, éventuellement, par courrier militaire spécialisé selon les conditions d'acheminement précisées à l'article 61 ;
- par certificat de courrier pour les programmes en coopération.

Article 68

LA CONSERVATION, LA DESTRUCTION ET LA REPRODUCTION DES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU CONFIDENTIEL-DÉFENSE

Les informations ou supports protégés classifiés au niveau Confidentiel-Défense sont conservés dans des **armoires fortes**.

Leur destruction, est mentionnée sur leur système d'enregistrement. Le matériel consommable (brouillons, etc ...) ayant servi à l'élaboration des informations ou supports protégés est détruit dès qu'il devient sans objet.

La reproduction des informations ou supports protégés classifiés Confidentiel-Défense peut être effectuée, par les autorités destinataires sous leur responsabilité et à condition de conserver sur un système d'enregistrement la **trace du nombre et des destinataires** des exemplaires reproduits, dans les conditions prévues à l'article 43.

Retour au sommaire

SECTION IV

LES INFORMATIONS «SPÉCIAL FRANCE»[13]

Article 69

LA DÉTERMINATION ET LE MARQUAGE

La **mention Spécial France** est employée pour des informations ou supports protégés ou non que l'autorité émettrice estime ne devoir être communiquées qu'aux nationaux français (justifiant bien entendu du besoin d'en connaître et, le cas échéant, de l'habilitation au niveau de classification des informations ou supports protégés). **Elle n'est pas une mention de classification.**

Cette mention signifie que les États étrangers et leurs ressortissants ne sauraient en aucun cas justifier du besoin de connaître ces informations et que celles-ci ne peuvent **en aucun cas** leur être communiquées totalement ou partiellement.

Le **timbre "Spécial France"** de **couleur bleue** est apposé en haut de page, immédiatement à droite ou au dessous du timbre de classification de l'information et, pour les supports non papier, conformément aux dispositions de l'article 55.

Article 70

LES MESURES DE SÉCURITÉ

Les mesures de sécurité à leur appliquer sont celles prescrites par le niveau de classification qui y est apposé. Leur acheminement est réalisé par des voies nationales ; si nécessaire, la mention Spécial France est indiquée sur l'enveloppe intérieure.

Ces informations ne sont jamais mentionnées sur les inventaires ou répertoires prescrits par les accords de sécurité ou règlements de sécurité relatifs aux accords internationaux.

[13] Instruction sur la protection des informations réservées à l'usage national n°507/SGDN/SSD du 15 mars 1972

Retour au sommaire

CHAPITRE III

LA PROTECTION DES SUPPORTS (MATÉRIELS) PROTÉGÉS ET DES ARCHIVES CLASSIFIÉES

———————

SECTION I

LA PROTECTION DES SUPPORTS (MATÉRIELS) PROTÉGÉS

Article 71

DISPOSITIONS GÉNÉRALES ET CLASSIFICATIONS

La protection des supports (matériels) protégés implique la mise en œuvre de **mesures de sécurité à tous les stades de la réalisation** (programmes, études, plans, fabrications ou constructions, essais etc…) de même que pour l'utilisation, l'entretien, la réparation et le transport jusqu'à leur mise hors service et destruction.

L'autorité responsable (directeur de programme lors de la fabrication, ou autorité détentrice lors de l'utilisation) détermine ce qui est à protéger et le niveau de classification retenu, qui peut être différent de celui couvrant les documents (notices, plans etc .) qui les concernent.

Il importe d'**éliminer toute possibilité de vues terrestres ou aériennes et l'utilisation de procédés techniques de détection ou d'identification**. L'un des moyens les plus efficaces pour assurer la protection des supports (matériels) protégés classifiés au niveau Secret Défense consiste à les entreposer dans une **«zone réservée»**. Cette zone doit être érigée en «zone protégée» afin de pouvoir sanctionner pénalement le non-respect de l'interdiction d'y pénétrer.

Article 72

LA PROTECTION DES SUPPORTS (MATÉRIELS) PROTÉGÉS HORS D'UNE ZONE PROTÉGÉE.

Les autorités responsables font prendre des mesures de protection adaptées pour les supports protégés et leurs éléments constitutifs, lorsqu'ils sont en service ou exposés aux vues.

Quand les matériels sont associés à des installations intéressant divers secteurs d'activité et classés points sensibles, les autorités responsables des points sensibles appliquent les dispositions en vigueur[16].

Article 73

LA PROTECTION DES SUPPORTS (MATÉRIELS) PROTÉGÉS EN COURS DE TRANSPORT

La **circulation et le transport** des supports (matériels) protégés nécessitent **des mesures particulières** de sécurité : protection contre les vues dans la mesure du possible et garde permanente pendant la durée de l'acheminement.

Les itinéraires sont choisis en fonction du degré de sécurité qu'ils présentent. Suivant le type de matériels à protéger et dès lors qu'ils figurent sur la liste tenue à jour par le ministre de la défense, il convient de se reporter aux dispositions particulières.[17] [18]

---

[16] Instruction interministérielle générale n° 4600/SGDN/MPS/SPRS/DR du 8 février 1993 sur la sécurité des points et réseaux sensibles.

[17] Instruction interministérielle N° 3100 /SGDN/ACD/PS/DR du 25 juin 1980 sur la sécurité des transports de certains matériels sensibles effectués sous responsabilité civile.

[18] Directive interministérielle N° 312/SGDN/ANS/DR du 21 août 1981 sur la sécurité nucléaire dans le domaine de la défense.

Pour les matériels relevant de l'instruction interministérielle objet du renvoi 16, les règles de responsabilité sont fixées par les articles 4 et 5 de cette instruction.

Pour les autres matériels ou équipements classifiés, l'autorité en ayant prescrit le mouvement assume la responsabilité des points suivants :

- mise en condition des matériels ;
- choix de l'itinéraire et des lieux d'étape, en accord avec les autorités civiles ou militaires intéressées ;
- organisation du convoyage ou de l'escorte et des dispositions techniques en cas de panne ou d'accident.

Le transport des supports protégés est effectué, sauf impossibilité absolue, **sous pavillon national**. Sinon, il doit être convoyé et toutes dispositions prises pour que la sécurité soit assurée sans discontinuité pendant toute la durée du transport.

Retour au sommaire

SECTION II

LA PROTECTION DES ARCHIVES PROTÉGÉES DE LA DÉFENSE NATIONALE

Article 74

LES PRINCIPES GÉNÉRAUX DE L'ARCHIVAGE

La **loi n° 79-18 du 3 janvier 1979** relative aux archives a institué un régime de conservation et de consultation des archives applicable à **toutes les archives publiques ou privées**.

Aux termes de l'article premier de la loi, *«les archives sont l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé, dans l'exercice de leur activité»*. Toute autorité détenant une information ou support protégé, produit ou reçu, a pour obligation de faire assurer sa conservation et sa protection conformément aux dispositions législatives et réglementaires, et aux règles de fonctionnement du service d'archives auquel il est rattaché.

Article 75

LE VERSEMENT AUX DÉPOTS D'ARCHIVES DES INFORMATIONS OU SUPPORTS PROTÉGÉS

Dès qu'ils ne sont plus utilisés habituellement, les informations ou supports protégés présentant un intérêt administratif et historique sont versés, selon la périodicité prévue par chaque ministre, aux dépôts d'archives suivants :

- ***services historiques des armées pour le ministère de la défense et les services rattachés ;***
- ***archives du ministère des affaires étrangères, pour ce qui le concerne ;***
- ***direction des archives de France - archives nationales - pour toutes les administrations et organismes civils gérant des archives publiques.***

Ces services sont les seuls équipés et habilités pour recevoir des informations ou supports protégés classifiés jusqu'au niveau Secret-Défense inclus.

Retour au sommaire

CHAPITRE IV

LA PROTECTION DES LIEUX DE TRAITEMENT DES INFORMATIONS OU SUPPORTS PROTÉGÉS

SECTION I

LES ZONES PROTÉGÉES ET LES ZONES RÉSERVÉES

Article 76

LA CRÉATION DE ZONES PROTÉGÉES

Les articles 413-7, et R. 413-1 à R. 413-5 du code pénal sont relatifs à la protection des zones protégées intéressant la défense nationale. Le fait, *« dans les services, établissements ou entreprises, publics ou privés, intéressant la défense nationale, de s'introduire, sans autorisation, à l'intérieur des locaux et terrains clos dans lesquels la libre circulation est interdite et qui sont délimités pour assurer la protection des installations, du matériel ou du secret des recherches, études ou fabrications »* est puni de six mois d'emprisonnement et de 7500 € d'amende.

Le besoin de protection est déterminé par le ministre qui a la charge des installations, du matériel ou des recherches, études, fabrications à caractère secret qu'il désigne.[19] Les autorités dont relèvent les services, établissements ou entreprises concernés peuvent recevoir, par décret, délégation pour déterminer ce besoin de protection.

La création de la zone protégée intervient par **arrêté du ministre** ayant déterminé le besoin de protection lorsque l'activité principale du service, de l'établissement ou de l'entreprise relève de ce ministre ; lorsque cette activité principale relève d'un autre ministre, l'implantation et les limites de zones protégées sont fixées par arrêté conjoint de ce ministre et du ministre ayant déterminé le besoin de protection.[20] Les autorités dont relèvent ces services, établissements ou entreprises peuvent recevoir, par décret, délégation pour prendre les arrêtés prévus par le présent article.[21] L'autorisation de pénétrer dans les lieux est accordée par le responsable de l'organisme ou par le ministre ayant déterminé le besoin de protection dans le cas de zones instituées pour préserver des secrets intéressant la défense nationale.

L'autorité responsable doit prendre les dispositions nécessaires pour rendre apparentes les mesures d'interdiction d'accès à la zone protégée. Des pancartes sont disposées à cet effet, en nombre suffisant, aux endroits appropriés.

Article 77

LA CRÉATION DE ZONES RÉSERVÉES POUR LES INFORMATIONS OU SUPPORTS PROTÉGÉS CLASSIFIÉS AU NIVEAU SECRET-DÉFENSE

La création de zones réservées a pour but d'interdire :

- l'accès aux systèmes d'information classifiés **Secret-Défense** qui pourrait permettre d'entraver ou de fausser le fonctionnement de ces systèmes, ainsi que l'introduction, la suppression ou la modification frauduleuse de données dans ces systèmes ;

---

[19] Article R413-2 du code pénal

[20] Article R413-3 du code pénal

[21] Ainsi, pour ce qui concerne le ministre de la défense, voir le décret n° 2001-745 du 24 août 2001 relatif à la détermination des autorités ayant qualité pour définir au nom du ministre de la défense le besoin de protection des zones protégées, procéder à leur délimitation et fixer les conditions dans lesquelles sont délivrées les autorisations d'y pénétrer

- toute pénétration, par vues et écoutes, directes ou indirectes, dans les lieux où des informations ou supports protégés classifiés au niveau Secret-Défense sont élaborés, traités, reçus ou détenus ;
- tout accès à ces informations par des personnes, même habilitées, n'ayant pas le besoin d'en connaître.

Chaque ministre veille à ce que des zones réservées soient créées, par décision des autorités responsables de la détention d'informations classifiées, dans tous les services et organismes qui, de manière habituelle, élaborent, traitent, reçoivent ou détiennent des informations ou supports protégés classifiés au niveau Secret-Défense. La création de zones réservées, le cas échéant temporaires, est par ailleurs recommandée dans les services ou organismes traitant occasionnellement d'informations ou supports protégés classifiés à ce niveau.

Une zone réservée ne peut être créée en dehors d'une zone protégée. Elle peut être incluse dans une zone protégée ou lui correspondre.

Pour les informations ou supports protégés classifiés **Confidentiel-Défense**, ne pouvant pas être rangés dans un coffre fort ou une armoire forte, une zone réservée peut être créée. Les autres informations ou supports protégés classifiés **Confidentiel-Défense** font l'objet de mesures appropriées dans un « local sécurisé » ou une « zone sécurisée ».

Article 78

LES NORMES DES ZONES RÉSERVÉES

Ces zones sont adaptées au traitement des informations ou supports protégés classifiés au niveau Secret-Défense.

La zone réservée répond aux normes suivantes :

- elle comprend au minimum un **local pourvu d'ouvertures en nombre restreint**, de **fenêtres protégées** et de **portes renforcées équipées de serrures de haute sécurité**[22] munies si possible de compteur d'ouverture ;
- ce local contient un **coffre-fort** ou une **armoire forte** de type approuvé;
- un **contrôle permanent de la zone** est organisé, s'appuyant au minimum sur un des systèmes de protection ci-après : gardes, dispositif de télésurveillance ou dispositif de détection d'intrusion et d'alarme relié à un poste de garde en mesure d'intervenir.

Des normes équivalentes peuvent être adoptées en tant que de besoin par chaque ministre pour répondre à la situation de certains locaux spécifiques.

Article 79

LE CONTRÔLE DES LOCAUX EN ZONE RÉSERVÉE

Pour chaque zone réservée, un responsable s'assurera que les mesures de protection prévues, dont notamment les règles d'accès à la zone réservée, sont appliquées.

Pendant les heures de travail, le contrôle de la zone réservée incombe aux personnels qui y sont employés. Avant toute absence, ils vérifient la mise en sûreté des informations ou supports protégés ainsi que la fermeture des coffres et bureaux.

En dehors des heures ouvrables, des inspections sont organisées par les autorités responsables, pour contrôler :

- le fonctionnement des systèmes de détection ;

[22] IGH code de la construction et de l'habitation art. L.122-1, L122-2, R.122-29, R.152-1 à R.152-3 et code de l'urbanisme, art.421-1, L 421-3, R 421 à 421-36, R 421-47 et suivants, R 460-7, R 490 et suivants et A 490-1.

- la fermeture des bureaux, coffres, armoires, etc.;
- le vidage des corbeilles à papier et l'absence dans celles-ci de brouillons, ou documents préparatoires aux informations classifiées ;
- l'absence hors des coffres de supports classifiés, hormis les matériels qui ne pourraient pas être soustraits aux vues directes.

Des rondes de sécurité sont régulièrement effectuées par des gardiens ayant fait l'objet d'un contrôle élémentaire et disposant de consignes écrites précisant leur mission. Ces rondes sont exécutées sans que les gardiens aient à pénétrer dans une zone réservée en l'absence du personnel.

Article 80

LE CONTRÔLE DES PERSONNES ET DES VISITEURS EN ZONE RÉSERVÉE

Les personnes en service ayant accès de par leurs fonctions à la zone réservée disposent d'un badge apparent.

Les visiteurs sont :
- munis d'une autorisation individuelle de l'autorité responsable ;
- pourvus d'un laissez-passer temporaire ;
- accompagnés pendant toute la durée de leur visite par une personne habilitée désignée parmi les personnels de la zone.

Les personnels de nettoyage :
- ont satisfait à un contrôle élémentaire ;
- appartiennent à une société ayant au préalable satisfait à une enquête de sécurité ;
- portent un badge apparent avec photo ;
- interviennent en présence des personnels affectés.

Retour au sommaire

SECTION II

LA PROTECTION DES RÉUNIONS DE TRAVAIL ET DES SALLES DE CONFÉRENCE

Article 81

LA PROTECTION DES LIEUX

L'autorité organisatrice doit veiller à la protection des informations ou supports protégés échangés au cours d'une réunion de travail, d'une conférence, d'un exercice ou d'une présentation de matériel.

Le local prévu pour la séance où sont traitées des informations ou supports protégés répond à des caractéristiques garantissant contre les indiscrétions :

- être à l'abri des interceptions par écoute directe ou indirecte (insonorisation, absence de microphone) et des prises de vues non autorisées ;
- n'être accessible qu'aux personnes autorisées (création éventuelle d'une zone réservée temporaire).

