Le 4 mars 2015

ARRETE

# Arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale

NOR: PRMD1132480A

Version consolidée au 4 mars 2015

Le Premier ministre,

Vu le code pénal, notamment ses articles 413-9 à 414-9 ;

Vu le code de la défense, notamment ses articles R.* 1132-2, R.* 1132-3, D. 1132-5 et R. 2311-1 à R. 2312-2 ;

Vu le code du travail ;

Vu le code des marchés publics ;

Vu la loi n° 75-1334 du 31 décembre 1975 modifiée relative à la sous-traitance ;

Vu le décret n° 2004-16 du 7 janvier 2004 modifié pris en application de l'article 4 du code des marchés publics et concernant certains marchés publics passés pour les besoins de la défense, notamment son article 17 ;

Vu le décret n° 2005-1124 du 6 septembre 2005 modifié pris pour l'application de l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 et fixant la liste des enquêtes administratives donnant lieu à la consultation des traitements automatisés de données personnelles mentionnés à l'article 21 de la loi n° 2003-239 du 18 mars 2003 ;

Vu la décision n° 2011-192 QPC du 10 novembre 2011 du Conseil constitutionnel,

Arrête :

## Article 1

L'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, ci-après annexée, est approuvée.

## Article 2

A modifié les dispositions suivantes :
- Abroge Arrêté du 23 juillet 2010 (Ab)
- Abroge Arrêté du 23 juillet 2010 - Annexe (Ab)

- Abroge Arrêté du 23 juillet 2010 - art. 1 (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. 2 (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. 3 (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Annexe (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Annexe (Glossaire) (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Annexe (Index) (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Annexe (Modèles) (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Annexe (Titre II : 19 à 38) (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Annexe (Titre III : 39 à 69) (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Annexe (Titre IV : 70 à 84) (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Annexe (Titre Ier : 1 à 18) (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Annexe (Titre V : 85 à 94) (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Annexe (Titre VI : 95 à 114) (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Annexe 1 (Références) (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Annexe 2 (Classification) (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Annexe 3 (Règles de protection) (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Annexes 4 à 14 (Ab)
- Abroge Arrêté du 23 juillet 2010 - art. Table des annexes (Ab)

**Article 3**

Le présent arrêté sera publié au Journal officiel de la République française.

**Annexe**

- Modifié par Décret n°2014-445 du 30 avril 2014 - art. 10

INSTRUCTION GÉNÉRALE INTERMINISTÉRIELLE N° 1300

SUR LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE

SOMMAIRE

Introduction

Cette nouvelle instruction générale interministérielle a été rendue nécessaire par les modifications issues de la loi n° 2009-928 du 31 juillet 2009 relative à la programmation militaire pour les années 2009 à 2014 et portant diverses dispositions relatives à la défense et du décret n° 2010-678 du 21 juin 2010 relatif à la protection du secret de la

défense nationale. Dans la continuité des prescriptions du Livre blanc sur la défense et la sécurité nationale de juin 2008, et conformément à la décision du Conseil constitutionnel en date du 10 novembre 2011 (1), elle vise à renforcer la sécurité juridique de la protection du secret de la défense nationale en tenant particulièrement compte de l'effacement du clivage traditionnel entre défense et sécurité.

Certaines informations présentent, en cas de divulgation, un risque tel d'atteinte à la défense et à la sécurité nationale que seules certaines personnes sont autorisées à y accéder. Considérer qu'une information présente ce risque conduit la puissance publique à la classifier, c'est-à-dire à lui conférer le caractère de secret de la défense nationale et à la faire bénéficier d'une protection juridique et matérielle stricte.

La présente instruction décrit l'organisation générale de la protection du secret de la défense nationale. En s'efforçant de clarifier les obligations juridiques et matérielles inhérentes à cette protection, elle précise les conditions dans lesquelles chaque ministre, pour le département dont il a la charge, met en œuvre l'application de ces dispositions, en veillant à limiter le nombre et le niveau des habilitations et la production de documents classifiés à ce qui est strictement nécessaire, afin de garantir la plus grande efficacité du dispositif.

Elle définit les procédures d'habilitation et de contrôle des personnes pouvant avoir accès au secret les conditions d'émission, de traitement, d'échange, de conservation ou de transport des documents classifiés et veille à leur protection. La sécurité des informations classifiées doit être une préoccupation majeure et constante de leur détenteur. Toute personne qui, contrevenant aux dispositions applicables, compromettrait le secret s'expose à des sanctions administratives et pénales.

L'instruction détermine les critères, les niveaux et les conditions de classification des informations et supports concernés ainsi que les règles d'accès aux lieux abritant de telles informations. Elle décrit la procédure qui, conciliant les deux objectifs constitutionnels que représentent la sauvegarde des intérêts de la nation et la recherche des auteurs des infractions pénales, permet à un magistrat, confronté aux règles applicables à la protection du secret, de mener sans compromission ses investigations.

Elle prend également en compte l'accroissement constaté des échanges d'informations classifiées, au niveau national, au niveau européen ou au niveau international. Dès lors que tous les Etats protègent leurs informations classifiées, la France, au titre des accords de sécurité qu'elle a conclus, est tenue de garantir, à charge de réciprocité, la protection des informations classifiées qui lui sont transmises par les Etats parties.

Enfin, la protection du secret ne se limite pas aux documents classifiés sur support papier et s'étend en particulier aux moyens informatiques et électroniques servant à leur élaboration, leur traitement, leur stockage et leur transmission. Les systèmes d'information et de communication, qui innervent aujourd'hui les infrastructures vitales, la vie économique et sociale comme l'action des pouvoirs publics, présentent des vulnérabilités propres. La menace constante d'une attaque informatique multiforme (2) et la possibilité, à tout moment, de compromission à l'insu même de l'utilisateur exigent en réponse des règles de sécurité des systèmes d'information adaptées à l'évolution rapide des techniques et un degré d'expertise fortement développé, diffusé auprès de tous les acteurs publics ou privés.

## TITRE Ier
## PRINCIPES ET ORGANISATION DE LA PROTECTION

La protection du secret concerne tous les domaines d'activité relevant de la défense et de la sécurité nationale : politique, militaire, diplomatique, scientifique, économique, industriel.
Sont classifiées les informations dont la divulgation est de nature à porter atteinte à la défense et à la sécurité nationale.
La France peut également protéger les informations échangées avec les organisations internationales et les Etats étrangers.
La protection du secret est assurée par une chaîne de responsabilité, qui s'applique aux domaines public et privé.
Le secrétariat général de la défense et de la sécurité nationale (SGDSN) est l'autorité nationale de sécurité ; il peut déléguer des autorités de sécurité dans des domaines particuliers.

Chapitre Ier

Principes généraux de la protection du secret

Article 1er

Fondements de la protection

Le secret de la défense nationale constitue une cible majeure pour les services étrangers et les groupements ou les individus isolés ayant pour objectif de déstabiliser l'Etat ou la société. Cette menace vise tous les domaines d'activité relevant de la défense et de la sécurité nationale : politique, militaire, diplomatique, scientifique, économique, industriel...
Certaines informations intéressant la défense et la sécurité nationale nécessitent une protection particulière, permettant d'en maîtriser et d'en limiter la diffusion, dans des conditions définies dans la présente instruction.
L'atteinte pouvant être portée à la défense et à la sécurité nationale par la divulgation de certaines informations ou de certains supports justifie leur classification. L'apposition de la marque de classification, telle que définie aux articles R. 2311-2, R. 2311-3 et R. 2311-4 du code de la défense, confère matériellement le caractère de secret aux informations ou supports concernés et justifie, en cas de violation de la réglementation applicable, la mise en œuvre de règles pénales spécifiques.
Il existe trois niveaux de classification : Très Secret Défense, Secret Défense, Confidentiel Défense (3). Peuvent faire l'objet de ces classifications les procédés, objets, documents, informations, réseaux informatiques, 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.
L'inobservation des mesures de protection induites par la classification génère la mise en œuvre du dispositif de répression pénale (4). La politique de protection du secret vise à rendre responsable, pénalement et administrativement, toute personne ayant accès à des informations ou supports classifiés.
Une information classifiée est compromise lorsqu'elle est portée à la connaissance du public ou d'une personne non habilitée ou n'ayant pas le besoin d'en connaître.
L'évaluation des risques de compromission des informations ou supports classifiés et des vulnérabilités des personnes ou des systèmes les traitant, au regard des intérêts fondamentaux de la nation, est essentielle afin de garantir la protection du secret. La stricte application des mesures de sécurité définies dans la présente instruction, complétée par la diffusion d'instructions et la sensibilisation des personnels, contribue à l'efficacité du dispositif et permet de lutter contre des actions malveillantes, souvent facilitées par l'ignorance, l'imprudence, l'inattention ou la négligence.
La protection du secret, qu'il s'agisse d'une information ou d'un support, doit être assurée par les personnes, physiques ou morales (5), de droit public ou de droit privé, y accédant. En cas de manquement, même involontaire, ces personnes se rendent coupables de compromission et encourent les sanctions prévues aux articles 413-10 et suivants du code

pénal.

## Article 2
## Définitions

La présente instruction emploiera les expressions suivantes :
- “habilitation”, pour désigner la décision explicite, délivrée à l’issue d’une procédure spécifique définie dans la présente instruction, permettant à une personne, en fonction de son besoin d’en connaître, d’avoir accès aux informations ou supports classifiés au niveau précisé dans la décision ainsi qu’au(x) niveau(x) inférieur(s) ;
- “informations ou supports classifiés” (6), pour désigner les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers présentant un caractère de secret de la défense nationale ;
- “systèmes d’information”, pour désigner l’ensemble des moyens informatiques ayant pour finalité d’élaborer, de traiter, de stocker, d’acheminer, de présenter ou de détruire l’information ;
- “contrat”, pour désigner tout contrat, toute convention, tout marché quel que soit son régime juridique ou sa dénomination, dans lequel un candidat ou un cocontractant, public ou privé, est amené à l’occasion de la passation du contrat ou de son exécution à connaître et éventuellement à détenir dans ses locaux des informations ou des supports classifiés.

## Article 3
## Champ d’application

Les dispositions de la présente instruction sont applicables dans toutes les administrations centrales, tous les services déconcentrés de l’Etat et établissements publics nationaux placés sous l’autorité d’un ministre, dans toutes les entités, publiques ou privées, concernées par le secret de la défense nationale, ainsi qu’à toute personne dépositaire, même à titre provisoire, d’un tel secret, y compris dans le cadre de la passation et de l’exécution d’un contrat.

Les informations ou supports classifiés confiés à la France en application d’un accord de sécurité bénéficient des mesures de protection du secret en fonction des concordances définies par ledit accord, dès lors qu’elles portent une mention de classification équivalente à l’un des trois niveaux définis (7).

## Article 4
## La classification

La décision de classifier au titre du secret de la défense nationale une information ou un support a pour conséquence de le placer sous la protection de dispositions spécifiques du code pénal (8). L’apposition du marquage de classification constitue le seul moyen de conférer cette protection particulière.

Les articles R. 2311-2 et R. 2311-3 du code de la défense définissent trois niveaux de classification :
- Très Secret Défense, réservé aux informations et supports qui concernent les priorités gouvernementales en matière de défense et de sécurité nationale et dont la divulgation est de nature à nuire très gravement à la défense nationale ;
- Secret Défense, réservé aux informations et supports dont la divulgation est de nature à nuire gravement à la défense nationale ;
- Confidentiel Défense, réservé aux informations et supports dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d’un secret classifié au niveau Très Secret Défense ou Secret Défense.

Une information n’ayant pas fait l’objet d’une décision de classification à l’un des trois niveaux définis n’est pas protégée pénalement au titre du secret de la défense nationale. Aussi, caractérise une faute, qu’il revient à l’autorité hiérarchique d’apprécier et, le cas

échéant, de sanctionner, le fait d'omettre de procéder à la classification d'une information dont la divulgation est de nature à nuire à la défense ou à la sécurité nationale.

Article 5
Mentions particulières de confidentialité

Certaines informations qu'il n'y a pas lieu de classifier peuvent cependant recevoir, de la part de leur émetteur, une marque de confidentialité destinée à restreindre leur diffusion à un domaine spécifique (précisé par une mention particulière [9]) ou à garantir leur protection (telle que Diffusion Restreinte).

Ces mentions, qui ne traduisent pas une classification, ne suffisent pas à conférer aux informations concernées la protection pénale propre au secret de la défense nationale. Leur seul objectif est de sensibiliser l'utilisateur à la nécessaire discrétion dont il doit faire preuve dans la manipulation des informations couvertes par cette mention.

L'auteur de la divulgation, qu'il relève de la sphère publique ou de la sphère privée, s'expose à des sanctions disciplinaires ou professionnelles (10), sans préjudice de l'application éventuelle des dispositions spécifiques au traitement et à la protection de données à caractère personnel (11).

La mention Diffusion Restreinte peut être apposée sur les informations et supports que l'émetteur entend soumettre à une restriction de diffusion. Contrairement à certaines réglementations étrangères, elle ne correspond pas à un niveau de classification mais a pour objet d'appeler l'attention de l'utilisateur sur la nécessité de faire preuve de discrétion dans le traitement de cette information. Elle indique que l'information ne doit pas être rendue publique et ne doit être communiquée qu'aux personnes ayant besoin de la connaître dans l'exercice de leurs attributions. Les règles énoncées dans l'annexe 3 sont appliquées à ces informations et supports.

Une mention de restriction de diffusion inférieure à l'équivalent de la classification française Confidentiel Défense, attribuée à un document par un Etat étranger ou une organisation internationale qui l'érige en niveau de classification soumet, en France, le document aux règles de protection énoncées dans l'annexe 3.

Article 6
L'accès aux secrets de la défense nationale

Seules des personnes qualifiées peuvent accéder aux secrets de la défense nationale. La qualification exige la réunion de deux conditions cumulatives :

- le besoin de connaître ou d'accéder à une information classifiée, attesté par l'autorité d'emploi : l'appréciation du besoin d'en connaître est fondée sur le principe selon lequel une personne ne peut avoir connaissance d'informations classifiées que dans la mesure où l'exercice de sa fonction ou l'accomplissement de sa mission l'exige (12). Elle est effectuée dans les conditions prévues par l'article 20 de la présente instruction ;
- la délivrance de l'habilitation correspondant au degré de classification de l'information considérée : la décision d'habilitation est une autorisation explicite, délivrée à l'issue d'une procédure spécifique définie dans la présente instruction, permettant à une personne, sous réserve du besoin d'en connaître, d'avoir accès aux informations ou supports classifiés au niveau précisé dans la décision ainsi qu'au(x) niveau(x) inférieur(s). La décision d'habilitation est assortie d'un engagement de respecter, après en avoir dûment pris connaissance, les obligations et les responsabilités liées à la protection des informations ou supports classifiés.

Article 7
Les lieux abritant des informations classifiées

Les lieux abritant des éléments couverts par le secret de défense nationale sont les locaux dans lesquels sont détenus des informations ou supports classifiés, quel qu'en soit le niveau, par des personnes par ailleurs habilitées au niveau requis.

L’accès à ces lieux, pour motif de service, est encadré par les dispositions relatives au droit du travail, aux contrats de prestation de service, au droit pénal, à la procédure pénale (13) ou issues de conventions internationales.

### Article 8
### Contrôles et inspections

Des contrôles et des inspections sont organisés périodiquement pour vérifier l’application, par les organismes émettant, recevant, traitant ou conservant des informations classifiées, des instructions et des directives relatives à la protection du secret.

Pour les organismes traitant des informations ou supports classifiés Très Secret Défense, les inspections et les contrôles sont assurés par le secrétariat général de la défense et de la sécurité nationale (SGDSN). Ce dernier propose toutes mesures propres à améliorer les conditions générales de sécurité. Les inspections et les contrôles sont organisés en liaison avec les départements ministériels. En cas d’anomalies constatées, le SGDSN peut saisir, par l’intermédiaire des ministres concernés, les services qui concourent à la répression des crimes et délits. 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.

A la demande du ministre, pour son département, ou à l’initiative des services enquêteurs, dans le cadre de leurs attributions, des contrôles et des inspections périodiques sont menés dans les organismes traitant des informations ou supports classifiés Secret Défense et Confidentiel Défense. Le SGDSN peut inspecter ces organismes.

## Chapitre II
## Organisation de la protection

La protection du secret relève de différentes autorités qui, en s’appuyant sur une organisation précise, s’assurent de la bonne application des mesures définies dans la présente instruction.

### Section 1
### Autorités compétentes

### Article 9
### Le Premier ministre

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

Les articles R. 2311-5, R. 2311-6 et R. 2311-7 du code de la défense précisent les compétences du Premier ministre, qui :

- pour le niveau Très Secret Défense :
- détermine les critères et les modalités d’organisation de la protection et définit des classifications spéciales correspondant aux différentes priorités gouvernementales ;
- fixe les conditions dans lesquelles chaque ministre, pour le département dont il a la charge, détermine les informations et supports qu’il y a lieu de classifier à ce niveau (14) ;
- pour les niveaux Secret Défense et Confidentiel Défense :
- fixe les conditions dans lesquelles chaque ministre, pour le département dont il a la charge, détermine les informations et supports qu’il y a lieu de classifier et les modalités de leur protection (15) ;
- pour les habilitations :
- définit la procédure préalable à la décision d’habilitation ;
- prend la décision d’habilitation pour le niveau Très Secret Défense et indique les classifications spéciales auxquelles la personne habilitée peut accéder (16).

Pour l’exercice de ces compétences, le Premier ministre est assisté par le secrétaire général de la défense et de la sécurité nationale.

### Article 10
### Le secrétaire général de la défense

et de la sécurité nationale (SGDSN)
Sous l'autorité du Premier ministre, le secrétaire général de la défense et de la sécurité nationale définit et coordonne sur le plan interministériel la politique de sécurité en matière de protection du secret de la défense nationale (17). A ce titre, il propose, diffuse, fait appliquer et contrôler les mesures nécessaires à la protection de ce secret (18).
Les compétences du SGDSN s'exercent dans le cadre national et international.
Au niveau national :
Pour tous les niveaux de classification, le SGDSN est chargé de la diffusion et du contrôle de l'application des mesures de protection du secret. A ce titre, il s'assure, sur la base d'un rapport qui doit lui être fourni annuellement, que celles-ci sont respectées au sein de chaque département ministériel.
Pour le niveau Très Secret Défense, il prend les décisions d'habilitation, par délégation du Premier ministre.
Il veille à la mise en œuvre des mesures relatives aux classifications spéciales et en assure le contrôle, notamment par le biais des inspections. Il définit et organise les réseaux de sécurité correspondants. Il désigne, pour chacune des classifications spéciales, un agent central de sécurité dont les missions sont définies par instruction particulière.
En matière de sécurité des systèmes d'information, les attributions du SGDSN sont définies au titre V de la présente instruction.
Au niveau international :
Le SGDSN, autorité nationale de sécurité (ANS) pour le secret de la défense nationale, pour l'application des accords et traités internationaux prévoyant une telle autorité, est l'interlocuteur des autorités de sécurité étrangères. Il négocie les accords généraux de sécurité avec les Etats étrangers, les organisations internationales, les institutions et les organes de l'Union européenne et il est consulté dès lors qu'un accord intéresse, dans son ensemble ou pour partie, la protection réciproque et l'échange d'informations classifiées.
Il est informé, par les ministères, de la négociation, dans leur domaine particulier, d'accords portant, dans leur ensemble ou pour partie, sur la protection réciproque et l'échange d'informations classifiées. Il participe, avec ses partenaires étrangers, à l'élaboration des réglementations au sein des comités de sécurité des organisations internationales et des institutions et organes de l'Union européenne. Il détermine les procédures d'habilitation requises et organise, dirige et contrôle les réseaux de sécurité correspondants.
Le SGDSN met en œuvre les accords internationaux relatifs aux habilitations pour les ressortissants français séjournant ou ayant séjourné à l'étranger et pour les ressortissants étrangers en France.
Le SGDSN assure, en application des accords internationaux, la sécurité des informations classifiées confiées à la France. Il définit en outre les mesures de protection des informations et supports dont la France est détentrice, qui ont été classifiés par un Etat étranger ou une organisation internationale et qui ne portent pas la mention d'un niveau de classification équivalent à ceux définis à l'article R. 2311-2 du code de la défense (19).

## Article 11
## Les ministres

Chaque ministre s'assure, dans le département dont il a la charge, de la mise en œuvre des dispositions relatives à la sécurité des informations ou supports classifiés détenus par tout service ou toute entité publique ou privée relevant de ses attributions. Il fait procéder à des inspections périodiques afin d'en vérifier l'application.
Il prend les décisions d'habilitation pour les niveaux Secret Défense et Confidentiel Défense.
Il détermine, dans les conditions fixées par le Premier ministre, les informations ou supports 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.
Pour ce qui relève de ses attributions, chaque ministre définit, par une instruction particulière (20), les conditions d'emploi des niveaux de classification Secret Défense et Confidentiel Défense et les informations qui doivent être classifiées au niveau Très Secret Défense.
En matière de sécurité des systèmes d'information, ses attributions sont définies au titre V de la présente instruction.

### Article 12
### Les hauts fonctionnaires de défense et de sécurité

Chaque ministre est assisté par un haut fonctionnaire de défense et de sécurité (HFDS) (21) dont les attributions sont fixées par le code de la défense (22). Le HFDS relève directement du ministre et dispose en propre d'un service spécialisé. Pour l'exercice de sa mission, il a autorité sur l'ensemble des directions et services du département ministériel (23).
Au sein du département ministériel dont il relève et des organismes rattachés à ce département, le HFDS est responsable de la diffusion et de l'application des dispositions relatives à la sécurité de défense et à la protection du secret. Il veille au bon fonctionnement des services qui gèrent les informations et supports classifiés, vérifie l'exactitude des inventaires, procède aux contrôles et inspections nécessaires et propose toutes dispositions destinées à renforcer l'efficacité des mesures de protection mises en place.
Il prend, par délégation du ministre, sous réserve d'autres délégations éventuellement accordées en vertu des dispositions de l'article R. 2311-8-1 du code de la défense, les décisions d'habilitation pour les niveaux Secret Défense et Confidentiel Défense. Il assure les liaisons nécessaires avec le SGDSN pour les habilitations au niveau Très Secret Défense, et, s'agissant des ressortissants étrangers ou des Français ayant vécu à l'étranger, pour les habilitations aux classifications nationales et internationales de niveaux Secret Défense et Confidentiel Défense.
Il est en liaison avec ses homologues des autres ministères et avec le secrétaire général de la défense et de la sécurité nationale, auquel il adresse, au plus tard le 31 mars, dans le cadre de son rapport annuel d'activités (24), une évaluation de la protection du secret au sein de son département et des organismes rattachés. Ce rapport indique notamment, par niveau, le nombre de personnes habilitées dans l'année, le nombre d'habilitations en cours de validité, le nombre de lieux abritant des éléments couverts par le secret de la défense nationale, le volume des documents classifiés, l'état des catalogues des emplois et des inventaires, le nombre d'inspections ou de contrôles effectués, les déficiences relevées dans le dispositif de protection du secret, les actions correctrices engagées, les cas de compromission constatés et les actions de formation ou de sensibilisation menées. Ce rapport est classifié au niveau Confidentiel Défense et marqué "Spécial France" (25).
Pour les départements ministériels utilisant des systèmes d'information nécessitant une protection, un fonctionnaire de sécurité des systèmes d'information (FSSI) est désigné par le HFDS et placé sous son autorité afin d'animer la politique de sécurité de ces systèmes et d'en contrôler l'application (26).
En fonction des structures propres à chaque ministère et si nécessaire, il peut être désigné, dans les organismes rattachés, les établissements publics sous tutelle, les entreprises publiques ou au sein du service du HFDS, au moins un fonctionnaire de sécurité. Ce dernier assiste le HFDS et, sous sa direction, contrôle notamment l'exécution des mesures de protection des informations classifiées.

## Section 2
## Organisation fonctionnelle

### Article 13
### Les délégations de signature et de compétence

Aux niveaux Confidentiel Défense et Secret Défense, les décisions d'habilitation sont prises par chaque ministre pour le département dont il a la charge. Les ministres disposent, pour les décisions d'habilitation, de la faculté d'accorder des délégations de signature aux HFDS ainsi qu'aux préfets pour les agents placés sous l'autorité de ces derniers et les personnes employées dans des organismes relevant de leurs attributions.
Pour l'habilitation des personnes morales, la signature peut être, en outre, déléguée par les ministres, en application d'accords ou de traités internationaux prévoyant explicitement une telle délégation, à une autorité de sécurité déléguée.
Le ministre de la défense peut déléguer la signature des décisions d'habilitation à certaines autorités relevant de son département ministériel.

## Article 14
## Le rôle des autorités hiérarchiques

Au sein des différents départements ministériels, des services déconcentrés et des armées, les autorités hiérarchiques civiles ou militaires ayant reçu délégation du ministre dont elles relèvent assument, chacune à son échelon et dans le cadre de ses attributions, la responsabilité des mesures de sécurité relatives à la protection du secret.
Au sein des entreprises publiques ou privées autorisées à traiter ou à détenir des informations ou des supports classifiés, l'autorité hiérarchique assume la responsabilité des mesures de sécurité relatives à la protection du secret.
Lorsque des informations ou supports classifiés au niveau Très Secret Défense doivent être utilisés au sein d'un organisme, l'autorité hiérarchique doit demander, dans les conditions fixées par une instruction particulière du Premier ministre, la création d'une antenne d'utilisation.
Pour la gestion, l'enregistrement et la conservation des informations ou supports classifiés au niveau Secret Défense, des bureaux de protection du secret sont créés dans des zones répondant aux normes de sécurité, conformément à la présente instruction.
Les autorités hiérarchiques doivent veiller à l'habilitation des personnels placés sous leur responsabilité et initier la procédure d'habilitation au niveau requis par le catalogue des emplois.

## Article 15
## L'officier de sécurité

L'officier de sécurité, nommé par le chef du service employeur, est le correspondant du HFDS et des services enquêteurs. Il a pour mission, sous les ordres de son autorité d'emploi et en fonction des modalités propres à chaque structure, de fixer les règles et consignes de sécurité à mettre en œuvre concernant les personnes et les informations ou supports classifiés, et d'en contrôler l'application. Il participe à l'instruction et à la sensibilisation du personnel en matière de protection du secret. Il est chargé de la gestion des habilitations et, en liaison avec les services enquêteurs, du contrôle des accès aux zones protégées. Il peut diriger le bureau de protection du secret.
Les entreprises publiques ou privées dépositaires de secrets de la défense nationale ou titulaires de marchés impliquant le traitement ou la détention d'informations ou de supports classifiés doivent désigner un officier de sécurité.

## Article 16
## Les autorités de sécurité déléguées

En application de l'article R. 2311-10-1 du code de la défense, une ou plusieurs autorités peuvent être désignées par l'ANS, sur proposition du ou des ministres intéressés, autorités de sécurité déléguées dans des domaines particuliers, comme le domaine industriel. Ces autorités de sécurité déléguées (ASD) sont responsables devant l'ANS de la mise en œuvre de la politique de sécurité du secret de la défense nationale dans le domaine déterminé et fournissent les orientations et l'assistance nécessaires à sa bonne application, en particulier dans le cadre des accords de sécurité.
En application d'accords ou de traités internationaux, l'ASD peut être notamment chargée

du traitement des habilitations des personnels relevant de son domaine de compétence, en liaison avec les ASD partenaires, nationales ou étrangères. Elle peut également, si l'accord ou le traité le prévoit, prendre elle-même la décision d'habilitation. Elle est chargée de la procédure d'autorisation d'accès aux zones protégées dont elle a la charge.

### Article 17

### Les réseaux de sécurité Très Secret Défense

La protection des informations ou supports classifiés au niveau Très Secret Défense est organisée dans le cadre de la réglementation particulière des classifications spéciales (27), qui complète les dispositions de caractère général de la présente instruction.

Aucun service ni organisme ne peut élaborer, traiter, stocker, acheminer, des informations ou supports classifiés au niveau Très Secret Défense sans y avoir été préalablement autorisé par le SGDSN. La circulation de ces informations par voie électronique est interdite.

Le service ou l'organisme doit en outre disposer impérativement d'une antenne d'utilisation de la classification spéciale correspondante. Ces antennes d'utilisation sont créées par décision du SGDSN sur proposition du ministre concerné. Par application du principe de cloisonnement de l'information, des antennes distinctes sont prévues pour chacune des classifications spéciales.

La circulation de ces informations et supports classifiés emprunte obligatoirement un réseau de sécurité constitué pour garantir la protection de chaque classification spéciale. Un agent central de sécurité, désigné par le SGDSN, exerce le contrôle centralisé de cette circulation au sein des différentes antennes d'utilisation.

Le responsable de chacune de ces antennes est choisi parmi les personnels admis à la classification spéciale et est assisté par un agent de sécurité, qui veille au respect des règles relatives à la protection du secret.

### Article 18

### Le bureau de protection du secret

Chaque ministre veille à la création d'un ou de plusieurs bureaux de protection du secret au sein desquels s'effectuent l'élaboration, le traitement, le marquage, le stockage et le suivi de la destruction des informations ou supports classifiés au niveau Secret Défense. Chaque bureau dresse l'inventaire annuel des informations ou supports classifiés qu'il traite.

Ce bureau est également responsable de l'enregistrement, de l'expédition, de la réception et de la circulation des supports classifiés au niveau Secret Défense, qui ne peuvent transiter que par son intermédiaire, à l'exclusion de ceux comportant la mention "ACSSI" (28), dont la gestion est définie au titre V de la présente instruction.

Ce bureau, composé exclusivement de personnes habilitées au niveau Secret Défense, est situé dans une zone réservée, répondant aux normes de sécurité définies dans la présente instruction (29).

Un tel bureau, obligatoire pour le niveau Secret Défense, est conseillé pour les informations ou supports de niveau Confidentiel Défense.

Pour remplir ses missions, le bureau de protection du secret peut mettre en place un système assurant par voie informatique les fonctions suivantes :

- identification du support d'information (numéro d'enregistrement arrivé ou départ, auteur ou service émetteur, date de création, domaine, titre ou objet, pagination, niveau de classification, mode et date prévue de déclassification, nombre d'exemplaires gérés par le bureau de protection du secret) ;
- traçabilité des événements concernant les exemplaires du support d'information (arrivée, départ, reproduction, archivage, destruction, déclassification, numéro de référence de l'événement, date de l'événement, référence individuelle des exemplaires, nom et fonction du détenteur physique de chaque exemplaire) ;
- modification éventuelle des données précédentes ;

- recherche sur les supports d'information (des détenteurs successifs d'un exemplaire, de la date de création, du service émetteur...) ;
- inventaire des supports d'information ;
- fourniture d'états relatifs aux actions effectuées sur les supports d'information (historique, fiche d'enregistrement, fiche de suivi, bordereau d'envoi, procès-verbal de destruction, avis de déclassification, archivage, reproduction...).

## TITRE II
## MESURES DE SÉCURITÉ RELATIVES AUX PERSONNES

Ne peuvent accéder aux informations classifiées que les personnes dûment habilitées et ayant le besoin d'en connaître.
L'habilitation est une procédure lourde qui ne doit être engagée que lorsqu'elle est strictement nécessaire et conforme au catalogue des emplois.
Le contrôle élémentaire permet de vérifier que l'on peut accorder à une personne un degré de confiance suffisant pour lui autoriser l'accès à un lieu abritant des secrets de la défense nationale ou lui confier une mission particulière.
Les décisions relatives aux habilitations sont notifiées aux intéressés.

### Chapitre Ier
### L'accès au secret de la défense nationale

#### Article 19
#### Principe

En vertu de l'article R. 2311-7 du code de la défense, nul n'est qualifié pour connaître des informations ou supports classifiés s'il n'est habilité au niveau requis et s'il n'a le besoin de les connaître.

#### Article 20
#### Catalogues des emplois

Les hauts fonctionnaires de défense et de sécurité (30) élaborent les instructions nécessaires pour faire établir, par l'autorité compétente, au sein de chaque service de l'Etat et organisme public ou privé, et pour chaque niveau de classification, la liste des emplois ou fonctions nécessitant l'accès à des informations ou supports classifiés. Ces listes sont désignées "catalogues des emplois". Il appartient aux HFDS de vérifier l'établissement de ces catalogues pour chacun des trois niveaux.
C'est en référence aux catalogues des emplois que les demandes d'habilitation sont établies. Lorsqu'une demande d'habilitation lui parvient, l'autorité d'habilitation vérifie l'inscription de la fonction concernée dans le catalogue des emplois correspondant . Elle examine, à titre exceptionnel, le bien-fondé de la demande lorsque l'emploi ne figure pas au catalogue.
Ces catalogues peuvent être établis par direction, par service ou au niveau des services déconcentrés de l'Etat. Ils sont mis à jour au moins une fois par an, notamment à l'occasion d'une réorganisation de service. Afin de faciliter l'actualisation, il est vérifié auprès des titulaires des postes répertoriés s'ils ont effectivement eu accès à des informations classifiées pour le niveau concerné.
L'autorité hiérarchique apprécie les postes ou fonctions requérant réellement l'accès à des informations ou supports classifiés. Elle s'efforce de limiter à ce qui est strictement nécessaire les demandes d'habilitation qui en résultent. Ainsi, il convient d'éviter les procédures d'habilitation engagées par facilité pour les personnels de tout un service, si chacun de ses membres n'a pas individuellement un besoin avéré d'accéder à un élément couvert par le secret de la défense nationale.
Dans les entreprises titulaires d'un contrat impliquant l'accès ou la détention d'informations ou de supports classifiés, un répertoire des personnes habilitées tient lieu de catalogue des emplois.

#### Article 21
#### Besoin d'en connaître

L’habilitation ne permet pas d’accéder sans limite à toute information ou à tout support classifié au niveau correspondant. Une personne habilitée n’accède à une information ou à un support classifié que si son autorité hiérarchique estime que cet accès est nécessaire à l’exercice de sa fonction ou à l’accomplissement de sa mission.
L’autorité hiérarchique apprécie de façon rigoureuse et mesurée le besoin de connaître des informations classifiées.

### Article 22
### Information des candidats à l’habilitation

Lors de leur demande d’habilitation, les candidats sont informés, par les mentions portées sur la notice individuelle qui leur est remise, des obligations induites par l’habilitation ainsi que des dispositions relatives à leur responsabilité pénale en cas de compromission (31).
A la notification d’une décision d’habilitation favorable par l’officier de sécurité, l’information initiale est complétée par une séance de sensibilisation aux risques de compromission puis, par la suite, par des rappels périodiques de la réglementation en vigueur.
Une sensibilisation aux menaces d’investigations ou d’approches par des individus ou des organisations étrangères est faite aux personnes devant se rendre hors du territoire national, que l’Etat de destination soit ou non lié à la France par un accord de sécurité. Avant leur départ, des règles de prudence élémentaire leur sont rappelées (32).

## Chapitre II
## L’habilitation

### Article 23
### Objet de l’habilitation

L’autorité hiérarchique doit veiller à l’habilitation du personnel placé sous sa responsabilité et, à ce titre, initier, par la constitution d’un dossier, la procédure d’habilitation au niveau requis par le catalogue des emplois.
La demande d’habilitation déclenche une procédure destinée à vérifier qu’une personne peut, sans risque pour la défense et la sécurité nationale ou pour sa propre sécurité, connaître des informations ou supports classifiés dans l’exercice de ses fonctions. La procédure comprend une enquête de sécurité permettant à l’autorité d’habilitation de prendre sa décision en toute connaissance de cause.
Les informations ou supports classifiés ne peuvent être portés à la connaissance de personnes non habilitées. Aussi, toute personne visant ou occupant un poste pour lequel le besoin d’une habilitation est avéré et qui refuserait de se soumettre à la procédure d’habilitation devra être écartée du poste considéré.

### Article 24
### Procédure d’habilitation

La procédure préalable à la décision d’habilitation est une opération coûteuse en temps et en personnel. Aussi, lorsqu’un poste à pourvoir exige une habilitation au niveau Secret Défense ou Confidentiel Défense, la procédure n’est engagée qu’au seul profit de la personne effectivement nommée dans l’emploi, sauf cas particulier. Anticiper la prise de poste en engageant la procédure d’habilitation sans attendre la prise effective de fonction peut être une mesure de bonne gestion, qui permet à la personne nouvellement affectée de prendre connaissance des informations classifiées sans perdre de temps. Il convient toutefois d’éviter toute surcharge inutile des services chargés de cette mission en limitant autant que possible le nombre de demandes d’habilitation.
Lorsque l’habilitation requise est du niveau Très Secret Défense, il revient à l’autorité d’emploi d’apprécier l’opportunité d’une enquête portant sur chacun des candidats au poste concerné.
1. Constitution du dossier :
Le dossier d’habilitation a pour objet de réunir les éléments qui seront vérifiés lors de l’enquête de sécurité (33).

