

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Direction de la protection et de la sécurité de l'État

**INSTRUCTION GÉNÉRALE INTERMINISTÉRIELLE
SUR LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE**

*Abroge et remplace l'instruction générale interministérielle
n° 1300/SGDSN/PSE/PSD du 13 novembre 2020*

SOMMAIRE

RÉFÉRENCES	6
GLOSSAIRE.....	7
INTRODUCTION.....	15
MIEUX CLASSIFIER.....	15
... POUR MIEUX PROTEGER	17
1 PRINCIPES GENERAUX	18
1.1 FONDEMENT DU SECRET DE LA DEFENSE NATIONALE.....	18
1.2 ACCES AU SECRET DE LA DEFENSE NATIONALE.....	18
1.2.1 Principes généraux.....	18
1.2.2 Cas spécifiques.....	19
1.2.3 Règles de communication des documents classifiés.....	25
1.3 PORTEE DES TIMBRES DE CLASSIFICATION <i>SECRET</i> ET <i>TRES SECRET</i> ET DE LA MENTION <i>DIFFUSION RESTREINTE</i>	26
1.3.1 Portée des timbres de classification Secret et Très Secret	26
1.3.2 Portée de la mention de protection Diffusion Restreinte, qui n'est pas un timbre de classification.....	27
1.4 RESPONSABILITE DES DEPOSITAIRES DU SECRET DE LA DEFENSE NATIONALE	27
1.4.1 Responsabilité de l'autorité émettrice et de l'auteur d'information classifiée	27
1.4.2 Répression pénale des atteintes au secret de la défense nationale	28
1.4.3 Sanction de la divulgation non autorisée d'informations et supports portant la mention de protection Diffusion Restreinte.....	32
2 STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE 33	
2.1 AUTORITES CHARGEES DU PILOTAGE DE LA PROTECTION DU SECRET DE LA DEFENSE NATIONALE.....	33
2.1.1 Au niveau interministériel.....	33
2.1.2 Au niveau ministériel.....	35
2.1.3 Cas spécifiques.....	37
2.2 CHAINES DE SECURITE ENCADRANT, SOUS LA RESPONSABILITE DU RESPONSABLE D'ORGANISME, LA MISE EN ŒUVRE DE LA PROTECTION DU SECRET DE LA DEFENSE NATIONALE	38
2.2.1 Responsabilité première du responsable d'organisme.....	38
2.2.2 Chaîne fonctionnelle de protection du secret.....	39
2.2.3 Chaîne fonctionnelle de sécurité des systèmes d'information.....	41
2.3 OUTILS DE PILOTAGE, DE MISE EN ŒUVRE ET DE SUIVI.....	44
2.3.1 Instructions ministérielles et documents d'application.....	44
2.3.2 Outils et mesures de suivi de l'activité « protection du secret »	46
2.3.3 Inspections, contrôles et audits	47
2.3.4 Rapport annuel sur la protection du secret de la défense nationale	48
3 MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES.... 49	
3.1 PORTEE ET FONDEMENT DE LA PROCEDURE D'HABILITATION	49
3.1.1 Portée de l'habilitation et besoin d'en connaître.....	49
3.1.2 Justification de la demande d'habilitation au regard du catalogue des emplois.....	49
3.1.3 Responsabilité de l'autorité hiérarchique ou administrative sollicitant l'habilitation	50
3.1.4 Personnes physiques habilitées ès qualités.....	51
3.2 DIFFERENTS TYPES DE PROCEDURE.....	51
3.2.1 Balance des risques dans le choix de la procédure.....	51
3.2.2 Procédure d'habilitation de droit commun.....	52