Le contrôle technique des lieux est effectué par le service chargé de la sécurité avant et, si nécessaire, pendant et après chaque séance.

Article 82

LA PROTECTION ET LE CONTRÔLE DES PERSONNES

L'autorité organisatrice précise, lors des invitations ou convocations à une réunion de travail, une conférence, un exercice ou une présentation de matériel, le niveau de classification des informations ou supports protégés qui seront communiqués, pour permettre la désignation de personnes habilitées au niveau requis et ayant «besoin d'en connaître». Les autorités destinataires de l'invitation adressent en temps utile, à l'autorité organisatrice, les noms et fonctions des personnes chargées de les représenter.

L'autorité organisatrice fait établir la liste de toutes les personnes participant à la séance, à quelque titre que ce soit : auditeurs, conférenciers, assistants, techniciens chargés des projections ou essais, etc… Elle s'assure de l'identité et du niveau des habilitations de chacun des participants présents, si besoin est, au vu de **certificats de sécurité** (Mle 07/IGI 1300). Elle s'assure que personne ne détienne, lors de la réunion, un téléphone portable, un assistant personnel (PDA) ou un ordinateur portable.

Article 83

LA PROTECTION DES INFORMATIONS OU SUPPORTS PROTÉGÉS AU COURS DES RÉUNIONS DE TRAVAIL ET DES CONFÉRENCES

I. Rôle de l'autorité organisatrice.

L'autorité organisatrice veille, en application des principes stricts de **cloisonnement** de l'information classifiée, en particulier pour les niveaux Très Secret-Défense et Secret-Défense, à ce que la communication demeure limitée à l'objet de la réunion. Cette autorité peut interdire toute prise de note ou tout enregistrement des interventions par les auditeurs.

Lors de conférences ou de présentations de matériels ouvertes à un vaste auditoire de composition variée, le responsable détermine au préalable les limites et le degré de précision à apporter à la communication. En cas de communication d'informations Très Secret-Défense ou Secret-Défense, l'organisateur consigne, dans un procès-verbal succinct à classifier éventuellement, les domaines d'information qui ont été exposés, les mesures prises pour en assurer la protection ainsi que la liste des participants avec la **mention de la justification de leur habilitation**.

II. Obligation des participants ou auditeurs.

Les auditeurs assument la pleine responsabilité de la protection de leurs documents de travail et de leurs notes, qui sont à classifier au niveau correspondant à celui des informations recueillies. Ces divers documents sont détruits par leurs soins dès qu'ils ont cessé d'être utiles.

Article 84

LES MESURES DE SÉCURITÉ A L'ISSUE D'UNE RÉUNION DE TRAVAIL OU D'UNE CONFÉRENCE

L'autorité organisatrice de l'activité fait procéder en fin de séance :

- à la récupération et à la mise en sécurité des informations ou supports protégés éventuellement mis à la disposition des auditeurs (documents, graphiques, plans, films, bandes d'enregistrement, etc…) ;
- à la destruction des supports provisoires et préparatoires.

Retour au sommaire

TITRE IV

LA PRÉVENTION DES COMPROMISSIONS DES INFORMATIONS OU SUPPORTS PROTÉGÉS

Article 85

LA SENSIBILISATION AUX RISQUES DE COMPROMISSION

La sécurité des informations ou supports protégés peut être compromise par inattention, négligence ou indiscrétion personnelle, par l'action des services de renseignement étrangers, par des groupes d'intérêts propres ou par des individus isolés.

Toute personne ayant accès aux secrets de la défense nationale est informée, au moment d'être habilitée, de sa **responsabilité pénale** et prend connaissance des procédures de sécurité préventive (cf. art. 27). Elle est sensibilisée aux risques consécutifs au non-respect des mesures de protection et à ceux présentés par l'usage des systèmes d'information.

Article 86

L'INSTRUCTION DES PERSONNES

I. Personnes titulaires d'une habilitation.

Toutes les personnes habilitées reçoivent une **instruction initiale**, complétée de **rappels périodiques**, afin d'entretenir et de parfaire leur connaissance des règles de sécurité. Dans la mesure du possible, elles suivent un stage de sensibilisation organisé à l'intérieur du département dont elles dépendent.

Il appartient aux ministres (HFD) de donner, à cet effet, les consignes complémentaires à la présente instruction.

II. Personnes en séjour à l'étranger.

Un effort particulier de **sensibilisation aux menaces d'investigations étrangères** est à faire au profit des personnes devant se rendre à l'étranger, notamment dans les pays non liés par des accords de sécurité avec la France. Avant leur départ, les **règles élémentaires de prudence** à respecter pour ne pas être mis en difficulté leur sont rappelées, en particulier celles relatives **au respect des lois du pays visité** en matière de correspondance, devises, visites d'installations sensibles ou circulation routière.

Cette sensibilisation incombe aux responsables de la sécurité de défense de chaque organisme, avec l'éventuel concours des services spécialisés.

Article 87

LA SENSIBILISATION DU PERSONNEL A LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE

Il appartient aux ministres, dont dépendent les organismes chargés de la formation des futurs cadres de la fonction publique et des armées, de donner les instructions nécessaires pour que soient programmés et organisés des **cycles de sensibilisation** de ces personnels à la protection du secret de la défense nationale.

De même, les hauts fonctionnaires de défense, ou les autorités déléguées, s'assurent que les cadres recrutés directement dans la fonction publique suivent, au moins avant toute demande d'habilitation, un tel cycle de sensibilisation, à organiser par chaque ministère ou par les services spécialisés.

Article 88

LA CONDUITE A TENIR EN CAS DE COMPROMISSION

La rapidité et la discrétion de l'intervention revêtent une importance primordiale pour limiter les conséquences de la compromission des informations ou supports protégés.

Il est rendu compte immédiatement de toute découverte de compromission possible à l'autorité hiérarchique et au responsable de la sécurité de l'organisme concerné. Dès que la compromission est avérée, celui-ci en informe directement et dans les plus brefs délais :

- *le service compétent du ministère de l'intérieur, chargé de procéder à l'enquête sous le contrôle de l'autorité judiciaire ;*
- *pour le ministère de la défense, le service compétent du ministère qui avise le service compétent du ministère de l'intérieur ;*
- *le HFD du ministère intéressé ;*
- *le SGDN (service de sécurité de défense).*

Les disparitions, vols, pertes accidentelles de supports classifiés ou les agressions contre les systèmes d'information font l'objet d'un **procès-verbal de perte ou d'agression informatique**, adressé :

- directement au HFD du ministère concerné ;
- dans un délai de trois jours par la voie hiérarchique du ministère concerné à l'autorité émettrice de l'information classifiée et au SGDN (service de sécurité de défense) pour les informer des conséquences éventuelles de la compromission.

Le chef de service devra prendre les mesures conservatoires pour éviter le renouvellement de tels faits.

Article 89

LES CONTRÔLES ET LES INSPECTIONS

I. Contrôles et inspections.

Des contrôles et inspections sont organisés périodiquement pour vérifier l'application par les organismes concernés des instructions et directives traitant de la protection globale des informations ou supports protégés.

Pour les organismes traitant des informations ou supports protégés classifiés Très Secret-Défense, ces contrôles sont assurés par le SGDN. Il propose toutes mesures propres à améliorer les conditions générales de sécurité. Ces inspections sont organisées en liaison avec les départements ministériels. En cas

d'anomalies constatées, le SGDN peut saisir par l'intermédiaire des ministres concernés, les services qui concourent à la répression des crimes et délits.

Pour les organismes traitant des informations ou supports protégés classifiés Secret-Défense et Confidentiel-Défense, chaque ministre (HFD) prescrit à l'intérieur de son département des contrôles et inspections périodiques en vue de vérifier l'application effective des instructions sur la protection des informations ou supports protégés. Le SGDN peut éventuellement inspecter des organismes traitant des informations ou supports protégés classifiés Secret-Défense.

Les rapports de synthèse incluant les mesures préconisées pour rectifier les déficiences constatées et leur planification sont adressés aux autorités responsables des organismes contrôlés et aux autorités ministérielles de tutelle.

II. Rapport d'évaluation de la protection du secret de défense.

Le secrétaire général de la défense nationale fait annuellement un rapport au Premier ministre sur la protection du secret de la défense nationale en France.

A cet effet, chaque haut fonctionnaire de défense[23] adresse, pour le **31 mars de chaque année**, au SGDN (service de sécurité de défense) un **rapport d'évaluation** sur la protection globale du secret de la défense nationale dans son département ministériel. Ce rapport, classifié Confidentiel-Défense Spécial France, dresse le bilan des contrôles effectués, des actions rectificatives engagées, de l'évolution des déficiences et compromissions constatées et de celle des effectifs habilités.

Fait à Paris, le 25 août 2003

Le Premier ministre
Jean-Pierre RAFFARIN

Retour au sommaire

[23] Pour le ministre de la défense, le chef du cabinet militaire.

LEXIQUE

Accord de sécurité : accord intergouvernemental conclu entre deux ou plusieurs États ou au sein d'une alliance multinationale et ayant pour objet la protection d'informations ou de supports protégés. Ces accords comprennent l'identification et la reconnaissance mutuelle des autorités nationales de sécurité, la correspondance des niveaux de classification, la reconnaissance mutuelle des habilitations de personnes, les modalités d'échange et de protection des informations et matériels classifiés.

Administrateur de sécurité : est chargé de la mise en œuvre, du maintien, du contrôle et de l'évolution des mesures de sécurité à appliquer à tout système d'information contenant des informations ou supports protégés classifiés au niveau Secret-Défense et Confidentiel-Défense.

Administrateur système : est chargé de la mise au point, de l'exploitation, de la maintenance, du contrôle et des évolutions du système informatique.

Agent de sécurité : est chargé d'appliquer les mesures de sécurité aux supports protégés classifiés Secret-Défense et d'en assurer la gestion. Il est nommé par le chef de l'organisme où est implanté le bureau Secret-Défense. Ses missions sont à distinguer de celles dévolues à l'agent de sécurité dans une entreprise titulaire d'un marché classé de défense, qui est désigné par le responsable de l'entreprise après agrément de l'administration ayant contracté le marché.

Agent de sécurité des SSI : chargé de la gestion et du suivi des moyens de sécurité des systèmes d'information se trouvant sur le ou les sites où s'exercent ses responsabilités notamment lorsque la gestion et le suivi des articles nécessitent une comptabilité individuelle.

Agrément : décision prise à l'issue d'une procédure d'habilitation ordinaire au profit d'une personne amenée à prendre occasionnellement connaissance d'informations ou supports protégés classifiés du niveau Très Secret-Défense de différentes classifications spéciales, du niveau Secret-Défense ou du niveau Confidentiel -Défense.

Agrément[24] d'un produit de sécurité **:** reconnaissance formelle que le produit de sécurité évalué peut protéger des informations jusqu'à un niveau spécifié dans les conditions d'emploi définies.

Antenne d'utilisation : bureau où sont émis, reçus, manipulés, expédiés et conservés les supports Très Secret-Défense.

Archivage : opération consistant à verser à un service d'archives des supports d'information lorsqu'ils ne sont plus d'utilisation habituelle. Les supports faisant encore l'objet d'une classification ne peuvent être archivés que dans certaines conditions et dans des services habilités à les recevoir. Un support classifié au niveau Très Secret-Défense ne peut en aucun cas être archivé.

Authenticité *:* propriété d'une information ou d'un traitement qui garantit son identité, son origine et éventuellement sa destination.

Autorité nationale de sécurité : organisme gouvernemental interministériel chargé des relations avec les autres États et les structures internationales en matière d'habilitation de personnes et de protection des informations ou supports protégés. En France, il s'agit du SGDN.

Autorité de sécurité désignée : autorité responsable devant l'autorité nationale de sécurité et chargée de faire connaître à l'industrie la politique nationale dans tous les domaines de la politique de sécurité industrielle ainsi que de donner des orientations et de fournir une aide pour sa mise en application.

Autorité qualifiée en matière de SSI : responsable de la sécurité des systèmes d'information dans les administrations centrales et les services déconcentrés de l'État, dans les établissements publics placés sous l'autorité d'un ministre ainsi que les organismes et établissements placés sous sa tutelle.

---

24 Instruction générale interministérielle nº900/DISSI/SCSSI/DR du 20 juillet 1993 sur la sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées.

Avis de sécurité : conclusion émise par un service spécialisé à l'issue d'investigations au sujet d'une personne et visant à détecter et évaluer les vulnérabilités de cette personne. L'avis de sécurité est une aide à la décision d'habilitation, mais il ne lie pas l'autorité responsable de la décision.

Besoin d'en connaître : nécessité impérieuse de prendre connaissance d'une information dans le cadre d'une fonction déterminée et pour la bonne exécution d'une mission précise.

Bureau Secret-Défense : bureau situé en zone réservée et dont l'existence est obligatoire pour procéder à l'élaboration, au marquage, au stockage, à l'acheminement, à l'enregistrement et au suivi destruction des informations ou supports protégés classifiés Secret-Défense.

Catalogue des emplois : dans un organisme, liste des emplois qui peuvent nécessiter l'accès aux informations ou supports protégés. Le catalogue est dressé sur le seul critère du besoin d'en connaître.

Certificat de sécurité *:* document probatoire de l'habilitation d'une personne au traitement d'informations ou supports protégés.

Classification spéciale : catégorie d'informations ou supports protégés classifiés au niveau Très Secret-Défense et répondant à la nécessité de cloisonnement. Les différentes classifications spéciales sont organisées en réseaux de sécurité constitués d'antennes d'utilisation. Par ailleurs, les habilitations de personnes au niveau Très Secret-Défense sont prononcées au titre d'une ou plusieurs classifications spéciales expressément désignées.

Compromission : prise de connaissance, certaine ou probable, d'une information ou support protégé par une ou plusieurs personnes non autorisées.

Confidentialité : caractère réservé d'une information ou d'un traitement dont l'accès est limité aux seules personnes admises à la (le) connaître pour les besoins du service, ou aux entités ou processus autorisés.

Décision d'habilitation : délivrée, au terme de la procédure d'habilitation, pour autoriser le titulaire de la décision à accéder aux informations ou supports protégés d'un niveau déterminé. L'intéressé est informé de la décision d'habilitation qui ne lui est jamais remise.

Décision d'habilitation provisoire : décision exceptionnelle et provisoire prise au vu d'un avis de sécurité provisoire et permettant l'accès d'une personne aux informations ou supports protégés. Cette autorisation prend fin lors de la délivrance de l'autorisation définitive ou au plus tard six mois après avoir été accordée.

Décision de sécurité convoyeur : accordée, non pas pour prendre connaissance d'informations ou supports protégés, mais pour assurer, durant le transport, la garde des informations ou supports protégés. Pour cette raison, cette décision est délivrée, non pas au terme de la procédure d'habilitation, mais après un contrôle élémentaire effectué auprès des services spécialisés relevant des départements ministériels de l'intérieur ou de la défense.

Déclassement : modification, par abaissement, du niveau de classification d'informations ou supports protégés.

Déclassification : suppression de tout niveau de classification d'informations ou supports protégés.

Disponibilité **:** propriété d'une information ou d'un traitement d'être, à la demande, utilisable par une personne ou un système.

Dossier d'habilitation : dossier constitué préalablement à une décision d'habilitation de personne. Il comporte la demande d'habilitation établie par l'autorité demandeuse et attestant le besoin d'en connaître, les notices individuelles renseignées par l'intéressé et des photographies d'identité récentes.