Afin de simplifier la constitution des dossiers de demande d'habilitation et d'en accélérer la circulation entre les différents acteurs, il convient de favoriser la dématérialisation des procédures.
Sous la forme dématérialisée, la demande d'habilitation et la notice individuelle peuvent être téléchargées et complétées par voie électronique. La transmission du service enquêteur peut se faire par voie électronique, à condition que le système d'information employé garantisse l'identification et l'authentification de l'émeteur comme du destinataire, assure la confidentialité et l'intégralité des données et permette de tracer les actions effectuées.
Lorsque le recours à la forme dématérialisée n'est pas possible, le dossier d'habilitation est constitué (34) de la demande d'habilitation formulée par le chef du service employeur attestant le besoin de connaître des informations ou supports classifiés à un niveau donné, pour une personne nommément désignée, assortie de la notice individuelle de sécurité, renseignée intégralement par l'intéressé et vérifiée par l'officier de sécurité du service ou de l'organisme dont il relève. Elle est établie en trois exemplaires (un original et deux photocopies, datées et revêtues de la signature originale du candidat) et de trois photographies d'identité originales, identiques et récentes.
Le dossier d'habilitation est adressé par le chef du service employeur à l'autorité d'habilitation (SGDSN, HFDS, ASD, préfet), qui vérifie qu'il est complet et le transmet pour instruction :
- pour le niveau Très Secret Défense, au SGDSN, qui fait mener l'enquête par les services enquêteurs compétents ;
- pour les niveaux Secret Défense et Confidentiel Défense, directement aux services enquêteurs compétents.
2. Instruction du dossier :
L'enquête de sécurité menée dans le cadre de la procédure d'habilitation est une enquête administrative permettant de déceler chez le candidat d'éventuelles vulnérabilités.
Elle est diligentée par :
- le service enquêteur du ministère de l'intérieur (35) pour les personnels civils (y compris ceux travaillant pour la gendarmerie) ou les organismes travaillant dans le domaine civil ;
- les services enquêteurs du ministère de la défense (36) pour les personnels civils ou militaires du ministère de la défense, les personnels militaires de la gendarmerie, les personnels employés dans les organismes ou entreprises travaillant au profit du ministère de la défense (37).
L'enquête administrative est fondée sur des critères objectifs permettant de déterminer si l'intéressé, par son comportement ou par son environnement proche, présente une vulnérabilité, soit parce qu'il constitue lui-même une menace pour le secret, soit parce qu'il se trouve exposé à un risque de chantage ou de pressions pouvant mettre en péril les intérêts de l'Etat, chantage ou pressions exercés par un service étranger de renseignement, un groupe terroriste, une organisation ou une personne se livrant à des activités subversives.
3. Clôture de l'instruction et avis de sécurité :
L'enquête administrative menée dans le cadre de l'habilitation s'achève par l'émission d'un avis de sécurité, par lequel le service enquêteur fait connaître ses conclusions techniques à la seule autorité compétente pour prendre la décision d'habilitation.
Cet avis est une évaluation des vulnérabilités éventuellement détectées lors de l'enquête et permet à l'autorité décisionnaire d'apprécier l'opportunité de l'habilitation de l'intéressé, au regard des éléments communiqués et des garanties qu'il présente pour le niveau d'habilitation requis.
Les conclusions de l'avis de sécurité sont de trois types (38) :
- avis sans objection , lorsque l'instruction n'a révélé aucun élément de vulnérabilité de nature à constituer un risque pour la sécurité des informations ou supports classifiés ni

pour celle de l'intéressé ;
- avis restrictif , lorsque l'intéressé présente certaines vulnérabilités constituant des risques directs ou indirects pour la sécurité des informations ou supports classifiés auxquels il aurait accès, mais que des mesures de sécurité spécifiques prises par l'officier de sécurité permettraient de maîtriser ;
- avis défavorable , lorsque des informations précises font apparaître que l'intéressé présente des vulnérabilités faisant peser sur le secret des risques tels qu'aucune mesure de sécurité ne semble suffisante à les neutraliser.
L'avis de sécurité est émis pour un niveau donné d'habilitation. L'avis sans objection est valable pour le niveau précisé ainsi que pour le(s) niveau(x) inférieur(s). Pour les avis restrictifs ou défavorables, les services enquêteurs se prononcent, au cas par cas, sur l'opportunité d'accorder une habilitation pour le(s) niveau(x) inférieur(s).
Les avis restrictifs ou défavorables peuvent être classifiés selon l'appréciation du service enquêteur.
Les avis restrictifs et défavorables sont assortis d'une fiche confidentielle indiquant les motifs de l'avis. Cette fiche est composée de deux parties distinctes, permettant de séparer les éléments, non classifiés, qui peuvent être communiqués au candidat, de ceux, le cas échéant classifiés, qui ne peuvent être portés qu'à la connaissance de la seule autorité d'habilitation. Ne pouvant être reproduite, la fiche confidentielle est retournée après communication et sans délai au service enquêteur qui l'a émise, aux fins de conservation.
La durée de validité de l'avis de sécurité est fonction du niveau d'habilitation demandé. Elle ne peut excéder :
- cinq ans pour le niveau Très Secret Défense ;
- sept ans pour le niveau Secret Défense ;
- dix ans pour le niveau Confidentiel Défense.
L'avis de sécurité ne constitue en soi ni une autorisation ni un refus et ne lie pas l'autorité d'habilitation, qui prend sa décision après avoir apprécié les différents éléments recueillis pendant l'instruction du dossier.

## Article 25
## La décision

La décision d'habilitation ou de refus d'habilitation est prononcée par l'autorité d'habilitation (39) au regard des conclusions du service enquêteur. Quel que soit le sens de l'avis de sécurité, auquel il n'est d'ailleurs fait aucune référence dans la décision, l'autorité d'habilitation peut admettre ou rejeter une demande d'habilitation.
L'autorité d'habilitation peut décider, lorsque l'enquête a mis en valeur des éléments de vulnérabilité, de n'accorder l'habilitation qu'après avoir pris des précautions particulières. Ainsi, afin de garantir le plus efficacement possible la protection des informations ou supports classifiés, l'attention de l'employeur, par une procédure de mise en garde, ou celle de l'intéressé lui-même, par une procédure de mise en éveil, est attirée sur les risques auxquels l'un ou l'autre se trouve exposé. Les procédures de mise en garde et de mise en éveil peuvent être cumulées.
1. La décision d'habilitation :
La décision d'habilitation est l'autorisation donnée à une personne, en fonction de son besoin d'en connaître, d'accéder aux informations ou supports classifiés au niveau précisé dans la décision, ainsi qu'au(x) niveau(x) inférieur(s).
Pour le niveau Très Secret Défense, la décision précise la classification spéciale concernée. Lorsqu'une personne doit avoir accès de façon régulière à des informations relevant de plusieurs classifications spéciales, une décision d'habilitation doit être émise pour chacune de ces classifications. Aussi une personne peut-elle être visée par plusieurs décisions d'habilitation.
2. La mise en garde :

Lorsqu'un avis de sécurité est restrictif ou défavorable, l'autorité d'habilitation peut néanmoins décider d'accorder l'habilitation tout en mettant en garde l'officier de sécurité compétent. Cette procédure permet à celui-ci de mettre en œuvre des mesures de sécurité ou de prendre des précautions particulières à l'égard de l'intéressé, si nécessaire avec le conseil du HFDS ou du service enquêteur. Le service enquêteur, en liaison avec le HFDS, apprécie, parmi les éléments révélés par l'enquête, ce qu'il convient de communiquer à l'officier de sécurité et, le cas échéant, à l'employeur.
A l'issue de l'entretien de mise en garde, une attestation particulière (40) est signée par l'officier de sécurité du service employeur. La décision d'habilitation n'est rendue qu'à l'issue de la procédure. L'attestation est conservée par l'autorité d'habilitation.
Au niveau Très Secret Défense, la procédure de mise en garde est menée par le SGDSN, qui conserve l'attestation.
3. La mise en éveil :
Lorsque l'autorité d'habilitation décide d'accorder l'habilitation sur la base d'un avis de sécurité restrictif ou en dépit d'un avis de sécurité défavorable, elle peut choisir de demander la mise en éveil de l'intéressé, qui consiste à sensibiliser ce dernier sur les éléments communicables de vulnérabilité révélés par l'enquête (41). La mise en éveil est menée par l'autorité d'habilitation, en présence de l'officier de sécurité concerné. L'autorité d'habilitation définit les modalités de la mise en éveil en liaison avec le service enquêteur et peut, au cas par cas, solliciter sa présence lors de l'entretien avec l'intéressé. Le cas échéant, l'officier de sécurité étudie avec ce service les mesures de sécurité complémentaires à mettre en œuvre au regard de la situation.
A l'issue de l'entretien de mise en éveil, une attestation particulière (42) est signée par le représentant de l'autorité d'habilitation, par l'officier de sécurité du service employeur et par l'intéressé.
La décision d'habilitation n'est rendue qu'à l'issue de la procédure. L'attestation est conservée par l'autorité d'habilitation.
Au niveau Très Secret Défense, la mise en éveil est menée par le SGDSN, qui conserve l'attestation.
4. Le refus d'habilitation :
L'intéressé est informé de la décision défavorable prise à son endroit. Un refus d'habilitation n'a pas à être motivé lorsqu'il repose sur des informations qui ont été classifiées (43).

## Article 26
## La notification de la décision

La décision prise par l'autorité d'habilitation est transmise à l'officier de sécurité. A réception, ce dernier notifie au candidat à l'habilitation la décision individuelle prise à son endroit, qu'elle soit favorable ou non.
1. Décision favorable et engagement de responsabilité :
La décision d'habilitation est notifiée par l'officier de sécurité compétent à l'intéressé, qui signe un engagement de responsabilité (44). Par cet acte, le candidat reconnaît avoir eu connaissance des obligations particulières imposées par l'accès à une information ou à un support classifié ainsi que des sanctions prévues par le code pénal en cas d'inobservation, délibérée ou non, de la réglementation protégeant le secret de la défense nationale.
Il est également notifié à l'intéressé qu'il est tenu d'informer au plus vite, pendant toute la durée de son habilitation, l'officier de sécurité dont il relève de tout changement affectant sa vie personnelle (mariage, divorce, PACS, établissement ou rupture d'une vie commune...), professionnelle ou son lieu de résidence. Il lui est signifié qu'il devra l'informer de toute relation suivie et fréquente dépassant le strict cadre professionnel avec un ou plusieurs ressortissants étrangers. L'officier de sécurité devra alors lui faire remplir, afin de mettre à jour les informations, une notice individuelle 94 A et la transmettre à l'autorité d'habilitation (sous forme électronique lorsque la procédure est dématérialisée).

Ce changement de situation pourra justifier un réexamen du dossier d'habilitation et, le cas échéant, la saisine du service enquêteur en vue de l'émission d'un nouvel avis.
Le second volet de cet engagement est signé par l'intéressé à la cessation de ses fonctions ou au retrait de l'habilitation, et précise que les obligations relatives à la protection des informations classifiées auxquelles il a pu être donné accès perdurent au-delà du terme mis à ses fonctions ou à son habilitation. Une fois signé, ce second volet est retourné à l'autorité d'habilitation.
2. Refus d'habilitation :
La décision de refus d'habilitation est notifiée à l'intéressé par l'officier de sécurité. A cette occasion l'intéressé est informé, selon les modalités définies par le département minintériel dont il dépend, des voies de recours et des délais qui lui sont ouverts pour contester cette décision.
Si le candidat sollicite, par l'exercice d'un recours, une explication du rejet de la demande d'habilitation, il obtient communication des motifs lorsqu'ils ne sont pas classifiés. Lorsqu'ils le sont, le candidat se voit opposer les règles applicables aux informations protégées par le secret.

## Article 27
## Durée de validité de l'habilitation

La durée de validité de l'habilitation est liée à la durée d'occupation du poste qui a justifié sa délivrance. Elle cesse lorsque l'intéressé quitte son emploi.
La décision d'habilitation précise en principe elle-même sa durée de validité. Elle ne peut excéder celle de l'avis de sécurité au regard duquel elle a été prise.
Au seul cas de demande de renouvellement de l'habilitation formulée dans les délais prévus à l'article 31, et si aucune observation n'a été émise par le service enquêteur, la décision d'habilitation est implicitement prorogée pour une durée maximale de douze mois.

## Article 28
## Habilitation et changement d'affectation

Lorsqu'une personne habilitée change d'affectation, son habilitation pour le poste initial prend fin (45) et une autre décision peut être prise, si la nouvelle affectation l'exige, sur la base de l'avis de sécurité en cours.
Si l'autorité d'habilitation compétente change, l'officier de sécurité du service quitté renvoie la décision d'habilitation et l'engagement de responsabilité à l'autorité qui a décidé de l'habilitation. Afin d'informer la nouvelle autorité d'habilitation qu'un avis de sécurité est en cours de validité, l'officier de sécurité du service quitté lui transmet un certificat de sécurité. Si l'avis est restrictif ou défavorable, la nouvelle autorité d'habilitation peut, pour prendre sa décision, demander à connaître les motifs qui l'ont justifié.
Pour le niveau Très Secret Défense, lorsque l'habilitation est devenue sans objet en raison du changement d'affectation de son titulaire, l'autorité compétente en avise le SGDSN et lui renvoie sans délai la décision d'habilitation ainsi que l'engagement de responsabilité (volet 2) dûment signé.

## Article 29
## Conservation des décisions

Pendant leur durée de validité, les décisions d'habilitation sont conservées par l'officier de sécurité du service employeur. Ces documents, qui portent une mention de protection (46), ne sont en aucun cas remis aux intéressés ni reproduits.
En cas de nécessité, il peut être remis aux intéressés, par l'autorité d'habilitation, un certificat de sécurité (47) délivré pour une mission déterminée et une période limitée. La délivrance de ces certificats peut être déléguée à l'officier de sécurité. Il est de la responsabilité de l'intéressé de procéder ou de faire procéder à la destruction de ce certificat dès le retour de mission.

Les éléments relatifs à l'habilitation des personnels sont conservés pour une durée que chaque ministre définit pour le département dont il a la charge. Cette durée ne peut pas être inférieure à cinq ans à compter de leur date de péremption.

## Article 30
## Répertoire des habilitations

Dans chaque département ministériel, il est tenu, pour chacun des trois niveaux de classification, un répertoire :
- des dossiers d'habilitation en cours d'instruction ;
- des habilitations en cours de validité.

Le SGDSN tient à jour le répertoire central des habilitations au niveau Très Secret Défense, y compris dans le domaine international.
Pour permettre au SGDSN d'évaluer le nombre total d'habilitations délivrées et de personnes ayant accès aux informations ou supports classifiés, le HFDS lui adresse, en fin d'année, un état des personnes relevant de son département ministériel habilitées aux niveaux Secret Défense et Confidentiel Défense, dans le cadre du rapport annuel d'évaluation mentionné à l'article 12 de la présente instruction.

## Article 31
## Fin de l'habilitation

L'habilitation prend fin de trois manières : soit lorsque l'intéressé quitte le poste qui a motivé son habilitation, soit lorsque la validité de l'habilitation expire, soit parce que l'habilitation est retirée.
1. Cessation des fonctions :
L'habilitation liée à l'occupation d'un poste ou à l'exercice d'une fonction déterminée expire lorsque son titulaire change d'affectation ou cesse ses fonctions. En quittant l'emploi précisé dans la décision d'habilitation, le titulaire signe, conformément aux dispositions de l'article 26 de la présente instruction, le second volet de l'engagement de responsabilité.
2. Expiration de validité et renouvellement :
Le titulaire d'une habilitation dont le terme fixé dans la décision arrive à échéance signe, conformément à l'article 26 précité, le second volet de son engagement de responsabilité.
Seule, au regard des dispositions de l'article 27 de la présente instruction, une demande de renouvellement, engagée dans les formes et les délais requis, permet de proroger provisoirement la validité de l'habilitation afin d'éviter une interruption inopportune des conditions d'emploi, de fonction ou de la mission du titulaire.
La demande de renouvellement doit être effectuée dans le délai de six mois et, au plus tard, un mois avant la date d'expiration de l'habilitation en cours. Elle est constituée d'un nouveau dossier de demande d'habilitation identique à celui décrit à l'article 24.
Lorsque la procédure peut être dématérialisée, la nouvelle demande est transmise dans les mêmes conditions que la demande initiale.
La validité de la décision initiale d'habilitation est prorogée d'une durée maximale de douze mois après péremption de l'avis de sécurité, lorsque le besoin de connaître des informations classifiées subsiste au-delà de la durée de validité de cet avis, conformément aux dispositions de l'article 27 de la présente instruction, et à la condition impérative qu'une demande de renouvellement ait été régulièrement engagée, dans l'attente des conclusions de l'instruction du nouveau dossier.
Cette prorogation est autorisée dans les mêmes conditions lorsqu'une demande, à un niveau supérieur, est formulée dans le délai de six à un mois (au plus tard) précédant la date d'expiration de l'habilitation en cours.
3. Retrait d'habilitation :
La décision d'habilitation ne confère pas à son bénéficiaire de droit acquis à son maintien.
L'habilitation peut être retirée en cours de validité ou à l'occasion d'une demande de renouvellement si l'intéressé ne remplit plus les conditions nécessaires à sa délivrance, ce qui peut être le cas lorsque des éléments de vulnérabilité apparaissent, signalés par

exemple par :
- le service enquêteur ;
- le supérieur hiérarchique ou l'officier de sécurité concerné, à la suite d'un changement de situation ou de comportement révélant un risque pour la défense et la sécurité nationale.
La décision de retrait est notifiée à l'intéressé dans les mêmes formes que le refus d'habilitation, décrites à l'article 26 de la présente instruction, sans que les motifs lui soient communiqués s'ils sont classifiés. L'intéressé est informé des voies de recours et des délais qui lui sont ouverts pour contester cette décision.

## Chapitre III
## Les cas particuliers

### Article 32
### La procédure de contrôle élémentaire

Différent de l'habilitation par sa nature et par son objet, le contrôle élémentaire est une enquête administrative simplifiée, sollicitée par l'autorité d'habilitation, destinée à s'assurer de l'intégrité d'une personne. Il garantit que le degré de confiance qu'il est possible d'accorder à cette personne est compatible avec la fonction, l'affectation ou le recrutement pour lequel elle est pressentie ou lui permet d'avoir accès à certaines zones protégées. Il est tout particulièrement applicable au cas du personnel d'entretien.
Les demandes de contrôle élémentaire sont instruites par le service enquêteur compétent, qui émet un avis adressé au demandeur. La durée de validité de cet avis est laissée à l'appréciation de chaque département ministériel.

### Article 33
### La décision d'agrément

Lorsqu'une personne dont le poste n'est pas inscrit au catalogue des emplois est amenée, dans le cadre de ses fonctions ou d'une mission particulière, de façon ponctuelle, à avoir accès à des informations ou à des supports classifiés ou à en prendre connaissance, elle peut se voir délivrer une décision d'agrément. Il en est de même lorsque l'intéressé est habilité à un niveau et qu'il a besoin, de façon ponctuelle, d'accéder à des informations classifiées à un niveau supérieur.
L'agrément accordé après demande dûment motivée par l'autorité responsable et à l'issue d'une procédure d'enquête administrative ordinaire, ou d'une procédure simplifiée conformément aux dispositions de l'article 34 de la présente instruction, autorise occasionnellement l'accès aux informations ou supports classifiés.
L'agrément ne doit en aucun cas être considéré comme une habilitation de réserve, accordée par précaution à un nombre indéfini de personnes pour satisfaire des besoins imprécis.
Au niveau Très Secret Défense, un catalogue des emplois nécessitant un agrément doit être établi.

### Article 34
### La procédure simplifiée

Les agents publics, fonctionnaires ou contractuels, civils ou militaires, peuvent être habilités au niveau Confidentiel Défense par l'autorité dont ils relèvent et sans intervention à cet effet d'un service enquêteur, sous réserve :
- d'avoir fait l'objet d'un contrôle élémentaire (48) au moment de leur recrutement ou de leur prise de fonctions ;
- d'occuper un poste figurant au catalogue des emplois ;
- de remplir la notice individuelle de sécurité, attestant sur l'honneur l'exactitude des informations mentionnées ;
- d'avoir signé l'engagement de responsabilité défini à l'article 26.
L'autorité hiérarchique peut à tout moment solliciter qu'une enquête administrative soit effectuée par le service enquêteur compétent.
La décision d'habilitation par procédure simplifiée est notifiée à l'intéressé dans les

conditions ordinaires.

Article 35

La procédure d'urgence

La procédure d'urgence est une procédure exceptionnelle permettant de délivrer à une personne une habilitation dans des délais très brefs, afin de lui permettre d'avoir accès à des informations ou à des supports classifiés dès sa prise de fonctions. La durée de validité de cette habilitation provisoire ne peut excéder six mois.

Peuvent en particulier bénéficier de cette procédure les personnes faisant partie des catégories suivantes :

- hauts fonctionnaires, diplomates, officiers généraux ;
- personnes envoyées en mission dans le cadre d'opérations inopinées ;
- responsables de haut niveau affectés dans des conditions ne permettant pas le respect des délais ordinaires.

Le dossier est constitué selon la procédure ordinaire mais le chef du service employeur doit, dans la demande, préciser et motiver l'urgence de l'habilitation et l'impossibilité de procéder autrement.

Pour le niveau Très Secret Défense, le SGDSN, au regard des éléments transmis par le chef du service employeur, est seul compétent pour engager une telle procédure.

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

La procédure d'urgence ne peut concerner qu'un nombre très limité de personnes. Elle ne remplace ni n'interrompt la procédure normale, qui se poursuit après l'émission de l'avis de sécurité provisoire.

Lorsqu'une habilitation provisoire a été accordée dans le cadre de la procédure d'urgence, sa validité expire :

- soit lorsque la décision d'habilitation ou de refus est prise par l'autorité compétente, à réception de l'avis de sécurité définitif, à l'issue de la procédure ordinaire d'habilitation ;
- soit au plus tard six mois après sa date d'émission.

Article 36

La décision de sécurité convoyeur

Sans préjudice des dispositions prévues aux articles 57 et suivants de la présente instructin, un document ou support classifié au niveau Confidentiel Défense ou Secret Défense ne peut être transporté que par des personnes habilitées au niveau approprié ou par des personnels internes au service ou à l'organisme titulaires d'une décision de sécurité convoyeur (49). Cette décision est délivrée par l'autorité d'habilitation après réalisation, par les services enquêteurs, d'un contrôle élémentaire valant, selon la demande de l'autorité d'habilitation, soit pour une mission particulière, soit pour une durée nécessairement inférieure à trois ans (50).

Cette décision n'autorise en aucun cas à prendre connaissance d'informations classifiées.

La décision peut être renouvelée. Lorsque la décision est accordée pour une durée déterminée, ne pouvant en aucun cas excéder trois ans, la demande de renouvellement doit nécessairement être effectuée avant l'expiration du délai fixé.

Pour le niveau Très Secret Défense, le convoyage répond à des modalités spécifiques, définies par instructions particulières (51).

Article 37

L'habilitation de ressortissants étrangers

Les ressortissants étrangers occupant un emploi nécessitant l'accès à des informations ou supports classifiés, et dans les limites du strict besoin d'en connaître, peuvent être habilités au niveau Confidentiel Défense ou Secret Défense.

La procédure d'habilitation est engagée par le ministre concerné, son délégataire (HFDS, préfet) ou l'autorité de sécurité déléguée (ASD). La décision d'habilitation est prise par la même autorité.
Le SGDSN, en sa qualité d'ANS, assure la liaison avec les ANS étrangères pour obtenir les éléments permettant l'instruction du dossier d'habilitation de l'intéressé. La communication avec les ANS étrangères a lieu par son intermédiaire. Toutefois, il peut autoriser des échanges directs entre les autorités de sécurité déléguées et leurs homologues étrangers.
Si l'habilitation intervient dans le cadre soit d'une organisation internationale possédant une réglementation propre relative à la protection des informations ou supports classifiés, soit d'un accord multilatéral comportant des dispositions particulières en ce domaine, soit d'un accord bilatéral de sécurité, il convient de se référer aux dispositions spécifiques de ces textes afin de déterminer les conditions et procédures d'habilitation à appliquer. En cas de difficulté, l'ANS définit la procédure.
Lorsque des dispositions le prévoient expressément, une habilitation accordée par une ANS étrangère peut être prise en compte par les autorités françaises compétentes lorsque le ressortissant étranger occupe en France un emploi nécessitant l'accès à des informations ou supports classifiés. Au regard du certificat de sécurité produit par l'ANS étrangère, une décision d'habilitation pourra être émise par l'autorité d'habilitation concernée.
Lorsqu'il n'existe aucun accord de sécurité entre la France et l'Etat dont l'intéressé est ressortissant, aucune habilitation, à aucun niveau, ne doit, en principe, être délivrée par une autorité française. A titre exceptionnel, si le besoin d'en connaître est avéré, l'autorité requérante peut saisir l'ANS française qui appréciera l'opportunité de l'habilitation et définira, le cas échéant, la procédure à suivre, avant de prendre sa décision.

Article 38

Portée de la décision d'habilitation en matière internationale

Toute décision d'habilitation aux informations ou supports classifiés du domaine national peut en soi, à défaut d'une habilitation spécifique et sous réserve du besoin d'en connaître, donner accès aux informations ou supports classifiés du niveau correspondant et des niveaux inférieurs des domaines internationaux ou confiés à la France en application de l'accord de sécurité conclu entre les Etats signataires du traité de l'Atlantique Nord, des dispositions juridiques mises en place dans le cadre de l'Union européenne et des accords de sécurité signés par la France.
Une décision d'habilitation aux informations ou supports classifiés du domaine international ne donne pas accès aux informations ou supports classifiés du domaine national.

TITRE III

MESURES DE SÉCURITÉ RELATIVES AUX INFORMATIONS

OU SUPPORTS CLASSIFIÉS

La décision de classifier une information ou un support au titre du secret de la défense nationale a pour objet de restreindre l'accès à cette information ou à ce support aux personnes préalablement habilitées et justifiant du besoin d'en connaître.
Elle est prise selon des critères définis par une instruction ministérielle.
Elle doit procéder d'une appréciation rigoureuse de son opportunité.
Elle place cette information ou ce support sous la protection de dispositions pénales spécifiques (52).
La classification est matérialisée par l'apposition d'une mention spécifique qui permet de caractériser l'infraction pénale en cas de compromission.

La compromission peut résulter d'un acte de malveillance comme d'une simple négligence.

## Chapitre Ier

## Principes généraux de la classification

### Section 1

### Les règles de classification

#### Article 39

#### Responsabilité de la décision de classification

Pour le niveau Très Secret Défense, les modalités de protection des informations ou supports classifiés sont déterminées par le Premier ministre dans des instructions particulières (53).
Pour les niveaux Secret Défense et Confidentiel Défense, chaque ministre détermine, dans les conditions fixées par le Premier ministre, les informations ou supports qu'il y a lieu de classifier à l'un ou l'autre de ces niveaux et les modalités d'organisation de leur protection.
Au sein de chaque ministère, la décision de classification est prise, sur proposition de l'auteur du document, au niveau hiérarchique le plus apte à évaluer les enjeux. Le responsable de cette décision, qui doit être en mesure de la justifier auprès de sa hiérarchie, est appelé autorité classificatrice ou autorité émettrice.
La décision de classifier résulte de l'analyse de l'importance de l'information au regard de son contexte, des textes applicables et des instructions du ministre compétent. L'autorité classificatrice veille à ce que le niveau de classification soit approprié à l'information ou au support concerné(e), c'est-à-dire à ce qu'il soit à la fois nécessaire et suffisant. Elle cherche ainsi à limiter la prolifération de documents classifiés et à éviter les classifications abusives, qui génèrent des coûts de gestion, des charges de travail importantes et altèrent la valeur du secret de la défense nationale. Cette évaluation comporte un risque d'erreur d'appréciation pouvant conduire, à l'inverse, à ce qu'une information justifiant une classification ne soit pas classifiée, ce qui constitue un manquement aux règles de protection du secret dont l'autorité émettrice est responsable (54).
En cas d'évolution, dans le temps ou en fonction des circonstances, de la sensibilité des informations classifiées, l'autorité classificatrice peut décider de procéder à leur déclassification, leur déclassement ou leur reclassement (55). Elle notifie sa décision de modification ou de suppression de classification aux destinataires de l'information ou du support.
Les cas manifestes de surclassification ou de sous-classification sont signalés par le(s) destinataire(s) à l'émetteur qui procédera, si nécessaire, à la modification appropriée, en informera l'ensemble des destinataires et prendra les mesures nécessaires pour éviter une compromission lorsque le document change de niveau.

#### Article 40

#### Critères de classification

Les critères de classification et l'importance de ne classifier que ce qui est réellement nécessaire sont énoncés dans une instruction ministérielle (56).
Le niveau de classification est déterminé par la nature de l'information ou du support classifié. La source de l'information peut également être prise en considération lorsque sa sensibilité justifie une protection (57).
Lorsqu'un document comprend diverses parties, les unes nécessitant une classification, les autres non, il convient de s'efforcer de les présenter de manière distincte afin de ne pas entraver la diffusion des informations non classifiées. La diffusion de la partie non classifiée du document est rendue possible en plaçant en annexe classifiée l'information couverte par le secret de la défense nationale.

Tout ensemble (58) de documents contenant des informations classifiées à des niveaux différents doit être classifié lui-même au moins au niveau le plus élevé de ces documents.
Un ensemble d'informations ou de supports, dit parfois "agrégat", est classifié si le regroupement des informations ou supports qui le composent le justifie, alors même qu'aucun de ses éléments, pris isolément, n'est classifié.
Un extrait d'information classifiée conserve le niveau de classification de l'information elle-même, à moins que l'autorité classificatrice en décide autrement (59).

Article 41

Identification de la classification

Une information ou un support, quel qu'il soit, acquiert juridiquement le caractère de secret de la défense nationale dès lors qu'il fait l'objet de mesures de classification destinées à restreindre sa diffusion, matérialisées par la mention de niveau de classification sur le support de l'information (60).
Les supports préparatoires ayant servi à l'élaboration de l'information classifiée (brouillons, impressions sur papier, matériels informatiques nomades [61]), qui ne sont pas identifiés, sont placés sous la responsabilité de celui qui les a élaborés. Ils doivent être détruits ou effacés le plus rapidement possible dès qu'ils sont devenus sans objet et, en tout état de cause, au plus tard lorsque le document classifié est émis.

Section 2

Le marquage

Article 42

Principe général du marquage

Le marquage, par ses trois éléments constitutifs que sont le timbre, l'identification et la pagination, permet de vérifier l'authenticité et l'intégrité du support. Chaque exemplaire d'un document classifié porte la mention du niveau de classification des informations qu'il contient.
Les paragraphes, alinéas, annexes, traitant d'informations classifiées à un niveau inférieur ou non classifiées, sont mis en évidence, s'il y a lieu, 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.
Jusqu'au niveau Secret Défense, les abréviations indiquant la classification peuvent être utilisées pour préciser le niveau de classification des paragraphes du texte. Les abréviations admises sont les suivantes :
- Confidentiel Défense : CD ;
- Secret Défense : SD.

Ces abréviations ne remplacent pas la mention de classification inscrite en toutes lettres sur le document papier, réalisée par le timbrage.
S'il est matériellement impossible d'apposer le marquage sur le support classifié ou contenant une information classifiée, il convient de mettre en œuvre des mesures de protection destinées à lever toute ambiguïté qui pourrait naître de l'absence de mention visible de classification. A cette fin, chaque ministère édicte, après avis du SGDSN, des directives particulières afin d'adapter aux caractéristiques des supports la réglementation relative au marquage, et de permettre leur identification au niveau de classification requis.
L'absence de mise en œuvre de ces consignes rend inopérante la protection pénale accordée au secret de la défense nationale. Le respect scrupuleux des consignes constitue par conséquent un enjeu majeur.

Article 43

Le marquage d'un support papier

Le marquage d'un support papier comprend à la fois le timbre, l'identification et la pagination :
- le timbre indique le niveau de classification et permet 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 ;
- la pagination consiste en la numérotation de chaque page et la mention du nombre total de pages contenues dans le document.

1. Timbre :

Le timbre de la mention de classification est apposé, avec une encre de couleur rouge, ou, à titre exceptionnel, d'une couleur contrastant avec celle du support, au milieu du haut et du bas de chaque page. Pour les documents reliés, un timbre d'un modèle de dimension supérieure est placé au milieu du bas de la couverture et de la page de garde (62).
Lorsque des documents sont élaborés sur un poste de travail informatique, le marquage doit être ajouté par voie électronique à l'en-tête et au pied de page.
Le timbre, dont la dimension peut être adaptée à celle du support, est définitif et toujours visible.

2. Identification :

Tout document classifié est identifié dès sa première page. En plus des références ordinaires de toute pièce administrative, des mesures particulières sont prises. Ainsi, sur la première page du document, figurent les références du service émetteur, de la date d'émission, du numéro d'enregistrement, le timbre du niveau de classification et celui indiquant l'échéance de la classification (c'est-à-dire la date à laquelle la classification du document est réévaluée ou le document déclassifié). Le cas échéant, la mention de déclassement ou de déclassification est apposée sur cette même page.
Pour les documents classifiés au niveau Secret Défense, chaque exemplaire est individualisé et le nombre total d'exemplaires est porté sur le document. Le numéro d'enregistrement émane du bureau de protection du secret compétent.

3. Pagination :

Chaque page du document est numérotée. Au bas de la première page est mentionné le nombre total de pages, d'annexes ou de plans qui composent le document.
Les pages de chaque annexe sont numérotées indépendamment de la pagination du document lui-même, et portent mention du nombre total de pages de l'annexe.
Pour les documents classifiés au niveau Secret Défense, les pages vierges et les feuilles intercalaires sont également numérotées. Toute page vierge porte en son centre la mention "PAS DE TEXTE".

## Article 44

## Le marquage d'un support non papier

Le marquage d'un support non papier d'information classifiée est adapté au type de support, définitif et toujours visible. Il consiste en un timbre et une identification.

1. Timbre :

Le timbre spécifiant le niveau de classification a une dimension adaptée à celle du support et comporte la mention de ce niveau en toutes lettres. En cas de difficultés pratiques, les abréviations précédemment évoquées peuvent y être substituées.

2. Identification :

L'identification des supports non papier d'informations classifiées est assurée par l'inscription des références et, le cas échéant, du volume de chacune des informations enregistrées. Lorsqu'il est impossible d'inscrire sur le support l'ensemble des références, l'identification est faite par le numéro d'enregistrement.
Pour le niveau Secret Défense, le numéro d'enregistrement est délivré par le bureau de protection du secret et est éventuellement assorti d'une fiche où sont inscrites les références réglementaires des informations contenues.

3. Pagination des documents électroniques :

Chaque page du document est numérotée. Au bas de la première page est mentionné le nombre total de pages, d'annexes ou de plans qui composent le document.

Les pages de chaque annexe sont numérotées indépendamment de la pagination du document lui-même, et portent mention du nombre total de pages de l'annexe.
Pour les documents classifiés au niveau Secret Défense, les pages vierges et les feuilles intercalaires sont également numérotées. Toute page vierge porte en son centre la mention "PAS DE TEXTE".
4. Dispositions particulières :
En raison de la possibilité technique de faire réapparaître des informations en principe effacées, un support informatique d'informations classifiées conserve toujours le niveau de classification qui lui a été initialement attribué. Il ne peut être déclassé ou déclassifié qu'à la condition que les informations qu'il contient ou a contenues aient elles-mêmes préalablement fait l'objet d'une telle mesure.

## Section 3
## Enregistrement

### Article 45
### L'enregistrement des informations

ou supports classifiés
Tout support contenant des informations classifiées est enregistré, dans l'ordre chronologique, par un système d'enregistrement manuel ou informatisé permettant l'identification des destinataires.
L'enregistrement établit sans ambiguïté l'attribution du support à un détenteur, personne physique, clairement identifiée. Ce détenteur assume alors la responsabilité de la protection du support. Cet enregistrement est la seule référence de cette attribution de responsabilité.
La mention de l'objet du document, si cet objet est lui-même classifié, ne doit pas figurer dans le système d'enregistrement, à moins que ce système ne soit classifié et dédié. Cette obligation de classifier et de dédier le système d'enregistrement lui-même s'impose au niveau Secret Défense.
Au niveau Confidentiel Défense, le système d'enregistrement peut être relié à une base de gestion du courrier sous réserve que l'accès à la base soit restreint et que celle-ci permette de tracer les documents jusqu'au détenteur final.
Au niveau Secret Défense, le système d'enregistrement est tenu à jour par le bureau de protection du secret. Les documents Secret Défense font obligatoirement l'objet d'une double numérotation, présentée sous forme de fraction : ils portent le numéro d'enregistrement de l'émetteur et le numéro d'enregistrement du bureau de protection du secret chargé de leur traitement.