Donnée *:* toute représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement.

Engagement de responsabilité : document en deux volets signés par le titulaire de l'habilitation lors de sa prise et de sa cessation de fonction. L'engagement a pour but de faire prendre conscience à cette personne de ses responsabilités pénales du fait de son habilitation aux informations ou supports protégés.

Fonctionnaire de sécurité de défense : assiste le HFD et contrôle sous sa direction notamment l'exécution des mesures de protection des informations ou supports protégés.

Fonctionnaire de sécurité des systèmes d'information : chargé de porter la réglementation interministérielle à la connaissance des organismes et entreprises concernés, d'élaborer la réglementation propre à son ministère, en définissant pour chaque type de système d'information, les mesures de protection nécessaires et de contrôler dans son département l'application de cette réglementation et l'efficacité des mesures prescrites.

Haut fonctionnaire de défense (HFD) : est chargé, dans les ministères autres que celui de la Défense, d'assister le ministre dans l'exercice de ses attributions de sécurité de défense et de protection du secret. Dans la présente instruction, désigne le haut fonctionnaire de défense ou l'autorité déléguée par le ministre de la défense.

Homologation de sécurité : déclaration par l'autorité d'homologation, au vu du dossier d'homologation, que le système d'information considéré est apte à traiter des informations d'un niveau de classification donné conformément aux objectifs de sécurité visés, et que les risques de sécurité résiduels induits sont acceptés et maîtrisés. L'homologation de sécurité reste valide tant que le SI opère dans les conditions approuvées par l'autorité d'homologation.

Identification : mention figurant sur un support d'information et précisant le numéro de l'exemplaire ainsi que son numéro d'enregistrement.

Information : tout renseignement ou tout élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement.

Information ou support protégé : renseignement, procédé, objet, document, donnée informatisée ou fichier présentant un caractère de secret de la défense nationale (cf. art.1er du décret du 17 juillet 1998).

Information sensible : information dont la confidentialité, la disponibilité et l'intégrité ne procèdent pas du secret de la défense nationale tel que défini par les articles 413-9 à 413-12 du code pénal et le décret 98-608. Une information sensible est néanmoins protégée par des dispositions telles que l'obligation de discrétion professionnelle, le secret professionnel, les textes sur les données nominatives et les obligations contractuelles. Les informations sensibles ne rentrent pas dans le champ de l'instruction 1300.

Intégrité : propriété assurant qu'une information ou un traitement n'a pas été modifié ou détruit de façon non autorisée.

Marquage : opération consistant à apposer sur un support classifié les mentions précisant son niveau de classification, la destination exclusivement nationale, le numéro d'exemplaire, le numéro d'enregistrement et la pagination pour un document papier.

Matériel classifié : objet, équipement, installation, système ou substance présentant un caractère de secret de la défense nationale et qui nécessite une protection appropriée Très Secret-Défense, Secret-Défense ou Confidentiel-Défense.

Mise en éveil : démarche effectuée par le service spécialisé auprès de la personne à habiliter, pour la sensibiliser sur ses vulnérabilités découvertes au cours de l'enquête.

Mise en garde : démarche effectuée par le service spécialisé visant à sensibiliser le chef du service employeur sur l'existence d'éléments pouvant présenter des risques de vulnérabilité pour la personne à habiliter.

Non-répudiation : impossibilité de nier la participation au traitement d'une information.

Notice individuelle : formulaire destiné à recueillir les renseignements nécessaires à l'habilitation d'une personne. Elle doit être renseignée par l'intéressé lui-même et constitue un élément majeur de la demande d'habilitation. Elle est exploitée par l'autorité chargée de prononcer la décision et par les services spécialisés.

Officier de sécurité : a pour mission, sous les ordres de son autorité d'emploi, de fixer les règles et consignes de sécurité à mettre en œuvre relatives aux personnes et aux informations ou supports protégés et d'en vérifier l'exécution.

Plans d'urgence : documents établis par les organismes détenteurs d'informations ou supports protégés et prévoyant, en cas de circonstances exceptionnelles, les modalités d'évacuation ou de destruction des supports d'information.

Procédure d'habilitation : consiste à vérifier qu'une personne peut sans risque pour la défense nationale ou pour sa propre sécurité, connaître des informations ou supports protégés dans l'exercice de ses fonctions.

Réseau de sécurité: ensemble des moyens humains, matériels et organisationnels qui permettent l'acheminement en toute sécurité des informations ou supports protégés à un niveau maximum déterminé, entre un ensemble de correspondants habilités.

Responsable de la classification : autorité émettrice d'informations qui leur attribue, en fonction de leur contenu, un niveau de classification approprié.

Refus d'habilitation : décision prise par l'autorité d'emploi, au vu de l'avis de sécurité ou de tout autre élément recueilli sur une personne, de ne pas habiliter cette personne. Sa notification à l'intéressé n'est pas obligatoire et sa motivation est encadrée par la loi 79-587 du 11 juillet 1979 sur la motivation des actes administratifs.

Renouvellement d'habilitation : procédure déclenchée à la fin de validité d'un avis de sécurité concernant une personne déjà habilitée en vue d'obtenir un avis actualisé. Ce nouvel avis permettra de prononcer une décision d'habilitation au profit de la personne qui présente encore le besoin d'en connaître.

Retrait d'habilitation : décision prise par l'autorité d'emploi, au vu d'éléments nouveaux de vulnérabilité, de supprimer l'habilitation d'une personne.

Sensibilisation : instruction périodiquement prodiguée aux personnes habilitées ou susceptibles d'être habilitées et destinée à leur faire prendre conscience des enjeux de la protection du secret de la défense nationale, des sanctions judiciaires et administratives encourues et de la nécessité d'appliquer les mesures de sécurité prescrites.

Service spécialisé : organisme d'État chargé de procéder aux investigations sur les personnes préalablement à une décision d'habilitation. Ces services rendent leurs conclusions sous la forme d'avis de sécurité.

Spécial France : mention figurant sur des supports d'information et précisant leur destination exclusivement nationale.

Support : tout moyen matériel, quelles qu'en soient la forme ou les caractéristiques physiques, permettant de recevoir, conserver ou restituer des informations ou des données.

Système d'information : ensemble des moyens humains et matériels ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire l'information.

Système informatique : ensemble des moyens informatiques et de télécommunication ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire des données.

Timbre : mention figurant sur un support d'information précisant son niveau de classification et, le cas échéant, son usage national exclusif. Le timbre possède des caractéristiques définies (dimensions, aspect).

Vulnérabilité : fait relatif à la situation d'une personne et qui amoindrit les garanties qu'elle présente en termes de protection des informations ou supports protégés. Il s'agit d'une fragilité qui peut entraîner des pressions de diverses natures et qui doit être prise en compte pour accorder avec ou sans restriction, refuser ou retirer l'accès aux informations ou supports protégés.

Zone protégée : zone créée par arrêté des ministres compétents et faisant l'objet d'une interdiction de pénétration sans autorisation, sanctionnée pénalement en cas d'infraction (articles 413-7 et R. 413-1 à R 413-5 du Code pénal).

Zone réservée : locaux et emplacements qui font l'objet de mesures de protection matérielle particulières et dont l'accès est réglementé et subordonné à des conditions spéciales.

Retour au sommaire

CODE PÉNAL
(extraits)

De la responsabilité pénale (Livre I - titre II - chapitre I)

Art. 121-2 Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7 et dans les cas prévus par la loi ou le règlement, des infractions commises, pour leur compte, par leurs organes ou représentants.

Toutefois, les collectivités territoriales et leurs groupements ne sont responsables pénalement que des infractions commises dans l'exercice d'activités susceptibles de faire l'objet de conventions de délégation de service public.

La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

. . . . . .

Des atteintes aux intérêts fondamentaux de la nation.(Livre IV - titre I)

Art. 410-1 Les intérêts fondamentaux de la nation s'entendent au sens du présent titre de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel.

De la trahison et de l'espionnage. (Livre IV - titre I - chapitre I)

Art. 411-1 Les faits définis par les articles 411-2 à 411-11 constituent la trahison lorsqu'ils sont commis par un Français ou un militaire au service de la France et l'espionnage lorsqu'ils sont commis par toute autre personne.

De la livraison de tout ou partie du territoire national, de forces armées ou de matériel à une puissance étrangère. (Livre IV - titre I - chapitre I - section I)

. . . . . .

Art. 411-3 Le fait de livrer à une puissance étrangère, à une entreprise ou une organisation étrangère ou sous contrôle étranger ou à leurs agents des matériels, constructions, équipements, installations, appareils affectés à la défense nationale est puni de trente ans de détention criminelle et de 450 000 € d'amende.

Des intelligences avec une puissance étrangère. (Livre IV - titre I - chapitre I - section II)

Art. 411-4 Le fait d'entretenir des intelligences avec une puissance étrangère, avec une entreprise ou organisation étrangère ou sous contrôle étranger ou avec leurs agents, en vue de susciter des hostilités ou des actes d'agression contre la France, est puni de trente ans de détention criminelle et de 450 000 € d'amende.

Est puni des mêmes peines le fait de fournir à une puissance étrangère, à une entreprise ou une organisation étrangère ou sous contrôle étranger ou à leurs agents les moyens d'entreprendre des hostilités ou d'accomplir des actes d'agression contre la France.

Art. 411-5 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 € d'amende.

De la livraison d'informations à une puissance étrangère. (Livre IV - titre I - chapitre I - section III)

Art. 411-6 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 € d'amende.

Art. 411-7 Le fait de recueillir ou de rassembler, en vue de les livrer 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 dix ans d'emprisonnement et de 150 000 € d'amende.

Art. 411-8 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 € d'amende.

Du sabotage.(Livre IV - titre I - chapitre I - section IV)

Art. 411-9 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 € 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 € d'amende.

De la fourniture de fausses informations. (Livre IV - titre I - chapitre I - section V)

Art. 411-10 Le fait de fournir, en vue de servir les intérêts d'une puissance étrangère, d'une entreprise ou 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 € d'amende.

De la provocation aux crimes prévus au présent chapitre (Livre IV - titre I - chapitre I - section VI)

Art. 411-11 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 € d'amende.

. . . . . .

Des atteintes à la sécurité des forces armées et aux zones protégées intéressant la défense nationale. (Livre IV - titre I - chapitre III - section I)

. . . . . .

Art. 413-5 Le fait, sans autorisation des autorités compétentes, de s'introduire frauduleusement sur un terrain, dans une construction ou dans un engin ou appareil quelconque affecté à l'autorité militaire ou placé sous son contrôle est puni d'un an d'emprisonnement et de 15 000 € d'amende.

Art. 413-6 Le fait, en vue de nuire à la défense nationale, d'entraver le fonctionnement normal des services, établissements ou entreprises, publics ou privés, intéressant la défense nationale, est puni de trois ans d'emprisonnement et de 45 000 € d'amende.

Art. 413-7 Est puni de six mois d'emprisonnement et de 7 500 € d'amende le fait, dans les services, établissements ou entreprises, publics ou privés, intéressant la défense nationale, de s'introduire, sans autorisation, à l'intérieur des locaux et terrains clos dans lesquels la libre circulation est interdite et qui sont délimités pour assurer la protection des installations, du matériel ou du secret des recherches, études ou fabrications.

Un décret en Conseil d'Etat détermine, d'une part, les conditions dans lesquelles il est procédé à la délimitation des locaux et terrains visés à l'alinéa précédent et, d'autre part, les conditions dans lesquelles les autorisations d'y pénétrer peuvent être délivrées.

Art. 413-8 La tentative des délits prévus aux articles 413-2 et 413-5 à 413-7 est punie des mêmes peines.

Des atteintes au secret de la défense nationale. (Livre IV - titre I - chapitre III - section II)

Art. 413-9 Présentent un caractère de secret de la défense nationale au sens de la présente section les renseignements, procédés, objets, documents, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion.

Peuvent faire l'objet de telles mesures, les renseignements, procédés, objets, documents, données informatisées ou fichiers dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

Les niveaux de classification des renseignements, procédés, objets, documents, données informatisées ou fichiers présentant un caractère de secret de la défense nationale et (L. n° 94-89 du 1er févr. 1994) «les autorités chargées de définir les modalités selon lesquelles est organisée leur protection» sont déterminés par décret en Conseil d'Etat.

Art. 413-10 Est puni de sept ans d'emprisonnement et de 100 000 € d'amende le fait, par toute personne dépositaire, soit par état ou profession, soit en raison d'une fonction ou d'une mission temporaire ou permanente, d'un renseignement, procédé, objet,

document, donnée informatisée ou fichier qui a un caractère de secret de la défense nationale, soit de le détruire, détourner, soustraire ou de le reproduire, soit de le porter à la connaissance du public ou d'une personne non qualifiée.

Est puni des mêmes peines le fait, par la personne dépositaire, d'avoir laissé détruire, détourner, soustraire, reproduire ou divulguer le renseignement, procédé, objet, document, donnée informatisée ou fichier visé à l'alinéa précédent.

Lorsque la personne dépositaire a agi par imprudence ou négligence, l'infraction est punie de trois ans d'emprisonnement et de 45 000 € d'amende.

Art. 413-11 Est puni de cinq ans d'emprisonnement et de 75 000 € d'amende le fait, par toute personne non visée à l'article 413-10 de :

1° S'assurer la possession d'un renseignement, procédé, objet, document, donnée informatisée ou fichier qui présente le caractère d'un secret de la défense nationale;

2° Détruire, soustraire ou reproduire, de quelque manière que ce soit, un tel renseignement, procédé, objet, document, donnée informatisée ou fichier;

3° Porter à la connaissance du public ou d'une personne non qualifiée un tel renseignement, procédé, objet, document, donnée informatisée ou fichier.

Art. 413-12 La tentative des délits prévus au premier alinéa de l'article 413-10 et à l'article 413-11 est punie des mêmes peines.

Dispositions transitoires (Livre IV - titre I - chapitre IV)

. . . . . .

Art. 414-7 Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent titre.

Les peines encourues par les personnes morales sont :

1° L'amende, suivant les modalités prévues par l'article 131-38;

2° Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Art. 414-8 Les dispositions des articles 411-1 à 411-11 et 413-1 à 413-12 sont applicables aux actes visés par ces dispositions qui seraient commis au préjudice des puissances signataires du traité de l'Atlantique-Nord.

Art. 414-9 Les dispositions des articles 411-6 à 411-8 et 413-10 à 413-12 sont applicables aux informations faisant l'objet de l'accord de sécurité relatif à certains échanges d'informations à caractère secret entre le Gouvernement de la République française et le Gouvernement du Royaume de Suède, signé à Stockholm le 22 octobre 1973.

. . . . . .

Des entraves à la saisine de la justice (Livre IV - titre III - chapitre IV - section I)

Art. 434-1 Le fait, pour quiconque ayant connaissance d'un crime dont il est encore possible de prévenir ou de limiter les effets, ou dont les auteurs sont susceptibles de commettre de nouveaux crimes qui pourraient être empêchés, de ne pas en informer les autorités judiciaires ou administratives est puni de trois ans d'emprisonnement et de 45 000 € d'amende.

Sont exceptés des dispositions qui précèdent, sauf en ce qui concerne les crimes commis sur les mineurs de quinze ans :

1° Les parents en ligne directe et leurs conjoints, ainsi que les frères et sœurs et leurs conjoints, de l'auteur ou du complice du crime ;

2° Le conjoint de l'auteur ou du complice du crime, ou la personne qui vit notoirement en situation maritale avec lui.

Sont également exceptées des dispositions du premier alinéa les personnes astreintes au secret dans les conditions prévues par l'article 226-13.

Art. 434-2 Lorsque le crime visé au premier alinéa de l'article 434-1 constitue une atteinte aux intérêts fondamentaux de la nation prévue par le titre Ier du présent livre ou un acte de terrorisme prévu par le titre II du présent livre, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende.

CODE DE PROCÉDURE PÉNALE

Des crimes et des délits en matière militaire et des crimes et délits contre les intérêts fondamentaux contre la nation
(Loi .n°82_621 du 21 juillet 1982)

Art.698-3 Lorsque le procureur de la République, le juge d'instruction et les officiers de police judiciaire sont amenés soit à constater des infractions dans les établissements militaires, soit à rechercher, en ces mêmes lieux des personnes ou des objets relatifs à ces infractions, ils doivent adresser à l'autorité militaire des réquisitions tendant à obtenir l'entrée dans ces établissements. Les réquisitions doivent, sauf nécessité préciser la nature et les motifs des investigations jugées nécessaires. L'autorité militaire est tenue de s'y soumettre et se fait représenter aux opérations.

Le Procureur de la République, le juge d'instruction et les officiers de police judiciaire veillent, en liaison avec le représentant de l'autorité militaire, au respect des prescriptions relatives au secret militaire. Le représentant de l'autorité militaire est tenu au respect du secret de l'enquête et de l'instruction.

Retour au sommaire

TEXTES LÉGISLATIFS

ORDONNANCE n° 59-147 du 7 janvier 1959
portant organisation générale de la défense nationale

(*Journal officiel* du 10 janvier 1959)

Le président du conseil des ministres,
Vu la Constitution, et notamment ses articles 34 et 92 ;
Le Conseil d'Etat entendu ;
Le conseil des ministres entendu,
Ordonne :

TITRE Ier
DISPOSITIONS GENERALES

***Article premier*. -** La défense a pour objet d'assurer en tout temps, en toutes circonstances et contre toutes les formes d'agression, la sécurité et l'intégrité du territoire, ainsi que la vie de la population.

Elle pourvoit de même au respect des alliances, traités et accords internationaux.

Les principes de défense de la Communauté sont déterminés par les autorités constitutionnellement responsables.

Les mesures d'application sont prises dans les conditions propres aux différents Etats membres de la Communauté.

. . . . . .

***Art. 9*. -** Le Premier ministre responsable de la défense nationale exerce la direction générale et la direction militaire de la défense. A ce titre, il formule les directives générales pour les négociations concernant la défense et suit le développement de ces négociations. Il décide de la préparation et de la conduite supérieure des opérations et assure la coordination de l'activité en matière de défense de l'ensemble des départements ministériels.

. . . . . .

***Art. 15*. -** Chaque ministre est responsable de la préparation et de l'exécution des mesures de défense incombant au département dont il a la charge.

Il est assisté, en ce qui concerne les départements autres que celui des armées, par un haut fonctionnaire désigné à cet effet.

Avant le 1er mai de chaque année, chaque ministre adresse au Premier ministre, pour la gestion suivante, dans le cadre des directives générales qu'il a reçues de lui, les plans concernant son action dans le domaine de la défense, assortis des renseignements nécessaires sur leurs incidences financières.

Le Premier ministre établit le programme d'ensemble.

. . . . . .

Art. 47. - La présente ordonnance sera publiée au *Journal officiel* de la République française et exécutée comme loi.

Fait à Paris, le 7 janvier 1959.

Charles DE GAULLE

Par le Président du conseil des ministres :
Le ministre d'Etat,
Guy MOLLET

Le ministre d'Etat,
Pierre PFLIMLIN

Le ministre d'Etat,
Félix HOUPHOUET-BOIGNY

Le garde des sceaux, ministre de la justice
Michel DEBRE

LOI n° 72-662 du 13 juillet 1972
portant statut général des militaires

(*Journal officiel* du 14 juillet 1972)

. . . . . .

Art. 18 - Indépendamment des dispositions du code pénal relatives à la violation du secret de la défense nationale ou du secret professionnel, les militaires sont liés par l'obligation de discrétion pour tout ce qui concerne les faits et informations dont ils ont connaissance dans l'exercice ou à l'occasion de leurs fonctions.

Tout détournement, toute communication contraire aux règlements, de pièces ou documents de service à des tiers sont interdits.

En dehors des cas expressément prévus par la réglementation en vigueur, les militaires ne peuvent être déliés de cette obligation de discrétion ou relevés de l'interdiction édictée à l'alinéa précédent qu'avec l'autorisation du ministre.

. . . . . .

_____

LOI n° 78-753 du 17 juillet 1978
portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal

(*Journal officiel* du 18 juillet 1978)

. . . . . .

Art. 2. –Sous réserve des dispositions de l'article 6, les documents administratifs sont de plein droit communi-cables aux personnes qui en font la demande, qu'ils émanent des administrations de l'Etat, des collectivités territoriales, des établissements publics ou des organismes, fussent-ils de droit privé, chargés de la gestion d'un service public.

. . . . . .

Art. 6. – Les administrations mentionnées à l'article 2 peuvent refuser de laisser consulter ou communiquer un document administratif dont la consultation ou la communication porterait atteinte :

- au secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif ;
- au secret de la défense nationale, de la politique extérieure ;
- à la monnaie et au crédit public, à la sûreté de l'Etat et à la sécurité publique ;
- au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, sauf autorisation donnée par l'autorité compétente ;
- au secret de la vie privée, des dossiers personnels et médicaux ;
- au secret en matière commerciale et industrielle ;
- à la recherche par les services compétents, des infractions fiscales et douanières ;
- ou de façon générale, aux secrets protégés par la loi.

Pour l'application des dispositions ci-dessus, les listes des documents administratifs qui ne peuvent être communiqués au public en raison de leur nature ou de leur objet sont fixées par arrêtés ministériels pris après avis de la commission d'accès aux documents administratifs.

. . . . . .

_____

LOI n° 79-587 du 11 juillet 1979
relative à la motivation des actes administratifs et à l'amélioration des relations entre l'administration et le public

(*Journal officiel* du 12 juillet 1979)

Art. 1er.-. Les personnes physiques ou morales ont le droit d'être informées sans délai des motifs des décisions administratives individuelles défavorables qui les concernent.

A cet effet, doivent être motivées les décisions qui :

- restreignent l'exercice des libertés publiques ou, de manière générale, constituent une mesure de police
- infligent une sanction ;
- subordonnent l'octroi d'une autorisation à des conditions restrictives ou imposent des sujétions ;
- retirent ou abrogent une décision créatrice de droits ;
- opposent une prescription, une forclusion ou une déchéance ;
- refusent un avantage dont l'attribution constitue un droit pour les personnes qui remplissent les conditions légales pour l'obtenir ;

«- refusent une autorisation, sauf lorsque la communication des motifs pourrait être de nature à porter atteinte à l'un des secrets ou intérêts protégés par les dispositions des deuxième à cinquième alinéas de l'article 6 de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public» *(article 26 de la loi n° 86-76 du 17 janvier 1986 portant diverses dispositions d'ordre social)*

. . . . . .

Art. 4 – Lorsque l'urgence absolue a empêché qu'une décision soit motivée, le défaut de motivation n'entache pas d'illégalité cette décision. Toutefois, si l'intéressé en fait la demande, l'autorité qui a pris la décision devra, dans un délai d'un mois, lui en communiquer les motifs.

Les dispositions de la présente loi ne dérogent pas aux textes législatifs interdisant la publication ou la divulgation de faits couverts par le secret.

. . . . . .

———————

LOI 83-634 du 13 juillet 1983
Portant droits et obligations des fonctionnaires

. . . . . .

Art. 26 – Les fonctionnaires sont tenus au secret professionnel dans le cadre des règles instituées dans le code pénal. Les fonctionnaires doivent faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont ils ont connaissance dans l'exercice ou à l'occasion de l'exercice de leurs fonctions. En dehors des cas expressément prévus par la réglementation en vigueur, notamment en matière de liberté d'accès aux documents administratifs, les fonctionnaires ne peuvent être déliés de cette obligation de discrétion professionnelle que par décision expresse de l'autorité dont ils dépendent.

. . . . . .

———————

LOI n° 98-567 du 8 juillet 1998
instituant une commission consultative du secret de la défense nationale

(*Journal officiel* du 9 juillet 1998)

L'Assemblée nationale et le Sénat ont délibéré,
L'Assemblée nationale a adopté,
Le Président de la République promulgue la loi dont la teneur suit :

Art. 1er - Il est institué une Commission consultative du secret de la défense nationale. Cette commission est une autorité administrative indépendante. Elle est chargée de donner un avis sur la déclassification et la communication d'informations ayant fait l'objet d'une classification en application des dispositions de l'article 413-9 du code pénal, à l'exclusion des informations dont les règles de classification ne relèvent pas des seules autorités françaises.

L'avis de la Commission consultative du secret de la défense nationale est rendu à la suite de la demande d'une juridiction française.

Art. 2. - La Commission consultative du secret de la défense nationale comprend cinq membres :

- un président, un vice-président qui le supplée en cas d'absence ou d'empêchement et un membre choisis par le Président de la République sur une liste de six membres du Conseil d'Etat, de la Cour de cassation ou de la Cour des comptes, établie conjointement par le vice-président du Conseil d'Etat, le premier président de la Cour de cassation et le premier président de la Cour des comptes;
- un député, désigné pour la durée de la législature par le président de l'Assemblée nationale;
- un sénateur, désigné après chaque renouvellement partiel du Sénat par le président du Sénat.

Le mandat des membres de la commission n'est pas renouvelable.

Le mandat des membres non parlementaires de la commission est de six ans.

Sauf démission, il ne peut être mis fin aux fonctions de membre de la commission qu'en cas d'empêchement constaté par celle-ci. Les membres de la commission désignés en remplacement de ceux dont le mandat a pris fin avant son terme normal sont nommés pour la durée restant à courir dudit mandat. Par dérogation au cinquième alinéa, lorsque leur nomination est intervenue moins de deux ans avant l'expiration du mandat de leur prédécesseur, ils peuvent être renouvelés en qualité de membre de la commission.

Art. 3. - Les crédits nécessaires à la commission pour l'accomplissement de sa mission sont inscrits au budget des services du Premier ministre.

Le président est ordonnateur des dépenses de la commission. Il nomme les agents de la commission.

Art. 4. - Une juridiction française dans le cadre d'une procédure engagée devant elle peut demander la déclassification et la communication d'informations, protégées au titre du secret de la défense nationale, à l'autorité administrative en charge de la classification.

Cette demande est motivée.

L'autorité administrative saisit sans délai la Commission consultative du secret de la défense nationale.

Art. 5. - Le président de la commission peut mener toutes investigations utiles.

Les membres de la commission sont autorisés à connaître de toute information classifiée dans le cadre de leur mission.

Ils sont astreints au respect du secret de la défense nationale protégé en application des articles 413-9 et suivants du code pénal pour les faits, actes ou renseignements dont ils ont pu avoir connaissance à raison de leurs fonctions.

La commission établit son règlement intérieur.

Art. 6. - Les ministres, les autorités publiques, les agents publics ne peuvent s'opposer à l'action de la commission pour quelque motif que ce soit et doivent prendre toutes mesures utiles pour la faciliter.

Art. 7. - La commission émet un avis dans un délai de deux mois à compter de sa saisine. Cet avis prend en considération les missions du service public de la justice, le respect de la présomption d'innocence et les droits de la défense, le respect des engagements internationaux de la France ainsi que la nécessité de préserver les capacités de défense et la sécurité des personnels.

En cas de partage égal des voix, celle du président est prépondérante.

Le sens de l'avis peut être favorable, favorable à une déclassification partielle ou défavorable.

L'avis de la commission est transmis à l'autorité administrative ayant procédé à la classification.

Art. 8. - Dans le délai de quinze jours francs à compter de la réception de l'avis de la commission, ou à l'expiration du délai de deux mois mentionné à l'article 7, l'autorité administrative notifie sa décision, assortie du sens de l'avis, à la juridiction ayant demandé la déclassification et la communication d'informations classifiées.

Le sens de l'avis de la commission est publié au *Journal officiel* de la République française.

Art. 9. - A l'occasion de la constitution de la première Commission consultative du secret de la défense nationale, le mandat des deux membres, autres que le président et les parlementaires, vient, par tirage au sort, à échéance au 30 septembre 2001 et au 30 septembre 2005.

Art. 10. - La présente loi est applicable dans les territoires d'outre-mer et dans la collectivité territoriale de Mayotte.

La présente loi sera exécutée comme loi de l'Etat.

Fait à Paris, le 8 juillet 1998

Jacques CHIRAC

Par le Président de la République :
Le Premier Ministre,
Lionel JOSPIN

Le garde des sceaux, ministre de la justice,
Elisabeth GUIGOU

Retour au sommaire

TEXTES RÉGLEMENTAIRES

Décret n° 78-78 du 25 janvier 1978 fixant les attributions du secrétaire général de la défense nationale

(*Journal officiel* du 26 janvier 1978)

. . . . . .

Art. 7.- Le secrétaire général de la défense nationale propose, diffuse, fait appliquer et contrôler les mesures nécessaires à la protection du secret de défense.

Art. 8. - Le secrétariat général de la défense nationale constitue un service du Premier ministre.

. . . . . .

Fait à Paris, le 25 janvier 1978.

Valéry GISCARD D'ESTAING.

Par le Président de la République :
Le Premier ministre,
Raymond BARRE.

Décret du 11 mars 1963 portant organisation de la sécurité de défense

(non publié au *Journal officiel*)

. . . . . .

Art.1er - Sous l'autorité du Premier ministre, le secrétaire général de la défense nationale est chargé d'étudier, de prescrire et de coordonner sur le plan interministériel les mesures propres à assurer la protection des secrets intéressant la défense nationale.

Le secrétaire général de la défense nationale veille à la mise en œuvre de ces mesures. Il a qualité pour la contrôler. Il a la possibilité en toutes circonstances de saisir, par l'intermédiaire des ministres intéressés, les services qui concourent à la répression des délits.

Art.2. - Les attributions de sécurité de défense définies ci-dessus n'affectent pas les responsabilités propres des ministres en matière de sécurité de défense.

Art.3. - Le secrétaire général de la défense nationale, à ce titre, dispose d'un service dont la composition est fixée par un décret.

Le chef de ce service peut se voir confier tout ou partie des attributions définies à l'article 1er du présent décret.

Art.4. - Le service de sécurité de défense est administré par le secrétariat général de la défense nationale. Les crédits nécessaires à son fonctionnement sont inscrits au budget du Premier ministre, secrétariat général de la défense nationale.

. . . . . .

Fait à Paris, le 11 mars 1963

Par le Président de la République : Charles DE GAULLE

Le Premier ministre,
Georges POMPIDOU.

Décret n° 80-243 du 3 avril 1980 relatif aux attributions des hauts fonctionnaires de défense

(*Journal officiel* du 5 avril 1980)

. . . . . .

Art. 1er. - Dans les départements autres que celui de la défense, le ministre est assisté pour l'exercice de ses responsabilités de défense par un ou, exceptionnellement, si les structures du département l'exigent, plusieurs hauts fonctionnaires de défense.

Art. 2. - Le haut fonctionnaire de défense est le conseiller du ministre pour toutes les questions relatives aux mesures de défense qui incombent à celui-ci en application de l'ordonnance du 7 janvier 1959. Il anime et coordonne la préparation de ces mesures et contrôle leur exécution.