## Section 4
## Durée de classification des informations

ou supports classifiés

### Article 46
### La durée de vie des classifications
La sensibilité d'une information ou d'un support classifié pouvant évoluer en fonction du temps ou des circonstances, il revient à l'autorité émettrice d'en apprécier la durée utile de classification. L'autorité émettrice mentionne sur le document (63) la date à partir de laquelle le document sera automatiquement déclassifié. Lorsque cette date ne peut être déterminée, l'autorité émettrice mentionne la date ou le délai au terme duquel le niveau de

classification devra être réexaminé. La réévaluation peut avoir pour résultat le maintien du niveau de classification, le déclassement ou la déclassification du document. L'autorité émettrice peut également fixer comme terme non pas une date mais un événement défini (par exemple, début de production d'un matériel, retrait de service d'un matériel, fin d'un exercice...), à la suite duquel le document sera automatiquement déclassé au niveau qu'elle aura précisé ou sera déclassifié. Elle conserve la possibilité de prolonger à tout moment le délai qu'elle a fixé.
En tout état de cause, la révision du besoin et du niveau de classification des informations ou supports doit être effectuée rigoureusement selon une périodicité inférieure ou égale à dix ans, précisément définie par chaque ministre pour le département dont il a la charge.
Cette rigueur de gestion s'impose d'autant plus que, dès l'expiration d'un délai de cinquante ans à compter de la date d'émission d'un document classifié, se pose, dans les conditions énoncées à l'article 63 de la présente instruction, la question de la communicabilité du document et de sa déclassification préalable.
Pour les informations ou supports classifiés étrangers, seule l'autorité étrangère émettrice peut procéder à une déclassification ou à un déclassement.

## Chapitre II
## Gestion des informations ou supports classifiés

### Section 1
### Conservation des informations ou supports classifiés

#### Article 47
#### Conditions matérielles de conservation

En dehors des périodes d'utilisation, les informations ou supports classifiés sont conservés dans des coffres-forts ou des armoires fortes conformes aux dispositions relatives aux meubles de sécurité énoncées dans la présente instruction. Aucune indication relative à la nature des informations n'est visible à l'extérieur du coffre ou de l'armoire.
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 clé du coffre-fort de cette autorité étant elle-même placée dans un coffre distinct.
Les combinaisons sont changées au moins tous les six mois, et à chaque fois qu'il y a mutation des utilisateurs, risque ou suspicion de compromission.
Les clés sont impérativement mises en sécurité, notamment hors des heures ouvrables, suivant une procédure clairement établie par chaque autorité responsable (dépôt dans un coffre mural, sans clé, à combinaisons et à commande unique ou avec ouverture par lecture 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 classifiés, sauf nécessités impérieuses de service ;
- les clés des coffres ou armoires où sont conservés de tels informations ou supports.
La responsabilité de la conservation des informations ou supports classifiés Secret Défense incombe à un détenteur responsable ou au chef du bureau de protection du secret.

### Section 2
### Reproduction

#### Article 48
#### Règles générales de la reproduction

La généralisation et la diversité des moyens de reproduction accroissent les risques de diffusion incontrôlée des informations ou supports classifiés.
Pour les niveaux Secret Défense et Confidentiel Défense, des consignes précises sont établies par chaque ministre ou par son représentant (HFDS) pour le département dont il a la charge afin de fixer :
- la désignation, par les directeurs ou chefs de service, des autorités habilitées à autoriser la reproduction ;
- les procédures de contrôle de la reproduction ;
- la nécessité de consigner sur un système d'enregistrement le nombre de pièces reproduites et leurs détenteurs.
Les matériels utilisés pour la reproduction d'informations classifiées (photocopieuses, télécopieurs, systèmes informatiques...) doivent être physiquement protégés afin d'en limiter l'emploi aux seules personnes autorisées. Les opérations de maintenance sur ces matériels sont effectuées dans des conditions permettant de garantir la sécurité des informations classifiées qui ont été reproduites, dans le respect des dispositions de la présente instruction. Il en est de même pour leur mise au rebut, qui doit garantir la destruction des mémoires de ces appareils.

Article 49

Reproduction totale

Au niveau Secret Défense, la reproduction totale d'informations ou supports classifiés n'est possible qu'avec l'autorisation préalable de l'autorité émettrice. Le dépositaire de l'information ou du support qui souhaite en effectuer une reproduction doit adresser une demande motivée à cette autorité. Si celle-ci consent à la reproduction (64), elle spécifie les numéros à attribuer aux exemplaires supplémentaires et porte mention de cette reproduction sur l'exemplaire en sa possession.
En cas d'urgence et à titre exceptionnel, le dépositaire peut s'affranchir de cette procédure à la condition de prendre les dispositions suivantes :
1. Limiter au minimum indispensable le nombre des reproductions ;
2. Procéder au marquage réglementaire en attribuant à chaque exemplaire 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 second étant le numéro individuel de l'exemplaire attribué par l'autorité émettrice du document ;
3. Porter si nécessaire, sur l'exemplaire reproduit, la destination qui en est faite ou établir une liste séparée des destinataires ;
4. Rendre compte sans délai à l'autorité émettrice du nombre de reproductions, des numéros de reproductions et de la destination des exemplaires. L'autorité émettrice porte mention de cette reproduction sur l'exemplaire en sa possession.
Au niveau Confidentiel Défense, la reproduction peut être effectuée par les autorités détentrices, sous leur responsabilité, à condition de conserver sur un système d'enregistrement la trace du nombre et des destinataires des exemplaires reproduits.

Article 50

Reproduction partielle

Les extraits de documents classifiés sont eux-mêmes classifiés au niveau approprié à leur contenu. Si un extrait de document classifié ne justifie pas lui-même une classification, son importance doit rester limitée de façon à ne pas compromettre, en cas de divulgation, l'information dont il a été extrait. La diffusion séquentielle d'extraits non classifiés par découpage de l'information classifiée est interdite.
Des extraits d'informations classifiées Confidentiel Défense ou Secret Défense peuvent

être reproduits par leur dépositaire dans les conditions fixées par l'article 49 de la présente instruction.
Lorsque des extraits de documents contenant des informations classifiées sont transférés sur un autre support, si ces extraits sont eux-mêmes classifiés, la mention de classification est reportée sur le nouveau support conformément aux prescriptions de la présente instruction.

Section 3

Inventaire

Article 51

La procédure d'inventaire

Les documents classifiés font l'objet d'un suivi permanent afin d'assurer leur traçabilité et leur prise en compte par des détenteurs habilités.
A cet effet, chaque ministre préconise les modalités d'inventaire et de suivi des documents classifiés Confidentiel Défense et Secret Défense détenus dans l'ensemble des services et organismes relevant de son département.
Un inventaire est effectué sous forme contradictoire à chaque mutation de personnel, l'ancien détenteur et le nouveau apposant tous deux leur signature sur le procès-verbal.
La période d'inventaire est mise à profit pour alléger la gestion des documents classifiés.
Les dates d'expiration de validité sont vérifiées aux fins de déclassement ou de déclassification : la réévaluation du niveau de protection des documents classifiés et, le cas échéant, leur destruction doivent être réalisées.
Au niveau Confidentiel Défense, il est conseillé de procéder à un inventaire annuel. Cet inventaire est à effectuer sous la responsabilité de chaque détenteur ou par un bureau spécialisé. S'il y est procédé, un procès-verbal en est dressé. A défaut, un récolement annuel doit être effectué selon les modalités définies par les directives ministérielles afin de vérifier la présence physique des documents.
Au niveau Secret Défense, l'inventaire annuel, obligatoire, est effectué par les bureaux de protection du secret en liaison avec les détenteurs. Les HFDS collationnent les procès-verbaux d'inventaires et en transmettent un bilan au SGDSN, au plus tard le 31 mars de chaque année, dans le cadre du rapport annuel d'évaluation précédemment mentionné.
Le procès-verbal d'inventaire annuel, dressé par chaque bureau de protection du secret, mentionne les références et l'identification de chaque support classifié Secret Défense, et est accompagné, le cas échéant (65), 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.

Section 4

La protection des matériels classifiés

Article 52

Dispositions générales et classifications

La protection des matériels classifiés implique la mise en œuvre de mesures de sécurité à tous les stades de la réalisation (programme, étude, plan, fabrication ou construction, essai, etc.) de même que pour l'utilisation, l'entretien, la réparation et le transport jusqu'à leur mise hors service et à leur destruction.
L'autorité responsable (directeur de programme jusqu'à la livraison ou autorité détentrice lors de l'utilisation) détermine les matériels à protéger et le niveau de classification à

retenir, qui peut être différent de celui couvrant les documents (notices, plans, etc.) qui les concernent.
Il importe d'éliminer toute possibilité de vue terrestre ou aérienne et l'utilisation de procédés techniques de détection et d'identification. Un moyen efficace d'assurer la protection des matériels classifiés au niveau Secret Défense consiste à les entreposer dans une zone répondant aux règles de protection définies par la présente instruction. La zone considérée devra être érigée en zone protégée afin de pouvoir sanctionner pénalement la violation de l'interdiction d'y pénétrer.
Lorsque les matériels sont en service ou exposés à la vue en dehors d'une zone protégée, les autorités responsables font prendre des mesures de protection adaptées pour les matériels classifiés et leurs éléments constitutifs.

Article 53

La protection des matériels classifiés en cours de transport

La circulation et le transport des matériels classifiés 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 matériel à protéger et dès lors que le matériel transporté figure sur la liste tenue à jour par le ministère de la défense, il convient de se reporter aux dispositions particulières (66).
Pour les autres matériels ou équipements classifiés, l'autorité en ayant prescrit le mouvement assume la responsabilité des tâches suivantes :
- conditionnement 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 matériels classifiés est effectué, sauf impossibilité absolue ou opération conjointe, par des moyens nationaux. A défaut, il doit être convoyé et toutes dispositions sont prises pour que la sécurité soit assurée sans discontinuité pendant toute la durée du transport.

## Chapitre III
## Diffusion et acheminement des informations

ou supports classifiés

### Section 1
### La diffusion et l'expédition des informations

ou supports classifiés

Article 54

La diffusion

Lorsqu'elle diffuse des informations ou supports classifiés, l'autorité d'expédition établit la liste des destinataires et s'assure qu'ils sont habilités au niveau de classification requis.
Au niveau Secret Défense, le nombre et le numéro des supports attribués à chaque destinataire ainsi que le numéro des exemplaires conservés par le service émetteur sont précisés dans la liste de diffusion (deux exemplaires au moins, dont un original destiné, à

terme, aux archives).
La liste des destinataires, lorsqu'elle constitue en elle-même un secret, n'est pas jointe à l'envoi de chacun des exemplaires du support.

Article 55

La diffusion, l'expédition et la réception d'informations

ou supports classifiés par voie électronique

La diffusion, l'expédition et la réception d'informations classifiées par voie électronique sont régies par les dispositions du titre V.

Article 56

L'expédition et la réception d'informations

ou supports classifiés

L'expédition d'informations ou supports classifiés est soumise à une procédure particulière qui permet d'assurer le suivi et de garantir l'intégrité physique du document grâce à un conditionnement spécial.
Les autorités d'expédition sont :
- au niveau Secret Défense, le bureau de protection du secret ;
- au niveau Confidentiel Défense, les personnels habilités, dans le respect du principe du besoin d'en connaître.
L'autorité émettrice procède, après marquage et enregistrement de chaque support, aux opérations suivantes :
1. Pour l'expédition :
Conditionnement :
L'envoi de supports d'informations ou de supports classifiés se fait sous double enveloppe présentant des garanties de solidité de nature à assurer au maximum l'intégrité physique des supports :
- l'enveloppe extérieure, plastifiée, porte l'indication du service expéditeur, l'adresse du destinataire (sans mention trop explicite de nature à attirer l'attention sur le caractère classifié du contenu) et la mention du suivi. Elle ne porte en aucun cas la mention du niveau de classification de l'information ou support qu'elle contient. Au niveau Secret Défense, chaque enveloppe est numérotée ;
- l'enveloppe intérieure de sécurité de bonne qualité, opaque, si possible du modèle toilé ou armé, doit interdire une ouverture ou une refermeture discrète. Elle porte le timbre du niveau de classification, la référence des supports transmis, le cachet de l'autorité expéditrice, le nom et la fonction du destinataire ainsi que l'indication du service ou de l'organisme dans lequel il est affecté.
Suivi de l'expédition :
Un bordereau d'envoi, sans timbre de classification ni indication de l'objet des informations envoyées, est placé dans l'enveloppe intérieure de sécurité dont il porte le numéro. Il comporte trois feuillets détachables A, B et B' (67) signés par le responsable de l'autorité expéditrice ou une personne désignée par lui.
Les feuillets A et B sont adressés au destinataire, qui conserve le premier à titre d'élément de preuve et renvoie le second à titre d'accusé de réception. Le feuillet B', de couleur, est conservé par l'expéditeur jusqu'à réception du feuillet B, qui lui est alors substitué.
2. Pour la réception :
Les formalités de réception sont assurées par le bureau de protection du secret de l'organisme destinataire ou, au niveau Confidentiel Défense, par le destinataire de l'envoi.
Il convient :
- de vérifier l'intégrité de l'emballage afin de déceler une éventuelle compromission ;

- d’enregistrer ou de faire enregistrer l’information ou le support classifié conformément aux dispositions de l’article 45 ;
- de signer et de renvoyer le feuillet B du bordereau d’envoi à titre d’accusé de réception.
A la réception de documents classifiés Secret Défense, le bureau de protection du secret les transmet au destinataire.

## Section 2
## Acheminement

### Article 57
### L’acheminement d’informations ou supports classifiés

sur le territoire national
Les procédures de transmission des supports classifiés doivent permettre de respecter des délais compatibles avec le degré d’urgence et d’assurer la meilleure protection des supports transmis.
L’acheminement de supports classifiés sur le territoire national se fait de la façon suivante :
1. A l’intérieur d’un même immeuble :
Afin d’éviter leur observation, les informations ou supports classifiés sont acheminés sur place, sous enveloppe, soit :
- par le détenteur lui-même ;
- par une autre personne habilitée ;
- par un convoyeur ou par une personne du service de courrier interne autorisé(e).
La position des informations et supports classifiés doit être suivie sans discontinuité, notamment dans le système d’enregistrement des documents classifiés.
Au niveau Secret Défense, un compte rendu au bureau de protection du secret doit être effectué.
Cette règle peut parfois être assouplie pour une communication brève et temporaire d’informations ou de supports classifiés. Le détenteur des supports classifiés, responsable de leur acheminement, en rend compte. Il doit en contrôler la position et les faire réintégrer dès que les nécessités du service le permettent.
2. Avec changement d’immeuble ou de zone géographique :
Pour le niveau Secret Défense, l’acheminement peut s’opérer :
- par convoyeur autorisé ou par toute personne habilitée au niveau requis : les informations ou supports classifiés 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 de protection du secret destinataire ;
- par voie militaire : dans les conditions fixées par les instructions du ministère de la défense.
A défaut de convoyeur ou de personne habilitée disponible dans des délais compatibles avec un degré d’urgence qui doit pouvoir être clairement justifié, la voie postale civile est autorisée sur le territoire national, à la condition impérative de recourir aux opérateurs postaux proposant des moyens de transports protégés, tels que l’envoi en pli chargé avec valeur déclarée ou la lettre recommandée avec accusé de réception.
Pour le niveau Confidentiel Défense, l’acheminement peut s’opérer :
- par convoyeur autorisé ou par toute personne habilitée au niveau requis : les informations ou supports classifiés 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 destinataire ;
- par voie militaire : dans les conditions fixées par les instructions du ministère de la défense ;

- par voie postale civile sur le territoire national, à la condition impérative de recourir aux opérateurs postaux proposant des moyens de transport protégés, tels que l'envoi en pli chargé avec valeur déclarée ou la lettre recommandée avec accusé de réception.
Cruciale, la fiabilité des opérateurs postaux chargés d'acheminer des documents classifiés dépend notamment de leur capacité à répondre aux exigences imposées par la présente instruction.
L'opérateur postal peut confier l'accomplissement d'une tâche à un sous-traitant mais la responsabilité de l'exécution lui incombe entièrement.
Seuls pourront être sollicités les opérateurs postaux :
- ayant un établissement sur le territoire national ;
- habilités ;
- disposant d'un programme de sécurité pour la prise en charge d'articles de valeur au moyen d'un service de signature comportant notamment une surveillance et un enregistrement permanents permettant d'identifier à tout moment le responsable de la garde des articles concernés soit par un registre de signature et de pointage, soit par un système électronique de suivi et d'enregistrement ;
- fournissant à l'expéditeur un justificatif de livraison sur le registre de signature et de pointage ou un reçu portant les numéros de colis ;
- garantissant que la livraison sera effectuée dans un délai maximal de 24 heures, ou avant une date et une heure données.
L'expéditeur s'assure de la date et de l'heure prévues de livraison et en avise aussitôt le service destinataire par télécopie banalisée ou par courrier électronique, en indiquant le bureau de dépôt du courrier et les références du support, à l'exclusion de leur objet et de leur caractère secret. A la réception du courrier, le bureau de protection du secret ou le destinataire en accuse réception. En cas de retard anormal, il y a suspicion de compromission et le bureau de protection du secret ou le service destinataire met en œuvre les dispositions de l'article 67.
Des contrôles (68) sont effectués auprès des opérateurs postaux en liaison avec les services spécialisés pour s'assurer que les conditions de conservation et d'acheminement des informations ou supports classifiés sont respectées.

## Article 58
## L'acheminement d'informations

ou supports classifiés vers l'étranger
Les informations ou supports classifiés envoyés à l'étranger ou transitant par des pays étrangers doivent être protégés en permanence pour interdire leur compromission pendant le transport, et notamment lors des escales.
Seuls les moyens suivants sont autorisés :
- courrier militaire spécialisé ;
- valise diplomatique et lettre de courrier ;
- certificat de courrier.
La voie postale peut être autorisée, pour les supports de niveau Confidentiel Défense, dans les conditions mentionnées à l'article 57 en ayant recours au service prioritaire "recommandé international" pour un envoi vers les pays de l'Union européenne ou de l'OTAN.
Pour les informations échangées dans le cadre d'un accord ou d'un programme international, il convient de se référer aux dispositions prévues par les réglementations applicables.
1. Courrier militaire spécialisé :
Les informations ou supports classifiés au niveau Secret Défense sont normalement acheminés par valise diplomatique ou éventuellement par courrier militaire spécialisé.

Pour les organismes militaires, le service convoyeur est le bureau de courrier de l'administration centrale (BCAC). 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 (69).

2. Valise diplomatique et lettre de courrier :

Lors de la remise des envois, au plus tard la veille du départ de la valise, à la division 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. A défaut, il y a lieu de prévoir des mesures particulières en fonction des instructions du ministère des affaires étrangères. Une "lettre de courrier" accrédite la qualité du porteur 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 ni être 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'Etat 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'Etat d'origine.

3. Certificat de courrier :

Lorsqu'un accord ou un règlement international de sécurité le prévoit, l'acheminement est possible par convoyeur autorisé, dans les conditions déterminées à l'article 57. Le convoyeur est alors muni d'un certificat de courrier pour un seul ou plusieurs voyages (70) délivré par l'ANS ou les autorités de sécurité déléguées. Il est rappelé au convoyeur qu'il s'engage, tout au long du voyage, à garder en sa possession ou sous sa surveillance directe le colis contenant les documents, équipements ou composants classifiés (71).

## Chapitre IV
## Destruction et archivage des informations

## ou supports classifiés

### Section 1
### Destruction des informations ou supports classifiés

#### Article 59
#### La procédure ordinaire

Lorsque des informations ou supports classifiés sont périmés ou devenus inutiles, il peut être procédé à leur destruction avec, pour le document original, l'accord de l'administration des archives (72). La destruction ne peut être réalisée que par des personnes habilitées.

Les supports préparatoires devenus sans objet sont détruits sans formalité particulière.

La destruction de tels documents est effectuée de façon à rendre impossible toute reconstitution même partielle des informations contenues sur les supports.

Les techniques de destruction sont adaptées au nombre et au type de supports à détruire. Les principales formes de destruction sont le brûlage, l'incinération, le broyage, le déchiquetage et la surtension électrique (73). Lorsque des documents classifiés doivent être transportés afin d'être incinérés, ils doivent impérativement avoir été préalablement déchiquetés et mélangés.

Après l'opération, un procès-verbal de destruction (74) est dressé. Les procès-verbaux de

destruction portent la signature de l'autorité détentrice et, pour les documents Secret Défense, celle d'un témoin habilité au niveau Secret Défense.
Au niveau Secret Défense, l'autorité détentrice du document informe par écrit l'autorité classificatrice que, sauf avis contraire de sa part, elle va procéder à la destruction du support. Sans réponse dans un délai de deux mois, l'autorité détentrice procède à la destruction du support et en rend compte à l'autorité classificatrice en lui adressant une copie du procès-verbal (75). Une copie de ce procès-verbal est également transmise au bureau de protection du secret.

### Article 60
### Evacuation et destruction d'urgence

Pour faire face à des circonstances exceptionnelles et en cas de menace immédiate nécessitant l'évacuation des bâtiments par le personnel ou la destruction des informations ou supports classifiés, des plans d'évacuation et de destruction d'urgence sont établis par chaque service ou organisme détenteur d'informations ou supports classifiés. Ces plans prévoient notamment les procédures d'accès, en toute circonstance, aux locaux et aux informations ou supports classifiés.
Les modalités d'exécution pratique de ces plans figurent sur des fiches disponibles en permanence, pour les personnes concernées, dans chaque service ou organisme détenteur. Elles précisent :
- la liste et la localisation des informations ou supports classifiés 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 l'ordre de destruction ou d'évacuation.
Le dispositif ainsi établi doit être contrôlé par une simulation, selon une périodicité définie par chaque ministère pour les niveaux Secret Défense et Confidentiel Défense, qui ne peut excéder trois ans.

## Section 2
## Archivage

### Article 61
### Les principes généraux de l'archivage d'informations

### ou de supports classifiés

Toute autorité détenant une information ou support classifié, produit ou reçu, a pour obligation de faire assurer sa conservation et sa protection conformément aux dispositions législatives ou réglementaires et aux règles de fonctionnement du service d'archives auquel il est rattaché.
Le code du patrimoine définit les archives comme l'ensemble des documents, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé, dans l'exercice de leur activité (76). Il institue un régime de conservation et de consultation des archives applicable à toutes les archives, publiques ou privées.

### Article 62
### Le versement des informations

ou supports classifiés aux archives

Les informations ou supports classifiés sont soumis aux dispositions générales du code du patrimoine relatives aux archives. A l'expiration de leur période d'utilisation courante, ils font l'objet d'un tri pour séparer les documents destinés à être conservés des documents dépourvus d'utilité administrative ou d'intérêt historique ou scientifique, destinés à l'élimination (77). A cette occasion, il est procédé, chaque fois que nécessaire, à la révision de leur niveau de classification.
Les dispositions suivantes s'appliquent aux documents qui, à l'expiration de leur période d'utilisation courante, restent classifiés :
1. La destruction :
La destruction d'informations ou supports classifiés s'opère dans les conditions décrites à l'article 59 de la présente instruction et conformément aux dispositions du code du patrimoine.
2. Le versement aux dépôts d'archives :
Dès qu'ils ne sont plus utilisés habituellement, les informations ou supports classifiés présentant un intérêt administratif et historique sont versés, selon la périodicité prévue par chaque ministre, aux dépôts d'archives suivants :
- le service historique de défense, pour le ministère de la défense et les services qui lui sont rattachés tant administrativement que pour la gestion des archives ;
- les archives du ministère des affaires étrangères et européennes, pour ce qui le concerne ;
- la direction générale des patrimoines de France, les archives nationales et services publics d'archives des collectivités territoriales, pour toutes les administrations et organismes civils gérant des archives publiques (par exemple la préfecture de police).
Ces services sont seuls équipés et habilités pour recevoir des informations ou supports classifiés jusqu'au niveau Secret Défense inclus. Ils ne peuvent pas accueillir d'informations ou de supports classifiés au niveau Très Secret Défense dont le versement aux archives n'est possible qu'après une procédure, obligatoire et préalable, de déclassement ou de déclassification.

Article 63
La communication au public des informations

ou supports classifiés versés aux archives

La communication au public d'informations ou de supports classifiés versés aux services d'archives relève des dispositions combinées du code pénal (78), du code du patrimoine (79), de la loi du 17 juillet 1978 précitée relative à l'amélioration des relations entre l'administration et le public (80), du décret du 3 décembre 1979 relatif aux archives de défense (81) et enfin du décret (82) du 1er décembre 1980 relatif au régime des archives du ministère des affaires étrangères.
Un document classifié versé aux archives publiques est en principe, à la condition expresse d'avoir été préalablement déclassifié, communicable de plein droit à l'expiration du délai de cinquante ans à compter de sa date d'émission ou de celle du document classifié le plus récent inclus dans le dossier. Ce délai est, en certaines circonstances, porté à soixante-quinze ans ou à cent ans (83). Un document peut être incommunicable quel que soit le délai écoulé. Ainsi ne peut en aucun cas être consultée une archive dont la communication présente le risque de diffuser des informations relatives aux armes de destruction massive (84).
Quelle que soit la durée d'incommunicabilité affectée au document classifié, sa communication n'est possible qu'après déclassification du document. Lorsque le service

détenteur des archives est saisi d'une demande de communication d'un document couvert par le secret de la défense nationale, il doit transmettre cette demande à l'autorité émettrice du document concerné. Cette autorité vérifie la durée d'incommunicabilité affectée au document. Si tous les délais applicables sont expirés, l'autorité émettrice procède à la déclassification. Le document ne peut être communiqué qu'à l'issue de cette procédure.
Une personne souhaitant consulter une archive classifiée avant l'expiration des délais de communicabilité applicables doit solliciter une dérogation (85). Le service d'archives détenteur saisi de la demande de dérogation transmet cette demande à l'autorité émettrice. Cette autorité doit toujours s'interroger sur l'opportunité de la déclassification du document. Si la classification reste justifiée, la communication est impossible et la dérogation est refusée.

## Chapitre V

## Les mentions additionnelles

## de limitation du champ de diffusion

### Article 64
### Principe général

Les informations et les supports classifiés devant faire l'objet de restrictions spécifiques de diffusion en raison de leur contenu portent, en plus de la mention éventuelle de leur niveau de classification, une mention particulière précisant les services, les Etats ou les organisations internationales pouvant y avoir accès (86). Cette mention, apposée par l'émetteur, a pour effet de circonscrire expressément le périmètre de circulation de ces informations et d'attirer l'attention sur le strict besoin d'en connaître. Les mesures de sécurité du niveau de classification qu'elles portent éventuellement sont appliquées et l'acheminement des informations ou des supports est réalisé de façon à garantir le respect du périmètre de diffusion ainsi délimité.

### Article 65
### Détermination et champ d'application "Spécial France"

La mention "Spécial France" n'est pas une mention de classification. Elle est employée pour les informations ou supports, classifiés ou non, que l'autorité émettrice estime devoir être divulgués aux seuls ressortissants français et qui ne sauraient, en aucune circonstance, être communiqués, en tout ou partie, à un Etat étranger ou à l'un de ses ressortissants, à une organisation internationale ni à une entreprise de droit étranger, même s'il existe avec cet Etat ou cette organisation un accord de sécurité. La mention "Spécial France" peut ne concerner que certaines parties d'un document.
Lorsque des informations marquées "Spécial France" sont classifiées, elles doivent, outre satisfaire aux mesures de sécurité appropriées à leur degré de protection, n'être transmises qu'à des personnes physiques ou morales françaises dûment habilitées et ayant le besoin d'en connaître.
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 44 de la présente instruction.
L'acheminement des informations ou supports classifiés est réalisé par des bureaux courriers nationaux et par des voies nationales. Si nécessaire, la mention Spécial France est indiquée sur l'enveloppe intérieure de sécurité.
Les informations "Spécial France" ne sont jamais mentionnées sur les inventaires ou répertoires prescrits par les accords de sécurité ou les règlements de sécurité.

Ces documents peuvent sortir des frontières du territoire par la valise diplomatique (87), qui constitue un circuit national protégé, garantissant la protection et le cloisonnement des informations transmises et impliquant la mise en œuvre, à tous les stades de l'acheminement, des mesures de sécurité appropriées au degré de classification éventuellement apposé. Il en est de même de la transmission par courrier militaire spécialisé ou, en cas d'urgence, de la lettre de courrier délivrée par le ministère des affaires étrangères (88).
Les règles applicables aux informations et supports matériels valent également pour les documents informatiques, qui ne peuvent être acheminés, par voie électronique, que par un canal national spécifique de transmission offrant toutes les garanties précitées de sécurité et de cloisonnement.

.....
(1) Décision du Conseil constitutionnel n° 2011-192 QPC du 10 novembre 2011.
(2) Blocages malveillants, destruction matérielle, neutralisation d'un système, vol ou altération de données, prise de contrôle d'un dispositif à des fins hostiles...
(3) Article R. 2311-2 du code de la défense.
(4) Articles 413-10 et suivants du code pénal.
(5) Au même titre que les personnes physiques, les personnes morales sont responsables pénalement des faits de compromission qui peuvent leur être imputés, en application des articles 121-2 et 414-7 du code pénal.
(6) Article R. 2311-1 du code de la défense.
(7) Articles 414-8 et 414-9 du code pénal.
(8) Articles 413-9 et suivants du code pénal.
(9) Par exemple, Confidentiel Personnel, Confidentiel Médical, Confidentiel Technologie, Confidentiel Industrie, Confidentiel Commercial, Confidentiel Concours, information non classifiée soumise à un contrôle, ou encore Spécial France (voir article 67 de la présente instruction).
(10) Article L. 4121-2 du code de la défense pour les militaires et article 26 de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.
(11) Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.
(12) Article R. 2311-7 du code de la défense.
(13) Titre IV de la présente instruction.
(14) Article R. 2311-5 du code de la défense.
(15) Article R. 2311-6 du code de la défense.
(16) Articles R. 2311-7 et R. 2311-8 du code de la défense.
(17) Article R. 2311-10 du code de la défense.
(18) Article D. 2311-12 du code de la défense.
(19) Article R. 2311-11, alinéa 2, du code de la défense.
(20) Recommandations pour la rédaction de cette instruction en annexe 2.
(21) En application de l'article R. 1143-1 du code de la défense et conformément à l'organisation spécifique de certains ministères, le ministre de la défense et le ministre des affaires étrangères sont assistés, pour leurs départements ministériels respectifs, d'un haut fonctionnaire correspondant de défense et de sécurité (HFCDS), le ministre de l'intérieur, d'un haut fonctionnaire de défense (HFD), et les autres ministres, d'un haut fonctionnaire de défense et de sécurité (HFDS). Dans la suite de l'instruction, le terme HFDS sera utilisé de façon générique.
(22) Articles R. 1143-1 et suivants du code de la défense.
(23) Article R. 1143-2 du code de la défense.

(24) Article R. 1143-8 du code de la défense.
(25) Le marquage “Spécial France” est traité à l’article 65 de la présente instruction.
(26) Article R. 1143-5 (8°) du code de la défense.
(27) Directive d’application pratique n° 02/SGDN/SSD/CD du 3 février 1986 sur l’organisation et le fonctionnement des classifications spéciales Très Secret Défense.
(28) Articles contrôlés de la sécurité des systèmes d’information, tels que définis par l’instruction interministérielle n° 910/SGDN/DISSI/SCSSI/SSD/DR du 19 décembre 1994.
(29) Article 74.
(30) Article 12 de la présente instruction.
(31) Articles 411-6 à 411-8 et 413-9 à 413-12 du code pénal.
(32) La recherche de renseignements demeure un objectif essentiel des services spéciaux étrangers. Ces derniers tentent d’exploiter tous les éléments de vulnérabilité présentés par les voyageurs. Il se peut qu’un voyageur ait été “ciblé” par les services de renseignement et de sécurité du pays de destination. Son comportement doit toujours tenir compte de ce risque potentiel. Aussi, différentes règles de prudence et de bon sens doivent être respectées au cours de tout déplacement à l’étranger. Des recommandations peuvent être faites avant le départ et utilement complétées par le passeport de conseils aux voyageurs édité par l’ANSSI énonçant les bonnes pratiques lors de missions à l’étranger avec, notamment, un téléphone mobile, un assistant personnel ou un ordinateur portable.
(33) Le recueil d’informations nominatives est subordonné à des conditions strictes, en application de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l’informatique, aux fichiers et aux libertés.
(34) Modèle 02/IGI 1300 en annexe.
(35) Direction générale de la sécurité intérieure.
(36) Direction de la protection et de la sécurité de la défense ou direction générale de la sécurité extérieure pour l’ensemble des personnels travaillant à son profit.
(37) Les dossiers des personnels militaires ou civils qui ont fait l’objet d’un avis de sécurité émis par les services enquêteurs du ministère de la défense leur restent rattachés, dans l’hypothèse d’une nouvelle enquête administrative, pendant un délai de cinq ans après la cessation de leurs fonctions.
(38) Chaque ministère peut décliner chacune de ces trois catégories pour l’adapter à ses besoins propres.
(39) Article R. 2311-8 du code de la défense.
(40) Modèle 17/IGI 1300 en annexe.
(41) Il peut s’agir par exemple de ses attaches avec l’étranger ou de diverses particularités de son environnement. Il revient aux services enquêteurs d’apprécier, pour chaque cas, ce qui peut constituer une vulnérabilité.
(42) Modèle 16/IGI 1300 en annexe.
(43) Les dispositions de l’article 1er de la loi n° 79-587 du 11 juillet 1979 modifiée relative à la motivation des actes administratifs et à l’amélioration des relations entre l’administration et le public imposent la motivation des décisions administratives défavorables. Il y est cependant fait exception notamment lorsque la consultation ou la communication de ces décisions porterait atteinte au secret de la défense nationale, par application 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 (article 6-2, b).
(44) Modèle 08/IGI 1300 en annexe.
(45) A l’exception d’une décision d’habilitation couvrant expressément plusieurs postes, conformément à l’article R. 2311-8 du code de la défense.
(46) Confidentiel Personnel.
(47) Modèle 05/IGI 1300 en annexe.
(48) Article 32 de la présente instruction.

(49) Modèle 04/IGI 1300 en annexe.
(50) Article 32 de la présente instruction et modèle 03/IGI 1300 en annexe.
(51) 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.
(52) Articles 413-9 et suivants du code pénal.
(53) Article R. 2311-5 du code de la défense et 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 reproduction totale ou partielle de ces informations ou de ces supports, qui ne peut être effectuée que par l'antenne émettrice, est formellement interdite aux détenteurs.
(54) Article 4 de la présente instruction.
(55) Ce qui signifie respectivement supprimer la classification, en baisser ou en relever le niveau. Ces opérations sont effectuées dans les mêmes formes que la classification.
(56) Voir guide de classification en annexe 2. Des guides complémentaires, correspondant aux besoins propres de chaque département, peuvent être déclinés.
(57) Par source, il est ici entendu le(s) système(s) de renseignement ayant permis de produire une information.
(58) Pages, paragraphes, annexes, appendices ou pièces jointes.
(59) Pour le marquage des paragraphes, voir article 42 de la présente instruction.
(60) Articles 2311-4 du code de la défense et 413-9 du code pénal.
(61) Clés USB, disquettes, CD, CD-ROM...
(62) Modèle 13/IGI 1300 en annexe.
(63) Voir modèle de timbre en annexe.
(64) Modèle 12/IGI 1300 en annexe.
(65) 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.
(66) 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 et instruction interministérielle n° 312/SGDN/ANS/DR du 21 août 1981 sur la sécurité nucléaire dans le domaine de la défense.
(67) Respectivement modèles 12/IGI 1300, 12 bis/IGI 1300 et 12 ter/IGI 1300 en annexe.
(68) Conformément aux dispositions du titre VI.
(69) Division de la valise diplomatique.
(70) Modèles 07/IGI 1300 (un seul voyage) et 07 bis/IGI 1300 (multivoyage) en annexe.
(71) Ce type d'acheminement ne bénéficiant pas de la protection accordée à la valise diplomatique selon la convention de Vienne du 18 avril 1961 (article 27), le colis acheminé peut être ouvert par les autorités étrangères.
(72) Article L. 212-2 du code du patrimoine.
(73) Le brûlage consiste à exposer l'ensemble du support ou la surface utile à une température de plus de 1 000 °C avec un chalumeau ; l'incinération est une combustion complète réduisant le support à l'état de cendres, destinée à empêcher toute dispersion de fragments ; le broyage consiste à réduire le support en pulpe afin que les morceaux résiduels n'excèdent pas 2 mm de diamètre ; le déchiquetage est une opération qui réduit le support en lambeaux de moins de 0,8 mm de large et 13 mm de long ; la surtension électrique consiste à détruire les circuits d'alimentation du support par une surtension positive immédiatement suivie d'une surtension négative (ce qui ne détruit toutefois pas les circuits eux-mêmes, qui contiennent l'information).
(74) Modèle 13/IGI 1300 en annexe.
(75) En cas de dissolution du service dont relevait l'autorité ayant procédé à la classification, la copie du procès-verbal de destruction est adressée au HFDS du ministère compétent.