Dans le cadre de ces fonctions :

Il veille à l'élaboration et, le cas échéant, à la mise en œuvre des plans de défense intéressant le département;

Il a vocation à représenter le ministre dans les commissions et réunions traitant des questions de défense;

Il est en liaison permanente avec le secrétaire général de la défense nationale ;

Il est responsable de l'application des dispositions relatives à la sécurité de défense et à la protection du secret (décret n°86-446 du 14 mars 1986, art.1er.), «ainsi qu'à la sécurité des systèmes d'information»;

Il est tenu informé de toutes les questions pouvant avoir une incidence en matière de défense au sein de son département.

Art. 3. - Le haut fonctionnaire de défense relève directement du ministre. Pour l'exercice de sa mission, il a autorité sur l'ensemble des directions et services du département.

Art. 4. - Le haut fonctionnaire de défense est nommé par décret sur proposition du ministre intéressé.

Art. 5. - Le ministre met à la disposition du haut fonctionnaire de défense, les moyens en personnel et en matériel nécessaires à l'exécution de sa mission.

. . . . . .

Fait à Paris, le 3 avril 1980. Valéry GISCARD D'ESTAING
Par le Président de la République :
Le Premier ministre,
Raymond BARRE

Décret n° 97-34 du 15 janvier 1997
relatif à la déconcentration des décisions administratives individuelles

(*Journal officiel* du 18 janvier 1997)

. . . . . .

Art. 1. - Les décisions administratives individuelles entrant dans le champ des compétences des administrations civiles de l'État, à l'exception de celles concernant les agents publics, sont prises par le préfet.

Toutefois, restent applicables les dispositions en vigueur à la date de publication du présent décret qui attribuent compétence pour prendre de telles décisions au préfet de zone, au préfet de région, aux chefs des services déconcentrés de l'État, aux magistrats de l'ordre administratif ou judiciaire et aux maires.

Art. 2. - Postérieurement à la publication du présent décret, des dérogations à la règle énoncée à l'article 1er peuvent être décidées dans les conditions suivantes :

1°. Des décrets en conseil d'État et en conseil des ministres fixent la liste des décisions qui sont prises par les ministres ou par décret ;

2°. Des décrets en Conseil d'État déterminent les décisions qui sont prises par le préfet de zone, le préfet de région, les chefs des services déconcentrés de l'État pour l'exercice des missions mentionnées aux articles 7 et 9 du décret n° 82-389 du 10 mai 1982 et aux articles 6 et 8 du décret n° 82-390 du 10 mai 1982 susvisés, les magistrats de l'ordre administratif ou judiciaire et les maires.

Art. 3. - Les dispositions de l'article 1er du présent décret entrent en vigueur le 1er janvier 1998. Les dispositions réglementaires contraires au présent décret sont abrogées à compter de la même date.

. . . . . .

Fait à Paris, le 15 janvier 1997. Jacques CHIRAC
Par le Président de la République :
Le Premier ministre,
Alain JUPPÉ

Décret n° 97-1206 du 19 décembre 1997 pris pour l'application à l'ensemble des ministres du 1° de l'article 2 du décret n° 97-34 du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles.

(*Journal officiel* du 21 décembre 1997)

. . . . . .

Art. 1er. - Les décisions administratives individuelles appartenant aux catégories de décisions dont la liste figure en annexe sont prises soit par les ministres, soit par décret selon que les dispositions en vigueur donnent compétence aux uns ou à l'autre.

Toutefois, restent applicables les dispositions en vigueur à la date de publication du présent décret qui attribuent compétence pour prendre de telles décisions au préfet, aux chefs des services à compétence nationale, au préfet de zone, au préfet de région, au préfet de police, au préfet maritime, aux autres autorités déconcentrées de l'État, aux magistrats de l'ordre administratif ou judiciaire et aux maires. Lorsque ces dispositions attribuent compétence par référence à un seuil, les règles de détermination de ce seuil demeurent en vigueur.

Art. 2. - Le présent décret entre en vigueur le 1er janvier 1998.

. . . . . .

ANNEXE

Liste des catégories de décisions administratives individuelles prises dans les conditions prévues au 1° de l'article 2 du décret du 15 janvier 1997

. . . . . .

11° Décisions d'habilitation à connaître les informations couvertes par le secret de la défense.

. . . . . .

Fait à Paris, le 19 décembre 1997. Jacques CHIRAC

Par le Président de la République :
Le Premier ministre,
Lionel JOSPIN

Décret n° 98-608 DU 17 JUILLET 1998 relatif à la protection des secrets de la défense nationale

(*Journal officiel* du 19 juillet 1998)

Le Premier ministre,
Sur le rapport du ministre de la défense,
Vu le code pénal, et notamment son article 413-9;
Vu l'ordonnance n° 59-147 du 7 janvier 1959 modifiée portant organisation générale de la défense, et notamment son article 1er;

. . . . . .

Décrète :

Art. 1er. - Les renseignements, procédés, objets, documents, données informatisées ou fichiers présentant un caractère de secret de la défense nationale sont dénommés dans le présent décret : «informations ou supports protégés».

Art. 2. - Les informations ou supports protégés font l'objet d'une classification comprenant trois niveaux :
1° Très Secret-Défense ;
2° Secret-Défense ;
3° Confidentiel-Défense.

Art. 3. - Le niveau Très Secret-Défense est réservé aux informations ou supports protégés dont la divulgation est de nature à nuire très gravement à la défense nationale et qui concernent les priorités gouvernementales en matière de défense.

Le niveau Secret-Défense est réservé aux informations ou supports protégés dont la divulgation est de nature à nuire gravement à la défense nationale.

Le niveau Confidentiel-Défense est réservé aux informations ou supports protégés dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale classifié au niveau Très Secret-Défense ou Secret-Défense.

Art. 4. - Les informations ou supports protégés portent la mention de leur niveau de classification.

Les modifications ou suppressions des mentions sont décidées par les autorités qui ont procédé à la classification.

Art. 5. - Le Premier ministre détermine les critères et les modalités d'organisation de la protection des informations ou supports protégés classifiés au niveau Très Secret-Défense.

Pour les informations ou supports protégés classifiés au niveau Très Secret-Défense, le Premier ministre définit les classifications spéciales dont ils font l'objet et qui correspondent aux différentes priorités gouvernementales.

Dans les conditions fixées par le Premier ministre, chaque ministre, pour ce qui relève de ses attributions, détermine les informations ou supports protégés qu'il y a lieu de classifier à ce niveau.

Art. 6. - Dans les conditions fixées par le Premier ministre, les informations ou supports protégés classifiés au niveau Secret-Défense ou Confidentiel-Défense, ainsi que les modalités d'organisation de leur protection, sont déterminés par chaque ministre pour le département dont il a la charge.

Art. 7. - Nul n'est qualifié pour connaître des informations ou supports protégés s'il n'a fait au préalable l'objet d'une décision d'habilitation et s'il n'a besoin de les connaître pour l'accomplissement de sa fonction ou de sa mission.

Art. 8. - La décision d'habilitation précise le niveau de classification des informations ou supports protégés dont le titulaire peut connaître. Elle intervient à la suite d'une procédure définie par le Premier ministre.

Elle est prise par le Premier ministre pour le niveau Très Secret-Défense et indique notamment la ou les catégories spéciales auxquelles la personne habilitée a accès.

Pour les niveaux de classification Secret-Défense et Confidentiel-Défense, la décision d'habilitation est prise par chaque ministre pour le département dont il a la charge.

Art. 9. - Le présent décret est applicable dans les territoires d'outre-mer et dans la collectivité territoriale de Mayotte.

Art. 10. - A l'article R. 413-6 du code pénal, les mots : «le décret n° 81-514 du 12 mai 1981 relatif à l'organisation de la protection des secrets et des informations concernant la défense nationale et la sûreté de l'État» sont remplacés par les mots suivants : «le décret n° 98-608 du 17 juillet 1998 relatif à la protection des secrets de la défense nationale».

Art. 11. - Le décret n° 81-514 du 12 mai 1981 relatif à l'organisation de la protection des secrets et des informations concernant la défense nationale et la sûreté de l'Etat est abrogé.

Art. 12. - Le garde des sceaux, ministre de la justice, le ministre de l'intérieur, le ministre de la défense et le secrétaire d'État à l'outre-mer sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait à Paris, le 17 juillet 1998

Lionel JOSPIN

Retour au sommaire

LISTE DES INSTRUCTIONS INTERMINISTÉRIELLES sur la protection du secret de la défense nationale

_____

- Instruction interministérielle n° **2100** /SGDN/SSD du 1er décembre 1975 pour l'application en France du système de sécurité de l'organisation du traité de l'Atlantique nord ;

- instruction interministérielle n° **900** /SGDN /SSD/DR du 20 juillet 1993 sur la sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées

- instruction interministérielle n° **2101** /SGDN/SSD/DR du 22 mai 1995 pour l'application en France du système de sécurité de l'Union de l'Europe occidentale ;

- directive n° **1223** /SGDN/SSD/DR du 17 décembre 1984 *(modifiée le 20 novembre 1990)* sur la protection matérielle des documents classifiés ;

- instruction interministérielle n° **2000** /SGDN/SSD/DR du 1er octobre 1986 sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'État dans les marchés et autres contrats ;

- directives n° **02**/SGDN/SSD/CD du 3 février 1986 d'application pratique sur l'organisation et le fonctionnement des classifications spéciales «Très Secret-Défense»;

- instruction interministérielle n° **1310** /SGDN/DEN/SSD/DR du 18 octobre 1996 pour l'enregistrement du courrier classifié.

Retour au sommaire

MODÈLES
de
notices, formulaires et décisions administratives

- notice individuelle de sécurité *(Modèle 01/IGI 1300);*
- demande ou renouvellement d'habilitation *(Mle 02/IGI 1300);*
- demande de contrôle élémentaire *(Mle 03/IGI 1300);*

- décision d'habilitation aux informations ou supports protégés *(Mle 04/IGI 1300);*
- décision de sécurité convoyeur *(Mle 05/IGI 1300);*

- certificat de sécurité *(Mle 07/IGI 1300);*
- engagement de responsabilité *(Mle 08/IGI 1300);*

- certificat de courrier *(Mle 09/IGI 1300);*
- certificat de courrier multivoyages *(Mle 09bis/IGI 1300);*
- liste inventaire *(Mle 10/IGI 1300);*

- demande de reproduction *(Mle 11/IGI 1300);*
- autorisation de reproduction *(Mle 12/IGI 1300);*

- procès-verbal de destruction *(Mle 13/IGI 1300);*

- bordereau d'envoi A *(Mle 14/IGI 1300);*
- bordereau d'envoi B *(Mle 14 bis/IGI 1300);*
- bordereau d'envoi B' *(Mle 14 ter/IGI 1300);*

- modèles de timbres de classification et de protection *(Mle 15/IGI 1300);*
- modèles de timbres de déclassification *(Mle 16/IGI 1300).*

Retour au sommaire

CONFIDENTIEL PERSONNEL

NOTICE INDIVIDUELLE (Modèle 94 A) *(Mle 01/IGI 1300)*

Photographie d'identité de face datant de moins de 1 an

ZONE RESERVEE A L'ORGANISME DEMANDEUR

ORGANISME DEMANDEUR :

TYPE DE PROCEDURE D'HABILITATION DEMANDEE (cochez une des 3 cases)

ADMISSION ☐ RENOUVELLEMENT ☐ REVISION ☐

HABILITATION : ***TRES SECRET*** ☐ ***SECRET*** ☐ ***CONFIDENTIEL*** ☐

AUTORITE DE DECISION A LAQUELLE DOIT ETRE RENVOYE L'AVIS DE SECURITE :

VISA DE L'AUTORITE DE L'ORGANISME DEMANDEUR ***le***

SIGNATURE DE L'AUTORITE

NOM FONCTION :

CANDIDAT A L'HABILITATION

NOM DE FAMILLE (de jeune fille suivi d'épouse X... pour les femmes mariées) (EN LETTRES MAJUSCULES) — *SEXE* M ☐ F ☐ — *DATE DE NAISSANCE*

PRENOMS (SOULIGNER LE PRENOM USUEL) | *SURNOM OU ALIAS EVENTUEL*

LIEU DE NAISSANCE | *CODE POSTAL* | *PAYS*

NATIONALITE(S) A LA NAISSANCE | *NATIONALITE(S) ACTUELLEMENT DETENUE(S)*

ANNEE D'ACQUISITION DE LA NATIONALITE FRANÇAISE | *ANNEE D'ARRIVEE en FRANCE* | *PAYS D'ORIGINE*

ADRESSE COMPLETE DU DOMICILE ACTUEL (N°, RUE, COMMUNE) (1) | *CODE POSTAL* | *DEPUIS LE* | *N° de téléphones -email*

ADRESSE COMPLETE DE LA RESIDENCE OCCASIONNELLE OU SECONDAIRE (y compris à l'étranger) (1) | *CODE POSTAL* | *DEPUIS LE* | *N° de téléphones -email*

DOMICILES ET RESIDENCES SUCCESSIFS PENDANT LES CINQ DERNIERES ANNEES (sauf domicile actuel, commencez par le plus récent) (1)

ADRESSE COMPLETE (N°, RUE, COMMUNE) (LE PAYS S'IL EST ETRANGER) | *CODE POSTAL* | *DATES*

SITUATION PROFESSIONNELLE ACTUELLE

CIVIL ☐ *FONCTION - PROFESSION* | *MILITAIRE* ☐ *GRADE - FONCTION* | *ARMEE OU ARME D'APPARTENANCE*

MINISTERE D'ORIGINE | *MINISTERE D'EMPLOI*

ORGANISME D'AFFECTATION | *DEPUIS LE*

ADRESSE PROFESSIONNELLE | *N° DE TELEPHONE E.MAIL - PROFESSIONNEL*

EMPLOIS SUCCESSIFS DES 5 DERNIERES ANNEES (1)

ETABLISSEMENT OU ORGANISME D'EMPLOI/ADRESSE(N°, RUE, COMMUNE) (PAYS S'IL EST ETRANGER)	*EMPLOI OU FONCTION (ex :secrétaire, etc.)*	*PERIODE*	*CODE POSTAL*

NIVEAU D'HABILITATION DEJA OBTENU : — *DATE :*

(1) Utiliser l'espace "Renseignements complémentaires"en page 4 si nécessaire

NIVEAU D'ETUDES ET CULTURE GENERALE

DIPLOMES OBTENUS OU NIVEAU EQUIVALENT	*LANGUES ETRANGERES*	*DEGRE DE CONNAISSANCE*

SITUATION DE FAMILLE ACTUELLE

Célibataire	*En instance de mariage*	*Marié(e)*	*Veuf(ve)*	*Séparé(e)*	*Divorcé(e)*	*En instance de remariage*	*Remarié(e)*	*Concubinage*	*Autre Situation*	*PACS*	*Nbre d'enfants (en chiffre)*
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

DATE ET LIEU DE MARIAGE OU DE LA PRESENTE SITUATION

SITUATION MILITAIRE ACTUELLE

Réformé dispensé-exempté	*Sous contrat*	*Carrière*	*Réserve*	*Autre situation*
☐	☐	☐	☐	☐

A NE REMPLIR QUE PAR LES MILITAIRES, OFFICIERS DE RESERVE OU LES PERSONNES AYANT QUITTE l'ARMEE DEPUIS MOINS DE CINQ ANS

NUMERO MATRICULE	*BUREAU DU SERVICE NATIONAL*	*CONTINGENT*

SITUATION DANS LA RESERVE →	*UNITE D'AFFECTATION*	*DEPUIS LE*

DOCUMENTS ADMINISTRATIFS

CARTE NATIONALE D'IDENTITE	*NUMERO*	*DATE DE DELIVRANCE*	*AUTORITE DE DELIVRANCE*
PASSEPORT	*NUMERO*	*DATE DE DELIVRANCE*	*AUTORITE DE DELIVRANCE*

VOYAGES ET SEJOURS A L'ETRANGER DANS LES 5 DERNIERES ANNEES EN PARTANT DU PLUS RECENT (1)

PAYS - LIEUX	*ANNEES*	*MOTIFS (professionnel / familial / touristique)*

ENFANTS (1)

Noms et prénoms	*Date de naissance*	*Lieu de naissance*	*Code postal*	*Nationalité*	*Domicile distinct éventuel*

Pour les enfants nés précédemment à la situation matrimoniale actuelle, ne les mentionner que s'ils résident au domicile du candidat.

	PERE DU CANDIDAT	MERE DU CANDIDAT
NOM – PRENOM (de jeune fille pour la mère)		
DATE ET LIEU DE NAISSANCE		
CODE POSTAL		
NATIONALITE DE NAISSANCE / NATIONALITE ACTUELLE		
DATE D'ARRIVEE en FRANCE / PAYS D'ORIGINE		
ANNEE D'ACQUISITION DE LA NATIONALITE FRANÇAISE		
ADRESSE COMPLETE DU DOMICILE ACTUELLE (CODE POSTAL) OU DERNIER DOMICILE AVANT LE DECES		
NOM ET ADRESSE DE L'EMPLOYEUR		

(1) Utiliser l'espace " Renseignements complémentaires" en page 4 si nécessaire.

CONJOINT OU CONCUBIN DU CANDIDAT

NOM DE FAMILLE (de jeune fille suivi d'épouse X... pour les femmes mariées) (EN LETTRES MAJUSCULES)	SEXE M ☐ F ☐	DATE DE NAISSANCE

PRENOMS (SOULIGNER LE PRENOM USUEL)	SURNOM OU ALIAS EVENTUEL

LIEU DE NAISSANCE	CODE POSTAL	PAYS

NATIONALITE(S) A LA NAISSANCE	NATIONALITE5S) ACTUELLEMENT DETENUE(S)

ANNEE D'ACQUISITION DE LA NATIONALITE FRANÇAISE	ANNEE D'ARRIVEE EN FRANCE	PAYS D'ORIGINE

ADRESSE COMPLETE DU DOMICILE ACTUEL (N°, RUE, COMMUNE) (1)	CODE POSTAL	DEPUIS LE	N° de téléphones - email
ADRESSE COMPLETE DE LA RESIDENCE OCCASIONNELLE OU SECONDAIRE (y compris à l'étranger) (1)	CODE POSTAL	DEPUIS LE	N° de téléphones - email

NIVEAU D'ETUDES ET CULTURE GENERALE

DIPLOMES OBTENUS OU NIVEAU EQUIVALENT	LANGUES ETRANGERES	DEGRE DE CONNAISSANCE

SITUATION PROFESSIONNELLE ACTUELLE

CIVIL ☐ FONCTION PROFESSION	MILITAIRE ☐ GRADE - FONCTION	ARMEE ET ARME D'APPARTENANCE

MINISTERE D'ORIGINE	MINISTERE D'EMPLOI

ORGANISME D'AFFECTATION	DEPUIS LE

ADRESSE PROFESSIONNELLE	N° DE TELEPHONE - E.MAIL PROFESSIONNEL

SITUATION DE FAMILLE PRECEDENTE

Célibataire	En instance de mariage	Marié(e)	Veuf(ve)	Séparé(e)	Divorcé(e)	En instance de remariage	Remarié(e)	Concubinage	Autre Situation	PACS	Nbre d'enfants (en chiffre)
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

DATE ET LIEU DE LA PRECEDENTE SITUATION

SITUATION MILITAIRE ACTUELLE (si le conjoint(e) est militaire en activité, officier de réserve ou ayant quitté l'armée depuis moins de 5 ans)

Réformé	Sous contrat	Carrière	Réserve	Autre situation
☐	☐	☐	☐	☐

NUMERO MATRICULE	BUREAU DU SERVICE NATIONAL	CONTINGENT

SITUATION DANS LA RESERVE	UNITE D'AFFECTATION	DEPUIS LE

PERE DU CONJOINT — MERE DU CONJOINT

NOM - PRENOM (de jeune fille pour la mère)		
DATE ET LIEU DE NAISSANCE		
CODE POSTAL		
NATIONALITE DE NAISSANCE / NATIONALITE ACTUELLE		
DATE D'ARRIVEE en FRANCE / PAYS D'ORIGINE		
ANNEE D'ACQUISITION DE LA NATIONALITE FRANÇAISE		
ADRESSE COMPLETE DU DOMICILE ACTUELLE (CODE POSTAL) OU DERNIER DOMICILE AVANT LE DECES		
NOM ET ADRESSE DE L'EMPLOYEUR		

RENSEIGNEMENTS DE SECURITE

Répondre par O**UI** ou par **NON** aux questions suivantes :

1) “Votre conjoint(e) ou concubin(e) s’est-il rendu à l’étranger au cours des 5 dernières années” ?

Si la réponse est positive, précisez les pays étrangers concernés ainsi que les dates et les motifs (professionnel, familial, touristique...)

2) Vous-même, ainsi que votre conjoint(e) ou concubin(e) :

a) “Pensez-vous avoir retenu l’attention d’un service de renseignement ou de sécurité étranger” ?

b) “Estimez-vous que des pressions ont été exercées sur vous, ou sur des membres de votre famille, à la suite d’un incident survenu sur le territoire étranger” ?

c) “Etes-vous en relations suivies, à titre professionnel ou privé, avec des ressortissants étrangers” ?

d) “Pensez-vous avoir été sollicité(e) en dehors de vos attributions professionnelles pour fournir des informations à caractère sensible” ?

e) “Avez-vous des proches parents résidant à l’étranger” ?

Si la réponse est positive, nommez les proches parents, les relations à titre privé avec des ressortissants étrangers, et le(s) pays concernés.

RENSEIGNEMENTS COMPLEMENTAIRES (éventuellement)

Précisez les autres personnes vivant sous le même toit : Nom - Prénoms - Lieu et date de naissance - nationalité - qualité ou degré de parenté

ATTESTATION

Je soussigné(e) (Nom, prénom) : _____

a) Reconnais être informé(e) en application de l’article 25 de la loi n°78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés :

- du caractère obligatoire des réponses qui me sont demandées.
- de ce qu’en l’absence de réponse aux questions posées, aucune décision ne pourra être prise quant à mon éventuelle habilitation.
- de ce que je dispose d’un droit d’accès et de rectification dans les conditions prévues aux articles 34 et suivants de la loi précipitée du 6 janvier 1978.

b) Certifie l’exactitude des renseignements que j’ai mentionnés par écrit dans la présente notice.

c) Déclare avoir pris connaissance des dispositions législatives et réglementaires relatives à la protection du secret de la défense nationale, (notamment des articles 413-9 à 413-12 du code pénal) et de l’instruction générale interministérielle sur la protection du secret de la défense nationale.

d) Reconnais être informé(e) que je m’expose à une peine de 3 ans d’emprisonnement et de 45.000 euros d’amende :

- en cas d’altération frauduleuse de la vérité, dans les conditions prévues à l’article 441-1 du code pénal,
- si, par mon imprudence ou ma négligence, un renseignement, procédé, une donnée informatisée ou un fichier dont je suis le dépositaire et qui a un caractère de secret de la défense nationale, a été détruit, détourné, soustrait, reproduit ou porté à la connaissance, soit du public soit d’une personne non qualifiée (article 413-10 du code pénal).

A LE SIGNATURE

Retour au sommaire

Ministère
Organisme demandeur
(timbre)
N° . . . /

DEMANDE[25] D'HABILITATION

- Renouvellement[26] -

Mle 02/IGI 1300

Niveau[27] de classification des informations ou supports protégés : . . . . . .

Renseignements d'identité :

- NOM[28] et Prénom : . . . . . .
- Date et lieu de naissance : . . . . . .

Renseignements professionnels :

- Grade ou titre : . . . . . .
- Emploi et fonctions exercées : . . . . . .

. . . . . .

- Habilitation déjà obtenue[29] *(s'il y a lieu)* : . . . . . .

Motifs :

L'emploi à occuper figure au poste n° . . . . dans le catalogue des emplois de mon organisme nécessitant une décision d'habilitation.

L'engagement de la procédure d'urgence[30] est souhaitable pour les raisons suivantes :

. . . . . .

. . . . . .

A . . . . . , le . . . . . .

Nom, qualité, signature de l'autorité hiérarchique compétente et cachet de l'organisme

Visa (n*om et signature)* de l'agent de sécurité, du fonctionnaire de sécurité ou du chef du bureau d'ordre ou de contrôle pour les informations de l'OTAN, de L'UE et cachet de l'organisme. A . . . . . , le	Visa (n*om et signature)* de l'agent central de sécurité ou du chef du bureau principal ou isolé pour les informations de l'OTAN, de l'UE et cachet de l'organisme. A . . . . . ., le . . . .

Retour au sommaire

[25] Joindre trois notices Mle 01/IGI 1300 (dont un original) et trois photos d'identité ; établir une demande pour chaque classification.
[26] Rayer les mentions inutiles.
[27] Pour le niveau Très-Secret, indiquer la classification spéciale et, le cas échéant, les catégories.
[28] Nom de jeune fille pour une femme mariée suivi de la mention "épouse "X".
[29] Joindre l'attestation Mle 07/IGI 1300 en cas de changement d'affectation.
[30] Utilisable à titre exceptionnel et pour urgence motivée.

Ministère
Organisme demandeur
(timbre)
N° . . . . . /

DEMANDE DE CONTROLE ÉLÉMENTAIRE

Mle 03/IGI 1300

Niveau de classification des informations ou supports protégés[31] :

- **Confidentiel-Défense ou Secret-Défense**, pour convoyeur n'ayant pas besoin d'en connaître.

Renseignements d'identité :

- NOM[32] et Prénom : . . . . . .

- Date et lieu de naissance : . . . . . .

- Nationalité à la naissance : . . . . . .
- Nationalité actuelle *(en cas de double nationalité, le préciser)* : . . . . . .
. . . . . .
- Domicile actuel : . . . . . .
. . . . . .
- Domicile antérieur *(si un changement est intervenu depuis moins de cinq ans)* : . . . . . .
. . . . . .

Renseignements professionnels :

- Grade ou titre : . . . . . .
. . . . . .
- Emploi et fonctions exercées : . . . . . .
. . . . . .
- Date d'expiration de la décision de sécurité convoyeur déjà obtenue *(s'il y a lieu)* :
. . . . . .

A . . . . . , le . . . . . .
Nom, qualité, signature de l'autorité hiérarchique compétente[33]
et cachet de l'organisme

Retour au sommaire

[31] Rayer les mentions inutiles.
[32] Nom de jeune fille pour une femme mariée suivi de la mention "épouse "X".
[33] Autorité de décision ayant reçu délégation à cet effet.

Ministère
Organisme employeur
(timbre)
N° /

DÉCISION D'HABILITATION aux informations ou supports protégés

Mle 04/IGI 1300

Le[34] . . . . . .

décide que

Monsieur, Madame **:** . . . . . .
(*NOM et Prénom)*

né(e) le **:** . . . . . .à : . . . . . .

grade ou titre **:** . . . . . .

fonctions exercées **:**. . . . . .

est habilité(e) aux informations ou supports protégés jusqu'au niveau et y compris :

- SECRET-DÉFENSE
- CONFIDENTIEL-DÉFENSE

Cette décision est valable jusqu'au [35] : . . . . . .

A . . . . . le. . . . . .
Nom, qualité, signature de l'autorité hiérarchique compétente[36]
et cachet de l'organisme

Retour au sommaire

[34] Autorité hiérarchique compétente.
[35] Date d'expiration de la décision.
[36] Autorité de décision ayant reçu délégation à cet effet.

Ministère
Organisme employeur
(timbre)
N° /

DÉCISION
DE SÉCURITÉ CONVOYEUR

Mle 05/IGI 1300

Le[37] . . . . . .

décide que

Monsieur, Madame **:** . . . . . .
(*NOM et Prénom)*

né(e) le **:** . . . . . .à : . . . . . .

grade ou titre **:** . . . . . .

fonctions exercées **:**. . . . . .

peut effectuer le convoyage(1) de supports protégés jusqu'au niveau et y compris[38] :

- SECRET-DÉFENSE
- CONFIDENTIEL-DÉFENSE

Cette décision est valable jusqu'au [39] : . . . . . .

A . . . . . le. . . . . .
Nom, qualité, signature de l'autorité hiérarchique compétente[40]
et cachet de l'organisme

Retour au sommaire

[37] Autorité hiérarchique compétente.
[38] Rayer les mentions inutiles
[39] Date d'expiration de la décision.
[40] Autorité de décision ayant reçu délégation à cet effet.

Ministère
Organisme employeur
(timbre)
N° /

CERTIFICAT DE SÉCURITÉ[41]

Mle 07/IGI 1300

Délivré par *(Ministère, organisme)* : . . . . . .
. . . . . .
Date et lieu de délivrance : . . . . . .

Numéro : . . . . . valable jusqu'au : . . . . . .

Objet / mission : . . . . . .

Il est certifié par le présent document que Monsieur, Madame

NOM et Prénom : . . . . . .

Grade et fonctions : . . . . . .

Date et lieu de naissance : . . . . . .

Détenteur du passeport / de la carte d'identité n° : . . . . . .

Délivré à : . . . . . en date du :. . . . . .

a fait l'objet d'une procédure d'habilitation pour la période du : . . . . . .au : . . . . . .

pour l'accès aux informations ou supports protégés au niveau[42] : . . . .

Conformément aux dispositions de l'Instruction interministérielle n°1300 sur la protection du secret de la défense nationale.
ou
Conformément aux dispositions de l'Instruction interministérielle n°2100 pour l'application en France du système de sécurité de l'OTAN[43]

NOM, qualité, signature de l'autorité délivrant le certificat et cachet de l'organisme

Retour au sommaire

[41] Certificat à retourner à l'autorité qui l'a délivré, à l'issue de la mission pour laquelle il a été accordé.
[42] Niveau de classification maximum
[43] Rayer la mention inutile

E N G A G E M E N T
DE RESPONSABILITÉ

Mle 08/IGI 1300

NOM et prénom : . . . . . .
Grade ou fonction : . . . . . .
Service employeur : . . . . . .

- 1er volet -

Je, soussigné(e), déclare :

- avoir pris **connaissance** de l'instruction générale interministérielle n° 1300 /SGDN sur la protection du secret de la défense nationale, ainsi que des dispositions du code pénal citées en annexe à l'instruction ;

- être pleinement conscient(e) de mes **responsabilités** en ce qui concerne la sauvegarde des informations ou supports protégés de la défense nationale.

- être informé(e) des **conséquences** prévues par la loi (code pénal, en particulier les articles 121-2, 411-1 à 411-11, 413-9 à 413-12 et 414-7 à 414-9) et les règlements administratifs, notamment pour le cas où sciemment ou par négligence, je laisserais lesdites informations ou supports protégés parvenir à des personnes non autorisées à en avoir connaissance.

En conséquence, **je m'engage à ne pas divulguer**, même après la cessation de mes fonctions, à des personnes non autorisées à "en connaître" les informations ou supports protégés dont j'aurai connaissance dans l'exercice de mes fonctions.

NOM, qualité, signature de l'autorité hiérarchique compétente attestant que l'intéressé(e) a été informé(e) de ses responsabilités à l'égard de la protection des informations ou supports protégés.