(76) Article L. 211-1 du code du patrimoine.
(77) Article L. 212-2 du code du patrimoine.
(78) Articles 413-10 et suivants du code pénal relatifs à la compromission.
(79) Articles L. 213-1 et L. 213-3 du code du patrimoine.
(80) Loi n° 78-753 du 17 juillet 1978 précitée.
(81) Décret n° 79-1035.
(82) Décret n° 80-975.
(83) Article L. 213-2 (3°, 4° et 5°) du code du patrimoine (annexe 1).
(84) Article L. 231-2 (II) du code du patrimoine.
(85) Dérogation aux règles de communicabilité des documents d'archives, prévue à l'article L. 213-3 du code du patrimoine et décret n° 79-1035 du 3 décembre 1979 (article 7).
(86) Article R. 2311-4 du code de la défense.

(87) Article 27 de la convention de Vienne de 1961.
(88) Article 58 de la présente instruction.

· Modifié par Décret n°2014-445 du 30 avril 2014 - art. 10

## Chapitre VI

## La compromission du secret de la défense nationale

Compromettre un secret de la défense nationale consiste à le révéler, en tout ou partie, à quelqu'un qui n'a pas à en connaître. Si la compromission délibérée est rare, les compromissions par négligence du détenteur ou par accès illicite sont fréquentes. La rivalité entre les Etats et la concurrence économique entre les entreprises nourrissent la recherche active d'informations classifiées ou stratégiques et exigent que la protection des informations ou supports classifiés demeure une préoccupation essentielle de toute personne ou tout service détenteur.

### Article 66

### Domaine d'application de la compromission

L'appropriation, la livraison ou la divulgation, à des personnes non habilitées ou n'ayant pas le besoin d'en connaître, de tout élément constituant un secret de la défense nationale constituent des agissements contre les intérêts de la nation, considérés comme particulièrement dangereux. Le code pénal consacre aux atteintes au secret de la défense nationale les articles 413-9 à 413-12 (89).

Constitue le délit de compromission le fait de divulguer ou de rendre possible la divulgation d'un secret de la défense nationale, c'est-à-dire de le rendre accessible à une ou plusieurs personnes n'étant pas qualifiée(s) pour y accéder.

Toute personne dépositaire d'éléments couverts par le secret de la défense nationale en est responsable. Elle a le devoir de s'opposer à la communication de ces éléments à une personne non qualifiée pour y accéder, sous peine d'être elle-même poursuivie du chef de compromission.

Pour une information classifiée, les agissements matériels par lesquels se traduit l'atteinte au secret de la défense nationale peuvent revêtir trois formes (90) :

— un acte positif, consistant à détruire, à soustraire ou à reproduire un secret que l'on détient ;

— une attitude passive, consistant à laisser détruire, détourner, reproduire ou divulguer un secret, soit par un autre dépositaire, soit par un tiers ;

— une attitude négligente ou imprudente, consistant à méconnaître les instructions et consignes administratives et portant de ce fait atteinte à la protection d'une information classifiée en l'exposant au risque d'être dévoilée.

L'auteur de l'infraction peut être une personne qualifiée (91) ou un tiers (92). Est qualifiée la personne qui, par son état, sa profession, sa fonction ou sa mission, temporaire ou permanente, est habilitée à avoir accès à une information classifiée et a le besoin d'en connaître. Est considérée comme tiers toute personne à laquelle l'accès au secret est interdit. A la différence de la personne qualifiée, le simple tiers ne peut se voir reprocher pénalement une attitude passive ou négligente.

La protection pénale est limitée aux informations ou supports faisant l'objet d'une mesure de classification. Tant que cette classification perdure, quelle qu'en soit l'ancienneté ou la pertinence, le délit de compromission conserve sa pleine application. Une personne habilitée n'est pas déliée de ses obligations lorsque cesse son habilitation (93).

Ces dispositions sont étendues aux actes commis au préjudice (94) :

— des puissances signataires du traité de l'Atlantique Nord ;

— de l'Organisation du traité de l'Atlantique Nord.

Elles s'appliquent également aux informations échangées (95) :

— en vertu d'un accord de sécurité régulièrement approuvé et ratifié, conclu entre la France et un ou plusieurs autres Etats étrangers ou une organisation internationale ;

— entre la France et une institution ou un organe de l'Union européenne et classifiées en vertu des règlements de sécurité de ces derniers, publiés au Journal officiel de l'Union européenne.

La qualité de secret est indépendante du nombre, parfois élevé, de personnes qui en connaissent la teneur.

L'infraction de compromission est constituée même si la divulgation n'est pas réalisée mais seulement rendue possible.

La tentative de compromission est sanctionnée comme le délit consommé (96).

La compromission est un délit. La nature singulière de l'infraction engendre des particularités procédurales importantes en matière d'ouverture des poursuites, de compétence juridictionnelle et de sanction applicable.

Outre les sanctions pénales, l'auteur d'un acte, commis délibérément ou non, qui compromet un secret de la défense nationale encourt le retrait de son habilitation et des sanctions disciplinaires, ce qui peut affecter gravement le déroulement de sa carrière.

Les personnes morales sont pénalement responsables des faits de compromission qui

leur sont imputables et encourent, outre une peine d'amende, l'interdiction d'exercer l'activité dans l'exercice ou à l'occasion de laquelle l'infraction a été commise (97).

### Article 67
### Procédure à suivre en cas de compromission

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

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. Qu'il y ait une compromission avérée ou une simple suspicion, doivent être directement et dans les plus brefs délais informés :

- soit le service compétent du ministère de l'intérieur (98) chargé de centraliser les cas et de procéder à l'enquête sous le contrôle de l'autorité judiciaire ;
- soit le service compétent du ministère de la défense (99), qui avise lui-même celui du ministère de l'intérieur ;
- le HFDS du ministère intéressé qui en avise lui-même le SGDSN.

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

- directement au HFDS du ministère concerné ;
- par la voie hiérarchique du ministère concerné, à l'autorité émettrice de l'information classifiée et au SGDSN, pour les informer des conséquences éventuelles de la compromission ;
- au service enquêteur concerné, s'il n'est pas lui-même l'émetteur du procès-verbal.

Le chef de service prend immédiatement, en liaison avec l'officier de sécurité, les mesures adéquates pour prévenir la réitération de tels faits.

Le fait de ne pas signaler de tels actes, favorisant la divulgation d'une information classifiée, fait encourir des sanctions administratives ou professionnelles.

Le ministère de l'intérieur, outre l'information obligatoirement donnée au cas par cas, fournit au SGDSN un bilan annuel des cas constatés et de l'état d'avancement des procédures ou des suites réservées à chacune d'elles.

Le rapport annuel d'évaluation de la protection du secret établi annuellement par les HFDS (100) indique le nombre de cas de compromission constatés ou soupçonnés ainsi que les suites données.

Lorsque la compromission porte sur des informations classifiées étrangères, l'ANS française informe dans les plus brefs délais l'ANS étrangère. Lorsqu'une ASD est concernée, elle informe dans les plus brefs délais l'ANS étrangère ainsi que l'ANS française. Lorsque ce sont des informations de niveau Secret Défense qui sont compromises, l'ASD rend compte à l'ANS française, qui transmettra elle-même l'information à son homologue étrangère.

## Chapitre VII
## L'accès des magistrats aux informations classifiées

Le premier rôle du juge judiciaire à l'égard du secret de la défense nationale est de sanctionner les manquements constatés à sa protection. Il arrive toutefois que le juge se voie lui-même opposer ce secret, au cours de ses investigations, par l'autorité responsable d'un document classifié dont elle lui refuse la communication. En effet, ni les magistrats ni les officiers de police judiciaire n'ont qualité pour connaître les éléments que couvre ce secret.

Or, si refuser l'accès au magistrat constitue le délit d'entrave à la justice (101), le lui accorder fait encourir les sanctions pénales applicables à la compromission. Afin de

dénouer ce paradoxe, de garantir la préservation du secret de la défense nationale tout en favorisant l'action de la justice et en évitant qu'il ne soit fait obstacle au bon déroulement d'une procédure judiciaire, les conditions dans lesquelles les magistrats peuvent accéder à une information classifiée utile à la manifestation de la vérité sont clairement définies.

Article 68

Moyens d'accès des magistrats aux informations classifiées

Pour obtenir communication d'éléments classifiés intéressant la procédure qu'il diligente, le magistrat dispose de trois possibilités : la perquisition, l'audition et la réquisition.

1. La perquisition :

La perquisition aux fins de saisie d'éléments classifiés suppose, dans la grande majorité des cas, que le magistrat pénètre dans des locaux où sont conservés de tels documents. Aussi la perquisition est-elle traitée dans les dispositions encadrant l'accès aux lieux abritant des secrets de la défense nationale (102).

2. L'audition :

Aucune autorité administrative ne peut autoriser l'un de ses agents à s'exprimer au sujet d'une information classifiée à moins que celle-ci n'ait été préalablement déclassifiée. Une personne habilitée, ne pouvant être déliée de ses obligations de protection du secret, ne peut en aucun cas être entendue par une juridiction sur des éléments restant classifiés sous peine d'encourir les sanctions applicables au délit de compromission.

3. La réquisition judiciaire :

La réquisition est le moyen le plus fréquemment utilisé par les juridictions en matière d'informations classifiées. Le magistrat adresse à l'autorité administrative dont relève la classification, c'est-à-dire au ministre compétent, une réquisition aux fins de transmission des éléments utiles à la manifestation de la vérité.

Deux situations peuvent se présenter :

- soit le magistrat a identifié le ou les éléments classifiés dont il requiert la communication et il adresse directement une demande de déclassification à l'autorité classificatrice ;
- soit le magistrat souhaite se voir communiquer un certain nombre d'éléments qu'il ne peut identifier avec précision ; il requiert alors de l'administration concernée qu'elle procède elle-même à la recherche de ces éléments, les trie et communique les éléments qui ne sont pas classifiés, les éléments classifiés devant faire préalablement l'objet d'une demande de déclassification.

Article 69

Procédure de déclassification d'une information classifiée

La déclassification d'une information classifiée, sollicitée par requête, peut être décidée après avis de la Commission consultative du secret de la défense nationale.

1. Requête en déclassification d'une information :

Une juridiction française peut demander, dans le cadre d'une procédure engagée devant elle, la déclassification d'éléments protégés par le secret de la défense nationale (103). Cette demande, motivée, est adressée à l'autorité administrative qui a procédé à la classification du document, qui saisit elle-même sans délai la Commission consultative du secret de la défense nationale (CCSDN).

La CCSDN, autorité administrative indépendante (104), rend un avis destiné à éclairer l'autorité classificatrice sur l'opportunité de déclassifier et de communiquer des informations désignées par la juridiction, à l'exclusion des informations dont les règles de classification ne relèvent pas des seules autorités françaises (105). Pour les éléments classifiés par des autorités étrangères ou des organismes internationaux comme l'OTAN ou l'Union européenne, il appartient au magistrat de s'adresser à l'autorité ou à l'organisme concerné. Il peut, s'il le souhaite, s'informer des procédures auprès du SGDSN, autorité nationale de sécurité.

La motivation énoncée par le magistrat requérant permet à la commission d'une part de contrôler la validité de sa saisine en s'assurant que les éléments dont la déclassification

est demandée intéressent effectivement la procédure, d'autre part de procéder au tri des pièces classifiées soumises à son appréciation afin de déterminer celles qui peuvent être utiles à la manifestation de la vérité.
2. L'avis de la Commission consultative du secret de la défense nationale :
La commission a accès à l'ensemble des éléments classifiés. Pour l'accomplissement de sa mission, elle est habilitée à procéder, le cas échéant, à l'ouverture des scellés des éléments classifiés qui lui sont remis. Elle en fait mention dans son procès-verbal de séance (106).
La CCSDN émet un avis dans le délai de deux mois à compter de sa saisine. Cet avis prend en considération les missions de service public de la justice, le respect de la présomption d'innocence et des 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. Le sens de l'avis peut être favorable, favorable partiellement ou défavorable à la déclassification. L'avis est transmis par la CCSDN au ministre concerné en sa qualité d'autorité classificatrice (107).
3. La décision de l'autorité classificatrice :
L'avis de la commission est consultatif. Le ministre a donc toute latitude pour ordonner une déclassification malgré un avis défavorable ou pour refuser la déclassification en dépit d'un avis favorable. Dans le délai de quinze jours francs à compter de la réception de l'avis de la CCSDN (108), le ministre compétent notifie sa décision, qui n'a pas à être motivée, assortie du sens de l'avis, à la juridiction concernée. Le sens de l'avis rendu par la CCSDN est publié au Journal officiel de la République française (109).
Chaque élément déclassifié est revêtu d'une mention expresse de déclassification précisant la date de la décision du ministre. L'élément peut ensuite être versé au dossier de la procédure afin d'y être examiné par le magistrat et soumis aux parties qui pourront en débattre contradictoirement. Le versement par erreur à un dossier judiciaire d'une pièce classifiée fait encourir des sanctions pénales.

# TITRE IV
# LA PROTECTION DES LIEUX

Les règles de sécurité applicables aux lieux sont mises en œuvre pour protéger les informations ou supports classifiés contre toute menace d'origine interne ou externe qui pourrait mettre en cause leur disponibilité, leur intégrité, leur confidentialité et afin d'empêcher qu'une personne non autorisée puisse y accéder.
Les mesures de protection physique appliquées à une information dépendent de son niveau de classification.
Tout système de protection physique doit s'appuyer sur une analyse des risques.
Un dispositif de protection est satisfaisant lorsqu'il retarde suffisamment l'intrusion pour permettre la mise en œuvre des moyens d'intervention avant que les éléments couverts par le secret de la défense nationale ne soient compromis.
Les contrôles élémentaires de personnes physiques ou morales sont prévus pour l'exécution de contrats sensibles dans des lieux abritant des secrets de la défense nationale.
L'accès d'un magistrat aux lieux abritant des secrets de la défense nationale se fait dans des conditions clairement définies et impliquant l'intervention de la CCSDN.

## Chapitre Ier
## Principes de protection physique des lieux

### Article 70
### Principes généraux

La protection physique est l'ensemble des mesures de sécurité destinées à garantir l'intégrité des bâtiments et des locaux spécifiquement dédiés aux informations ou supports classifiés, ainsi que la fiabilité des meubles dans lesquels ils sont conservés, afin d'éviter

toute perte, dégradation ou compromission. Elle vise aussi à faciliter l'identification du ou des auteurs d'une éventuelle intrusion.
Le degré de sécurité physique à appliquer aux lieux pour assurer leur protection dépend du niveau de classification des documents qu'ils abritent, de leur volume et des menaces auxquelles ils sont exposés le dispositif global de protection et la solution technique retenue reposent sur les conclusions de l'évaluation des menaces et des contraintes inhérentes à l'environnement du site, ainsi que des méthodes de travail et de gestion des informations ou supports classifiés concernés (par exemple, en fonction de la circulation de ces informations ou supports dans le site et du nombre de personnes y ayant accès). Les vulnérabilités liées aux systèmes d'information doivent également être prises en compte.
Cet ensemble de mesures de protection se compose de quatre éléments combinés ou dissociés en fonction du niveau de classification :
- un ou plusieurs dispositifs de protection (les obstacles) ;
- un ou plusieurs dispositifs de détection et d'alarme ;
- des moyens d'intervention articulés sur des procédures et des consignes préétablies ;
- un ou plusieurs dispositifs de dissuasion (indications).
Ainsi, un dispositif de sécurité satisfaisant a pour objectif, en retardant l'intrusion (aucun obstacle n'étant infranchissable), de permettre la mise en œuvre des moyens d'intervention, alertés et guidés par les dispositifs de détection avant que les informations ou supports classifiés ne soient compromis.
Pour être efficace, un système de protection physique doit s'appuyer sur une analyse précise des risques et :
- être multiple, c'est-à-dire, dans une logique de défense en profondeur, comporter plusieurs dispositifs successifs, complémentaires, de nature différente, associés ou combinés à un ou plusieurs dispositifs de détection-alarme reposant eux-mêmes sur des principes différents ;
- être homogène, c'est-à-dire garantir la même efficacité en tous points, l'intrusion s'opérant toujours dans la zone de moindre résistance et la valeur d'un système équivalant à celle de son élément le plus faible ;
- être dissuasif, c'est-à-dire contribuer à réduire le risque d'une tentative d'intrusion ;
- être contrôlé, c'est-à-dire être testé fréquemment afin de vérifier qu'il est en état opérationnel ;
- être traçable, c'est-à-dire fournir tout moyen pouvant apporter un historique du fonctionnement des différents composants.
Afin d'éviter l'intrusion, à l'intérieur d'un site ou d'un local protégé, d'une personne non autorisée qui représente toujours une menace pour les informations ou supports classifiés détenus, la protection physique comprend nécessairement un système de contrôle d'accès (110).
Le contrôle d'accès constitue un moyen matériel de s'assurer qu'une personne qui demande à pénétrer dans un lieu ou à accéder à une information a le droit de le faire. Il a donc pour objectif :
- de filtrer les flux de circulation, les individus et les véhicules qui souhaitent entrer ou sortir d'un site, d'un bâtiment ou d'un local ;
- de contrôler les individus et les véhicules dans les zones protégées ;
- d'empêcher ou de limiter les déplacements de personnes non autorisées.
Le contrôle d'accès comprend des mécanismes de différents niveaux :
- l'autorisation d'accès ;
- l'identification et/ou l'authentification de la personne ;
- la traçabilité, afin d'identifier a posteriori celui qui est entré ou sorti.
La sécurisation physique des accès d'énergie, des locaux techniques et des moyens de communication participe également de la protection physique des informations ou

supports classifiés.

Article 71
Les modalités matérielles de protection

Les types de mesures de protection physique, leur articulation selon le type de barrière et les mesures spécifiques aux niveaux supérieurs de classification sont détaillés en annexes 5 à 7.
Le système de protection physique de toute information ou support classifié est constitué de plusieurs “barrières” cohérentes, inclusives et successives :
- l’emprise du bâtiment et/ou le bâtiment lui-même ;
- le local qui contient le meuble ;
- le meuble dans lequel est conservé l’information ou le support classifié.
Le degré de protection de l’ensemble du dispositif est fonction du niveau de protection assuré par les mesures appliquées à chacune de ces “barrières”. Pour définir un seuil minimal de protection physique, il est donc nécessaire de classer chacune des barrières en fonction du degré de résistance qu’elle oppose aux tentatives d’intrusion. Ces classes sont détaillées à l’annexe 6. Les classes de protection physique fixées dans cette annexe, selon les niveaux de classification des supports à protéger, sont des seuils minimaux à respecter impérativement.
La classe minimale du meuble à utiliser pour assurer la conservation des informations ou supports classifiés est définie en fonction de la classe des autres barrières conformément aux tableaux de l’annexe 6.
Sur un territoire étranger et compte tenu de leur environnement particulier, les organismes détenteurs d’informations ou de supports classifiés doivent, hors le cas d’opérations extérieures, appliquer les mesures de protection décrites dans la présente instruction.
Par ailleurs et compte tenu de leur environnement particulier, les locaux dans lesquels sont conservés les informations ou les supports classifiés peuvent faire l’objet de dispositions de sécurité complémentaires, ces mesures devant procéder d’une analyse précise des risques effectuée par le responsable du site concerné.
Les règles de protection d’une organisation internationale pourront être retenues dans une représentation française située physiquement au sein d’une entité relevant de cette organisation ou appliquant, en vertu d’accords de sécurité en vigueur, des mesures cohérentes avec lesdites règles.
Lorsque les circonstances imposent la détention d’informations classifiées mais ne permettent pas la mise en place des moyens adéquats de protection physique, des mesures compensatoires sont prises afin de conserver le même niveau de protection. Ces mesures de substitution doivent procéder d’une analyse précise des risques, effectuée par le responsable du site concerné, et être validées par le service enquêteur compétent. Le niveau de protection doit en toute hypothèse être suffisant pour permettre la prise en compte du délai réel d’intervention avant l’intrusion.

Article 72
Consultation des services enquêteurs

pour la protection physique des documents Secret Défense
Le traitement et la conservation, dans des locaux, d’informations ou de supports classifiés de niveau Secret Défense et plus ne peut intervenir, sauf en cas d’impossibilité majeure, qu’après avis des services enquêteurs quant à l’aptitude de ces locaux à accueillir de tels documents.
En raison de la diversité des dispositifs de protection disponibles sur le marché et de l’évolution constante des techniques utilisées, les autorités concernées peuvent, en cas de besoin, consulter les services enquêteurs compétents des ministères de la défense et de

l'intérieur sur l'efficacité des matériels et des systèmes de protection qu'ils désirent installer ou afin de vérifier la validité des matériels et systèmes en place.
Les services enquêteurs s'assurent notamment que l'analyse de risques et les mesures de protection physique, qu'elles soient réglementaires ou compensatoires, prennent en compte le délai réel écoulé entre la détection de l'intrusion, la résistance des moyens mécaniques et la possibilité d'une intervention.

## Chapitre II

## Les zones protégées

### Article 73
### Définition

L'objet de la zone protégée est d'assurer aux lieux intéressant la défense nationale, qu'il s'agisse de services, d'établissements ou d'entreprises, publiques ou privées, une protection juridique contre les intrusions, complémentaire de la protection physique évoquée précédemment. Elles sont érigées en fonction du besoin de protection déterminé par le ministre compétent.
La zone protégée est définie à l'article 413-7 du code pénal. Elle consiste en tout local ou terrain clos délimité, où la libre circulation est interdite et l'accès soumis à autorisation afin de protéger les installations, les matériels, le secret des recherches, des études ou des fabrications ou les informations ou supports classifiés qui s'y trouvent. Les limites sont visibles et ne peuvent être franchies par inadvertance.
Les modalités de création de la zone protégée sont définies aux articles R. 413-1 à R. 413-5 du code pénal.
Des mesures d'interdiction d'accès sont prises par l'autorité responsable. L'ensemble des accès doit être contrôlé en permanence afin que toute pénétration à l'intérieur d'une zone protégée ne puisse être exécutée par ignorance. A cet effet, des pancartes sont disposées en nombre suffisant aux endroits appropriés.
L'autorisation de pénétrer dans une zone est donnée par le chef du service, de l'établissement ou de l'entreprise, selon les directives et sous le contrôle de l'autorité ayant décidé de la création de la zone protégée.
En vertu des dispositions pénales précitées, toute personne non autorisée s'introduisant dans une zone protégée encourt une peine correctionnelle.

## Chapitre III

## Les zones réservées

### Article 74
### Création des zones réservées

L'institution de zones réservées a pour but d'apporter une protection renforcée aux informations et supports ainsi qu'aux systèmes d'information classifiés au niveau Secret Défense.
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 classifiés au niveau Secret Défense. La création de zones réservées, le cas échéant temporaires, est par ailleurs recommandée dans les services ou les organismes traitant occasionnellement d'informations ou supports 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.
Les mesures de sécurité applicables aux zones réservées sont définies à l'annexe 7.

## Chapitre IV

## Lieux abritant temporairement des secrets : la protection

## des réunions de travail et des salles de conférences

### Article 75
### La préparation et l'organisation des réunions de travail

### et des conférences

L'autorité organisatrice doit veiller à la protection des informations ou supports classifiés 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 au cours de laquelle sont traités des informations ou supports classifiés doit :

- 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 protégée temporaire).

Le contrôle technique des lieux est effectué de manière régulière par le service chargé de la sécurité.

L'autorité organisatrice précise, lors des invitations ou convocations à une réunion de travail, à une conférence, à un exercice ou à une présentation de matériel, le niveau de classification des informations ou supports classifiés qui seront communiqués, pour permettre la désignation de personnes habilitées au niveau requis et ayant besoin d'en connaître. Les limites et le degré de précision à apporter à la communication, au cours de conférences ou de présentations de matériels, doivent être déterminés au préalable par le responsable.

Les autorités destinataires de l'invitation adressent en temps utile à l'autorité organisatrice les noms et fonctions des personnes chargées de les représenter ainsi que leur niveau d'habilitation. L'autorité organisatrice établit alors 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.

### Article 76
### La protection des informations ou supports classifiés

### au cours des réunions de travail et des conférences

L'autorité organisatrice s'assure de l'identité et du niveau d'habilitation de chacun des participants présents au vu, si besoin est, de certificats de sécurité (111). Elle s'assure que personne ne détienne, lors de la réunion, d'appareil permettant la captation, la réémission et l'enregistrement d'informations tels que, par exemple, un téléphone mobile, un assistant personnel (PDA) ou un ordinateur portable.

L'autorité organisatrice peut interdire toute prise de note ou tout enregistrement des interventions par les auditeurs. Elle 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.

Dans certains établissements affectés aux besoins de la défense et de la sécurité nationales, des installations radioélectriques de brouillage peuvent être utilisées aux fins de rendre inopérants, tant pour l'émission que pour la réception, les appareils de communications électroniques de tous types (téléphones mobiles et ordinateurs portables

par exemple) (112).

### Article 77
### Les mesures de sécurité à l'issue d'une réunion de travail

### ou d'une conférence

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 mention de la justification de leur habilitation.
L'autorité organisatrice de la réunion fait procéder en fin de séance :
- à la récupération et à la mise en sécurité des informations ou supports classifiés éventuellement mis à la disposition des auditeurs (documents, graphiques, plans, films, bandes d'enregistrement, etc.) ;
- à la destruction des supports provisoires et préparatoires.
Les auditeurs et les participants 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 documents sont détruits par leurs soins dès qu'ils ont cessé d'être utiles.
La transmission des notes prises par les participants ou de leurs comptes rendus de réunion s'effectue par les voies prévues aux articles 57 et 58 de la présente instruction.
Une liste de contrôle des tâches à effectuer tout au long de la préparation, de la tenue et de la fin de la réunion figure à l'annexe 8.

## Chapitre V
## L'accès des personnes non qualifiées

### aux lieux abritant des secrets de la défense nationale

La nécessité d'exécuter une prestation de service, qu'il s'agisse d'un contrat sensible ou de l'obligation d'intervenir en urgence, ou une mission de contrôle peut rendre indispensable l'accès de personnes non qualifiées à des lieux abritant des éléments couverts par le secret de la défense nationale.

### Article 78
### Accès de personnes non qualifiées

### aux lieux abritant des secrets de la défense nationale

1. L'expression "contrat sensible" recouvre tout contrat ou marché, quels que soient son régime juridique ou sa dénomination, à l'exception des contrats de travail, dont l'exécution s'exerce au profit d'un service ou dans un lieu abritant des informations ou supports classifiés dans lequel un cocontractant de l'administration, public ou privé, prend des mesures de précaution, y compris dans les contrats de travail de ses employés, tendant à assurer que les conditions d'exécution de la prestation ne mettent pas en cause la sûreté ou les intérêts essentiels de l'Etat.
Un contrôle élémentaire de la personne morale peut être sollicité par l'autorité contractante, sur la base des éléments fournis dans le cadre du marché. Ce contrôle élémentaire est conclu par un avis. Un avis avec réserve peut conduire l'autorité contractante à écarter la candidature de l'entreprise concernée. L'avis émis par le service enquêteur est consigné sur une fiche navette (113) qui est adressée à l'autorité contractante ou au pouvoir adjudicateur.
Les contrats sensibles comportent une clause de protection du secret conforme à la

clause type figurant à l'annexe 10. L'autorité contractante peut compléter ou adapter la clause type selon les spécificités dudit contrat, sans toutefois être contraire à cette clause. Elle peut prescrire cette clause type, ainsi complétée ou adaptée, dans les contrats sensibles de sous-traitance.
2. Dans le cas d'un contrat sensible portant sur le convoyage d'informations ou supports classifiés, sur le gardiennage de lieux abritant des éléments couverts par le secret de défense nationale, quels qu'ils soient, ainsi que sur l'entretien ou la maintenance dans de telles zones, ont seules le droit d'exécuter ce contrat les personnes appartenant à l'entreprise concernée qui ont fait l'objet au préalable d'un contrôle élémentaire défini à l'article 32.
3. Les contrats de travail des personnes exécutant un contrat sensible comportent une clause de protection du secret présentée en annexe 9. Lorsqu'un salarié exécutant un contrat de travail ordinaire se trouve soumis aux conditions applicables aux contrats sensibles, un avenant conforme aux présentes dispositions est introduit dans son contrat de travail.
Les parties au contrat de travail peuvent compléter ou adapter la clause mentionnée précédemment selon les spécificités dudit contrat sensible sans jamais lui être contraires.
4. Les personnels d'intervention en matière de secours, de sécurité ou d'incendie, agissant dans des cas d'urgence avérée, sont autorisés à procéder aux opérations requises par la situation sans être soumis aux formalités ordinaires. Si, dans des circonstances exceptionnelles, l'une de ces personnes accède fortuitement à un secret de la défense nationale, elle s'expose, en cas de divulgation, aux peines prévues à l'article 413-11 du code pénal.

## Article 79
## Accès des personnes non qualifiées

### en raison d'une mission de contrôle

Certaines personnes, en leur qualité particulière et pour l'exercice d'attributions conférées par la loi, peuvent avoir à pénétrer dans les zones abritant des secrets sans pour autant avoir la qualité ni la nécessité d'accéder à ces secrets. Tel est le cas notamment des personnes chargées de visites ou de contrôles dans le cadre de la législation du travail ou encore d'inspections internationales effectuées en application d'une convention (114).
Ces personnes doivent être autorisées par l'autorité responsable du site à pénétrer dans les zones dans lesquelles sont traités des informations ou des supports classifiés et font préalablement l'objet d'une vérification d'identité et d'un contrôle de leur qualité.
En matière de législation sociale, les entreprises liées par un contrat tel que défini au titre VI de la présente instruction (115) doivent s'efforcer de concilier l'impératif de protection du secret de la défense nationale avec la nécessité d'appliquer les règles propres au droit du travail (116).
En principe, aucune entreprise ne doit faire obstacle aux missions d'inspection, d'enquête ou de contrôle menées par les médecins inspecteurs du travail, inspecteurs, contrôleurs, ingénieurs de prévention et fonctionnaires assimilés qui disposent, pour l'exercice de leurs attributions (117), du droit d'entrée dans tout établissement où travaillent des salariés (118), de la possibilité d'effectuer tout prélèvement aux fins d'analyse (119) et de se faire présenter tous livres, registres et documents utiles à l'accomplissement de leur mission (120). Cependant, lorsque l'entreprise détient des éléments couverts par le secret de la défense nationale et conformément aux dispositions précédentes, seule l'autorité responsable du site peut les autoriser à pénétrer dans les zones où sont traités des informations ou des supports classifiés, et ce après contrôle de la qualité et vérification de l'identité de ces fonctionnaires (121).
Cependant, bien que ces personnels s'engagent à ne rien révéler des secrets de fabrication ou procédés d'exploitation qui pourraient leur être révélés à cette occasion

(122), sous peine d'encourir des poursuites sur le fondement de la violation du secret professionnel (123), ils ne sont nullement autorisés, sauf à être dûment habilités et à justifier du besoin d'en connaître pour le bon accomplissement de leur mission, à accéder ou à prendre connaissance d'informations ou supports classifiés, cet accès restant subordonné au respect des règles énoncées par la présente instruction.
De manière générale, les règles de protection du secret de la défense nationale s'appliquent à toute inspection ou à tout contrôle prévu par des dispositions législatives ou réglementaires.
Si, dans des circonstances exceptionnelles, l'un de ces intervenants accède à un secret de la défense nationale, il est tenu de ne pas le divulguer, sous peine de s'exposer aux dispositions de l'article 413-11 du code pénal. A cet effet, toutes ces personnes sont dûment informées de leurs obligations par leur autorité d'emploi.

## Chapitre VI
## L'accès des magistrats aux lieux abritant des éléments couverts par le secret de la défense nationale

### Article 80
### Magistrat et protection du secret de la défense nationale

Conciliant les deux impératifs que constituent la recherche des auteurs d'infractions pénales et la protection du secret de la défense nationale, la création de lieux bénéficiant d'une protection particulière est assortie de dispositions prévoyant clairement la procédure par laquelle un magistrat peut y pénétrer en toute légalité (124). Ces dispositions, applicables aux lieux abritant des secrets sont édictées à peine de nullité de la procédure judiciaire (125).
Dans le but de faire connaître ces dispositions, l'autorité responsable du site ou l'autorité déléguée élabore, à l'intention des personnels affectés au site, des consignes concernant la conduite à tenir en cas de perquisition. Ces consignes se réfèrent à une instruction ou une circulaire ministérielle et visent à faciliter le déroulement de l'opération.

### Article 81
### Accès d'un magistrat aux lieux abritant des secrets de la défense nationale

1. Consultation de la liste délimitant les lieux abritant des secrets de la défense nationale.
La liste des lieux abritant des éléments couverts par le secret de la défense nationale est établie par arrêté du Premier ministre mais n'est pas publiée. Elle précise, pour chaque lieu, l'organisme concerné, les pièces clairement déterminées, et l'implantation du site où sont conservés les informations ou supports classifiés. Les HFDS sont tenus de mettre à jour régulièrement la liste relevant de leur ministère.
La liste est transmise à la Commission consultative du secret de la défense nationale (CCSDN) et au ministre de la justice. Ce dernier organise un accès sécurisé à cette liste permettant à chaque magistrat qui envisage une perquisition de vérifier si le lieu concerné y figure (126).
2. Procédure d'accès.
Un magistrat peut, lorsqu'il estime cet acte nécessaire au bon déroulement de la procédure qu'il instruit, effectuer une perquisition dans un lieu précisément identifié comme abritant des éléments classifiés, à la seule condition d'être accompagné du président de la Commission consultative du secret de la défense nationale (CCSDN), de son représentant membre de la Commission ou d'un délégué, dûment habilité (127).
Le magistrat qui entend procéder à une telle opération doit préalablement transmettre par écrit au président de la CCSDN, les informations utiles à l'accomplissement de sa mission.
Le président (ou son délégué) se transporte sur les lieux sans délai. Dès le début de la perquisition, le magistrat informe le président de la CCSDN ainsi que le chef

d'établissement, son délégué ou le responsable du site de la nature de l'infraction sur laquelle portent ses investigations, des raisons justifiant l'opération, de son objet et des lieux visés.
Seul le président de la CCSDN ou son représentant (membre de la commission ou délégué), assisté de toute personne habilitée à cet effet, pourra, sans risque de compromission, prendre connaissance des documents classifiés et, en fonction de l'objet de la recherche du magistrat, trier les éléments classifiés et sélectionner ceux qui peuvent être utiles à la justice.
Le magistrat ne peut saisir, parmi les éléments classifiés, que les documents relatifs aux infractions sur lesquelles portent ses investigations. Si les nécessités de l'enquête justifient que les originaux des éléments classifiés soient saisis, des copies sont laissées à leur détenteur.
Chaque document classifié saisi est, après inventaire par le président de la CCSDN, placé sous scellé. Les scellés sont remis au président de la Commission qui en devient gardien.
Un procès-verbal relatant les opérations effectuées et procédant à l'inventaire des documents classifiés saisis est dressé mais il n'est pas joint au dossier de la procédure. Il est remis au président de la Commission.
La déclassification des documents concernés est ensuite traitée selon la procédure décrite à l'article 69 (128).

### Article 82
### Les cas particuliers

1. Dissimulation délictueuse.
Le fait de dissimuler, dans des lieux identifiés comme abritant des secrets de la défense nationale, des procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers non classifiés, en tentant de les faire indûment bénéficier de la protection attachée au secret de la défense nationale (129), expose son auteur aux sanctions réprimant le délit d'entrave à la justice (130).
2. Découverte incidente d'un élément classifié.
Lorsqu'à l'occasion d'une perquisition dans un lieu non identifié comme abritant des secrets de la défense nationale, un ou plusieurs éléments classifiés sont incidemment découverts, le magistrat, présent sur les lieux ou immédiatement avisé par l'officier de police judiciaire, en informe le président de la CCSDN. Les éléments classifiés sont placés sous scellés sans qu'il soit pris connaissance de leur contenu, par le magistrat ou l'officier de police judiciaire qui les a découverts, puis sont remis ou transmis, conformément aux règles protégeant le secret de la défense nationale, au président de la CCSDN afin qu'il en assure la garde (131). Le procès-verbal relatant les opérations relatives à ces éléments classifiés n'est pas joint au dossier de la procédure judiciaire mais remis au président de la CCSDN.
La déclassification et la communication des éléments ainsi placés sous scellés relèvent de la procédure ordinaire précédemment décrite. La CCSDN transmet les scellés, avec son avis, à l'autorité émettrice.