A . . . . . , le . . . . . .
signature de l'intéressé(e)

- 2ème volet -RAPPEL

A compter de la date de cessation des fonctions, pour lesquelles une décision d'habilitation aux informations ou supports protégés de la défense nationale m'a été accordée, **je m'engage à ne pas divulguer** à des personnes non autorisées à "en connaître" les informations ou supports protégés dont j'ai eu connaissance dans l'exercice de mes fonctions et à **ne pas conserver** par-devers moi tout document ou support protégé.

Je reconnais être informé(e) des **conséquences** prévues par la loi (code pénal, en particulier les articles 121-2, 411-1 à 411-11, 413-9 à 413-12 et 414-7 à 414-9) et les règlements administratifs, notamment pour le cas où, sciemment ou par négligence, je porterais à la connaissance de personnes non autorisées, les dites informations ou supports protégés.

NOM, qualité, signature de l'autorité hiérarchique compétente attestant que l'intéressé(e) a été informé de ses responsabilités à l'égard de la protection des informations ou supports protégés.

A . . . . . ., le . . . . . .
signature de l'intéressé(e)

Retour au sommaire

Ministère
Organisme employeur
(timbre)
N° . . . /

Reproduction interdite

CERTIFICAT DE COURRIER

(COURIER CERTIFICATE) Mle 09/IGI 1300

pour le convoiement international par convoyeur autorisé de DOCUMENTS/EQUIPEMENTS/COMPOSANTS CLASSIFIES

for international carriage of classified DOCUMENTS, EQUIPEMENTS AND/OR COMPONENTS

Nom du programme/projet ……..…….……..
Name of program/project

Il est certifié que le porteur Monsieur/Madame (nom, prénom et titre)……..……
This is to certify that the bearer, Mr/Mrs (name and title)

Né(e) le (jour, mois, année) – Born on (day/month/year) **:** ……..……**en (pays) –** in (country) **:**…….....……

Ressortissant (pays) – A national of (country) **:**……...….

Titulaire du passeport ou de la carte d'identité n° - Holder of passport/identity card n° **:**……...

Délivré(e) par (autorité) :…….……**le (jour, mois, année) :**…….
Issued by (issuing authority) on (day, month, year)

Et employé(e) par (société ou organisme) :……..……...
And employed with (company or organisation)

Est autorisé(e) à effectuer le voyage décrit ci-dessous avec l'envoi suivant: (indiquer n° des paquets, poids dimensions de chaque colis)
Is authorised to carry on the journey detailed below with the following consignment: (number, weight and dimensions of each package)

……
……
……

Itinéraire: départ le (date): ...…..…..... **de (pays) :** ...…..…..... **à (pays) :** ...…..….....
Itinerary: departure on (date) from (country) to (country)

Via (pays traversés) : ……..……..
through (countries)

Retour prévu le (date) – anticipated return (date) **:** …….....

L'attention des autorités des douanes, de police et/ou des services d'immigration est attirée sur les points donnés au dos de ce certificat.
The attention of Customs, Police, and/or Immigration Officials is drawn to the points stated on the back of this certificate.

Officier/Agent de sécurité de la société ou de l'établissement **Company security officer** (Cachet ou timbre et signature) (Stamp and signature) **Date :**	**Autorité de sécurité désignée** **Designed Security Authority** (Cachet ou timbre et signature) (Stamp and signature) **Date :**

Retour au sommaire

L’attention des autorités des douanes, de police et/ou des services d’immigration est attirée sur les points suivants:
The attention of Customs, Police, and/or Immigration Officials is drawn to the following:

- Le contenu de cet envoi est classifié dans l’intérêt de la sécurité nationale des pays cités ci-dessus;
  The material comprising this consignment is classified in the interests of national security of the countries here above;

- Il est demandé que l’envoi ne soit inspecté que par des personnes dûment autorisées ou titulaires d’une autorisation spéciale.
  It is requested that the consignment will not be inspected by other than properly authorised persons or those having special permission.

- Si une inspection est jugée nécessaire, il est demandé qu’elle soit effectuée dans une zone hors de vue des personnes qui n’ont pas une nécessité d’accès aux informations et en présence du courrier.
  If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not have a need-to-know and in the presence of the courier.

- Il est demandé que le paquet s’il a été ouvert pour inspection, soit muni, après avoir été refermé, de la preuve de cette ouverture, par signature et cachet et par annotation des documents d’expédition (s’il y en a) attestant l’ouverture de l’envoi.
  It is requested that the package, if opened for inspection, be marked after reclosing to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.

- Les fonctionnaires des douanes, de la police et /ou des services d’immigration des pays traversés, à l’entrée ou à la sortie, sont priés d’apporter leur assistance en cas de besoin afin que l’envoi soit amené à destination en toute sécurité.
  Customs, Police, and/or Immigration officials of countries to be transmitted, entered or exited are requested to give assistance if necessary to assure successful and secure delivery of the consignment.

Annexe au certificat de courrier n°

INSTRUCTIONS A L'ATTENTION DU CONVOYEUR AUTORISÉ

Annexe à l'ordre de mission . . . . . pour le transport international par convoyeur autorisé de documents, équipements et/ou composants classifiés

Vous avez été désigné pour convoyer un envoi classifié. Un « certificat de courrier » vous a été délivré. Avant le début du voyage, vous serez informé des règlements de sécurité relatifs au convoiement d'envois classifiés et de vos obligations en matière de sécurité durant ledit voyage (comportement à adopter, itinéraire, horaire, etc.).Il vous sera également demandé de signer une déclaration attestant que vous avez lu et compris les obligations relatives à la sécurité et que vous vous y conformez.

Votre attention est appelée sur les généralités suivantes :

1. Vous serez tenu pour responsable de l'envoi décrit dans le certificat de courrier.
2. Tout au long du voyage, cet envoi classifié devra rester en votre possession ou sous votre surveillance directe.
3. L'envoi ne devra pas être ouvert en cours de route, sauf dans les circonstances exposées au paragraphe 10 ci-dessous.
4. Vous ne devrez ni parler de cet envoi classifié ni le montrer dans un lieu public.
5. Cet envoi classifié ne doit en aucun cas être laissé sans surveillance durant les arrêts nocturnes. Les installations militaires ou des sociétés industrielles, ayant les habilitations appropriées, pourront être utilisées. Dans ce domaine, vous serez renseigné par l'Agent/Officier de sécurité de votre société ou organisme.
6. Durant le convoiement d'un envoi classifié, il vous est interdit de dévier du plan de voyage fourni.
7. En cas d'urgence, vous devrez prendre les mesures que vous jugerez nécessaires à la protection de l'envoi, mais en aucun cas vous ne devrez permettre que l'envoi ne reste pas en votre possession; à cette fin, vos instructions précisent comment entrer en rapport avec les organismes de sécurité des pays dans lesquels vous passerez en transit (cf. paragraphe 12 ci-après). Si ces précisions ne vous ont pas été fournies, demandez les à l'Agent/l'Officier de sécurité de votre société ou organisme.
8. Il vous appartient, à vous-même et à l'Agent/Officier de sécurité de votre société ou organisme de vous assurer que les documents nécessaires à votre sortie du territoire et à votre voyage (passeport, certificats de change, carnet sanitaire, etc…) sont complets et en cours de validité.
9. Si des circonstances imprévues vous obligent à remettre l'envoi à des personnes autres que les représentants désignés de la société ou du gouvernement que vous devez joindre, vous le remettrez uniquement à des agents autorisés de l'un des points de contact énumérés au paragraphe 12.
10. Il ne vous est conféré aucune immunité par rapport aux fouilles effectuées par les services de douanes, de police et/ou d'immigration des différents pays dont vous traverserez la frontière ; de ce fait, au cas où des agents demanderaient à connaître le contenu de l'envoi, vous leur montrerez votre «certificat de courrier» et la présente note et vous insisterez pour les présenter au chef du service de douane, de police et/ou d'immigration en personne ; cette démarche devrait normalement suffire à faire passer l'envoi sans qu'il soit ouvert. Toutefois, si le chef du service de douane, de police et/ou d'immigration demande à voir effectivement le contenu de l'envoi, vous pourrez ouvrir celui-ci, à condition que cela soit fait hors de la vue de tierces personnes.

    Vous devrez prendre la précaution de ne montrer à l'agent intéressé qu'une partie du contenu suffisante pour le convaincre que l'envoi ne contient aucun autre objet, et vous lui demanderez de refermer l'emballage ou de vous aider à le refermer immédiatement après achèvement de l'inspection.

    Vous demanderez au chef du service de douane, de police et/ou d'immigration de fournir la preuve de l'ouverture et de l'inspection des colis en y apposant sa signature et son cachet après fermeture et en confirmant au verso des listes inventaires que l'envoi a été ouvert.

S’il vous a été demandé d’ouvrir l’envoi dans les circonstances exposées ci-dessus, vous devrez le faire savoir à l’Agent/Officier de sécurité de la société ou de l’organisme destinataire et à l’Agent/Officier de sécurité de la société ou de l’organisme expéditeur, qui devront en informer les autorités de sécurité compétentes de leur gouvernement respectif (Autorité Nationale de Sécurité/Autorité de Sécurité Désignée).

11. A votre retour , vous devrez produire un récépissé de l’envoi, signé par l’Agent/Officier de sécurité de la société ou de l’organisme ayant reçu l’envoi ou par une autorité de sécurité compétence du gouvernement destinataire.

12. Au cours de votre itinéraire, vous pourrez entrer en rapport avec les autorités ci-après pour leur demander assistance :……..…….....
.....
.....
.....

Annexe au certificat de courrier n°

DÉCLARATION DU CONVOYEUR AUTORISÉ

Monsieur/Madame (nom, prénom) : ...….....….....

de (nom de la société ou de l'organisme) :

Fonction dans la société ou l'organisme : …….....….

DÉCLARATION :

L'Agent/Officier de sécurité de (nom de la société ou de l'organisme) :

m'a remis les notes concernant la manipulation et la garde des documents/équipements classifiés que je dois transporter. Je les ai lues et comprises.

Je conserverai à tout moment, durant le voyage, ces documents/équipements classifiés et n'ouvrirai pas le colis à moins d'en être requis par les autorités douanières.

A mon arrivée, je remettrai au dépositaire désigné, contre signature du récépissé, les documents/équipements classifiés destinés à la société/organisation réceptionnaire.

Fait à (lieu): ……..... , le (date) : …….

Signature du courrier : …….……..

En présence de (nom, prénom et signature de l'Agent/Officier de sécurité) :

Annexe au certificat de courrier
n°

ITINÉRAIRE AUTORISÉ

Détails de l'itinéraire :
Details of Itinerary :

Départ le (date) : ...….....….....
Departure on (date)

De (pays) : ...….....….....
From (country)

A (pays) : ...….....….....
To (country)

Via (pays traversés) : …….....….…
Through (countries)

Arrêts autorisés (pays) : …….....….…
Authorised stops (countries)

Retour prévu le (date) – anticipated return (date) **:** …….....

Références du bordereau d'envoi ou du récépissé – References of receipt or inventory list **:** …….....

Compte rendu à remplir et signer à la fin du voyage :

Je déclare sur l'honneur que durant le voyage correspondant au présent descriptif, il ne s'est produit à ma connaissance aucun événement ou acte, de mon fait ou du fait d'autrui, de nature à compromettre la sécurité de l'envoi, à l'exception des éléments signalés ci-dessous, le cas échéant :

Fait à (lieu): ……..... , le (date) : ……. Signature du courrier : ……..

En présence de (nom, prénom et signature de l'Agent/Officier de sécurité)

CERTIFICAT DE COURRIER MULTIVOYAGES

(MULTI-TRAVELS COURIER CERTIFICATE) Mle 09bis/IGI 1300

pour le convoiement international par convoyeur autorisé de DOCUMENTS/EQUIPEMENTS/COMPOSANTS CLASSIFIES

for international carriage of classified DOCUMENTS, EQUIPEMENTS AND/OR COMPONENTS

Nom du programme/projet ……..……..
Name of program/project

Il est certifié que le porteur Monsieur/Madame (nom, prénom et titre)……..
This is to certify that the bearer, Mr/Mrs (name and title)

Né(e) le (jour, mois, année) – Born on (day/month/year) **:** ……..……**en (pays) –** in (country) **:**…….....……

Ressortissant (pays) – A national of (country) **:**…….....……..

Titulaire du passeport ou de la carte d'identité n° - Holder of passport/identity card n° **:**……

Délivré(e) par (autorité) :…….……**le (jour, mois, année) :**……..
Issued by (issuing authority) on (day, month, year)

Et employé(e) par (société ou organisme) :……..……...
And employed with (company or organisation)

Est autorisé(e) à transporter des documents, équipements et matériels classifiés entre les pays suivants :
Is authorised to carry classified documents, equipments and components between the following countries :

…….

Le porteur ci-dessus est autorisé à utiliser le présent certificat autant que de besoin, pour des transports

The bearer above is authorised to use the present certificate as many times as necessary , for classified shipments between the

classifiés entre les pays ci-dessus jusqu'au (date de validité):……

countries here above until (validity date):

Chaque envoi est accompagné d'un descriptif de transport.

Each sending is attached with a description of shipment.

L'attention des autorités des douanes, de police et/ou des services d'immigration est attirée sur les points donnés au dos de ce certificat

The attention of Customs, Police, and/or Immigration Officials is drawn to the points stated on the back of this certificate.

Officier/Agent de sécurité de la société ou de l'établissement **Company security officer** (Cachet ou timbre et signature) (Stamp and signature) **Date :**	**Autorité de sécurité désignée** **Designed Security Authority** (Cachet ou timbre et signature) (Stamp and signature) **Date :**

Retour au sommaire

L'attention des autorités des douanes, de police et/ou des services d'immigration est attirée sur les points suivants:
The attention of Customs, Police, and/or Immigration Officials is drawn to the following:

- Le contenu de cet envoi est classifié dans l'intérêt de la sécurité nationale des pays cités ci-dessus;
  The material comprising this consignment is classified in the interests of national security of the countries here above;

- Il est demandé que l'envoi ne soit inspecté que par des personnes dûment autorisées ou titulaires d'une autorisation spéciale.
  It is requested that the consignment will not be inspected by other than properly authorised persons or those having special permission.

- Si une inspection est jugée nécessaire, il est demandé qu'elle soit effectuée dans une zone hors de vue
  des personnes qui n'ont pas une nécessité d'accès aux informations et en présence du courrier.
  If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not have a need-to-know and in the presence of the courier.

- Il est demandé que le paquet s'il a été ouvert pour inspection, soit muni, après avoir été refermé, de la preuve de cette ouverture, par signature et cachet et par annotation des documents d'expédition (s'il y en a) attestant l'ouverture de l'envoi.
  It is requested that the package, if opened for inspection, be marked after reclosing to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.

- Les fonctionnaires des douanes, de la police et /ou des services d'immigration des pays traversés, à l'entrée ou à la sortie, sont priés d'apporter leur assistance en cas de besoin afin que l'envoi soit amené à destination en toute sécurité.
  Customs, Police, and/or Immigration officials of countries to be transmitted, entered or exited are requested to give assistance if necessary to assure successful and secure delivery of the consignment.

Annexe au certificat de courrier multivoyages n°

INSTRUCTIONS A L'ATTENTION DU CONVOYEUR AUTORISÉ

Annexe à l'ordre de mission . . . . . pour le transport international par convoyeur autorisé de documents, équipements et/ou composants classifiés

Vous avez été désigné pour convoyer un envoi classifié. Un « certificat de courrier » vous a été délivré. Avant le début du voyage, vous serez informé des règlements de sécurité relatifs au convoiement d'envois classifiés et de vos obligations en matière de sécurité durant ledit voyage (comportement à adopter, itinéraire, horaire, etc.).Il vous sera également demandé de signer une déclaration attestant que vous avez lu et compris les obligations relatives à la sécurité et que vous vous y conformez.

Votre attention est appelée sur les généralités suivantes :

1-Vous serez tenu pour responsable de l'envoi décrit dans le certificat de courrier.

2-Tout au long du voyage, cet envoi classifié devra rester en votre possession ou sous votre surveillance directe.

3-L'envoi ne devra pas être ouvert en cours de route, sauf dans les circonstances exposées au paragraphe 10 ci-dessous.

4-Vous ne devrez ni parler de cet envoi classifié ni le montrer dans un lieu public.

5-Cet envoi classifié ne doit en aucun cas être laissé sans surveillance durant les arrêts nocturnes. Les installations militaires ou des sociétés industrielles, ayant les habilitations appropriées, pourront être utilisées. Dans ce domaine, vous serez renseigné par l'Agent/Officier de sécurité de votre société ou organisme.

6-Durant le convoiement d'un envoi classifié, il vous est interdit de dévier du plan de voyage fourni.

7-En cas d'urgence, vous devrez prendre les mesures que vous jugerez nécessaires à la protection de l'envoi, mais en aucun cas vous ne devrez permettre que l'envoi ne reste pas en votre possession; à cette fin, vos instructions précisent comment entrer en rapport avec les organismes de sécurité des pays dans lesquels vous passerez en transit (cf. paragraphe 12 ci-après). Si ces précisions ne vous ont pas été fournies, demandez les à l'Agent/l'Officier de sécurité de votre société ou organisme.

8-Il vous appartient, à vous-même et à l'Agent/Officier de sécurité de votre société ou organisme de vous assurer que les documents nécessaires à votre sortie du territoire et à votre voyage (passeport, certificats de change, carnet sanitaire, etc…) sont complets et en cours de validité.

9-Si des circonstances imprévues vous obligent à remettre l'envoi à des personnes autres que les représentants désignés de la société ou du gouvernement que vous devez joindre, vous le remettrez uniquement à des agents autorisés de l'un des points de contact énumérés au paragraphe 12.

10-Il ne vous est conféré aucune immunité par rapport aux fouilles effectuées par les services de douanes, de police et/ou d'immigration des différents pays dont vous traverserez la frontière ; de ce fait, au cas où des agents demanderaient à connaître le contenu de l'envoi, vous leur montrerez votre «certificat de courrier» et la présente note et vous insisterez pour les présenter au chef du service de douane, de police et/ou d'immigration en personne ; cette démarche devrait normalement suffire à faire passer l'envoi sans qu'il soit ouvert. Toutefois, si le chef du service de douane, de police et/ou d'immigration demande à voir effectivement le contenu de l'envoi, vous pourrez ouvrir celui-ci, à condition que cela soit fait hors de la vue de tierces personnes.

Vous devrez prendre la précaution de ne montrer à l'agent intéressé qu'une partie du contenu suffisante pour le convaincre que l'envoi ne contient aucun autre objet, et vous lui demanderez de refermer l'emballage ou de vous aider à le refermer immédiatement après achèvement de l'inspection.

Vous demanderez au chef du service de douane, de police et/ou d'immigration de fournir la preuve de l'ouverture et de l'inspection des colis en y apposant sa signature et son cachet après fermeture et en confirmant au verso des listes inventaires que l'envoi a été ouvert.

S’il vous a été demandé d’ouvrir l’envoi dans les circonstances exposées ci-dessus, vous devrez le faire savoir à l’Agent/Officier de sécurité de la société ou de l’organisme destinataire et à l’Agent/Officier de sécurité de la société ou de l’organisme expéditeur, qui devront en informer les autorités de sécurité compétentes de leur gouvernement respectif (Autorité Nationale de Sécurité/Autorité de Sécurité Désignée).

11-A votre retour , vous devrez produire un récépissé de l’envoi, signé par l’Agent/Officier de sécurité de la société ou de l’organisme ayant reçu l’envoi ou par une autorité de sécurité compétence du gouvernement destinataire.

12-Au cours de votre itinéraire, vous pourrez entrer en rapport avec les autorités ci-après pour leur demander assistance :……..…….....
.....
.....
.....

Annexe au certificat de courrier multivoyages n°

DÉCLARATION DU CONVOYEUR AUTORISÉ

Monsieur/Madame (nom, prénom) : ..…....….....

de (nom de la société ou de l'organisme) :

Fonction dans la société ou l'organisme : ……..…….

DÉCLARATION :

L'Agent/Officier de sécurité de (nom de la société ou de l'organisme) :

m'a remis les notes concernant la manipulation et la garde des documents/équipements classifiés que je dois transporter. Je les ai lues et comprises.

Je conserverai à tout moment, durant les voyages, ces documents/équipements classifiés et n'ouvrirai pas de colis à moins d'en être requis par les autorités douanières.

A chaque arrivée, je remettrai au dépositaire désigné, contre signature du récépissé, les documents/équipements classifiés destinés à la société/organisation réceptionnaire.

Fait à (lieu): ……..... , le (date) : …….

Signature du courrier : …….……..
En présence de (nom, prénom et signature de l'Agent/Officier de sécurité):

Annexe au certificat de courrier multivoyages n°

DESCRIPTIF DE TRANSPORT N°

Transport du (date) : ..... **au (date) :** ..... **effectué par (nom prénom) :** .....
Transport from (date) to (date) bearer (name)

Itinéraire de (pays) : ...….....….....….....**à (pays) :** ...….....….....….....
Itinerary from (country) to (country)

Via (pays traversés) : …….....….....**Arrêts autorisés (pays) :** …….....….....
Through (countries) Authorised stops (countries)

Références du bordereau d'envoi ou du récépissé : …….....….…..….
References of receipt or inventory list

Descriptif de l'envoi (nombres de paquets, dimensions et éventuellement poids de chaque paquet) :
Description of the shipment (number of package, dimensions and, if needed weight of each package)

Coordonnées des autorités susceptibles d'être contactées en cas de besoin :
Officials you may contact to request assistance

Signature de l'Officier / Agent de sécurité

Compte rendu à remplir et signer à la fin du voyage :

Je déclare sur l'honneur que durant le voyage correspondant au présent descriptif, il ne s'est produit à ma connaissance aucun événement ou acte, de mon fait ou du fait d'autrui, de nature à compromettre la sécurité de l'envoi, à l'exception des éléments signalés ci-dessous, le cas échéant :

Fait à (lieu): ……..…..... , le (date) : ……. Signature du courrier : …….……..

En présence de (nom, prénom et signature de l'Officier / Agent de sécurité): .....

LISTE INVENTAIRE

Mle 10 /IGI 1300

Liste inventaire établie au titre du certificat de courrier N° . . . . . *./.* . . . . . *du* . . . . . *.20..*

A . . . . . , le . . . . . 20..

DOCUMENTS . . . . . .

ÉQUIPEMENTS . . . . . .

COMPOSANTS . . . . . .

NIVEAU DE CLASSIFICATION . . . . . .

L'inventaire inscrit au verso a été approuvé par : . . . . . .
(NOM, prénom, adresse, directeur de programme, projet ou contrat)

Référence de l'autorisation : . . . . . .
(accordée par le directeur de programme pour le Secret-Défense)

Toute inspection au verso a été avalisée par : . . . . . .
(NOM, prénom, adresse, directeur de programme, projet ou contrat)

Référence de l'autorisation : . . . . . .
(accordée par le directeur de programme pour le Secret-Défense)

Convoyeur autorisé : . . . . . .
(NOM, Prénom et signature)

Officier ou agent de sécurité expéditeur : . . . . . .
(NOM, Prénom et signature)

RÉCÉPISSE(1)

Date et heure de remise de l'envoi au destinataire : le. . . . . à . . . . . .heures . . .

Cachet, timbre ou sceau officiel de l'organisme ou de la société destinataire

NOM et fonction du signataire

(1) Rayer si mention inutile
Nombre d'exemplaires :
- Procédure liste inventaire sans récépissé
- Procédure liste inventaire avec récépissé
- archivage définitif : 1 ex officier ou agent de sécurité expéditeur (dernier exemplaire en retour)

INVENTAIRE

Numéro d'ordre	Description précise des documents, équipements et/ou composants classifiés	Nombre d' exemplaires ou quantités	Nombre de pages par document y compris annexes	Nombre total de pages	Nombre de paquets
	TOTAL	. . . . .		. . . . .	

PARTIE RÉSERVÉE EN CAS D'INSPECTION DU OU DES COLIS :

- Visa et sceau du chef :

- des douanes

- de la police

- des services de l'immigration

SCEAU

Retour au sommaire

Ministère
Organisme employeur
(timbre)
N° . . . /

DEMANDE DE REPRODUCTION de supports protégés classifiés Secret-Défense

Mle 11/IGI 1300

Renseignements[44] concernant le support classifié dont la reproduction est demandée :

- Références :
  - numéro d'enregistrement et timbre : . . . . . .
  - date de création : . . . . . .
- Numéro de l'exemplaire à partir duquel la reproduction sera effectuée : . . . . . .

Organisme demandeur : . . . . . .
. . . . . .

Motif succinct de la demande : . . . . . .
. . . . . .

Copies demandées :

- Nombre : . . . . . .
- Numérotage : . . . . . .
- diffusion : . . . . . .

A . .. . , le . . . . . .
Nom, qualité, signature de l'autorité responsable de la demande et cachet de l'organisme.

Retour au sommaire

[44] L'objet de l'information ou du support ne doit en aucun cas être mentionné.

Ministère
Organisme employeur
(timbre)
N° . . . ./

AUTORISATION DE REPRODUCTION de supports protégés classifiés Secret-Défense

Mle 12/IGI 1300

Support protégé classifié Secret-défense dont la reproduction est autorisée :

- Références :
  - numéro d'enregistrement et timbre : . . . . . .
  - date de création : . . . . . .
- Numéro de l'exemplaire à partir duquel la reproduction sera effectuée : . . . . . .

Organisme demandeur : . . . . . .

- Référence de la demande : . . . . . .
  . . . . . .

Copies autorisées :

- Nombre : . . . . . .
- Numérotage : . . . . . .
- Diffusion : . . . . . .

A . . . . . , le . . . . . .
Nom, qualité, signature de l'autorité émettrice de l'information et cachet de l'organisme.

Destinataires :

Retour au sommaire

Ministère
Organisme employeur
(timbre)

A . . . . . , le . . . . . .
N°_____/

PROCÈS-VERBAL DE DESTRUCTION
de support(s) d'information protégé(s) classifié(s) Secret-Défense

Mle 13/IGI 1300

- Date de la destruction : . . . . . .
- Grade, nom et fonction du détenteur responsable : . . . . . .
. . . . . .

Référence des informations ou supports[45]	**Date**	**Catégorie** (éventuellement)	**Numéro des Exemplaires**

Nous soussignés, certifions que le(s) support(s) d'information protégé (s) désigné(s) ci-dessus a (ont) été détruit(s) ce jour, en notre présence et celle du détenteur responsable.

Nom, fonction et signature du témoin

Nom, fonction, signature du détenteur responsable et cachet de l'organisme

Copie à[46] :
- . . . . . .

[45] Les références doivent être portées sur le procès-verbal de telle manière qu'il soit impossible de les modifier ou de les compléter ultérieurement, en ajoutant par exemple, entre deux mentions, les références d'un autre document, information ou support.
[46] Autorité ayant donné l'ordre de destruction.

Retour au sommaire

Ministère
Organisme
timbre
N° . . . /

A . . . . . , le . . . . . .

BORDEREAU A - B - B' [47]
de transmission d'informations ou supports protégés classifiés
Secret-Défense Confidentiel-Défense[48]
Mle 14/IGI 1300

Références[49]	**Date**	**Nombre d'exemplaires**	**Nombre d'annexes**

DESTINATAIRE : . . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .

Nom, qualité, signature de l'expéditeur et cachet de l'organisme

Reçu le : . . . . . .

Par : . . . . . .

[47] A : à conserver par le destinataire.
B : à renvoyer sans délai à l'expéditeur après émargement.
B' : à conserver en archives par l'expéditeur jusqu'à réception du feuillet B qui lui sera substitué.
[48] Rayer la mention inutile
[49] A l'exclusion de l'objet qui ne doit jamais être mentionné.

Ministère
Organisme-
timbre
N° . . . . /

A . . . . . , le . . . . . .

BORDEREAU A - **B** - B' [50]
de transmission d'informations ou supports protégés classifiés Secret-Défense Confidentiel-Défense[51]
Mle 14 bis/IGI 1300

Références[52]	**Date**	**Nombre d'exemplaires**	**Nombre d'annexes**

DESTINATAIRE : . . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .

Nom, qualité, signature de l'expéditeur et cachet de l'organisme

Reçu le : . . . . . .

Par : . . . . . .
(Nom, qualité signature et cachet de l'organisme)

[50] A : à conserver par le destinataire.
B : à renvoyer sans délai à l'expéditeur après émargement.
B' : à conserver en archives par l'expéditeur jusqu'à réception du feuillet B qui lui sera substitué.
[51] Rayer la mention inutile
[52] A l'exclusion de l'objet qui ne doit jamais être mentionné.

Ministère
Organisme
timbre
N° . . . . /

A . . . . . , le . . . . . .

BORDEREAU A - B - **B'**[53]
de transmission d'informations ou supports protégés classifiés Secret-Défense Confidentiel-Défense[54]
Mle 14 ter/IGI 1300

Références[55]	**Date**	**Nombre d'exemplaires**	**Nombre d'annexes**

DESTINATAIRE : . . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .

[53] A conserver en archives par l'expéditeur jusqu'à réception du feuillet B qui lui sera substitué.
[54] Rayer la mention inutile
[55] A l'exclusion de l'objet qui ne doit jamais être mentionné.

Retour au sommaire

MODÈLES DE TIMBRES[56] de classification et de protection

I – Couverture[57] et 1ère page de garde du document

SECRET DEFENSE

Toute personne qui détient ce document sans avoir qualité pour le connaître tombe sous le coup des dispositions du code pénal réprimant les atteintes au secret de la défense nationale.

CONFIDENTIEL DEFENSE

Ce document ne doit être communiqué qu'aux personnes qualifiées pour le connaître

II – Pages internes du document ou correspondance[58]

SECRET DEFENSE

Lettres de 4 mm de hauteur sur 3 mm de largeur ; cadre et lettres de 1,5 mm d'épaisseur

CONFIDENTIEL DEFENSE

Lettres de 4 mm de hauteur sur 2 mm de largeur ; cadre et lettres de 1 mm d'épaisseur

SPECIAL FRANCE

Lettres de 4 mm de hauteur sur 2 mm de largeur ; cadre et lettres de 1 mm d'épaisseur

[56] Les timbres sont apposés avec une encre indélébile de couleur rouge, sauf le timbre Spécial France qui est apposé en bleu.
[57] Au milieu du bas de la couverture.
[58] Au milieu du haut et du bas de la couverture.

Retour au sommaire

Mle 16/IGI 1300

MODÈLES DE TIMBRES de déclassement ou de déclassification

1° - Pour déclasser une information ou un support

Le déclassement du niveau SECRET-DEFENSE au niveau CONFIDENTIEL-DEFENSE pourra intervenir à compter du : . . . . . .

A déclasser CONFIDENTIEL-DEFENSE après accord de l'autorité émettrice

2° - Pour déclassifier une information ou un support

A déclassifier à compter du :

A déclassifier sur ordre de l'autorité émettrice

Retour au sommaire