## TITRE V
## MESURES DE SÉCURITÉ RELATIVES AUX SYSTÈMES D'INFORMATION

Pour les systèmes d'information traitant d'informations classifiées s'appliquent les règles de la présente instruction et des instructions spécifiques d'application émises par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ;
La SSI concerne tous les acteurs ayant une responsabilité dans la mise en œuvre de ces principes et mesures : les services informatiques pour la sécurité logique et les autres aspects de la sécurité informatique, les directions métiers pour les droits d'accès aux informations, et les responsables de la sécurité physique des locaux ;
La chaîne fonctionnelle de sécurité des systèmes d'information, placée sous l'autorité du

HFDS dans les ministères, ou d'une structure de sécurité équivalente dans les organismes ne relevant pas d'un département ministériel, est chargée de prescrire, d'appliquer pour ce qui la concerne, et de contrôler les mesures de sécurité nécessaires ; ces dernières doivent viser la disponibilité, la confidentialité et l'intégrité, en restant proportionnées aux enjeux des informations et des systèmes concernés ;
L'homologation est l'acte formel par lequel l'autorité responsable certifie, après évaluation des risques, que la protection des informations et du système est assurée au niveau requis.

Article 83

Champ d'application

Le présent titre précise les mesures à appliquer pour protéger les informations classifiées dans les systèmes informatisés de traitement de l'information.
Ces mesures s'appliquent à tout système d'information ayant vocation à traiter des informations classifiées, qu'il soit placé sous la responsabilité d'un département ministériel (administration centrale ou service déconcentré), d'un organisme ou d'un établissement qui en relève, d'un organisme public ou privé ayant passé un contrat concernant la défense ou la sécurité nationale, ou plus généralement de toute personne publique ou privée qui traite de telles informations.
Des instructions et des directives techniques complètent en tant que de besoin les mesures générales exposées dans la présente instruction.

Chapitre Ier

L'organisation des responsabilités

relatives aux systèmes d'information

Article 84

Les instances interministérielles chargées de la sécurité

des systèmes d'information

1. Le Secrétariat général de la défense

et de la sécurité nationale (SGDSN)

Le SGDSN propose et met en œuvre la politique du Gouvernement en matière de sécurité des systèmes d'information (132), notamment pour les systèmes traitant d'informations relevant dusystème d'information secret de la défense nationale. Il s'assure que le Président de la République et le Gouvernement disposent des moyens de communication électronique nécessaires en matière de défense et de sécurité nationale. Il est à ce titre également chargé de garantir la sécurité de ces moyens de communication. Il dispose à cette fin d'un service à compétence nationale, l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

2. L'Agence nationale de la sécurité

des systèmes d'information (ANSSI)
L'ANSSI est l'autorité nationale en matière de défense et de sécurité des systèmes d'information (133). Elle assiste le Secrétaire général de la défense et de la sécurité nationale dans l'exercice de ses attributions dans le domaine de la sécurité des systèmes

d’information.

3. Le comité stratégique de la sécurité

des systèmes d’information

Ce comité propose au Premier ministre les orientations stratégiques en matière de sécurité des systèmes d’information et suit leur mise en œuvre (134).
Il est présidé par le Secrétaire général de la défense et de la sécurité nationale. Son secrétariat est assuré par l’ANSSI.

## Article 85
## Les départements ministériels

Chaque ministre est responsable, dans le département et les organismes dont il a la charge, de la sécurité des systèmes d’information. Il met en place un réseau de responsabilités, dénommé “chaîne fonctionnelle” de la sécurité des systèmes d’information, chargé d’appliquer la réglementation, de mettre en œuvre les mesures et d’en contrôler l’application.
L’organisation de cette chaîne de responsabilités, décrite dans le présent chapitre, peut être adaptée dans chaque département ministériel en fonction de contraintes particulières.
En matière de sécurité des systèmes d’information, le HFDS, sous la responsabilité du ministre, anime la politique de sécurité des systèmes d’information et en contrôle l’application (135). En particulier, il veille au déploiement, dans son ministère, des moyens sécurisés gouvernementaux de communication électronique. Il désigne un fonctionnaire de sécurité des systèmes d’information (FSSI) pour l’assister dans ce domaine.
Le HFDS est plus particulièrement chargé :
- de diffuser les instructions interministérielles relatives à la sécurité des systèmes d’information à l’ensemble des personnels concernés et d’en préciser les modalités d’application ;
- d’élaborer les instructions particulières pour son ministère, en définissant, pour chaque type de système d’information, les mesures de protection nécessaires ;
- de contrôler l’application de ces instructions et l’efficacité des mesures prescrites ;
- de recenser les besoins de protection des systèmes d’information et de veiller à ce qu’ils soient satisfaits ;
- de prescrire les inspections et les contrôles nécessaires pour vérifier l’application effective des instructions et des directives traitant de la sécurité des systèmes d’information ;
- d’organiser la sensibilisation des personnels, et particulièrement des autorités qualifiées et agents de sécurité des systèmes d’information, et de contrôler la formation des personnels.

## Article 86
## Autorités qualifiées et agents de sécurité

### 1. L’autorité qualifiée en sécurité

des systèmes d’information (AQSSI)

Les autorités qualifiées sont responsables de la sécurité des systèmes d’information au niveau d’un service, d’une direction d’un ministère, au niveau d’un organisme ou d’un établissement relevant d’un ministère.
Les autorités qualifiées sont désignées par le ministre pour le département et les organismes dont il a la charge. Leur responsabilité ne peut être déléguée.

En liaison avec le HFDS et le FSSI du département ministériel dont elle relève, l'autorité qualifiée est notamment chargée :
- de définir, à partir des objectifs de sécurité qu'il fixe, ou, pour les systèmes traitant d'informations classifiées, des objectifs de sécurité fixés par la présente instruction, une politique de sécurité des systèmes d'information adaptée à son service, sa direction, son établissement ou son organisme ;
- de s'assurer que les dispositions réglementaires et, le cas échéant, contractuelles sur la sécurité des systèmes d'information sont appliquées ;
- de faire appliquer les consignes et les directives internes ;
- de s'assurer que des contrôles internes de sécurité sont régulièrement effectués ;
- d'organiser la sensibilisation la formation du personnel aux questions de sécurité, en particulier en matière de systèmes d'information ;
- de s'assurer de la mise en œuvre des procédures réglementaires prescrites pour l'homologation des systèmes, pour l'agrément des dispositifs de sécurité et pour la gestion des articles contrôlés de la sécurité des systèmes d'information (ACSSI) (136) ;
- de désigner les autorités d'homologation des systèmes relevant de sa responsabilité.
Dans le cas d'un organisme qui ne relève pas d'un ministre, notamment un organisme privé, il appartient au responsable de cet organisme de désigner, en son sein, une personne ayant la fonction d'autorité qualifiée au sens du présent article.

2. L'agent, le responsable ou l'officier de sécurité

des systèmes d'information (ASSI, RSSI, OSSI)

Les autorités qualifiées peuvent se faire assister par un ou plusieurs agents, responsables ou officiers de sécurité des systèmes d'information (ASSI, RSSI, OSSI) (137). Elles précisent, lors de leur désignation, le périmètre de leurs attributions et leur dépendance hiérarchique. Ce périmètre peut être un service, une direction ou un organisme, dans sa totalité, un ou plusieurs systèmes d'information, ou un établissement.
Ces agents assurent principalement les fonctions opérationnelles de la sécurité des systèmes d'information. Ils peuvent être notamment chargés :
- d'être les contacts privilégiés des utilisateurs du système pour les questions de sécurité ;
- d'assurer la formation et la sensibilisation des responsables, des informaticiens et des usagers en matière de sécurité des systèmes d'information ;
- de tenir à jour la liste des personnels ayant accès aux systèmes d'information ;
- de faire surveiller en permanence les activités des personnes extérieures appelées à effectuer des interventions sur les systèmes d'information ;
- de s'assurer de l'application, par les personnels d'exploitation et les utilisateurs, des règles de sécurité prescrites ;
- d'assurer leur sensibilisation aux mesures de sécurité et de les informer de toutes modification des conditions d'emploi du système ;
- de veiller à la mise en œuvre des mesures de protection prescrites, d'établir des consignes particulières et de contrôler leur application ;
- d'assurer la gestion, la comptabilité et le suivi des ACSSI dans leur périmètre de responsabilité, et d'en assurer périodiquement l'inventaire ;
- d'établir les consignes de sécurité relatives à la conservation, au stockage et à la destruction des ACSSI ;
- de vérifier périodiquement l'installation et le bon fonctionnement des dispositifs de sécurité ;
- de veiller au respect des procédures opérationnelles de sécurité propres au système d'information ;
- de surveiller les opérations de maintenance ;

- de rendre compte de toute anomalie constatée ou de tout incident de sécurité.

Article 87

L'administrateur de la sécurité d'un système

Pour chaque système d'information traitant d'informations classifiées, l'autorité responsable de l'emploi du système désigne un administrateur de la sécurité pour mettre en œuvre les mesures opérationnelles de sécurité. A cet effet, l'administrateur est notamment chargé, en liaison avec l'ASSI concerné :
- de l'installation des logiciels correctifs de sécurité et des logiciels de protection ;
- de la gestion des moyens d'accès et d'authentification du système ;
- de la gestion des comptes et des droits d'accès des utilisateurs ;
- de l'exploitation des alertes de sécurité et des journaux de sécurité.

L'administrateur rend compte à l'ASSI de toute vulnérabilité du système qu'il détecte, de tout incident de sécurité et de toute difficulté dans l'application des mesures de sécurité. L'administrateur de la sécurité administrateur de sécurité doit dans la mesure du possible être distinct de l'administrateur du système. Il doit être habilité au niveau de classification des informations traitées par le système et au minimum au niveau Secret Défense.

Chapitre II

La protection des systèmes d'information

Article 88

Principes généraux de protection

des systèmes d'information

L'objectif général de la protection d'un système d'information est de garantir l'intégrité, l'authenticité, la confidentialité et la disponibilité des informations traitées par ce système. La protection d'un système d'information s'appuie sur des principes portant sur l'organisation et sur les moyens techniques, auxquels s'ajoutent des principes de défense en profondeur. Ces principes doivent être respectés strictement dès lors que le système est susceptible de traiter des informations classifiées.

1. Principes relatifs à l'organisation

Ces principes comprennent :
- la prise en compte de la sécurité : la sécurité du système d'information doit être prise en compte dans toutes les phases de la vie du système, sous le contrôle de l'autorité d'homologation, notamment lors des études de conception et de spécification du système, tout au long de son exploitation et lors de son retrait du service ;
- la politique de sécurité du système d'information : une politique de sécurité définissant les principes et les exigences, techniques et organisationnels, de sécurité du système doit être établie et approuvée par l'autorité d'homologation. Cette politique s'appuie sur une gestion des risques prenant en compte les menaces pesant sur le système et sur les informations, et les vulnérabilités identifiées sur le système ;
- l'homologation du système : tout système doit être homologué (138) par une autorité désignée conformément à l'article 90 avant sa mise en service opérationnel ;
- l'organisation de la chaîne des responsabilités : il convient d'identifier clairement les personnes qui ont des responsabilités dans la sécurité du système d'information, de les habiliter au niveau requis et de veiller à les informer des menaces pesant sur le système et sur les informations ;
- le contrôle de la sécurité du système en phase d'exploitation : la mise en œuvre des mesures de sécurité et le respect des conditions dont est assortie l'homologation sont contrôlés tout au long de l'exploitation du système d'information notamment en conduisant régulièrement des audits de sécurité ;

- la gestion des incidents de sécurité : des procédures de détection et de traitement des incidents de sécurité susceptibles d'affecter la sécurité du système d'information doivent être mises en place. Il est rendu compte à l'autorité d'homologation des incidents rencontrés et des moyens mis en œuvre pour leur traitement. L'ANSSI est tenue informée des incidents et de leurs caractéristiques techniques affectant les systèmes d'information traitant d'informations classifiées.

2. Principes relatifs aux moyens techniques

Ces principes comprennent :

- la protection technique du système : le système d'information doit être conçu de manière à protéger l'information qu'il traite et à garantir son intégrité, sa disponibilité et la confidentialité des informations sensibles relatives à sa conception et à son paramétrage de sécurité ;
- la gestion des composants sensibles du système : une gestion des ACSSI et des autres composants sensibles du système d'information doit être mise en place, permettant d'en assurer la traçabilité tout au long de leur cycle de vie, conformément à l'article 91 ;
- la protection physique du système : les mesures de protection physique d'un système d'information doivent être appliquées ;
- la gestion et le contrôle des accès au système : le système d'information doit être conçu et géré de manière à ne permettre son accès (139) qu'aux seules personnes ayant le niveau d'habilitation requis et le besoin d'en connaître ;
- l'agrément des dispositifs de sécurité : des dispositifs de sécurité agréés par l'ANSSI conformément à l'article 89 du présent chapitre doivent être utilisés (140).

3. Principes de défense en profondeur

La protection d'un système d'information nécessite d'exploiter tout un ensemble de techniques de sécurité, afin de réduire les risques lorsqu'un composant particulier de sécurité est compromis ou défaillant. Cette défense en profondeur se décline en cinq axes majeurs :

- prévenir : éviter la présence ou l'apparition de failles de sécurité ;
- bloquer : empêcher les attaques de parvenir jusqu'aux composants de sécurité du système ;
- contenir : limiter les conséquences de la compromission d'un composant de sécurité du système ;
- détecter : pouvoir identifier, en vue d'y réagir, les incidents et les compromissions survenant sur le système d'information ;
- réparer : disposer de moyens pour remettre le système en fonctionnement et en conditions de sécurité à la suite d'un incident ou d'une compromission.

Article 89

Agrément des dispositifs de sécurité

Les dispositifs de sécurité sont des moyens matériels ou logiciels destinés à protéger les informations traitées par le système ou à protéger le système lui-même. Ces dispositifs peuvent être développés pour un usage général ou spécifiquement pour un système particulier.

Ces dispositifs mettent en œuvre différents types de fonctions et de mécanismes de sécurité, notamment :

- des fonctions de cryptologie, chiffrant les informations stockées ou transmises sur des réseaux et assurant la signature, l'authentification ou la gestion de clés cryptographiques ;
- des fonctions de contrôle d'accès aux informations, comme l'authentification, le filtrage, le cloisonnement logique entre niveaux de sécurité ou le marquage des informations ;
- des fonctions ou des mécanismes destinés à protéger le dispositif lui-même, comme l'enregistrement et l'imputabilité des accès au dispositif, à empêcher ou à détecter les

intrusions physiques ou logiques non autorisées, à garantir la protection, ou l'effacement le cas échéant, des données sensibles stockées, et plus généralement toute fonction ou tout mécanisme destiné à garantir l'intégrité et la disponibilité du dispositif ;
- des fonctions d'administration et de gestion sécurisée du dispositif ;
- des fonctions protégeant la transmission d'un signal radio, notamment contre le brouillage ;
- des fonctions ou des mécanismes limitant les émissions de signaux compromettants.
Un dispositif de sécurité mis en place dans un système d'information qui traite d'informations classifiées doit être agréé par l'ANSSI lorsqu'il est utilisé, en complément de mesures organisationnelles de sécurité, comme un moyen essentiel de protection contre les accès non autorisés aux informations classifiées ou au système.
Exceptionnellement, en fonction de l'étude des risques qui a été menée et des conditions particulières d'emploi, l'autorité d'homologation peut décider de ne pas recourir à un dispositif agréé. Cette décision doit être expressément justifiée au regard des risques qui en découlent et motivée dans la décision d'homologation du système.
L'agrément est habituellement demandé par l'autorité chargée du développement du dispositif de sécurité, ou à défaut par l'autorité responsable de l'emploi du système. Il est délivré à l'issue d'une évaluation de sécurité du dispositif, réalisée par un ou plusieurs laboratoires agréés par l'ANSSI. Cette évaluation a pour objectif de vérifier la cohérence des objectifs de sécurité, identifiés dans la cible de sécurité, au regard des menaces, et d'évaluer l'efficacité des fonctions et des mécanismes de sécurité. En fonction des résultats de l'évaluation, l'ANSSI peut prononcer un agrément qui atteste de l'aptitude du dispositif à protéger les informations classifiées à un niveau spécifié, dans des conditions d'emploi identifiées. A l'issue de sa période de validité, un agrément doit faire l'objet d'un renouvellementrenouvellement d'habilitation pouvant nécessiter de réévaluer le dispositif. En raison de l'évolution des menaces ou de la découverte de vulnérabilités, un agrément peut être retiré avant son échéance.
Pour assurer le bon déroulement de la procédure d'agrément ou de son renouvellement d'habilitation, l'autorité l'ayant demandé doit mettre en place une commission d'agrément réunissant, outre cette autorité, l'ANSSI, les laboratoires d'évaluation concernés et, le cas échéant, l'autorité d'emploi du système.

Article 90

L'homologation de sécurité

1. Démarche d'homologation

Il est nécessaire de mettre en œuvre une démarche dite "d'homologation" pour permettre d'identifier, d'atteindre puis de maintenir un niveau de risque de sécurité acceptable pour le système d'information considéré, compte tenu du besoin de protection requis. Cette démarche s'appuie sur une gestion globale des risques de sécurité concernant l'ensemble du système d'information tout au long de son cycle de vie.
L'homologation de sécurité d'un système est globale en ce qu'elle inclut dans son périmètre tout ce qui peut avoir un impact sur la sécurité du système, de nature technique ou organisationnelle. En particulier, il devra être tenu le plus grand compte :
- des interconnexions avec d'autres systèmes ;
- des supports amovibles ;
- des accès à distance par des utilisateurs "nomades" ;
- des opérations de maintenance, d'exploitation ou de télégestion du système, notamment lorsqu'elles sont effectuées par des prestataires externes.
Tout système d'information traitant d'informations classifiées 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 classifiées du niveau de classification retenu conformément aux objectifs de sécurité visés, et que cette autorité

accepte les risques résiduels de sécurité. Lorsque le système recourt à des dispositifs de sécurité agréés par l'ANSSI, l'autorité d'homologation prend en compte les conditions attachées à ces agréments.

2. Autorité et commission d'homologation

L'homologation est prononcée par une autorité désignée dans les conditions suivantes :
- dans le cas où le système d'information traite d'informations classifiées au niveau Très Secret Défense, le SGDSN est l'autorité d'homologation ;
- dans le cas où le système d'information appartient à une administration, un service, un organisme ou un établissement relevant de la responsabilité d'un ministre, l'autorité qualifiée concernée désigne l'autorité d'homologation ;
- dans le cas où le système d'information relève de la responsabilité de plusieurs ministres, une autorité d'homologation unique est désignée conjointement par les ministres intéressés ;
- dans les autres cas, notamment lorsque le système d'information appartient à un organisme privé, la désignation de l'autorité d'homologation relève de la responsabilité du ou des organismes concernés par le système d'information.

L'autorité d'homologation doit être choisie au niveau hiérarchique suffisant pour assumer la responsabilité afférente à la décision d'homologation, et notamment pour accepter les risques résiduels. Elle est en principe l'autorité chargée de l'emploi du système. Elle peut être l'autorité qualifiée.

L'autorité d'homologation met en place une commission d'homologation chargée de l'assister et de préparer la décision d'homologation. Une telle commission comprend notamment des représentants des utilisateurs du système, et des responsables de l'exploitation et de la sécurité du système. En tant qu'autorité nationale en matière de sécurité des systèmes d'information, l'ANSSI peut participer à toute commission d'homologation. Elle en est membre de droit lorsque le SGDSNautorité nationale de sécurité est l'autorité d'homologation.

3. Décision d'homologation

La décision d'homologation est prise après l'examen du dossier d'homologation. Celui-ci comporte notamment :
- une analyse de risques ;
- la politique de sécurité du système ;
- les procédures d'exploitation de la sécurité ;
- la gestion des risques résiduels ;
- les résultats des tests et des audits menés pour vérifier la conformité du système à la politique de sécurité et aux procédures d'exploitation ;
- le cas échéant, les agréments des dispositifs de sécurité.

La décision d'homologation doit intervenir avant la mise en service opérationnel du système. Cependant, de façon exceptionnelle, lorsque l'urgence opérationnelle le requiert, il peut être procédé à une mise en service provisoire, sans attendre l'homologation du système, en tenant compte de l'avancement de la procédure d'homologation et des risques résiduels de sécurité. Dans ce cas, la mise en service définitive interviendra ultérieurement, lorsque l'homologation de sécurité aura été prononcée.

La décision d'homologation est prononcée pour une durée maximale :
- de cinq ans pour un système d'information au niveau Confidentiel Défense ;
- de deux ans pour un système d'information au niveau Secret Défense ou Très Secret Défense.

L'ANSSI est destinataire de toute décision d'homologation portant sur les systèmes d'information traitant d'informations classifiées. Elle peut demander le dossier d'homologation correspondant.

4. Contrôle et renouvellement de l’homologation

L’autorité d’homologation fixe les conditions du maintien de l’homologation de sécurité au cours du cycle de vie du système d’information. Elle contrôle régulièrement que le système fonctionne effectivement selon les conditions qu’elle a approuvées, en particulier après des opérations de maintien en condition opérationnelle.

L’autorité d’homologation examine le besoin de renouvellement de l’homologation avant le terme prévu notamment lorsque :

- les conditions d’exploitation du système ont été modifiées ;
- des nouvelles fonctionnalités ou applications ont été installées ;
- le système a été interconnecté à de nouveaux systèmes ;
- des problèmes d’application des mesures de sécurité ou des conditions de maintien de l’homologation ont été révélés, par exemple lors d’un audit de sécurité ;
- les menaces sur le système ont évolué ;
- de nouvelles vulnérabilités ont été découvertes ;
- le système a fait l’objet d’un incident de sécurité.

Article 91

Articles contrôlés de la sécurité

des systèmes d’information (ACSSI)

Certains moyens, tels que les dispositifs de sécurité ou leurs composants, et certaines informations relatives à ces moyens (spécifications algorithmiques, documents de conception, clés de chiffrement, rapports d’évaluation, etc.) peuvent nécessiter la mise en œuvre d’une gestion spécifique visant à assurer leur traçabilité tout au long de leur cycle de vie. Il s’agit des moyens et des informations, qu’ils soient eux-mêmes classifiés ou non, qu’il est essentiel de pouvoir localiser à tout moment et en particulier en cas de compromission suspectée ou avérée.

Ces moyens et informations sont appelés “articles contrôlés de la sécurité des systèmes d’information” (ACSSI). Ils portent un marquage spécifique les identifiant, en plus, le cas échéant, de leur mention de classification.

La décision de classer ACSSI un moyen ou une information est prise par l’ANSSI après avis de la commission d’agrément du dispositif de sécurité concerné. Dans le cas où le dispositif de sécurité n’est pas soumis à agrément du dispositif de sécurité n’est pas soumis à agrément, l’autorité d’homologation d’un système d’information qui met en œuvre un tel dispositif de sécurité peut décider après avis de la commission d’homologation de classer ACSSI ce dispositif ou ses composants ou les informations qui y sont liées.

Les principes de gestion des ACSSI ont pour objectif :

- de former, de sensibiliser et de responsabiliser les détenteurs de tels moyens et informations ;
- d’assurer la comptabilité de ces moyens et informations, et d’en établir l’inventaire à un niveau central ou local, selon les besoins, de façon qu’ils puissent être localisés à tout moment ;
- de gérer leur diffusion ;
- de contrôler périodiquement leur localisation et leur état ;
- d’informer la chaîne fonctionnelle de toute compromission suspectée ou avérée à la suite d’événements tels que la perte, le vol ou la disparition, même temporaire ;
- de s’assurer de leur destruction.

Article 92

Systèmes d'information particuliers

1. Traitement des informations "Spécial France"
Les systèmes d'information susceptibles de traiter des informations portant la mention "Spécial France" (141) doivent faire en outre l'objet de mesures de sécurité particulières pour garantir que les utilisateurs étrangers qui auraient un besoin d'accès légitime au système ne puissent accéder aux informations dont l'accès n'est autorisé qu'aux seuls utilisateurs français.

2. Echanges internationaux
Lorsque des informations classifiées sont transmises dans des systèmes d'information relevant de la responsabilité d'Etats étrangers ou d'organisations internationales, des mesures de protection doivent être fixées par des accords ou des règlements de sécurité avec ces partenaires, qui assurent à ces informations un niveau de protection au moins équivalent à celui prévu dans la présente instruction.
La protection des systèmes d'information traitant d'informations classifiées confiées à la France par des Etats étrangers ou par des organisations internationales, est assurée conformément aux accords et aux règlements de sécurité établis avec ces partenaires. Ces accords et règlements font, le cas échéant, l'objet d'instructions complémentaires pour l'application de ces mesures en France. AA défaut de tels accords ou règlements, les dispositions de la présente instruction s'appliquent à ces systèmes.

...
(89) Ces dispositions ne sont pas les seules à protéger le secret, les articles consacrés à la trahison et à l'espionnage y faisant également référence, de manière indirecte (articles 411-6 pour la livraison d'un secret à une puissance étrangère, 411-7 pour la collecte de renseignements à fin de transmission à une puissance étrangère, 411-8 pour l'exercice d'une activité ayant pour but la livraison de renseignements à une puissance étrangère).
(90) Articles 413-10 et 413-11 du code pénal.
(91) Articles 413-10 et 413-10-1 du code pénal.
(92) Articles 413-11 et 413-11-1 du code pénal.
(93) Ainsi, par exemple, une personne ne peut déposer devant une juridiction en révélant des éléments classifiés, à moins que ceux-ci n'aient été préalablement déclassifiés.
(94) Article 418-8 du code pénal.
(95) Article 414-9 du code pénal.
(96) Article 413-12 du code pénal.
(97) Articles 121-2 et 414-7 du code pénal.
(98) Direction générale de la sécurité intérieure.
(99) La direction de la protection et de la sécurité de défense (DPSD), direction générale de la sécurité extérieure (DGSE) pour son domaine de compétence. (100) Article 12 de la présente instruction.
(101) Article 434-4 du code pénal.
(102) Article 81 de la présente instruction.
(103) Article L. 2312-4 du code de la défense.
(104) Créé par une loi du 8 juillet 1998, cet organisme consultatif indépendant fait l'objet des articles L. 2311-1 à L. 2311-8 du code de la défense.
(105) Article L. 2312-1 du code de la défense.
(106) Article L. 2312-5 du code de la défense.
(107) Article L. 2312-7 du code de la défese.
(108) Ou à l'expiration du délai de deux mois imparti à la CCSDN pour formuler son avis.
(109) Article L. 2312-8 du code de la défense.
(110) Annexe 4.

(111) Modèle 05/IGI 1300 en annexe.
(112) Article L. 33-3 du code des postes et communications électroniques.
(113) Modèle 17/IGI1300.
(114) Dans cette hypothèse, des procédures particulières sont mises en œuvre, notamment dans le cadre des inspections par mise en demeure prévues par la convention internationale pour l'interdiction des armes chimiques, signée à Paris le 13 janvier 1993.
(115) Les dispositions suivantes ne s'appliquent en effet pas à l'Etat, ni aux collectivités territoriales ni à leurs établissements publics administratifs (articles L. 8113-8 et L. 8114-3 du code du travail).
(116) Articles L. 8112-1 à L. 8123-4 du code du travail. La paix des relations sociales, la sécurité des salariés et la lutte contre le travail illégal peuvent contribuer à la protection du secret de la défense nationale.
(117) Articles L. 8112-1 du code du travail pour les inspecteurs, L. 8113-11 pour les contrôleurs, L. 8123-1 pour les médecins inspecteurs, L. 8123-4 pour les ingénieurs de prévention.
(118) Articles L. 8113-3 à L. 8113-5 et L. 8123-3 et L. 8123-4 du code du travail.
(119) Articles L. 8113-3 à L. 8113-5 du code du travail.
(120) Articles L. 8113-4 et L. 8123-4 du code du travail.
(121) Articles L. 8114-1 et L. 8114-2 du code du travail : le refus du responsable du site de se prêter à ces opérations constitue le délit d'entrave.
(122) Articles L. 8113-10 et L. 8123-5 du code du travail.
(123) Article 226-13 du code pénal.
(124) Article 56-4 du code de procédure pénale.
(125) Article 56-4 (IV) du code de procédure pénale.
(126) Articles 56-4 du code de procédure pénale et R. 2311-9-1 du code de la défense.
(127) Articles 56-4 du code de procédure pénale et R. 2312-1 du code de la défense.
(128) Articles L. 2312-4 à L. 2312-8 du code de la défense.
(129) Article 56-4, alinéa 4, du code de procédure pénale.
(130) Article 434-4 du code pénal, qui prévoit et réprime comme caractérisant le délit d'entrave à la justice le fait de faire obstacle à la manifestation de la vérité, notamment par la destruction, la soustraction, le recel ou l'altération d'un document public ou privé ou d'un objet de nature à faciliter la découverte d'un crime ou d'un délit, la recherche des preuves ou la condamnation des coupables.
(131) Article 56-4 (II) du code de procédure pénale.
(132) Article R. 1132-3 du code de la défense.
(133) Décret n° 2009-834 du 7 juillet 2009, article 3.
(134) Décret n° 2009-834 du 7 juillet 2009, article 7.
(135) Article R. 1143-5 du code de la défense.
(136) Article 91 de la présente instruction.
(137) Désignés sous l'appellation d'ASSI dans la suite de l'instruction.
(138) Article R. 2311-6-1 du code de la défense.
(139) Article R. 2311-7-1 du code de la défense.
(140) Article R. 2311-6-1 du code de la défense.
(141) Conformément à l'article R. 2311-4 du code de la défense.

## TITRE VI

## LA PROTECTION DU SECRET DANS LES CONTRATS

Les personnes morales de droit privé, de la même façon que les personnes physiques, doivent être habilitées pour l'exécution de travaux classifiés ;

La détention par un contractant d'informations ou de supports classifiés est conditionnée

par l'aptitude physique des locaux à accueillir de tels informations ou supports.

Article 93

Principes généraux de sécurité

La sécurité des informations ou supports classifiés dans les contrats, entendus au sens de l'article 2 de la présente instruction, est garantie par l'insertion de stipulations répondant aux présentes prescriptions et précisant les obligations des contractants. Tout contrat de sous-traitance (142) d'un marché nécessitant l'accès aux informations ou supports classifiés obéit aux règles de la présente instruction, y compris dans la phase précontractuelle.

Tout contrat qui implique l'accès aux informations ou supports classifiés comporte des clauses de protection du secret précisant les obligations des contractants telles que définies en annexe 9. Le titulaire d'un tel contrat s'engage, sous sa responsabilité pénale et contractuelle, à assurer la protection des informations ou supports classifiés qu'il aura à détenir ou à connaître au titre de ce contrat en tenant compte des dispositions particulières stipulées dans l'annexe de sécurité se rapportant au contrat.

L'aptitude physique à détenir des informations ou supports classifiés est conditionnée par le respect des dispositions législatives et réglementaires en matière de protection du secret de la défense nationale. Le titulaire d'un contrat dont l'objet implique la détention d'informations ou de supports classifiés est tenu de mettre en œuvre dans son ou ses établissements les mesures de sécurité requises pour assurer la protection du secret de la défense nationale conformément à l'article 71. A l'égard de toute personne qu'il emploie, qu'il reçoit ou avec laquelle il a des liens, le titulaire du contrat concerné prend toutes mesures utiles pour contrôler, et le cas échéant limiter, l'accès aux parties de ses installations dans lesquelles la protection des informations ou supports classifiés le justifie.

Chapitre Ier
Mesures de sécurité dans la négociation

et la passation des contrats

Section 1
Phase précontractuelle

Article 94
Obligations de l'autorité contractante

Dès le début d'une procédure de passation d'un contrat ou s'il y a lieu dans l'avis d'appel public à la concurrence, l'autorité contractante est tenue d'informer les futurs candidats du délai imparti pour fournir les documents nécessaires à l'habilitation et, si le contrat nécessite la détention d'informations ou de supports classifiés, les documents nécessaires pour faire procéder à l'évaluation de l'aptitude physique de l'entreprise à détenir de tels informations ou supports. Ce délai ne peut être inférieur à quinze jours à compter de la date de l'information délivrée par l'autorité contractante. A cet effet, l'autorité contractante communique tous les formulaires nécessaires ou les modalités pour se les procurer et, le cas échéant, le service compétent pour traiter le dossier.
Les candidats à des contrats nécessitant la détention d'informations ou de supports

classifiés sont informés des normes physiques à satisfaire et des obligations induites par la détention de tels informations ou supports et du fait que le début des travaux classifiés est suspendu à l'évaluation de l'aptitude qui peut, le cas échéant, intervenir après la notification du contrat.
Lorsque le dossier est incomplet, l'autorité contractante informe les soumissionnaires des pièces manquantes, qui devront être fournies avant l'expiration du délai fixé.
L'autorité contractante informe l'autorité d'habilitation des candidats retenus et lui transmet le projet d'annexe de sécurité. L'autorité d'habilitation transmet le dossier de demande d'habilitation au service enquêteur compétent dès réception de cette information.

## Article 95
## Obligations du soumissionnaire

Tout candidat, personne physique ou morale, à un contrat, quels que soient sa nationalité, la forme ou le statut juridique de l'entreprise, doit faire l'objet d'une habilitation dans les conditions définies au présent titre. A cet effet, dans le cadre de sa candidature, la personne morale ou physique soumissionnaire doit présenter un dossier de demande d'habilitation ou un certificat de sécurité en cours de validité attestant de son habilitation. Sous réserve des dispositions de l'article 97 de la présente instruction, ce dossier d'habilitation doit être conforme à l'annexe 11.
A l'appui de sa candidature à un contrat dont l'exécution implique la détention d'informations ou de supports classifiés, l'entreprise, quelle que soit sa nationalité, doit, en outre, s'engager à déposer un dossier d'aptitude pour chacun des établissements situés sur le territoire français dans lesquels il est envisagé d'exécuter des travaux classifiés. Ce dossier est destiné à l'évaluation de l'aptitude desdits établissements à assurer la protection des éléments couverts par le secret de la défense nationale.
A défaut d'avoir fourni ou complété le ou les dossiers mentionnés aux paragraphes 1 et 2 du présent article dans les délais fixés, le soumissionnaire est réputé avoir renoncé à demander une habilitation aux informations et supports classifiés pour le contrat considéré.

## Article 96
## Communication d'informations

classifiées en phase précontractuelle

Dès lors que la prise de connaissance d'informations classifiées est nécessaire dans la phase précontractuelle, et notamment pour l'élaboration et la soumission de l'offre, l'habilitation des personnes physiques est possible sans que la personne morale qui les emploie ne soit elle-même habilitée, à condition que la procédure d'habilitation la concernant ait été initiée. A cet effet, le soumissionnaire doit désigner parmi son personnel, au plus tard lorsque sa candidature a été retenue pour établir une offre, une ou plusieurs personnes qui accéderont aux informations ou supports classifiés dans le strict besoin d'élaboration de l'offre.
Si les personnes désignées en application de la présente section ne sont pas titulaires d'une habilitation ou si la décision d'habilitation les concernant n'est pas appropriée aux besoins du contrat, le soumissionnaire dont elles relèvent dépose simultanément une demande d'habilitation pour chacune d'elles. Cette demande est instruite et fait l'objet d'une décision d'habilitation provisoire ou d'une décision de refus délivrée dans les conditions et délais prévus au titre II (chapitre 2) de la présente instruction. Les habilitations provisoires délivrées en application de la procédure définie à la présente section ne préjugent pas de l'habilitation de la personne morale pour exécuter ledit

contrat.
L'autorité contractante définit la liste des personnes autorisées à prendre connaissance d'informations et supports classifiés dans le cadre de l'élaboration de l'offre et fixe les lieux et les modalités d'exploitation des éléments couverts par le secret de la défense nationale. Ces lieux doivent présenter les garanties de protection inhérentes au niveau d'informations classifiées traitées telles que définies à l'article 71.
Les candidats non retenus détenant des informations et supports classifiés sont tenus de les restituer à leur émetteur dès la notification du rejet de leur offre et selon les modalités définies par l'autorité contractante.

### Article 97
### Cas des entreprises étrangères

Toute entreprise de droit étranger candidate à un contrat est tenue, à l'appui de sa candidature, de produire une attestation justifiant de son habilitation ou de la procédure en cours engagée à cette fin. Cette attestation est délivrée par une autorité d'habilitation de l'Etat dont elle relève lorsque cet Etat a conclu un accord de sécurité bilatéral ou multilatéral couvrant les échanges d'informations ou supports classifiés avec la France.
L'autorité d'habilitation peut saisir le secrétariat général de la défense et de la sécurité nationale, autorité nationale de sécurité, ou l'autorité de sécurité déléguée mentionnée dans l'accord de sécurité aux fins de requérir l'autorité nationale de sécurité de l'Etat de nationalité de l'entreprise candidate en vue de procéder à l'habilitation appropriée de cette entreprise.
Aucune entreprise candidate de droit étranger ne peut être retenue lorsque l'exécution du contrat conclu dans le cadre du présent titre implique la détention ou l'échange d'informations ou supports classifiés portant la mention "Spécial France" (143).

### Article 98
### Cas des entreprises françaises qui soumissionnent

dans un cadre international

Les entreprises françaises candidates à un contrat nécessitant l'accès à des informations classifiées en dehors du cadre national et pour lesquelles une habilitation est requise, adressent, si elles ne sont pas déjà titulaires d'une habilitation, leur dossier d'habilitation soit au secrétariat général de la défense et de la sécurité nationale en sa qualité d'autorité nationale de sécurité soit à l'autorité de sécurité déléguée mentionnée dans l'accord de sécurité applicable entre la France et le pays au profit duquel elles soumissionnent. Une entreprise déjà habilitée s'adresse à son autorité d'habilitation pour une extension éventuelle du domaine d'habilitation. L'autorité d'habilitation transmet, le cas échéant, les éléments à l'autorité nationale de sécurité pour la délivrance d'une attestation d'habilitation appropriée.

## Section 2
## La procédure d'habilitation

### Article 99
### L'enquête préalable

Afin d'évaluer si une entreprise ne présente pas de vulnérabilité pour la défense et la sécurité nationale, les investigations menées par le service enquêteur portent notamment sur les détenteurs réels du pouvoir de direction et de contrôle ainsi que sur le ou les

actionnaires. L'autorité nationale de sécurité de l'Etat de la nationalité des dirigeants ou des actionnaires peut être consultée. Le sens de l'enquête de vulnérabilité n'affecte en rien l'honorabilité de l'entreprise concernée ni celle de ses dirigeants.
Au terme des investigations, le service enquêteur émet un avis de sécurité qui n'est communiqué qu'à l'autorité d'habilitation.
Les conclusions de l'avis de sécurité sont de trois types :
- "avis sans objection", lorsque l'instruction n'a révélé aucun élément de vulnérabilité de nature à constituer un risque pour la sécurité des informations ou supports classifiés ni pour celle de la personne morale ;
- "avis restrictif", lorsque la personne morale présente certaines vulnérabilités constituant des risques directs ou indirects pour la sécurité des informations ou supports classifiés auxquels elle aurait accès, mais que des mesures de sécurité spécifiques prises par l'officier de sécurité permettraient de maîtriser ;
- "avis défavorable", lorsque des informations précises font apparaître que la personne morale présente des vulnérabilités faisant peser des risques tels qu'aucune mesure de sécurité ne semble suffisante à les neutraliser.
L'avis de sécurité est émis pour un niveau donné d'habilitation. L'avis "sans objection" est valable pour le niveau précisé ainsi que pour le(s) niveau(x) inférieur(s). Pour les avis restrictifs ou défavorables, les services enquêteurs se prononcent, au cas par cas, sur l'opportunité d'accorder une habilitation pour le(s) niveau(x) inférieur(s).
Les avis restrictifs ou défavorables ne sont pas classifiés. Ils sont assortis d'une fiche confidentielle indiquant les motifs de l'avis. Cette fiche, classifiée en tout ou partie, explicite les motifs de vulnérabilité décelés lors de l'enquête. Ces motifs ne peuvent être portés qu'à la connaissance de la seule autorité d'habilitation. Ne pouvant être reproduite, la fiche confidentielle est retournée après communication et sans délai au service enquêteur qui l'a émise, aux fins de conservation.
Toutefois, afin de permettre la reconnaissance des habilitations entre autorités d'habilitation, l'avis de sécurité ainsi que tous les éléments relatifs à l'habilitation de la personne morale concernée peuvent être transmis entre autorités d'habilitation. Sauf changement dans la situation de fait ou de droit de l'entreprise, la durée de validité de l'avis de sécurité émis est fixée conformément aux dispositions de l'article 24.

## Article 100
## L'habilitation de la personne morale

L'habilitation du contractant est une décision explicite qui est délivrée par l'autorité d'habilitation sur la base de l'avis de sécurité émis par l'un des services enquêteurs désignés à l'article 24.
L'autorité d'habilitation prend sa décision au vu de l'avis de sécurité émis avant la date d'attribution du contrat, sans être liée par cet avis. En cas d'urgence justifiée et après saisine du service enquêteur, l'autorité d'habilitation prend en dernier ressort, si elle l'estime nécessaire, sa décision au vu de tout autre élément utile en sa possession.
La décision de refus d'habilitation est notifiée au représentant de la personne morale dans les conditions définies à l'article 26. Une décision de refus ne préjuge pas de la conclusion de contrats de toute nature n'impliquant pas la mise en œuvre de mesures de protection du secret de la défense nationale.
Les décisions d'habilitation délivrées à l'occasion de la passation d'un contrat nécessitant la prise de connaissance d'informations classifiées ou leur détention comportent une date limite de validité fixée par l'autorité d'habilitation ainsi que, s'il y a lieu, un domaine de validité. La durée de validité de la décision d'habilitation peut être distincte de celle de l'avis de sécurité, sans pouvoir lui être supérieure.

## Article 101
## Durée de validité de l’habilitation

des personnes morales

L’habilitation délivrée à une entreprise par un ministère à l’occasion d’un contrat nécessitant l’accès ou la détention d’informations ou supports classifiés demeure valable pour toute autre consultation d’une autorité contractante relevant de ce même ministère, à l’occasion d’un autre contrat, dans les limites de date et de domaine de validité de cette habilitation et sauf changement dans la situation de fait ou de droit de l’entreprise considérée.
L’habilitation en cours de validité précédemment délivrée par un autre département ministériel, dont une attestation peut être établie, est étendue au nouveau contrat sauf changement dans la situation de droit ou de fait du soumissionnaire. L’autorité d’habilitation, le cas échéant après examen du dossier transmis, à sa demande, par l’autorité ayant précédemment habilité le soumissionnaire, peut prendre une décision d’habilitation relative au domaine du nouveau contrat si l’habilitation précédemment délivrée a été limitée à un domaine particulier.
Si la décision d’habilitation arrive à expiration au cours de l’exécution d’un contrat régi par les présentes dispositions, une demande de renouvellement doit être déposée auprès de l’autorité d’habilitation, dans les six mois et, au plus tard, un mois avant cette date d’expiration. La durée de validité de la décision est alors prorogée dans les conditions définies à l’article 31.
Tout changement affectant le titulaire d’une habilitation, personne morale ou personne physique, intervenant après la décision doit être signalé à l’autorité d’habilitation afin de lui permettre de reconsidérer sa décision.

## Article 102
## Confidentialité de l’habilitation

de la personne morale

La personne morale titulaire d’une décision d’habilitation ne peut faire publiquement état de cette décision ou s’en prévaloir, ni communiquer à des tiers des informations se référant à des travaux classifiés sauf autorisation expresse de l’autorité contractante de référence.

## Article 103
## L’habilitation des personnes physiques

Sont seules autorisées à connaître des informations ou supports classifiés pour le compte d’une entreprise habilitée les personnes appartenant à cette entreprise qui ont fait l’objet au préalable d’une décision d’habilitation délivrée dans les conditions prévues à l’article 24. Sauf exception, le niveau de cette habilitation ne peut excéder celui de l’habilitation de la personne morale.
Il pourra être fait recours à l’agrément défini à l’article 33 pour un accès ponctuel à des informations classifiées à un niveau supérieur à celui de l’habilitation de la personne morale.
Les contrats de travail privés ou publics des personnes mentionnées au premier alinéa comportent une clause de protection du secret conforme à la clause type figurant à l’annexe 9 (4°). En cas de changement d’affectation amenant le salarié à travailler dans les conditions définies au premier alinéa, le contrat de travail fait l’objet d’un avenant écrit

conforme aux présentes dispositions. Les parties au contrat de travail peuvent compléter ou adapter la clause type selon les spécificités dudit contrat sans lui être contraire.

## Section 3
## Phase de contractualisation

### Article 104
### Conditions de signature du contrat

L'autorité contractante ne peut signer aucun contrat nécessitant la connaissance d'informations classifiées avant réception de l'attestation d'habilitation de la personne morale ou physique candidate retenue, établie, sauf dans le cas d'une procédure d'urgence, sur la base de l'avis de sécurité du service enquêteur.
Lorsque le contrat nécessite la détention d'informations classifiées, la validation définitive de l'aptitude, sur la base d'un dossier établi conformément aux prescriptions de l'annexe 13, doit avoir été transmise à l'autorité contractante avant le début des travaux classifiés mais peut être communiquée à l'entreprise après la notification du contrat. Dans ce cas, et selon le calendrier établi en liaison avec le service enquêteur et l'autorité contractante, la date de début d'exécution du contrat est précisée au moment de la notification dans les conditions suivantes :
1. Un contrôle initial d'aptitude portant sur les mesures prises par l'entreprise habilitée pour assurer la sécurité des informations ou supports classifiés est effectué par le service enquêteur dans le ou les établissements concernés, préalablement à tout commencement d'exécution des travaux classifiés. A l'issue de ce contrôle, l'avis technique délivré par le service enquêteur est transmis à l'autorité contractante et notifié au contractant. A réception de cet avis, et s'il est sans réserve, le responsable de l'entreprise établit une attestation (144) certifiant la mise aux normes des locaux du ou des établissements concernés.
2. Si l'avis technique fait état de carences dans le dispositif de sécurité mis en œuvre au sein de l'entreprise, le titulaire est tenu de s'engager à mettre en œuvre toutes les mesures nécessaires à la mise en conformité de son établissement dans un délai défini en liaison avec le service enquêteur et l'autorité contractante et compatible avec la date de début des travaux classifiés.
3. A l'issue des travaux de mise aux normes et au plus tard à la date d'expiration du délai stipulé lors de la notification, la certification de l'aptitude mentionnée au paragraphe 1 du présent article (145) est transmise par le responsable de l'entreprise à l'autorité contractante, qui en informe le service enquêteur et peut le solliciter pour diligenter un contrôle.
4. Si l'attestation n'est pas parvenue dans le délai prédéfini ou si des carences sont constatées lors des contrôles effectués par le service enquêteur, une mise en demeure de se conformer aux prescriptions de l'article 71 est effectuée. Le défaut d'exécution des travaux engage la responsabilité du titulaire.
Si le titulaire dispose d'un local apte au traitement d'informations ou de supports classifiés ayant fait l'objet d'un avis d'aptitude dans le cadre d'un précédent contrat, il communique à l'autorité contractante de référence cet avis ainsi que l'attestation de non-changement des conditions qui ont amené la délivrance de l'avis d'aptitude (146).

# Chapitre II
# Mesures de sécurité liées à l'exécution des contrats

## Section 1
## La structure de sécurité

## Article 105
## Le responsable de la politique de sécurité de l'entreprise

Sous sa responsabilité pénale et contractuelle et celle de la personne morale, le chef de l'entreprise titulaire du contrat est tenu de mettre en œuvre les prescriptions réglementaires pour assurer la sécurité des informations ou supports classifiés. A ce titre, une politique de sécurité garantissant la mise en œuvre du dispositif de protection des informations ou supports classifiés au sein de l'entreprise et, le cas échéant, de ses différents établissements doit être établie. Pour l'élaboration et la mise en œuvre de la politique de sécurité, le représentant de la personne morale désigne une ou plusieurs personnes à la fonction d'officier de sécurité. Les personnes ainsi désignées doivent avoir un niveau hiérarchique suffisant dans l'entreprise et disposer de tous les moyens nécessaires pour accomplir les missions qui leur sont confiées. A cet effet, elles sont rattachées dans l'exercice de leurs missions de sécurité au chef d'entreprise et agissent pour le compte et sous la responsabilité de ce dernier.
L'officier de sécurité doit faire l'objet d'un agrément par l'autorité d'habilitation. Pour être agréé, l'officier de sécurité doit être préalablement habilité. Cet agrément peut être délivré pour une période probatoire de douze mois au plus. A l'issue de cette période probatoire, sauf décision explicite contraire, l'agrément est réputé confirmé. L'agrément peut être retiré à tout moment par l'autorité d'habilitation, notamment lorsque son titulaire cesse d'être habilité. Dans ce cas, le chef de l'entreprise titulaire du contrat concerné doit proposer un nouveau titulaire dans les mêmes conditions et dans les plus brefs délais.
En fonction des besoins de protection du secret dans chaque établissement de l'entreprise, le chef de l'entreprise titulaire d'un contrat impliquant la détention d'éléments classifiés peut désigner un ou plusieurs adjoints à l'officier de sécurité, qui est alors identifié comme officier central de l'entreprise. Ses adjoints sont appelés officiers de sécurité d'établissement.
Dès lors que des systèmes d'information hébergent et traitent des informations classifiées, le chef d'entreprise doit également désigner un officier de sécurité affecté à la sécurité des systèmes d'information afin de renforcer la structure de sécurité. Cette fonction peut être exercée par l'officier de sécurité ou sous son autorité.
Les dispositions de la présente section sont applicables à tout adjoint d'un officier de sécurité.
Le chef d'entreprise peut, le cas échéant, désigner des correspondants de sécurité au sein de subdivisions physiques ou opérationnelles de l'entreprise pour consolider l'action de l'officier de sécurité au sein de ces subdivisions. Placés, pour cette mission, sous le contrôle opérationnel d'un officier de sécurité, ces correspondants de sécurité ne font pas l'objet de l'agrément prescrit ci-dessus.

## Article 106
## Rôle et obligations de l'officier de sécurité

Sous l'autorité du chef de l'entreprise, l'officier de sécurité est chargé de l'organisation générale de la sécurité de l'établissement, et notamment des relations, au titre de sa fonction, avec le service enquêteur, les autorités d'habilitation et les autorités contractantes.
1. A ce titre, il est amené à s'assurer notamment :
- de l'application des règles de sécurité énoncées dans les différents textes au sein de l'établissement ;
- de la gestion des dossiers d'habilitation du personnel de l'établissement en fonction du besoin d'en connaître ; il est également chargé des demandes d'habilitation de

sous-traitants éventuels. Il est tenu de signaler au service enquêteur les éléments de vulnérabilité portés à sa connaissance apparaissant après la décision d'habilitation et de signaler à l'autorité d'habilitation tout changement dans les statuts de la personne morale ;
- de la tenue à jour d'un registre des membres du personnel titulaires d'une habilitation et auxquels l'accès est autorisé, dans le cadre du contrat et d'éventuels contrats de sous-traitance. Ce registre indique les dates de délivrance et de fin de validité ainsi que le niveau de ces habilitations ;
- de fournir, à la demande du service enquêteur, des renseignements sur toutes les personnes qui seront appelées à avoir accès à des informations classifiées ;
- de la sensibilisation et de la formation du personnel ;
- de signaler les compromissions du secret avérées ou supposées, dans les conditions définies à l'article 67 ;
- de la gestion et de la mise à jour des annexes de sécurité des contrats de droit public ou de droit privé ;
- de la mise à jour du dossier de sécurité.
2. Dans le cadre des contrats impliquant la détention d'informations ou de supports classifiés, il est en outre chargé :
- du contrôle permanent de la gestion et de la protection des informations ou supports classifiés ;
- de la gestion et du suivi des ACSSI ;
- de la gestion des demandes d'autorisation d'accès au périmètre d'accès restreint et de la gestion des contrôles élémentaires pour l'accès des personnels extérieurs à l'établissement ;
- de l'application des règles internationales en matière de visites de ressortissants étrangers se rendant dans l'établissement dont il a la charge ;
- de l'application des règles internationales en matière de visites à l'étranger des personnels de son établissement ;
- de la sensibilisation aux prescriptions de sécurité à respecter dans l'établissement par les différents intervenants ;
- du respect des dispositions réglementaires en matière d'accès, de manipulation, de conservation, de reproduction et de destruction des informations classifiées.

## Section 2
## L'annexe de sécurité

### Article 107
### Contenu de l'annexe de sécurité

Tout contrat comporte une annexe de sécurité qui énumère les instructions de sécurité relatives au contrat. Lorsque son contenu le justifie, elle peut être classifiée en tout ou partie. Elle peut être modifiée en cours d'exécution du contrat à l'initiative de l'autorité contractante ou sur proposition du titulaire du contrat.
L'autorité contractante approuve l'annexe de sécurité du contrat et les annexes de sécurité des éventuels contrats de sous-traitance. Le suivi des annexes de sécurité des contrats de sous-traitance est effectué par le primo-contractant sous sa responsabilité et sous le contrôle de l'autorité contractante de référence. Les modalités de ce contrôle peuvent être définies dans des clauses particulières ou dans l'annexe de sécurité du contrat principal.
L'annexe de sécurité porte sur les prescriptions mentionnées en annexe 13. Celles-ci peuvent être adaptées par l'autorité contractante en liaison avec le titulaire sans pouvoir leur être contraires.

### Article 108
### Cas de la sous-traitance

Tout contrat nécessitant la détention d'informations ou de supports classifiés donnant lieu à au moins un contrat de sous-traitance nécessitant lui-même un accès à des informations ou supports classifiés doit intégrer dans son annexe de sécurité la liste des sous-traitants concernés, les travaux réalisés et leurs dates prévisionnelles de début et de fin d'exécution ainsi que les informations et supports classifiés dont la connaissance est nécessaire à leur réalisation. La modification de l'annexe de sécurité peut se faire a posteriori sous réserve de l'accord de l'autorité contractante de référence.

## Section 3
## Suivi de l'exécution

### Article 109
### Obligations du titulaire

Durant l'exécution du contrat, le titulaire est tenu de mettre en œuvre les mesures de sécurité requises pour assurer la protection des informations classifiées. En particulier, dans le cadre de la détention d'informations ou de supports classifiés, il contrôle l'accès à ses installations et doit se soumettre à des contrôles d'aptitude périodiques tout au long de l'exécution du contrat. Il est tenu d'informer l'autorité d'habilitation et le service enquêteur de tout changement de fait ou de droit dans la situation de l'entreprise ou des personnels participant à l'exécution du contrat.

### Article 110
### Obligations spécifiques des primocontractants

Les primocontractants doivent garantir, en outre, l'application par leurs sous-traitants de conditions de sécurité non moins strictes que celles prévues dans le contrat. Les primocontractants doivent demander l'autorisation à l'autorité contractante de référence pour communiquer des informations classifiées à des sous-traitants. Selon les modalités définies par les parties, cette autorisation peut porter sur tout ou partie des informations classifiées, selon le besoin d'en connaître, en fonction de l'étendue des prestations définies par le contrat de sous-traitance.
Il ne peut être communiqué à des sous-traitants des informations ou supports classifiés se rapportant audit contrat avant que ces sous-traitants, ainsi que leurs employés ayant à en connaître, n'aient fait l'objet d'une décision d'habilitation. L'éventuelle détention d'informations et supports classifiés par les sous-traitants ne peut se faire que sous couvert de contrats avec annexe de sécurité approuvée par l'autorité contractante de référence.

### Article 111
### Les contrôles de sécurité et d'aptitude

Des contrôles d'aptitude et des inspections peuvent être diligentés périodiquement dans les locaux des entreprises, conformément à l'article 8, pour vérifier l'application de la présente instruction pendant l'exécution de chaque contrat.
Sous la responsabilité du chef d'entreprise, les locaux de l'entreprise titulaire doivent être réaménagés en conformité avec les dispositions réglementaires en vigueur lorsqu'ils ne présentent plus les garanties suffisantes pour la sécurité des informations ou supports classifiés. Pendant les travaux de réaménagement de ces locaux, l'entreprise prend toutes

mesures pour assurer la sécurité des informations ou supports classifiés. Après chaque mise en conformité, un contrôle donnant lieu à un nouvel avis d'aptitude des locaux concernés peut être effectué par le service enquêteur et la procédure mentionnée à l'article 104 s'applique. Tout refus de mise en conformité ou tout retard pour se mettre en conformité peut être considéré comme un non-respect des engagements contractuels en matière de protection du secret et entraîner le prononcé des sanctions prévues au contrat, sans préjudice d'éventuelles sanctions pénales.

### Article 112
### Mesures particulières en fin d'exécution du contrat

Lorsque les travaux classifiés sont terminés, le titulaire du contrat doit en informer dans le délai d'un mois l'autorité contractante, qui lui précise la destination à donner aux informations ou supports classifiés qu'il détenait jusqu'alors. L'annexe de sécurité mentionnée est clôturée. A cet effet, les modalités d'archivage des informations ou supports classifiés sont définies par l'autorité contractante de référence en liaison avec les services concernés.
L'annexe de sécurité d'un contrat ayant généré un ou plusieurs contrats de sous-traitance ne peut être clôturée qu'après la clôture de toutes les annexes de sécurité de sous-traitance.
Lorsque après la clôture d'une annexe de sécurité l'entreprise conserve des informations ou des supports classifiés, elle doit faire l'objet d'une décision d'habilitation valide et d'un suivi par un service enquêteur, quand bien même cette entreprise ne serait titulaire d'aucun autre contrat générant l'accès à des éléments couverts par le secret de la défense nationale.

## Glossaire

Accord de sécurité : accord intergouvernemental conclu entre au moins deux Etats ou au sein d'une alliance multinationale et ayant pour objet la protection d'informations ou de supports classifiés. 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 de transmission et de protection des informations et supports classifiés.
Administrateur de sécurité : personne chargée 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 classifiés aux niveaux Secret Défense ou Confidentiel Défense.
Administrateur système : personne chargée de la mise au point, de l'exploitation, de la maintenance, du contrôle et des évolutions du système informatique.
Agent de sécurité des SSI : personne chargée 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 classifiés du niveau Très Secret Défense de différentes classifications spéciales, du niveau Secret Défense ou du niveau Confidentiel Défense.
Agrément 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 informations ou supports classifiés Très Secret Défense.
Aptitude : capacité d'une entreprise à traiter ou à détenir des informations ou des supports classifiés. Cette capacité, évaluée par un service enquêteur, est fondée sur le contrôle de l'ensemble des mesures de sécurité physique mises en œuvre par le titulaire du contrat pour un ou plusieurs établissements et incluant, si nécessaire, la sécurité des systèmes d'information.
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 contractante : toute personne publique ou privée, y compris dans le cas des contrats de sous-traitance, qui fait appel à un fournisseur ou à un prestataire pour l'exécution d'un contrat ou d'un marché. Lorsque le marché est régi par les dispositions du code des marchés publics, l'expression "autorité contractante" désigne le pouvoir adjudicateur. Lorsqu'un marché régi par les dispositions du code des marchés publics entraîne des contrats de sous-traitance, le pouvoir adjudicateur à l'origine de celui-ci est appelé "autorité contractante de référence".
Autorité d'habilitation : autorité compétente pour solliciter une enquête d'habilitation ou un contrôle élémentaire et émettre la décision.
Autorité nationale de sécurité (ANS) : organisme gouvernemental chargé des relations avec les autres Etats et les structures internationales en matière d'habilitation de personnes et de protection des informations ou supports classifiés. En France, l'autorité nationale de sécurité est le secrétaire général de la défense et de la sécurité nationale.
Autorité de sécurité déléguée (ASD) : autorité responsable devant l'autorité nationale de sécurité (ANS) et chargée de faire connaître aux entreprises la politique nationale dans un domaine, notamment industriel, 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'Etat, dans les établissements publics placés sous l'autorité d'un ministre ainsi que dans les organismes et établissements relevant de ses attributions.
Avis de sécurité : conclusion émise par un service enquêteur à l'issue d'investigations se rapportant à une personne et visant à détecter et à 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, pour la bonne exécution d'une mission précise.
Bureau de protection du secret : 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, au suivi et à la destruction des informations ou supports classifiés Secret Défense.
Catalogue des emplois : dans un organisme, liste des emplois qui peuvent nécessiter l'accès aux informations ou supports classifiés. Le catalogue est dressé sur le seul critère du besoin d'en connaître.
Certificat de sécurité : document prouvant l'habilitation d'une personne au traitement d'informations ou supports classifiés à un niveau précisé.
Classification spéciale : catégorie d'informations ou supports classifiés au niveau Très

Secret Défense et répondant à la nécessité de cloisonnement. Les classifications spéciales sont organisées en réseaux de sécurité constitués d'antennes d'utilisation. Les habilitations au niveau Très Secret Défense sont prononcées au titre d'une ou plusieurs classifications spéciales expressément désignées.
Compromission : prise de connaissance, certaine ou possible, d'une information ou d'un support classifié par une ou plusieurs personnes non qualifiées.
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.
Contrôle élémentaire : enquête administrative simplifiée, destinée à s'assurer de l'intégrité d'une personne et sollicitée par l'autorité d'habilitation, l'autorité contractante ou le responsable d'un site afin d'autoriser son accès à un établissement ou pour assurer, durant un transport, la garde d'informations ou de supports classifiés.
Décision d'habilitation : acte administratif autorisant, au terme de la procédure d'habilitation, le titulaire, en fonction de son besoin d'en connaître, à accéder aux informations ou aux supports classifiés 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 temporaire prise au vu d'un avis de sécurité provisoire et permettant l'accès d'une personne aux informations ou supports classifiés. Cette autorisation prend fin lors de la délivrance de la décision définitive et au plus tard six mois après avoir été accordée.
Décision de sécurité convoyeur : autorisation accordée non pas pour prendre connaissance d'informations ou de supports classifiés, mais pour assurer, durant le transport, la garde des informations ou des supports classifiés. 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 enquêteurs des ministères de l'intérieur et de la défense.
Déclassement : modification, par abaissement, du niveau de classification d'informations ou supports classifiés.
Déclassification : suppression de la classification d'informations ou supports classifiés à quelque niveau que ce soit.
Disponibilité : propriété d'une information ou d'un traitement d'être utilisable à la demande par une personne ou par un système.
Dossier d'habilitation : dossier constitué en vue de l'habilitation d'une personne. Il comporte la demande d'habilitation établie par l'autorité demanderesse et attestant le besoin d'en connaître, la notice individuelle renseignée par l'intéressé et une photographie d'identité récente.
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 rappeler à cette personne la responsabilité pénale qui lui incombe du fait de son habilitation. La signature de l'encart central du formulaire de l'engagement de responsabilité par l'intéressé vaut prise de connaissance de la décision.
Entreprise étrangère : tout soumissionnaire à un contrat dont le siège social n'est pas situé en France.
Fonctionnaire de sécurité de défense (FSD) : personne assistant le HFDS et contrôlant sous sa direction, notamment, l'exécution des mesures de protection des informations ou des supports classifiés.
Fonctionnaire de sécurité des systèmes d'information (FSSI) : personne chargée 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.
Habilitation d'une personne morale de droit privé : décision rendue à l'issue d'une procédure permettant d'apprécier les garanties offertes par la personne morale de droit privé et d'évaluer l'intérêt porté par ses dirigeants à la protection du secret de la défense nationale et aux aspects liés à la sécurité des informations ou des supports classifiés.
Haut fonctionnaire de défense et de sécurité (HFDS) : personne chargée d'assister le ministre dans l'exercice de ses attributions de sécurité, de défense et de protection du secret. Il est, dans certains ministères, appelé haut fonctionnaire correspondant de sécurité et de défense (HFCDS) ou haut fonctionnaire de défense (HFD).
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 sont acceptés et maîtrisés. L'homologation de sécurité reste valide tant que le système d'information (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.
Imputabilité : capacité à identifier l'auteur d'une action.
Information : tout renseignement ou tout élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, à un enregistrement ou à un traitement.
Information ou support classifié : procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier présentant un caractère de secret de la défense nationale (art. 413-9 du code pénal).
Intégrité : propriété assurant qu'une information ou un traitement n'a pas été modifié ou détruit de façon non autorisée.
Lieux abritant des éléments classifiés : locaux dans lesquels sont détenus des informations ou supports classifiés, quel qu'en soit le niveau.
Marquage : opération consistant à apposer sur un support classifié les mentions précisant son niveau de classification, le numéro d'exemplaire, le numéro d'enregistrement, la pagination pour un document papier et, le cas échéant, la destination exclusivement nationale.
Matériel classifié : objet, équipement, installation, système ou substance présentant un caractère de secret de la défense nationale et qui nécessite une protection appropriée au niveau Très Secret Défense, Secret Défense ou Confidentiel Défense.
Mise en éveil : démarche initiée par l'autorité d'habilitation auprès de la personne à habiliter pour la sensibiliser à ses vulnérabilités découvertes au cours de l'enquête administrative.
Mise en garde : démarche initiée par l'autorité d'habilitation visant à sensibiliser l'officier de sécurité du service employeur d'une personne sur l'existence d'éléments pouvant présenter un risque de vulnérabilité de 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 du dossier d'habilitation. Elle est exploitée par l'autorité chargée de prononcer la décision et par les services enquêteurs.
Officier de sécurité : nommé par le chef du service employeur, il est le correspondant du HFDS et des services enquêteurs. Il a pour mission, sous les ordres de son autorité d'emploi et en fonction des modalités propres à chaque structure, de fixer les règles et consignes de sécurité à mettre en œuvre concernant les personnes et les informations ou

supports classifiés et d'en contrôler l'application. Il participe à l'instruction et à la sensibilisation du personnel en matière de protection du secret. Il est chargé de la gestion des habilitations et, en liaison avec les services enquêteurs, du contrôle des accès aux zones protégées. Il dirige le bureau de protection du secret.
Ses missions sont à distinguer de celles dévolues à l'officier de sécurité dans une entreprise titulaire d'un contrat, qui est désigné par le responsable de l'entreprise après agrément de l'administration contractante.
Personne qualifiée : est qualifiée, au sens de l'article 413-10 du code pénal, la personne qui, par son état, sa profession, sa fonction ou sa mission, temporaire ou permanente, est habilitée à avoir accès à une information classifiée et a le besoin d'en connaître.
Plan d'urgence : document établi par un organisme détenteur d'informations ou supports classifiés, prévoyant, en cas de circonstances exceptionnelles, les modalités d'évacuation ou de destruction des supports d'information.
Primocontractant : est ainsi dénommé celui qui, dans le cadre d'un marché public, a conclu le contrat avec la personne publique, maître d'ouvrage, et qui confie, sous sa responsabilité, tout ou partie de l'exécution de ce contrat à un ou plusieurs sous-traitants.
Procédure d'habilitation : procédure visant à s'assurer qu'une personne peut, sans risque pour la défense nationale ou pour sa propre sécurité, connaître des informations ou supports classifiés dans l'exercice de ses fonctions.
Reclassement : modification, par relèvement, du niveau de classification d'informations ou de supports classifiés.
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 motivation est régie par la loi n° 79-587 du 11 juillet 1979 sur la motivation des actes administratifs.
Réseau de sécurité : ensemble des moyens humains, matériels et organisationnels qui permettent l'acheminement en toute sécurité des informations ou supports classifiés à un niveau déterminé (et en deçà), 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.
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.
Responsable de l'entreprise : personne représentant une personne morale pour un contrat et ayant le pouvoir d'engager celle-ci.
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 enquêteur : service d'Etat chargé de procéder aux investigations sur les personnes préalablement à une décision d'habilitation ou dans le cadre d'un contrôle élémentaire, d'évaluer l'aptitude des locaux et de contrôler les mesures de sécurité. Ces services rendent leurs conclusions sous la forme d'avis de sécurité.
Soumissionnaire : toute personne morale candidate à un contrat. Dans les cas précisément identifiés dans la présente instruction, le soumissionnaire peut être une personne physique.
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 et les caractéristiques

physiques, permettant de recevoir, de conserver ou de restituer des informations ou des données.
Système d'information : ensemble des moyens informatiques ayant pour finalité d'élaborer, de traiter, de stocker, d'acheminer, de présenter ou de détruire des informations.
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).
Titulaire : toute personne attributaire d'un contrat. Lorsque le contrat est un marché public avec sous-traitance, le titulaire de ce marché est appelé "primocontractant".
Travaux classifiés : prestations, quelle qu'en soit la nature, nécessitant l'accès à des informations ou à des supports classifiés.
Vulnérabilité : fait relatif à la situation d'une personne et qui amoindrit les garanties qu'elle présente pour la protection des informations ou supports classifiés. Il s'agit d'une fragilité qui peut donner lieu à des pressions de diverses natures et qui doit être prise en compte pour accorder avec ou sans restriction, pour refuser ou pour retirer l'accès aux informations ou supports classifiés.
Zone protégée : zone créée par arrêté des ministres intéressés et faisant l'objet d'une interdiction d'accès sans autorisation, sanctionnée pénalement en cas d'infraction (articles 413-7 et R. 413-1 à R. 413-5 du code pénal).
Zone réservée : local ou emplacement qui fait l'objet de mesures de protection matérielle particulières et dont l'accès est réglementé et subordonné à des conditions spéciales.

## Index

Déclassement
Déclassification
Disponibilité
Dossier d’habilitation
E
Engagement de responsabilité
H
Haut fonctionnaire de défense et de sécurité
Homologation de sécurité
I
Identification
L
Lieux abritant des éléments classifiés
M
Marquage
Matériel classifié
Mise en éveil
Mise en garde
N
Notice individuelle
O
Officier de sécurité
P
Procédure d’habilitation
R
Reclassement
Refus d’habilitation
Renouvellement d’habilitation
Réseau de sécurité
S
Sécurité des systèmes d’information
Sensibilisation
Service enquêteur
Système d’information
T
Timbre
V
Vulnérabilité
Z
Zone protégée
Zone réservée

## A N N E X E S
## TABLE DES ANNEXES

## A N N E X E 1
## TEXTES DE RÉFÉRENCE

### Code pénal

### Partie législative

121-2
Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7, 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, sous réserve des dispositions du quatrième alinéa de l'article 121-3.
226-13
La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire est punie d'un an d'emprisonnement et de 15 000 euros d'amende.
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 euros d'amende.
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 euros d'amende.
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 euros d'amende.

413-7

Est puni de six mois d'emprisonnement et de 7 500 euros 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.

413-9

Présentent un caractère de secret de la défense nationale au sens de la présente section les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès.

Peuvent faire l'objet de telles mesures les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers dont la divulgation ou auxquels l'accès 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 procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers présentant un caractère de secret de la défense nationale et les autorités chargées de définir les modalités selon lesquelles est organisée leur protection sont déterminés par décret en Conseil d'Etat.

413-10

Est puni de sept ans d'emprisonnement et de 100 000 euros 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 procédé, objet, document, information, réseau informatique, 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 d'en donner l'accès à une personne non qualifiée ou 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 accéder à, détruire, détourner, soustraire, reproduire ou divulguer le procédé, objet, document, information, réseau informatique, 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 euros d'amende.

413-11

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

1° S'assurer la possession, accéder à, ou prendre connaissance d'un procédé, objet, document, information, réseau informatique, 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 procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier ;

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

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.

414-7
Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent titre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par 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.
414-8
Les dispositions des articles 411-1 à 411-11 et 413-1 à 413-12 sont applicables aux actes mentionnés par ces dispositions qui seraient commis au préjudice :
1° Des puissances signataires du traité de l'Atlantique Nord ;
2° De l'organisation du traité de l'Atlantique Nord.
414-9
Les dispositions des articles 411-6 à 411-11 et 413-9 à 413-12 sont applicables :
1° Aux informations échangées en vertu d'un accord de sécurité relatif à la protection des informations classifiées, conclu entre la France et un ou des Etats étrangers ou une organisation internationale, régulièrement approuvé et publié ;
2° Aux informations échangées entre la France et une institution ou un organe de l'Union européenne et classifiées en vertu des règlements de sécurité de ces derniers qui ont fait l'objet d'une publication au Journal officiel de l'Union européenne.
434-4
Est puni de trois ans d'emprisonnement et de 45 000 euros d'amende le fait, en vue de faire obstacle à la manifestation de la vérité :
1° De modifier l'état des lieux d'un crime ou d'un délit soit par l'altération, la falsification ou l'effacement des traces ou indices, soit par l'apport, le déplacement ou la suppression d'objets quelconques ;
2° De détruire, soustraire, receler ou altérer un document public ou privé ou un objet de nature à faciliter la découverte d'un crime ou d'un délit, la recherche des preuves ou la condamnation des coupables.
Lorsque les faits prévus au présent article sont commis par une personne qui, par ses fonctions, est appelée à concourir à la manifestation de la vérité, la peine est portée à cinq ans d'emprisonnement et à 75 000 euros d'amende.
414-7
Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent titre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par 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.
226-13
La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende.
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 euros d'amende.
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 euros d'amende.

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 euros d'amende.

## Partie réglementaire

R. 413-1

Les zones protégées que constituent les locaux et terrains clos mentionnés à l'article 413-7 sont délimitées dans les conditions prévues à la présente section.

R. 413-2

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.

Les autorités dont relèvent les services, établissements ou entreprises concernés peuvent recevoir par décret délégation pour déterminer ce besoin de protection.

R. 413-3

Lorsque l'activité principale du service, de l'établissement ou de l'entreprise relève du ministre ayant déterminé le besoin de protection, l'implantation et les limites des zones protégées sont fixées par arrêté de ce ministre.

Lorsque l'activité principale du service, de l'établissement ou de l'entreprise 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.

Les autorités dont relèvent ces services, établissements ou entreprises peuvent recevoir par décret délégation pour prendre les arrêtés prévus par le présent article.

R. 413-4

L'arrêté portant création d'une zone protégée est notifié au chef du service, de l'établissement ou de l'entreprise. Celui-ci prend alors, sous le contrôle de l'autorité qui a déterminé le besoin de protection, toutes dispositions pour rendre apparentes les limites de la zone et les mesures d'interdiction dont elle est l'objet.

Un exemplaire de l'arrêté est adressé, pour leur information et éventuellement aux fins d'application des dispositions qui les concernent, au ministre de l'intérieur et aux préfets territorialement compétents.

R. 413-5

L'autorisation de pénétrer dans la zone protégée est donnée par le chef du service, de l'établissement ou de l'entreprise, selon les directives et sous le contrôle du ministre ayant déterminé le besoin de protection.

Toutefois, lorsque la zone a été instituée pour protéger des recherches, études ou fabrications qui doivent être tenues secrètes dans l'intérêt de la défense nationale, l'autorisation est délivrée par le ministre qui a déterminé le besoin de protection.

Dans tous les cas, l'autorisation est délivrée par écrit. Elle peut être retirée à tout moment dans les mêmes formes.

## Code de procédure pénale

56-4

I. - Lorsqu'une perquisition est envisagée dans un lieu précisément identifié, abritant des éléments couverts par le secret de la défense nationale, la perquisition ne peut être

réalisée que par un magistrat en présence du président de la Commission consultative du secret de la défense nationale. Ce dernier peut être représenté par un membre de la commission ou par des délégués, dûment habilités au secret de la défense nationale, qu'il désigne selon des modalités déterminées par décret en Conseil d'Etat. Le président ou son représentant peut être assisté de toute personne habilitée à cet effet.
La liste des lieux visés au premier alinéa est établie de façon précise et limitative par arrêté du Premier ministre. Cette liste, régulièrement actualisée, est communiquée à la Commission consultative du secret de la défense nationale ainsi qu'au ministre de la justice, qui la rendent accessible aux magistrats de façon sécurisée. Le magistrat vérifie si le lieu dans lequel il souhaite effectuer une perquisition figure sur cette liste.
Les conditions de délimitation des lieux abritant des éléments couverts par le secret de la défense nationale sont déterminées par décret en Conseil d'Etat.
Le fait de dissimuler dans les lieux visés à l'alinéa précédent des procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers non classifiés, en tentant de les faire bénéficier de la protection attachée au secret de la défense nationale, expose son auteur aux sanctions prévues à l'article 434-4 du code pénal.
La perquisition ne peut être effectuée qu'en vertu d'une décision écrite du magistrat qui indique au président de la Commission consultative du secret de la défense nationale les informations utiles à l'accomplissement de sa mission. Le président de la commission ou son représentant se transporte sur les lieux sans délai. Au commencement de la perquisition, le magistrat porte à la connaissance du président de la commission ou de son représentant, ainsi qu'à celle du chef d'établissement ou de son délégué, ou du responsable du lieu, la nature de l'infraction ou des infractions sur lesquelles portent les investigations, les raisons justifiant la perquisition, son objet et les lieux visés par cette perquisition.
Seul le président de la Commission consultative du secret de la défense nationale, son représentant et, s'il y a lieu, les personnes qui l'assistent peuvent prendre connaissance d'éléments classifiés découverts sur les lieux. Le magistrat ne peut saisir, parmi les éléments classifiés, que ceux relatifs aux infractions sur lesquelles portent les investigations. Si les nécessités de l'enquête justifient que les éléments classifiés soient saisis en original, des copies sont laissées à leur détenteur.
Chaque élément classifié saisi est, après inventaire par le président de la commission consultative, placé sous scellé. Les scellés sont remis au président de la Commission consultative du secret de la défense nationale qui en devient gardien. Les opérations relatives aux éléments classifiés saisis ainsi que l'inventaire de ces éléments font l'objet d'un procès-verbal qui n'est pas joint au dossier de la procédure et qui est conservé par le président de la commission consultative.
La déclassification et la communication des éléments mentionnés dans l'inventaire relèvent de la procédure prévue par les articles L. 2312-4 et suivants du code de la défense.
II. - Lorsqu'à l'occasion d'une perquisition un lieu se révèle abriter des éléments couverts par le secret de la défense nationale, le magistrat présent sur le lieu ou immédiatement avisé par l'officier de police judiciaire en informe le président de la Commission consultative du secret de la défense nationale. Les éléments classifiés sont placés sous scellés, sans en prendre connaissance, par le magistrat ou l'officier de police judiciaire qui les a découverts, puis sont remis ou transmis, par tout moyen en conformité avec la réglementation applicable aux secrets de la défense nationale, au président de la commission afin qu'il en assure la garde. Les opérations relatives aux éléments classifiés font l'objet d'un procès-verbal qui n'est pas joint au dossier de la procédure. La déclassification et la communication des éléments ainsi placés sous scellés relèvent de la procédure prévue par les articles L. 2312-4 et suivants du code de la défense.

III. - Les dispositions du présent article sont édictées à peine de nullité.

# Code de la défense

## Partie législative

L. 1111-1
La stratégie de sécurité nationale a pour objet d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République, et de déterminer les réponses que les pouvoirs publics doivent y apporter.
L'ensemble des politiques publiques concourt à la sécurité nationale.
La politique de défense a pour objet d'assurer l'intégrité du territoire et la protection de la population contre les agressions armées. Elle contribue à la lutte contre les autres menaces susceptibles de mettre en cause la sécurité nationale. Elle pourvoit au respect des alliances, des traités et des accords internationaux et participe, dans le cadre des traités européens en vigueur, à la politique européenne de sécurité et de défense commune.
L. 2311-1
Les règles relatives à la définition des informations concernées par les dispositions du présent chapitre sont définies par l'article 413-9 du code pénal.
L. 2312-1
La Commission consultative du secret de la défense nationale 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.
L. 2312-2
La Commission consultative du secret de la défense nationale comprend cinq membres :
1° 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 ;
2° Un député, désigné pour la durée de la législature par le président de l'Assemblée nationale ;
3° 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.
L. 2312-3
Les crédits nécessaires à la commission pour l'accomplissement de sa mission sont inscrits au programme de la mission "Direction de l'action du Gouvernement" relatif à la protection des droits et des libertés fondamentales.

Le président est ordonnateur des dépenses de la commission. Il nomme les agents de la commission.
L. 2312-4
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.
L. 2312-5
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.
Pour l'accomplissement de sa mission, la commission, ou sur délégation de celle-ci, son président, est habilitée, nonobstant les dispositions des articles 56 et 97 du code de procédure pénale, à procéder à l'ouverture des scellés des éléments classifiés qui lui sont remis. La commission en fait mention dans son procès-verbal de séance. Les documents sont restitués à l'autorité administrative par la commission lors de la transmission de son avis.
La commission établit son règlement intérieur.
L. 2312-6
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 prennent toutes mesures utiles pour la faciliter.
L. 2312-7
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.
L. 2312-8
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 L. 2312-7, 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.
L. 4121-2
Les opinions ou croyances, notamment philosophiques, religieuses ou politiques, sont libres.
Elles ne peuvent cependant être exprimées qu'en dehors du service et avec la réserve exigée par l'état militaire. Cette règle s'applique à tous les moyens d'expression. Elle ne fait pas obstacle au libre exercice des cultes dans les enceintes militaires et à bord des bâtiments de la flotte.

Indépendamment des dispositions du code pénal relatives à la violation du secret de la défense nationale et du secret professionnel, les militaires doivent faire preuve de discrétion 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 loi, les militaires ne peuvent être déliés de cette obligation que par décision expresse de l'autorité dont ils dépendent.
L'usage de moyens de communication et d'information, quels qu'ils soient, peut être restreint ou interdit pour assurer la protection des militaires en opération, l'exécution de leur mission ou la sécurité des activités militaires.

## Partie réglementaire

R.* 1132-1
Le secrétariat général de la défense et de la sécurité nationale constitue un service du Premier ministre.
R.* 1132-2
Le secrétaire général de la défense et de la sécurité nationale assure le secrétariat du conseil de défense et de sécurité nationale. Conformément aux directives du Président de la République et du Premier ministre, il conduit, en liaison avec les départements ministériels concernés, les travaux préparatoires aux réunions. Il prépare les relevés de décisions, notifie les décisions prises et en suit l'exécution.
R.* 1132-3
Le secrétaire général de la défense et de la sécurité nationale assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. A ce titre :
1° Il anime et coordonne les travaux interministériels relatifs à la politique de défense et de sécurité nationale et aux politiques publiques qui y concourent ;
2° En liaison avec les départements ministériels concernés, il suit l'évolution des crises et des conflits internationaux pouvant affecter les intérêts de la France en matière de défense et de sécurité nationale et étudie les dispositions susceptibles d'être prises. Il est associé à la préparation et au déroulement des négociations ou des réunions internationales ayant des implications sur la défense et la sécurité nationale et est tenu informé de leurs résultats ;
3° Il propose, diffuse et fait appliquer et contrôler les mesures nécessaires à la protection du secret de la défense nationale. Il prépare la réglementation interministérielle en matière de défense et de sécurité nationale, en assure la diffusion et en suit l'application ;
4° En appui du coordonnateur national du renseignement, il concourt à l'adaptation du cadre juridique dans lequel s'inscrit l'action des services de renseignement et à la planification de leurs moyens et assure l'organisation des groupes interministériels d'analyse et de synthèse en matière de renseignement ;
5° Il élabore la planification interministérielle de défense et de sécurité nationale, veille à son application et conduit des exercices interministériels la mettant en œuvre. Il coordonne la préparation et la mise en œuvre des mesures de défense et de sécurité nationale incombant aux divers départements ministériels et s'assure de la coordination des moyens civils et militaires prévus en cas de crise majeure ;
6° Il s'assure que le Président de la République et le Gouvernement disposent des moyens de commandement et de communications électroniques nécessaires en matière de défense et de sécurité nationale et en fait assurer le fonctionnement ;
7° Il propose au Premier ministre et met en œuvre la politique du Gouvernement en matière de sécurité des systèmes d'information. Il dispose à cette fin du service à compétence nationale dénommé "Agence nationale de la sécurité des systèmes d'information" ;

8° Il veille à la cohérence des actions entreprises en matière de politique de recherche scientifique et de projets technologiques intéressant la défense et la sécurité nationale et contribue à la protection des intérêts nationaux stratégiques dans ce domaine.
R. 1143-1
Pour l'exercice de leurs responsabilités en matière de défense et de sécurité :
1° Le ministre de la défense et le ministre des affaires étrangères désignent, pour leurs départements ministériels respectifs, un haut fonctionnaire correspondant de défense et de sécurité, dont ils précisent par arrêté les modalités selon lesquelles ils exercent leurs missions ;
2° Le ministre de l'intérieur est assisté par un haut fonctionnaire de défense ;
3° Les autres ministres sont assistés par un haut fonctionnaire de défense et de sécurité.
R. 1143-2
Les hauts fonctionnaires mentionnés à l'article R. 1143-1 relèvent directement du ministre. Pour l'exercice de leur mission, ils ont autorité sur l'ensemble des directions et services du ministère.
Ils disposent en propre d'un service spécialisé de défense, ou de défense et de sécurité. Ils peuvent assister plusieurs ministres et disposer d'un ou de plusieurs hauts fonctionnaires adjoints.
Ils sont en liaison permanente avec le secrétaire général de la défense et de la sécurité nationale et avec leurs homologues des autres ministères.
R. 1143-5
Les hauts fonctionnaires mentionnés à l'article R. 1143-1 animent et coordonnent, au sein du département dont ils relèvent, la politique en matière de défense, de vigilance, de prévention de crise et de situation d'urgence. Ils contrôlent la préparation des mesures d'application. A cet effet :
1° Ils veillent à la diffusion des plans, des doctrines d'emploi et des directives gouvernementales en matière de défense et de sécurité et coordonnent l'élaboration des plans ministériels et des instructions d'application ;
2° Ils s'assurent de la connaissance et de la bonne application de la planification de défense et de sécurité au sein du département ministériel dont ils relèvent, par des actions de sensibilisation et de formation et par des exercices interministériels et ministériels de mise en œuvre des plans ;
3° Ils sont chargés de l'organisation et du maintien en condition opérationnelle du dispositif ministériel de situation d'urgence ; ils s'assurent notamment de la mise en place et du bon fonctionnement d'un dispositif permanent de veille et d'alerte ;
4° Ils s'assurent de l'élaboration et de la mise en œuvre des politiques de sécurité dans les secteurs d'activité relevant de leur ministère, notamment lorsqu'ils sont reconnus d'importance vitale ;
5° Ils conseillent le ministre sur les mesures de protection des biens et des personnes au sein de leur ministère ; ils peuvent être chargés de l'application de ces mesures ;
6° Ils veillent à la protection du patrimoine scientifique et technique ;
7° Ils veillent au déploiement dans leur ministère des moyens sécurisés de communication électronique gouvernementale et des outils de situation d'urgence ; ils s'assurent de leur bon fonctionnement ;
8° Ils animent la politique de sécurité des systèmes d'information et contrôlent l'application de celle-ci ;
9° Ils peuvent participer, dans le cadre fixé par le ministre dont ils relèvent et sous l'égide du secrétariat général de la défense et de la sécurité nationale, à la mise en œuvre de la politique nationale en matière d'intelligence économique.
R. 1143-6
Les hauts fonctionnaires mentionnés à l'article R. 1143-1 sont responsables, au sein du département ministériel dont ils relèvent, de l'application des dispositions relatives à la

sécurité de défense et à la protection du secret prévues par les articles R. 2311-1 et suivants du code de la défense relatifs à la protection du secret de la défense nationale.
Dans les organismes rattachés à ce même département ministériel, ces hauts fonctionnaires sont responsables de la diffusion des dispositions relatives à la sécurité de défense et à la protection du secret et en contrôlent l'application.

R. 1143-8

Les hauts fonctionnaires mentionnés à l'article R. 1143-1 adressent chaque année à leur ministre et au secrétaire général de la défense et de la sécurité nationale un compte rendu de leurs activités.
Le secrétaire général de la défense et de la sécurité nationale présente au Président de la République et au Premier ministre la synthèse de ces comptes rendus.

R. 2311-1

Les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers présentant un caractère de secret de la défense nationale sont dénommés dans le présent chapitre : "informations et supports classifiés".

R. 2311-2

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

R. 2311-3

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

R. 2311-4

Les informations et supports classifiés portent la mention de leur niveau de classification.
Les informations et supports classifiés qui ne doivent être communiqués, totalement ou partiellement, en raison de leur contenu qu'à certaines organisations internationales ou à certains Etats ou à leurs ressortissants, portent, en sus de la mention de leur niveau de classification, une mention particulière précisant les Etats, leurs ressortissants ou les organisations internationales pouvant y avoir accès.
Les informations et supports classifiés qui ne doivent en aucun cas être communiqués totalement ou partiellement à des organisations internationales, à des Etats étrangers ou à leurs ressortissants portent, en sus de la mention de leur niveau de classification, la mention particulière "Spécial France".
Les modifications du niveau de classification et la déclassification ainsi que les modifications et les suppressions des mentions particulières sont décidées par les autorités qui ont procédé à la classification.

R. 2311-5

Le Premier ministre détermine les critères et les modalités d'organisation de la protection des informations et supports classifiés au niveau Très Secret Défense.
Pour les informations et supports 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 et supports qu'il y a lieu de classifier à ce niveau.

R. 2311-6

Dans les conditions fixées par le Premier ministre, les informations et supports classifiés au niveau Secret Défense ou Confidentiel Défense ainsi que les modalités d'organisation de leur protection sont déterminés par chaque ministre pour les administrations et les organismes relevant de son département ministériel.

R. 2311-6-1

Les systèmes d'information contenant des informations classifiées font l'objet, préalablement à leur emploi, d'une homologation de sécurité à un niveau au moins égal au niveau de classification de ces informations.

La protection de ces systèmes d'information doit, dans des conditions fixées par arrêté du Premier ministre, au regard notamment des menaces pesant sur la disponibilité et l'intégrité de ces systèmes et sur la confidentialité et l'intégrité des informations qu'ils contiennent, être assurée par des dispositifs, matériels ou logiciels agréés par l'Agence nationale de la sécurité des systèmes d'information.

L'autorité responsable de l'emploi du système d'information atteste de l'aptitude du système à assurer notamment, au niveau requis, la disponibilité et l'intégrité du système ainsi que la confidentialité et l'intégrité des informations que ce dernier contient. Cette attestation vaut homologation de sécurité. Un arrêté du Premier ministre fixe les conditions d'application de ces dispositions.

R. 2311-7

Nul n'est qualifié pour connaître des informations ou supports classifiés s'il n'a fait au préalable l'objet d'une décision d'habilitation et s'il n'a besoin, selon l'appréciation de l'autorité d'emploi sous laquelle il est placé, au regard notamment du catalogue des emplois justifiant une habilitation établi par cette autorité, de les connaître pour l'exercice de sa fonction ou l'accomplissement de sa mission.

R. 2311-7-1

Nul n'est qualifié pour accéder à un système d'information ou à ses dispositifs, matériels ou logiciels, de protection, lorsque cet accès permet de connaître des informations classifiées qui y sont contenues ou de modifier les dispositifs de protection de ces informations, s'il n'a fait au préalable l'objet d'une décision d'habilitation et s'il n'a besoin, selon l'appréciation de l'autorité responsable de l'emploi du système, d'y accéder pour l'exercice de sa fonction ou l'accomplissement de sa mission.

R. 2311-7-2

Les habilitations mentionnées aux articles R. 2311-7 et R. 2311-7-1 peuvent être délivrées à des personnes physiques ainsi qu'à des personnes morales.

R. 2311-8

La décision d'habilitation précise le niveau de classification des informations et supports classifiés dont le titulaire peut connaître ainsi que le ou les emplois qu'elle concerne. 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.

R. 2311-8-1

Chaque ministre peut déléguer par arrêté au préfet territorialement compétent la signature des décisions d'habilitation à connaître des informations couvertes par le secret de la défense nationale des agents de son département ministériel placés sous l'autorité du préfet et des personnes employées dans des organismes relevant de ses attributions.

R. 2311-8-2

Le ministre de la défense peut déléguer, par arrêté, ses pouvoirs en matière de décisions

d’habilitation à connaître des informations et supports couverts par le secret de la défense nationale, aux autorités suivantes, relevant de son département ministériel :
1° Les chefs d’état-major ;
2° Le secrétaire général pour l’administration, les directeurs généraux, les directeurs et chefs de service d’administration centrale ;
3° Le chef du contrôle général des armées et les membres des corps d’inspection directement rattachés au ministre ;
4° Les commandants des formations, les commandants organiques et opérationnels des forces et interarmées, les commandants des formations administratives ou des organismes administrés comme tels, ainsi que les directeurs ou chefs des organismes n’appartenant pas à l’administration centrale du ministère de la défense.
Les délégataires mentionnés aux 1° à 4° peuvent déléguer leur signature à leurs subordonnés.
R. 2311-9
Le ministre de la défense ou le commandement est habilité à restreindre l’usage de moyens de communication et d’information, quels qu’ils soient, pour assurer la protection des militaires en opération, l’exécution de la mission ou la sécurité des activités militaires.
La détention et l’usage d’appareils photographiques, cinématographiques, téléphoniques, télématiques ou enregistreurs ainsi que de postes émetteurs ou récepteurs de radiodiffusion ou télévision dans les enceintes et établissements militaires ou en campagne, dans les cantonnements et véhicules, ainsi qu’à bord des bâtiments de la flotte et des aéronefs, peuvent être soumis à autorisation préalable.
La publication ou la cession de films, de photographies ou d’enregistrements pris dans les enceintes, établissements militaires, bâtiments de la flotte et aéronefs, ou à l’occasion d’opérations, de manœuvre ou de toute autre activité militaire est soumise à l’autorisation préalable du commandant de la formation administrative.
R. 2311-9-1
La liste des lieux abritant des éléments classifiés des éléments couverts par le secret de la défense nationale mentionnée au deuxième alinéa de l’article 56-4 du code de procédure pénale est établie, par arrêté du Premier ministre, sur proposition des ministres intéressés.
La liste désigne les lieux en cause dans des conditions de nature à permettre l’identification exacte de ceux-ci par la Commission consultative du secret de la défense nationale et les magistrats. Elle peut comporter des catégories de locaux, classés par département ministériel, lorsque cette désignation suffit à l’identification des lieux ou, dans le cas contraire, des localisations individuelles. Elle est régulièrement actualisée.
La liste est transmise au ministre de la justice et au président de la Commission consultative du secret de la défense nationale. Le ministre de la justice met en œuvre, dans des conditions définies par arrêté du Premier ministre, un accès sécurisé à la liste, de nature à préserver la confidentialité de celle-ci et permettant à chaque magistrat de vérifier si le lieu dans lequel il souhaite effectuer une perquisition figure sur cette liste.
R. 2311-10
Sous l’autorité du Premier ministre, le secrétaire général de la défense et de la sécurité 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. Il a qualité d’autorité nationale de sécurité pour le secret de la défense nationale, pour l’application des accords et traités internationaux prévoyant une telle autorité.
Le secrétaire général de la défense et de la sécurité nationale veille à la mise en œuvre des mesures mentionnées au premier alinéa. 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.
Les attributions de sécurité de défense définies ci-dessus n’affectent pas les

responsabilités propres des ministres en cette matière.
R. 2311-10-1
Le secrétaire général de la défense et de la sécurité nationale peut, en sa qualité d'autorité nationale de sécurité pour le secret de la défense nationale, nommer dans des domaines particuliers, notamment dans le domaine industriel, sur proposition du ou des ministres intéressés, une autorité de sécurité déléguée.
R. 2311-11
Le secrétaire général de la défense et de la sécurité nationale, conformément aux dispositions de l'article R. 2311-10, prescrit, coordonne et contrôle l'application des mesures propres à assurer la protection du secret dans les rapports entre la France et les Etats étrangers.
Il assure, en application des accords internationaux, la sécurité des informations classifiées confiées à la France.
Il définit les mesures de protection des informations et supports dont la France est détentrice, qui ont été classifiés par un Etat étranger ou une organisation internationale et qui ne portent pas la mention d'un niveau de classification équivalent à ceux définis à l'article R. 2311-2.
Il définit les mesures propres à assurer la protection des informations nationales confiées à des Etats étrangers ou à des organisations internationales.
D.* 2311-12
Pour l'exercice de ses attributions mentionnées aux articles R. 2311-10 et R. 2311-11, le secrétaire général de la défense et de la sécurité nationale dispose d'un service de sécurité de défense.
R. 2312-1
Le président de la commission consultative du secret de la défense nationale peut lors de perquisitions réalisées par un magistrat, en application du I de l'article 56-4 du code de procédure pénale, se faire représenter par un membre de la commission ou un délégué choisi sur une liste établie par la commission. En ce cas, il procède à la désignation de ce représentant dès la réception de la décision du magistrat.
Peuvent figurer sur la liste le secrétaire général et les anciens membres de la Commission consultative du secret de la défense nationale, ainsi que des personnes présentant des garanties au regard des deux objectifs constitutionnels de recherche des auteurs d'infractions pénales et de sauvegarde des intérêts fondamentaux de la nation, et n'exerçant pas de fonctions susceptibles de leur donner à connaître de la procédure judiciaire à l'origine de la perquisition. Les personnes figurant sur la liste doivent être habilitées au secret de la défense nationale pour l'accomplissement de leur mission.
Le choix du représentant doit permettre la présence effective de celui-ci sur le lieu de la perquisition envisagée par le magistrat, pendant toute la durée prévisible de celle-ci.
R. 2312-2
Le magistrat et le représentant désigné par le président de la Commission consultative du secret de la défense nationale sont, par tous moyens, immédiatement informés de la désignation réalisée par le président.
R. 2313-1
Les règles relatives aux services d'archives relevant du ministère de la défense sont définies par le décret n° 79-1035 du 3 décembre 1979 relatif aux archives de la défense et par l'article 4 du décret n° 79-1037 du 3 décembre 1979 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques.

## Code du patrimoine

L. 211-1

Les archives sont l'ensemble des documents, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité.
L. 212-2
A l'expiration de leur période d'utilisation courante, les archives publiques autres que celles mentionnées à l'article L. 212-3 font l'objet d'une sélection pour séparer les documents à conserver des documents dépourvus d'utilité administrative ou d'intérêt historique ou scientifique, destinés à l'élimination.
La liste des documents ou catégories de documents destinés à l'élimination ainsi que les conditions de leur élimination sont fixées par accord entre l'autorité qui les a produits ou reçus et l'administration des archives.
L. 213-1
Les archives publiques sont, sous réserve des dispositions de l'article L. 213-2, communicables de plein droit.
L'accès à ces archives s'exerce dans les conditions définies pour les documents administratifs à l'article 4 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.
L. 213-2
Par dérogation aux dispositions de l'article L. 213-1 :
I. - Les archives publiques sont communicables de plein droit à l'expiration d'un délai de :
1° Vingt-cinq ans à compter de la date du document ou du document le plus récent inclus dans le dossier :
a) Pour les documents dont la communication porte atteinte au secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif, à la conduite des relations extérieures, à la monnaie et au crédit public, au secret en matière commerciale et industrielle, à la recherche par les services compétents des infractions fiscales et douanières ou au secret en matière de statistiques sauf lorsque sont en cause des données collectées au moyen de questionnaires ayant trait aux faits et comportements d'ordre privé mentionnées aux 4° et 5° ;
b) Pour les documents mentionnés au 1° du I de l'article 6 de la loi n° 78-753 du 17 juillet 1978, à l'exception des documents produits dans le cadre d'un contrat de prestation de services exécuté pour le compte d'une ou de plusieurs personnes déterminées lorsque ces documents entrent, du fait de leur contenu, dans le champ d'application des 3° ou 4° du présent I ;
2° Vingt-cinq ans à compter de la date du décès de l'intéressé, pour les documents dont la communication porte atteinte au secret médical. Si la date du décès n'est pas connue, le délai est de cent vingt ans à compter de la date de naissance de la personne en cause ;
3° Cinquante ans à compter de la date du document ou du document le plus récent inclus dans le dossier, pour les documents dont la communication porte atteinte au secret de la défense nationale, aux intérêts fondamentaux de l'Etat dans la conduite de la politique extérieure, à la sûreté de l'Etat, à la sécurité publique, à la sécurité des personnes ou à la protection de la vie privée, à l'exception des documents mentionnés aux 4° et 5°. Le même délai s'applique aux documents qui portent une appréciation ou un jugement de valeur sur une personne physique, nommément désignée ou facilement identifiable, ou qui font apparaître le comportement d'une personne dans des conditions susceptibles de lui porter préjudice.
Le même délai s'applique aux documents relatifs à la construction, à l'équipement et au fonctionnement des ouvrages, bâtiments ou parties de bâtiment utilisés pour la détention des personnes ou recevant habituellement des personnes détenues. Ce délai est décompté depuis la fin de l'affectation à ces usages des ouvrages, bâtiments ou parties de bâtiment en cause ;

4° Soixante-quinze ans à compter de la date du document ou du document le plus récent inclus dans le dossier, ou un délai de vingt-cinq ans à compter de la date du décès de l'intéressé si ce dernier délai est plus bref :
a) Pour les documents dont la communication porte atteinte au secret en matière de statistiques lorsque sont en cause des données collectées au moyen de questionnaires ayant trait aux faits et comportements d'ordre privé ;
b) Pour les documents relatifs aux enquêtes réalisées par les services de la police judiciaire ;
c) Pour les documents relatifs aux affaires portées devant les juridictions, sous réserve des dispositions particulières relatives aux jugements, et à l'exécution des décisions de justice ;
d) Pour les minutes et répertoires des officiers publics ou ministériels ;
e) Pour les registres de naissance et de mariage de l'état civil, à compter de leur clôture ;
5° Cent ans à compter de la date du document ou du document le plus récent inclus dans le dossier, ou un délai de vingt-cinq ans à compter de la date du décès de l'intéressé si ce dernier délai est plus bref, pour les documents mentionnés au 4° qui se rapportent à une personne mineure.
Les mêmes délais s'appliquent aux documents couverts ou ayant été couverts par le secret de la défense nationale dont la communication est de nature à porter atteinte à la sécurité de personnes nommément désignées ou facilement identifiables. Il en est de même pour les documents relatifs aux enquêtes réalisées par les services de la police judiciaire, aux affaires portées devant les juridictions, sous réserve des dispositions particulières relatives aux jugements, et à l'exécution des décisions de justice dont la communication porte atteinte à l'intimité de la vie sexuelle des personnes.
II. - Ne peuvent être consultées les archives publiques dont la communication est susceptible d'entraîner la diffusion d'informations permettant de concevoir, fabriquer, utiliser ou localiser des armes nucléaires, biologiques, chimiques ou toutes autres armes ayant des effets directs ou indirects de destruction d'un niveau analogue.
III. - L'administration des archives peut également, après accord de l'autorité dont émanent les documents, décider l'ouverture anticipée de fonds ou parties de fonds d'archives publiques.
L. 213-3
I. - L'autorisation de consultation de documents d'archives publiques avant l'expiration des délais fixés au I de l'article L. 213-2 peut être accordée aux personnes qui en font la demande dans la mesure où l'intérêt qui s'attache à la consultation de ces documents ne conduit pas à porter une atteinte excessive aux intérêts que la loi a entendu protéger.
Sous réserve, en ce qui concerne les minutes et répertoires des notaires, des dispositions de l'article 23 de la loi du 25 ventôse an xi contenant organisation du notariat, l'autorisation est accordée par l'administration des archives aux personnes qui en font la demande après accord de l'autorité dont émanent les documents.
Le temps de réponse à une demande de consultation ne peut excéder deux mois à compter de l'enregistrement de la demande.
II. - L'administration des archives peut également, après accord de l'autorité dont émanent les documents, décider l'ouverture anticipée de fonds ou parties de fonds d'archives publiques.
L. 213-4
Le versement des documents d'archives publiques émanant du Président de la République, du Premier ministre et des autres membres du Gouvernement peut être assorti de la signature entre la partie versante et l'administration des archives d'un protocole relatif aux conditions de traitement, de conservation, de valorisation ou de communication du fonds versé, pendant la durée des délais prévus à l'article L. 213-2. Les stipulations de ce protocole peuvent également s'appliquer aux documents d'archives

publiques émanant des collaborateurs personnels de l'autorité signataire.
Pour l'application de l'article L. 213-3, l'accord de la partie versante requis pour autoriser la consultation ou l'ouverture anticipée du fonds est donné par le signataire du protocole.
Le protocole cesse de plein droit d'avoir effet en cas de décès du signataire et, en tout état de cause, à la date d'expiration des délais prévus à l'article L. 213-2.
Les documents d'archives publiques versés antérieurement à la publication de la loi n° 2008-696 du 15 juillet 2008 relative aux archives demeurent régis par les protocoles alors signés. Toutefois, les clauses de ces protocoles relatives au mandataire désigné par l'autorité signataire cessent d'être applicables vingt-cinq ans après le décès du signataire.
L. 213-5
Toute administration détentrice d'archives publiques ou privées est tenue de motiver tout refus qu'elle oppose à une demande de communication de documents d'archives.
L. 213-6
Les services publics d'archives qui reçoivent des archives privées à titre de don, de legs, de cession ou de dépôt sont tenus de respecter les stipulations du donateur, de l'auteur du legs, du cédant ou du déposant quant à la conservation et à la communication de ces archives.
L. 213-7
Les dispositions des articles L. 213-1 à L. 213-3, L. 213-5, L. 213-6 et L. 213-8 sont affichées de façon apparente dans les locaux ouverts au public des services publics d'archives.
Article 26 de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires :
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.

## A N N E X E 2
## GUIDE DE CLASSIFICATION : RECOMMANDATIONS POUR L'ÉLABORATION DE L'INSTRUCTION MINISTÉRIELLE PARTICULIÈRE RELATIVE À LA PROTECTION DU SECRET

Il revient à chaque ministre, pour ce qui relève de ses attributions, de définir dans une instruction particulière :
a) Les conditions d'emploi des niveaux de classification Secret Défense et Confidentiel Défense. Il fixe notamment :
- le champ d'application de chacun des niveaux Secret Défense et Confidentiel Défense et dresse la nomenclature des informations ou catégories d'informations qui devront être couvertes par le secret ;
- les critères objectifs à considérer pour apprécier le caractère secret de l'information (par exemple l'importance dans l'organisation et la politique de défense et de sécurité nationale, le domaine concerné, la nature de la source...) ;
- les autorités responsables de la classification.
b) Les informations ou catégories d'informations qui doivent être classifiées Très Secret :

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

Les éléments suivants peuvent être pris comme référence pour procéder à la classification au niveau le plus pertinent. Ils ne sont donnés qu'à titre indicatif et ne sauraient constituer une liste exhaustive.

1. Le niveau Très Secret Défense est réservé aux informations ou supports qui concernent les priorités gouvernementales en matière de défense et de sécurité nationale et dont la divulgation non autorisée est de nature à nuire très gravement à la défense nationale.

La compromission de telles informations entraînerait :
- une menace directe de la stabilité interne de la France ou de pays alliés ou amis ;
- un préjudice exceptionnellement grave aux relations avec des gouvernements alliés ou amis ;
- un préjudice exceptionnellement grave à l'efficacité opérationnelle, y compris dans le cadre d'opérations combinées, à la sécurité des forces armées nationales, au maintien de l'efficacité d'opérations de sécurité ou de renseignement fondamentales pour la nation ;
- un préjudice grave pour l'économie française ;
- le risque de perte d'un grand nombre de vies humaines.

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

La compromission de telles informations pourrait :
- provoquer des tensions internationales ;
- nuire gravement aux relations avec des gouvernements alliés ou amis ;
- nuire gravement à l'efficacité opérationnelle d'actions de sécurité ou de renseignement ;
- causer un préjudice matériel important aux intérêts financiers, monétaires, économiques ou commerciaux de la France ;
- menacer directement des vies humaines, nuire gravement à l'ordre public, à la sécurité ou à la liberté des personnes.

3. Le niveau Confidentiel Défense est réservé aux informations ou aux supports 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.

La compromission de telles informations :
- porterait un préjudice important en matière de relations diplomatiques (protestations officielles ou sanctions) ;
- représenterait une entrave grave à l'élaboration ou au fonctionnement des principales politiques de la France ;
- nuirait à l'efficacité opérationnelle, y compris dans le cadre d'opérations combinées, à la sécurité des forces armées nationales, au maintien de l'efficacité d'opérations de sécurité ou de renseignement ;
- provoquerait la cessation ou de fortes perturbations d'activités ayant un rapport avec la continuité de la vie nationale ;
- irait à l'encontre des intérêts financiers, monétaires, économiques ou commerciaux de la France ;
- compromettrait de manière substantielle la viabilité financière de grandes organisations ;
- créerait un obstacle aux enquêtes relatives à des infractions graves ou faciliterait la commission de ces infractions ;
- causerait une atteinte ou préjudice à la sécurité ou à la liberté des personnes.

Il est rappelé que la décision de classifier une information est un acte important par les contraintes qu'il induit en matière de protection et les conséquences judiciaires qu'il peut générer. Une sur-classification engendre une inflation de documents protégés, dévalorise

la notion de secret et s'accompagne de surcoûts. A l'inverse, une sous-classification ne garantit pas à l'information une protection suffisante.

## A N N E X E 3
## RÈGLES DE PROTECTION DES INFORMATIONS OU SUPPORTS

## PORTANT LA MENTION : DIFFUSION RESTREINTE

La mention Diffusion restreinte (DR) n'est pas un niveau de classification mais une mention de protection. Son objectif principal est de sensibiliser l'utilisateur à la nécessaire discrétion dont il doit faire preuve dans la manipulation des informations couvertes par cette mention.

1. Teneur des informations de Diffusion restreinte :

L'application de cette mention relève de la nécessité d'éviter la divulgation, dans le domaine public, d'informations dont le regroupement ou l'exploitation pourraient :

- conduire à la découverte d'une information classifiée ;
- porter atteinte à la sécurité ou à l'ordre public, au renom des institutions, à la vie privée de leurs membres ;
- porter préjudice aux intérêts économiques ou financiers de sociétés privées ou d'établissements publics.

Doivent notamment recevoir au minimum la mention Diffusion restreinte :

- les documents définissant, en termes généraux, les objectifs, options, critères de choix retenus dans les différents domaines de l'activité militaire nationale ou de la sécurité opérationnelle ou technique et qui peuvent ne pas être classifiés ;
- les documents relatifs à l'ordre public (comptes rendus d'événements...) ;
- les documents non classifiés dont la diffusion doit être limitée et contrôlée conformément aux dispositions d'un accord de sécurité conclu avec un pays étranger ;
- les documents d'exercice dont la confidentialité n'a qu'un intérêt limité et temporaire ;
- les documents ou informations émanant d'un ministère qui souhaite en limiter et en contrôler la diffusion.

La mention Diffusion restreinte n'est pas destinée à protéger des informations à caractère personnel, mais cette possibilité n'est pas exclue (par exemple, rapport sur le moral d'un groupe, compte rendu d'événement...).

2. Condition d'emploi de la mention Diffusion restreinte :

Il appartient à chaque autorité des administrations de l'Etat, chef d'établissement ou chef de service, de décider si la diffusion d'une information doit être restreinte ou non.

Tout signataire d'un document contenant des informations répondant aux critères précisés ci-dessus est responsable de l'attribution de la mention Diffusion restreinte.

Les informations Diffusion restreinte ne doivent être communiquées qu'aux personnes qui ont besoin de les connaître pour nécessité du service, c'est-à-dire dans les limites de leurs attributions :

- les personnels civils et militaires des ministères ;
- les personnels désignés d'entreprises titulaires d'un marché public passé par un organisme relevant d'un ministère ; ces personnels devront être informés des règles de discrétion à appliquer vis-à-vis des informations et de leurs responsabilités contractuelles.

D'une manière générale, un document Diffusion restreinte émis par un ministère ne peut être communiqué qu'aux seules personnes appartenant à ce ministère et aux organismes ayant besoin d'en connaître avec lesquels il entretient des relations.

3. Elaboration et marquage :

L'élaboration des documents Diffusion restreinte ne peut être effectuée que dans les

locaux ou enceintes d'un ministère ou d'organismes publics ou privés offrant des conditions de sécurité suffisantes interdisant l'accès de personnes non autorisées à ces documents.
Les documents Diffusion restreinte doivent être identifiés sur la première page avec les références de l'organisme émetteur, la date d'émission et le numéro d'enregistrement.
Ils doivent porter le marquage suivant :
- sur chaque page, le timbre Diffusion restreinte apposé au milieu du haut de la page ;
- pour les messages et autres documents informatiques, la mention Diffusion restreinte rappelée en début de chaque page ;
- pour les documents reliés, le timbre Diffusion restreinte apposé au milieu de la page de garde et de la couverture.
4. Expédition et circulation :
La transmission interne des documents Diffusion restreinte peut être effectuée :
- à l'intérieur :
- d'un local, d'une enceinte ou d'un bâtiment relevant d'un ministère, par toute personne de ce ministère ;
- d'un organisme public ou privé dans le cadre d'un marché public, sous enveloppe ou par personne désignée par le titulaire du marché ;
- vers l'extérieur :
- sous double enveloppe, l'enveloppe intérieure portant la mention Diffusion restreinte et les références du document, l'enveloppe extérieure ne comportant que les indications nécessaires à la transmission ;
- par voie postale (civile ou militaire) en France métropolitaine, vers les départements ou les collectivités d'outre-mer ou vers l'étranger (147), par un moyen garantissant la bonne réception du document.
5. Conservation, destruction et reproduction :
Les documents marqués Diffusion restreinte sont enregistrés au départ et à l'arrivée selon les règles appliquées à tout document administratif non classifié.
Ils doivent être conservés dans des meubles fermant à clés.
Leur destruction a lieu sous la responsabilité des détenteurs, sans mention particulière sur les documents d'enregistrement du courrier.
Leur reproduction doit rester limitée aux seuls besoins du service.
6. Sécurité des systèmes d'information :
Les systèmes d'information destinés au traitement, au stockage ou à la transmission des informations Diffusion restreinte font l'objet d'une homologation de sécurité. Une instruction établie par l'ANSSI définit les règles applicables aux systèmes d'information pour ce niveau.
Lorsque l'urgence de leur traitement ou de leur transmission est plus importante que la protection de leur confidentialité, des informations Diffusion restreinte peuvent, à titre exceptionnel, être traitées ou transmises sur des systèmes n'ayant pas fait l'objet d'une homologation de sécurité au niveau Diffusion restreinte.

...
(142) Au sens de la loi n° 75-1334 du 31 décembre 1975 relative à la sous-traitance.
(143) Conformément aux dispositions de l'article 65 de la présente instruction.
(144) Annexe 12, modèle A.
(145) Annexe 12, modèle B.
(146) Annexe 12, modèle A.
(147) Pour les documents portant la mention Spécial France ces dispositions sont à combiner avec celles de l'article 65 de la présente instruction.

A N N E X E 4

# LE CONTRÔLE D’ACCÈS

Le contrôle d’accès consiste à vérifier si une personne demandant à accéder à un lieu ou à une information a le droit de le faire.

Comme exposé à l’article 70, il a pour objectifs :

— de filtrer les flux de circulation, les individus et les véhicules qui souhaitent entrer ou sortir d’un site, d’un bâtiment ou d’un local ;

— de contrôler les individus et les véhicules dans les zones protégées ;

— d’empêcher ou de limiter les déplacements de personnes non autorisées.

Il s’intègre dans un dispositif global de sécurité fondé sur son association avec les protections intérieure, périmétrique et périphérique.

Il comprend les moyens d’identification, de traitement et de freinage.

1. Le moyen d’identification est le dispositif permettant de recueillir les droits d’accès de l’individu et de les transmettre à un moyen de traitement.

2. Le moyen de traitement est le dispositif qui valide, selon les droits accordés, les informations fournies par le moyen de contrôle afin de lever l’obstacle et de libérer le passage.

Le moyen de traitement recouvre trois méthodes :

— l’action d’une personne ;

— l’action d’un système automatisé ;

— la combinaison des deux.

3. Le moyen de freinage est le dispositif servant à faire obstacle à l’intrusion et permettant de gagner le temps nécessaire à l’intervention.

Le contrôle d’accès repose sur les principes suivants :

— l’homogénéité (entre les moyens de contrôle d’accès et les autres moyens de protection retenus) ;

— la succession de filtres (le contrôle des accédants doit être réparti dans la profondeur, en plusieurs couches) ;

— la proportionnalité à la menace (le contrôle doit être adapté aux agresseurs potentiels) ;

— l’adaptation aux accédants (il doit être accepté par ses utilisateurs courants).

Les solutions techniques retenues dépendent des besoins :

— à quoi va-t-il servir (accéder à un bâtiment, une zone, un local) ?

— qui va être contrôlé (militaires, personnels civils, scientifiques, personnels d'entretien, techniciens, personnel de maintenance) ?

— contre quelle menace faut-il se protéger (menace interne, vandalisme, espionnage oui renseignement) ?

Avant tout choix de conception, un audit est nécessaire afin d'avoir une bonne connaissance du site, ce qui permet :

— d'identifier, de localiser, de hiérarchiser les cibles d'un site et les zones précises à contrôler ;

— d'analyser les flux d'individus, de véhicules à chaque point d'accès ;

— de constater les niveaux existants de protection des zones (ouvertures, parois, existence ou non de systèmes de contrôle comme les lecteurs de badges, obstacles au passage, niveau de résistance de ces obstacles à l'effraction, homogénéité de ces différents points...) ;

— d'identifier les menaces potentielles (intrusion involontaire ou de curieux, pénétration délibérée de personnes initiées et/ou équipées, complicité interne...) ;

— de prendre en compte les contraintes (architecturales, réglementaires (incendie, protection du secret de la défense nationale...).

Exemples de moyens mécaniques ou électroniques utilisés pour contrôler les accès : portillons d'accès, tourniquets tripodes, barrières, sas, interphones, vidéophones, claviers à code, lecteurs de badge, lecteurs biométriques...

## A N N E X E 5

## LES TYPES DE MESURES DE PROTECTION PHYSIQUE

L'ensemble des mesures de sécurité relatif à la protection physique est destiné à garantir l'intégrité des bâtiments et des locaux spécifiquement dédiés aux informations ou supports classifiés ainsi que la fiabilité des meubles dans lesquels ils sont conservés, afin d'éviter toute perte, dégradation ou compromission.

Il est rappelé que le niveau de classification des informations et supports détermine les menaces et les vulnérabilités à prendre en compte et conditionne le dispositif de protection.

Les mesures de protection physique mettent en œuvre des moyens techniques ou humains et reposent sur une organisation particulière, coordonnant l'ensemble. Elles comprennent :

— des mesures statiques à base de dispositifs matériels. Elles constituent l'essentiel des moyens de protection (murs, clôtures, portes, armoires fortes...) et de détection (radar volumétrique, contact d'ouverture, détecteur sismique...) et assurent la protection passive et active. Elles incluent aussi l'installation de systèmes de contrôle d'accès hiérarchisés

selon le besoin d'en connaître (tels que badge ou lecteur biométrique) ;

— des mesures dynamiques mettant en jeu des personnes (gardes, rondes de surveillance, filtrage, éléments d'intervention présents sur le site ou extérieurs) qui contribuent à la détection par des actions de surveillance et assurent l'intervention adéquate en cas d'intrusion ;

— des mesures technologiques nouvelles dont l'emploi devra être parfaitement connu, testé par les utilisateurs et, le cas échéant, complété par des procédés mécaniques plus traditionnels ;

— des dispositifs technologiques nouveaux dont l'emploi devra être parfaitement connu, testé par les services enquêteurs des ministères de la défense et de l'intérieur, éprouvé par les utilisateurs et qui devront, le cas échéant, être complétés par des mécanismes plus traditionnels.

Les mesures de protection physique font l'objet d'un suivi rigoureux et de toute mise à jour nécessaire pour préserver l'efficacité de l'ensemble du dispositif de sécurité.

## A N N E X E 6

## LES BARRIÈRES DE PROTECTION PHYSIQUE

## ET LEUR RÉPARTITION EN CLASSES

Les barrières sont réparties en classes indiquant leur degré de résistance à une tentative d'intrusion. Chacune des barrières est répartie en quatre classes, de la moins fiable à la plus sûre. Un contrôle d'accès et une procédure d'intervention s'imposent pour toutes les classes.

1. Classes du bâtiment et/ou de l'emprise :

Classe 4 : enceinte protégée (clôture d'une hauteur supérieure à 2,15 m ou, dans le cas où les murs du bâtiment constituent l'enceinte, protection de toutes les ouvertures situées à moins de 5,50 m au-dessus du niveau du sol) mais absence de gardes permanents ou de dispositif de détection alarme.

Classe 3 : protection de la classe 4 + gardes permanents effectuant des rondes de surveillance dans les locaux et l'emprise ou dispositif de détection-alarme relié à un élément d'intervention extérieur (gendarmerie, commissariat de police, société de gardiennage).

Classe 2 : protection de la classe 3 + dispositifs de détection-alarme (éclairage, télésurveillance, vidéosurveillance, détection périmétrique ou périphérique) + présence de gardes permanents.

Classe 1 : protection de la classe 2 + dispositifs de détection-alarme pour les locaux (détection périphérique ou volumétrique) ou les meubles (détection ponctuelle) + traçabilité des accès (registre et vidéosurveillance).

Les dispositifs électroniques de filtrage ne peuvent pas à eux seuls garantir l'intégrité des accès aux bâtiments et/ou aux emprises. Ils doivent obligatoirement être complétés par

des systèmes mécaniques de fermeture activés en dehors des heures normales d'occupation des bâtiments.

2. Classes du local :

Les parois ainsi que les plafonds et les sols des locaux doivent avoir une résistance suffisante.

Classe d : local avec porte à serrure mécanique ordinaire, équipée d'une sûreté à clé dont, si possible, l'ébauche est protégée, et fenêtres sans protection.

Classe c : local avec porte à serrure mécanique de haute sécurité (multipoints), équipée d'une sûreté à clé dont l'ébauche est protégée et fenêtres protégées lorsqu'elles sont situées à moins de 5,5 m d'un lieu accessible (sol, toit, corniche, descente d'eau pluviale, promontoire).

La protection des fenêtres doit être assurée :

— soit par des barres en acier de 2 cm de diamètre au moins, espacées de 11 cm au plus ;

— soit par un vitrage anti-effraction. Les fenêtres doivent être alors munies d'un dispositif de limitation d'ouverture de manière à empêcher toute intrusion.

Classe b : local avec porte renforcée (en bois plein ou recouverte de feuilles d'acier) équipée d'un système anti-dégondage, à serrure mécanique de haute sécurité avec détecteur ou compteur d'ouverture ; les autres ouvertures doivent être protégées comme pour la classe c.

Classe a : chambre forte dont la porte est au minimum équipée des systèmes de sécurité des armoires fortes de classe B. Les parois des locaux doivent avoir une résistance au moins équivalente à 15 cm de béton.

3. Classes du meuble :

Les meubles de sécurité destinés à la conservation des informations ou supports classifiés se répartissent en trois classes et ne pourront pas être ouverts frauduleusement sans effraction. Ils sont donc conçus pour que toute tentative d'ouverture illégitime laisse des traces visibles. Ils seront dotés par défaut de serrure mécanique satisfaisant à la norme maximale de sécurité de leur pays de conception.

Classe C : armoire dite forte, à un ou deux battants, à structure métallique d'au moins 2 millimètres d'épaisseur, munie d'une serrure mécanique à combinaison silencieuse et à manœuvre discrète qui permet de s'affranchir de la conservation des clés. Les battants doivent posséder un système d'accrochage du côté du pivot interdisant le démontage des portes en cas de sectionnement des gonds, lorsque le meuble est condamné. Les pênes, inaccessibles de l'extérieur, ne doivent pas pouvoir être démontés.

Classe B : armoire forte de structure identique à la classe C ;

+ un renforcement de la structure de la zone située derrière les organes essentiels (148) dont la présence peut être vérifiée visuellement par démontage du foncet de porte (face

intérieure de la porte) ;

+ un dispositif délateur, à déclenchement mécanique et thermique, bloquant définitivement les mécanismes d'ouverture en cas de tentative d'ouverture illégitime ;

+ un plombage du foncet de porte (face intérieure de la porte) permettant de détecter aisément un démontage ;

+ un système à clé interdisant l'accès au dispositif de changement de la combinaison pour les modèles mécaniques ;

+ un système d'asservissement, interdisant la sortie des pênes de la porte principale lorsque l'autre battant n'est pas fermé, s'il ne s'agit pas d'une porte à battant unique ;

+ un dispositif qui interdise aux pênes de la porte principale, une fois sortis, de se rétracter à moins que la combinaison soit à nouveau composée ;

+ un compteur d'ouverture non falsifiable et non réutilisable, sans dispositif de remise à zéro et protégé par le foncet ;

+ une serrure mécanique à combinaison silencieuse et à manœuvre discrète est à recommander. L'emploi d'une serrure électronique peut être autorisé s'il est justifié (149). Elle doit alors être de haut de gamme (150), posséder une mémoire permettant son audit, éventuellement pouvoir être paramétrée pour n'être ouverte que dans des plages horaires choisies, comporter un dispositif permettant à un usager de déclencher une alarme auprès d'un service de sécurité lorsque l'ouverture est effectuée sous la menace.

Le meuble équipé d'une combinaison électronique devra comporter une serrure mécanique à clé facilement permutable en supplément. Cette clé devra être prisonnière de la serrure tant que le pêne de la combinaison et les pênes du meuble ne sont pas sortis portes fermées ;

+ un système de tringlerie métallique en acier assurant sur la porte principale une répartition géographique de plusieurs pênes horizontaux et verticaux. Si une poignée actionne ce système, elle doit posséder un point de rupture pour éviter un effort trop conséquent sur la tringlerie.

Les portes seront dépourvues de toute plaque de propreté et de tout enjoliveur.

Classe A : coffre-fort blindé sur toutes ses faces, d'un poids minimum à vide de 500 kilogrammes ou, à défaut, fixé au mur, au sol ou sur une plaque métallique dont la plus petite dimension est supérieure à la plus grande dimension des issues du local.

Ce meuble devra comporter tous les systèmes de sécurité de la classe B et, en plus :

— une ou plusieurs serrures pouvant s'adapter à un nouveau jeu de clés (serrures mécaniques dites à clé facilement permutable [151]) ;

— au moins une serrure dont la clé reste prisonnière du mécanisme tant que le pêne de la combinaison et les pênes du meuble ne sont pas sortis porte fermée.

D'une manière générale, la marque et le numéro de série du meuble sont estampillés de

façon apparente et inaltérable, à l'extérieur de celui-ci, sur des parties fixes et sur des parties mobiles. Le numéro de série et l'année de fabrication de chaque serrure figurent sur celles-ci.

Tableaux de combinaison des classes

Les tableaux suivants indiquent les différentes combinaisons possibles entre les classes des trois barrières afin d'obtenir un niveau de sécurité minimal en fonction de chacune des classifications.

Tableau 1

Niveau Très Secret Défense

| CLASSE DU BÂTIMENT ou de l'emprise | CLASSE DU LOCAL | | | |
|---|---|---|---|---|
| | a | b | c | d |
| 1 | C | B | Interdit | Interdit |
| 2 | B | A | Interdit | Interdit |
| 3 | A | Interdit | Interdit | Interdit |
| 4 | Interdit | Interdit | Interdit | Interdit |

Tableau 2

Niveau Secret Défense

| CLASSE DU BÂTIMENT ou de l'emprise | CLASSE DU LOCAL | | | |
|---|---|---|---|---|
| | a | b | c | d |
| 1 | C | C | Interdit | Interdit |
| 2 | C | C | Interdit | Interdit |
| 3 | C | C | Interdit | Interdit |
| 4 | Interdit | Interdit | Interdit | Interdit |

Tableau 3

Niveau Confidentiel Défense

| CLASSE DU BÂTIMENT<br><br>ou de l'emprise | CLASSE DU LOCAL | | | |
|---|---|---|---|---|
| | a | b | c | d |
| 1 | C | C | C | C |
| 2 | C | C | C | C |
| 3 | C | C | C | B |
| 4 | C | C | B | Interdit |

(148) Serrures, combinaisons, mécanismes assurant les fonctionnalités du meuble.

(149) L'emploi d'une serrure électronique peut être justifié si des fonctions d'audit mono ou multi-utilisateurs d'ouverture, dans des plages horaires définies par le ou les utilisateurs, d'alarme sous contrainte, ou de retardateur d'ouverture sont nécessaires.

(150) Serrure qui offre des possibilités de paramétrage d'ouverture et de fermeture. Elle offre la possibilité de varier les codes suivant les horaires et les utilisateurs.

(151) Serrure à clé qui a la faculté de pouvoir être paramétrée pour être ouverte par un nouveau jeu de clés sans démontage du mécanisme. Cette action doit annuler la possibilité d'ouverture avec l'ancien jeu.

## A N N E X E 7

## MESURES APPLICABLES AUX ZONES RÉSERVÉES

Dès lors que des documents d'un niveau de classification égal ou supérieur à Secret Défense sont traités dans des locaux, des mesures particulières de sécurité doivent être mises en place. Ces mesures de sécurité permettent de définir les zones réservées, elles-mêmes obligatoirement situées en zone protégée, conformément aux dispositions de l'article 74 de la présente instruction.

La protection des informations ou supports classifiés se traduit par un durcissement des mesures de protection physique et de contrôle d'accès, qui a pour but d'empêcher :

— tout accès à ces informations par des personnes, même habilitées, n'ayant pas besoin d'en connaître ;

— toute pénétration, par vues et écoutes, directes ou indirectes, dans les lieux où des secrets sont élaborés, traités, reçus ou détenus ;

— l'accès aux systèmes d'information classifiés au niveau 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.

Le traitement ou la conservation d'informations ou supports classifiés dans ces locaux ne peut intervenir, sauf en cas d'impossibilité majeure, qu'après avis des services enquêteurs quant à l'aptitude de ces locaux à accueillir des documents de niveau Secret Défense ou supérieur.

Lorsque des services ou des organismes sont amenés à traiter de tels documents de manière occasionnelle, il est recommandé d'appliquer temporairement les mesures de sécurité détaillées plus haut.

Les lieux abritant des éléments classifiés au niveau Secret Défense ou supérieur répondent aux normes suivantes :

— ils comprennent, au minimum, un local pourvu d'ouvertures en nombre restreint, de fenêtres protégées et de portes renforcées équipées de serrures de haute sécurité munies si possible de compteur d'ouverture ;

— ce local contient un meuble de sécurité de type approuvé ;

— un contrôle permanent du lieu est organisé, s'appuyant au minimum sur un des systèmes de protection décrits en annexe 5.

Des normes équivalentes peuvent être adoptées, si nécessaire, par chaque ministre afin de répondre à la situation particulière de certains locaux.

Les contrôles des locaux :

Pour chaque lieu, un responsable s'assure que les mesures de protection prévues, dont notamment les règles d'accès au site, sont appliquées.

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

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

— le fonctionnement des systèmes de détection ;

— la fermeture des bureaux, des coffres, des armoires, etc. ;

— le vidage des corbeilles à papier et l'absence dans celles-ci de brouillons ou de 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 ces zones réservées en l'absence du personnel, sauf nécessité de service (levée de doute, réglementation particulière, urgence avérée).

Le contrôle des personnes et des visiteurs dans des lieux abritant des éléments classifiés des éléments couverts par le secret :

Les personnes en service ayant accès de par leurs fonctions au lieu abritant des éléments classifiés des éléments couverts par le secret d'un niveau Secret Défense ou supérieur 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 du lieu.

Les personnels d'entretien :

— 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 du lieu.

## A N N E X E 8

## GUIDE DES MESURES DE SÉCURITÉ APPLICABLES AU COURS

## DES RÉUNIONS IMPLIQUANT DES INFORMATIONS CLASSIFIÉES

Avant la réunion :

1. L'organisateur détermine le niveau de classification de la réunion et demande le nom des personnes qui assisteront à la réunion afin d'établir la liste des participants.

2. L'organisateur s'assure que l'officier de sécurité reçoive la liste des participants afin de vérifier que leur habilitation est valide et correspond au niveau des informations ou supports qui vont être traités.

3. L'officier de sécurité s'assure que la salle accueillant la réunion répond aux conditions de sécurité inhérentes au niveau de classification des informations qui seront abordées.

Au début de la réunion :

5. L'officier de sécurité s'assure que l'identité de chaque participant est vérifiée et conforme à la liste des participants, validée préalablement par ses soins.

6. L'organisateur indique aux participants le niveau maximal de classification des informations qui seront abordées au cours de la réunion et les règles de sécurité correspondantes.

7. L’organisateur, assisté par l’officier de sécurité s’assure que les mesures de sécurité concernant les téléphones portables et autres appareils électroniques sont appliquées.

Pendant la réunion :

8. Le niveau maximal de classification des informations évoquées au cours de la réunion ne doit pas dépasser le niveau d’habilitation de chaque participant ainsi que les capacités de protection de la salle accueillant la réunion.

9. L’organisateur veille à ce que la communication d’informations classifiées reste limitée à l’objet de la réunion.

10. Pendant les pauses, les participants sont autorisés à quitter la salle de réunion si la sécurité des documents classifiés qui y sont laissés est assurée.

11. Les informations classifiées ne doivent pas être discutées en dehors de la salle de réunion.

12. Toute faille dans la sécurité pendant la réunion doit être notifiée à l’organisateur et à l’officier de sécurité qui en informe les participants.

A l’issue de la réunion :

13. Les documents classifiés sont récupérés, rangés ou détruit sous la responsabilité de l’organisateur et de l’officier de sécurité dès lors qu’ils cessent d’être utiles.

14. L’organisateur dresse un procès-verbal de la réunion comprenant les domaines évoqués, les mesures prises pour assurer la protection des informations classifiées et la liste des participants.

16. Lorsque les participants sont autorisés à prendre des notes au cours de la réunion, ils sont informés par l’organisateur de leur responsabilité en matière de protection du secret.

## A N N E X E 9

## CLAUSES TYPES CONTRACTUELLES DE PROTECTION

## DU SECRET DE LA DÉFENSE NATIONALE

Les présentes clauses sont insérées dans les contrats en application de la présente instruction. Elles peuvent être adaptées ou complétées par l’autorité contractante mais ne peuvent leur être contraires.

1. Clause générale de protection du secret :

Dans le cadre des dispositions législatives et réglementaires en matière de protection du secret de la défense nationale, le titulaire du contrat s’engage à assurer la protection des informations ou supports classifiés qu’il aura à connaître et/ou à détenir au titre du présent contrat, en tenant compte des dispositions particulières stipulées dans l’annexe de sécurité au présent contrat.

Il reconnaît avoir pris connaissance des textes suivants portant sur ses obligations résultant de la connaissance et de la détention d'informations ou supports classifiés couverts par le secret de la défense nationale :

— le code pénal, notamment en ses articles 413-9 à 414-9 ;

— l'instruction générale interministérielle n° 1300 relative à la protection du secret de la défense nationale.

Il déclare se soumettre aux obligations résultant pour lui de l'application de ces dispositions ainsi qu'à celles découlant de l'ensemble des textes législatifs et réglementaires relatifs à la protection du secret de la défense nationale.

Toute violation ou inobservation par le titulaire des mesures de sécurité, même dans les cas où elles résultent d'une imprudence ou d'une négligence, peut entraîner la résiliation du contrat à ses torts et le retrait de l'habilitation de l'entreprise à l'accès aux informations ou supports classifiés, sans préjudice des peines prévues par les dispositions des articles 413-9 à 413-12 du code pénal.

2. Stipulations additionnelles relatives aux contrats nécessitant la détention d'informations ou de supports classifiés par le titulaire :

Les locaux de travail du titulaire du contrat doivent présenter toutes les garanties pour assurer la protection du secret de la défense nationale et peuvent faire l'objet de contrôles de l'autorité contractante.

Le titulaire s'engage à signaler toute modification susceptible de remettre en cause les garanties que présentent ses locaux pour la protection des informations ou supports classifiés communiqués au titre du présent contrat.

A l'achèvement des travaux classifiés, le titulaire dispose d'un délai d'un mois pour en informer l'autorité contractante qui lui indique la destination à donner aux informations ou supports classifiés jusqu'alors détenus par le titulaire. Celui-ci s'engage à respecter cette destination. En cas de non-respect de ces stipulations, le titulaire encourt une sanction stipulée au contrat.

En cas d'inexécution des travaux requis par le service enquêteur chargé de la vérification d'aptitude physique des locaux dans les conditions définies dans l'instruction générale interministérielle n° 1300 relative à la protection du secret de la défense nationale, la responsabilité du titulaire est engagée.

3. Stipulations additionnelles pour les contrats de recherche ou d'étude :

Le titulaire du contrat reconnaît à l'autorité contractante le pouvoir de faire rechercher parmi les documents et matériels qui se trouveraient en sa possession les informations ou supports classifiés se rapportant au contrat et à faire apposer les scellés sur les coffres et locaux à l'intérieur desquels les documents et matériels réclamés par l'administration seront regroupés en vue d'assurer leur protection.

Les informations ou supports classifiés énumérés à l'annexe de sécurité doivent être intégralement retournés à l'autorité contractante.

Les locaux de travail du titulaire du contrat doivent présenter toutes les garanties pour assurer la protection du secret de la défense nationale et peuvent faire l'objet de contrôles.

4. Stipulations de protection du secret pour le contrat de travail d'une personne habilitée :

Dans le cadre des dispositions législatives et réglementaires en matière de protection du secret de la défense nationale, le titulaire du contrat de travail s'engage à respecter les mesures qui lui sont prescrites pour assurer, lors de l'exécution dudit contrat, la protection des informations ou supports classifiés qu'il peut, sous réserve du besoin d'en connaître, être amené à connaître ou à détenir, selon les conditions de son habilitation préalable par l'autorité administrative compétente, et dans les limites de validité et de niveau de secret mentionnées sur la décision d'habilitation.

Il reconnaît avoir pris connaissance des articles 413-9 à 413-12 du code pénal, de l'instruction générale interministérielle n° 1300 relative à la protection du secret de la défense nationale ainsi que des dispositions prises pour garantir la protection des informations ou supports classifiés.

5. Stipulations de protection du secret pour le contrat de travail d'une personne non habilitée :

Dans le cadre des dispositions législatives et réglementaires en matière de protection du secret de la défense nationale, le titulaire du contrat de travail s'engage à respecter les mesures qui lui sont prescrites pour assurer lors de l'exécution du contrat la protection des informations ou supports classifiés qui peuvent être détenus dans le service au profit duquel le contrat est exécuté ou dans tout lieu dans lequel ce contrat est exécuté.

Il reconnaît avoir pris connaissance des articles 413-9 à 413-12 du code pénal ainsi que des dispositions prises pour garantir la protection des informations ou supports classifiés.

## A N N E X E 10

## CLAUSE TYPE CONTRACTUELLE DE PROTECTION DU SECRET

## DE LA DÉFENSE NATIONALE POUR LES CONTRATS SENSIBLES

1. Dans le cadre des dispositions législatives et réglementaires en matière de protection du secret de la défense nationale, le titulaire s'engage à prendre toutes les mesures utiles pour assurer lors de l'exécution du contrat la protection absolue des informations ou supports classifiés qui peuvent être détenus dans le service, au profit duquel le contrat est exécuté ou dans tout lieu dans lequel ce contrat est exécuté.

2. Le titulaire reconnaît :

— avoir pris connaissance des articles 413-9 à 413-12 du code pénal ;

— qu'il n'a pas à connaître ou détenir les informations couvertes par le secret de la défense nationale.

3. Le titulaire reconnaît avoir fait signer par tous les personnels, appelés sous sa responsabilité à un titre quelconque à intervenir pour son compte pour exécuter les prestations, une déclaration individuelle par laquelle lesdits personnels attestent :

— avoir pris connaissance des articles 413-9 à 413-12 du code pénal ;

— qu'ils n'ont pas, sous peine de poursuite pénale, à connaître ou détenir des informations couvertes par le secret de la défense nationale.

4. Le titulaire s'engage à ce que seules les personnes ayant préalablement souscrit la déclaration précitée accèdent au lieu d'exécution des prestations.

5. Le titulaire s'engage à remettre à l'autorité contractante la ou les déclarations individuelles ci-dessus avant tout accès du personnel concerné au lieu d'exécution des prestations.

6. Aucune dérogation aux prescriptions ci-dessus ne pourra être acceptée de l'autorité contractante ou exigée d'elle, y compris en vue de pourvoir au remplacement inopiné, fortuit ou même urgent d'un personnel du titulaire.

7. Le non-respect ou l'inobservation par le titulaire de ces mesures de sécurité, même dans les cas où elles résultent d'une imprudence ou d'une négligence, peut entraîner le prononcé d'une sanction contractuelle, sans préjudice des sanctions pénales.

## A N N E X E 11

Vous pouvez consulter la notice ainsi que l'appendice 1 dans le

JOn° 279 du 02/12/2011 texte numéro 1

## Appendice 2

LISTE DES PIÈCES CONSTITUTIVES DU DOSSIER D'APTITUDE

D'UN ÉTABLISSEMENT POUR L'EXÉCUTION D'UN CONTRAT AVEC DÉTENTION D'ISC

1. Documents à fournir par l'entreprise à habiliter (renseignements sur le lieu d'exécution des travaux classifiés) :

— extrait en cours de validité du registre du commerce et des sociétés (modèle L bis) ou copie du bail de location ;

— organigramme fonctionnel et nominatif de l'établissement ;

— notice individuelle de sécurité 94/A (modèle 01 de l'IGI 1300) et lettre de proposition de chaque OS pressenti ;

— plan de masse de l’établissement ;

— organisation et moyens de protection et de gardiennage de l’établissement ;

— identification et description de la protection, actuelle et envisagée, du local ou des locaux où sont exécutés les travaux protégés ;

— dossier de sécurité des SI ;

— liste des sous-traitants intervenant dans l’établissement, faisant ressortir les entreprises prestataires de services au titre d’un contrat à clause de sécurité ou d’un contrat sensible ;

— lettre du dirigeant de l’entreprise, par laquelle celui-ci s’engage à mettre en place, avant le début des travaux protégés, les dispositions qui sont nécessaires pour garantir la protection des informations et supports classifiés qui lui sont confiés.

2. Document préparé par l’autorité contractante ou le contractant (complément à la définition et à la justification du besoin d’en connaître) :

— annexe de sécurité ou projet d’annexe de sécurité.

## A N N E X E 12

Vous pouvez consulter les modèles d’attestation dans le JO

n° 279 du 02/12/2011 texte numéro 1

## A N N E X E 13

PRESCRIPTIONS RELATIVES AUX ANNEXES DE SÉCURITÉ

L’annexe de sécurité porte sur les éléments suivants :

— l’engagement pris par le titulaire de s’assurer que les personnes qui ont besoin d’avoir accès à des informations classifiées dans l’exercice de leurs fonctions ont fait l’objet de l’habilitation de sécurité appropriée ;

— l’engagement pris par le contractant de s’assurer que toutes les personnes qui ont accès à des informations ou supports classifiés sont informées de leur responsabilité en matière de protection desdites informations en vertu des lois et règlements appropriés ;

— l’engagement de signaler toute infraction effective ou supposée aux lois et règlements afférents à la protection des informations classifiées relevant du contrat ;

— les autorités compétentes chargées de coordonner la protection des informations ou supports classifiés en rapport avec le contrat ;

— les locaux dans lesquels le contrat doit être exécuté, dont la liste peut évoluer ;

— la liste des informations ou supports classifiés, leurs niveaux respectifs de classification et les conditions de protection dont chaque information doit faire l'objet conformément aux prescriptions de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale et à la procédure de communication des changements de niveau de classification ;

— les mesures particulières de sécurité qui doivent être prises pour l'exécution de ce contrat en vue de garantir la protection des informations ou supports classifiés ;

— les modes de communication et les moyens de transmission électronique ;

— l'identification des sous-traitants ;

— les modalités de communication des informations classifiées aux sous-traitants ;

— la procédure de transmission des informations classifiées ;

— les modalités de gestion prévisionnelle des informations ou supports classifiés une fois le contrat achevé.

Un exemplaire de l'annexe de sécurité est transmis au service enquêteur chargé du suivi de l'entreprise.

Modèles de notices, de formulaires

et de décisions administratives

Demande ou renouvellement d'habilitation et notice individuelle de sécurité (modèle 01/IGI 1300).

Demande de contrôle élémentaire (modèle 02/IGI 1300).

Décision d'habilitation aux informations ou aux supports classifiés (modèle 03/IGI 1300).

Décision de sécurité convoyeur (modèle 04/IGI 1300).

Certificat de sécurité (modèle 05/IGI 1300).

Engagement de responsabilité (modèle 06/IGI 1300).

Certificat de courrier (modèle 07/IGI 1300).

Certificat de courrier multivoyages (modèle 07 bis/IGI 1300).

Liste inventaire (modèle 08/IGI 1300).

Demande de reproduction de support(s) classifié(s) Secret Défense (modèle 09/IGI 1300).

Autorisation de reproduction de support(s) classifié(s) Secret Défense (modèle 10/IGI

1300).

Procès-verbal de destruction de support(s) d'information classifié(s) Secret Défense (modèle 11/IGI 1300).

Bordereau A de transmission d'informations ou de supports classifiés (modèle 12/IGI 1300).

Bordereau B de transmission d'informations ou de supports classifiés (modèle 12 bis/IGI 1300).

Bordereau B' de transmission d'informations ou de supports classifiés (modèle 12 ter/IGI 1300).

Modèles de timbres de classification et de protection (modèle 13/IGI 1300).

Modèles de timbres de déclassement ou de déclassification (modèle 14/IGI 1300).

Attestation de mise en garde (modèle 15/IGI 1300).

Attestation de mise en éveil (modèle 16/IGI 1300).

Fiche navette entre l'autorité contractante ou le pouvoir adjudicateur et le service enquêteur relative à un avis sur une entreprise pour exécuter un contrat sensible (modèle 17/IGI 1300).
Vous pouvez consulter les notices dans le

JOn° 279 du 02/12/2011 texte numéro 1

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 crossed, 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 À 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'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'officier de sécurité de votre société ou organisme.

8. Il vous appartient, à vous-même et à l'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'officier de sécurité de la société ou de l'organisme destinataire et à l'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 déléguée).

11. A votre retour, vous devrez produire un récépissé de l'envoi, signé par l'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 :

Vous pouvez consulter la déclaration dans le

JOn° 279 du 02/12/2011 texte numéro 1

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 À 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'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 sécuritéservice spécialisé des pays dans lesquels vous passerez en transit (voir paragraphe 12 ci-après). Si ces précisions ne vous ont pas été fournies, demandez-les à l'officier de sécurité de votre société ou organisme.

8. Il vous appartient, à vous-même et à l'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'officier de sécurité de la société ou de l'organisme destinataire et à l'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 déléguée).

11. A votre retour, vous devrez produire un récépissé de l'envoi, signé par l'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 :

Vous pouvez consulter la déclaration dans le

JOn° 279 du 02/12/2011 texte numéro 1

Fait le 30 novembre 2011.

Pour le Premier ministre et par délégation :
Le secrétaire général de la défense
et de la sécurité nationale,
F. Delon