3.2.3	<i>Procédure simplifiée</i>	52
3.2.4	<i>Procédure d'urgence</i>	52
3.2.5	<i>Habilitation des ressortissants étrangers</i>	53
3.2.6	<i>Habilitation des ressortissants français au profit d'une organisation internationale, d'une institution, d'un organisme ou d'un organe de l'Union européenne ou d'une personne morale de droit étranger</i>	54
3.3	DEROULEMENT DES PROCEDURES D'HABILITATION	55
3.3.1	<i>Procédures de droit commun</i>	55
3.3.2	<i>Procédure d'urgence</i>	58
3.4	DECISION D'HABILITATION OU DE REFUS D'HABILITATION	59
3.4.1	<i>Typologie des décisions</i>	59
3.4.2	<i>Notification de la décision</i>	60
3.4.3	<i>Obligation de discrétion de la personne habilitée</i>	61
3.4.4	<i>Portée de la décision en matière internationale</i>	61
3.5	CYCLE DE VIE DE LA DECISION D'HABILITATION	61
3.5.1	<i>Durée de validité</i>	61
3.5.2	<i>Abrogation explicite d'une décision d'habilitation</i>	61
3.5.3	<i>Enquêtes administratives pendant la durée de l'habilitation</i>	62
3.5.4	<i>Conservation des décisions</i>	62
3.5.5	<i>Certificat de sécurité</i>	62
3.5.6	<i>Renouvellement</i>	62
3.5.7	<i>Portabilité de l'avis de sécurité en cas de changement de fonction ou de mission nécessitant une nouvelle habilitation</i>	62
3.5.8	<i>Cessation ou modification des droits associés à l'habilitation</i>	63
3.6	FORMATION ET SENSIBILISATION DE LA PERSONNE HABILITEE	63
4	MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES.....	65
4.1	ÉTABLISSEMENTS PUBLICS DE L'ÉTAT	65
4.2	OPERATEURS D'IMPORTANCE VITALE	65
4.3	AUTRES PERSONNES MORALES ASSOCIEES A LA PROTECTION DES INTERETS FONDAMENTAUX DE LA NATION	66
4.4	MESURES APPLICABLES DANS LE CADRE D'UN CONTRAT DE LA COMMANDE PUBLIQUE, D'UN CONTRAT DE SOUS-TRAITANCE OU D'UN SOUS-CONTRAT A UN CONTRAT DE LA COMMANDE PUBLIQUE OU D'UN CONTRAT DE SUBVENTION	66
4.4.1	<i>Avant signature du contrat</i>	67
4.4.2	<i>Exécution du contrat</i>	73
4.4.3	<i>Résiliation et terme du contrat</i>	77
4.5	MESURES DE SECURITE APPLICABLES EN CAS DE CESSATION D'ACTIVITE OU DE DISSOLUTION DE LA PERSONNE MORALE	77
5	SECURITE DES LIEUX.....	78
5.1	PRINCIPE DE DEFENSE EN PROFONDEUR ET ANALYSE DE RISQUES	78
5.2	PROTECTION PHYSIQUE	79
5.2.1	<i>Règles générales</i>	79
5.2.2	<i>Dispositif global de protection</i>	79
5.3	CONTROLE D'ACCES	80
5.3.1	<i>Contrôle physique des accès</i>	80
5.3.2	<i>Accès des personnes non habilitées dans le cadre de l'exécution d'un contrat « sensible »</i>	81
5.3.3	<i>Vérification de la protection physique par les services enquêteurs</i>	83
5.4	SECURISATION DES SALLES, BUREAUX ET EQUIPEMENTS	85

5.4.1	Principe d'identification	85
5.4.2	Politique du bureau propre et de l'écran vide	85
5.4.3	Organisation des réunions	85
5.5	PROTECTION CONTRE LES MENACES EXTERIEURES ET ENVIRONNEMENTALES	85
6	SECURITE DES SYSTEMES D'INFORMATIONS CLASSIFIES.....	86
6.1	HOMOLOGATION DU SYSTEME D'INFORMATION CLASSIFIE.....	86
6.1.1	Démarche d'homologation.....	86
6.1.2	Autorité d'homologation	87
6.1.3	Commission d'homologation.....	87
6.1.4	Dossier d'homologation.....	88
6.1.5	Durée de la décision d'homologation	89
6.1.6	Contrôle et renouvellement de l'homologation.....	89
6.1.7	Procédure dérogatoire en cas d'urgence opérationnelle.....	89
6.2	HOMOLOGATION DES INTERCONNEXIONS D'UN SYSTEME D'INFORMATION CLASSIFIE.....	90
6.2.1	Interconnexion entre deux systèmes d'information classifiés de même niveau.....	90
6.2.2	Autres interconnexions.....	90
6.3	MESURES DE SECURITE APPLICABLES EN CAS DE SOUS-TRAITANCE DU DEVELOPPEMENT OU DE LA MAINTENANCE D'UN SYSTEME D'INFORMATION CLASSIFIE	91
6.4	MESURES DE SECURITE PHYSIQUES ET PRISE EN COMPTE DES SIGNAUX PARASITES COMPROMETTANTS .	92
6.4.1	Lieu abritant le système d'information classifié	92
6.4.2	Matériel classifié laissé sans surveillance par son détenteur	92
6.5	MESURES DE SECURITE INHERENTES AU SYSTEME D'INFORMATION CLASSIFIE	92
6.5.1	Dispositifs de sécurité	92
6.5.2	Recours à des dispositifs de sécurité agréés	93
6.6	CONCEPTION ET EXPLOITATION DU SYSTEME D'INFORMATION	93
6.6.1	Administration des systèmes d'information classifiés	93
6.6.2	Maîtrise des logiciels en exploitation.....	94
6.6.3	Contrôle d'accès aux systèmes d'information classifiés	94
6.6.4	Supervision logicielle de la sécurité et traçabilité	97
6.6.5	Maintenance et maintien en condition opérationnelle et en condition de sécurité	98
6.6.6	Cloisonnement.....	99
6.6.7	Mécanismes de filtrage des flux de données.....	99
6.6.8	Gestion de la continuité et de la reprise de l'activité.....	100
6.7	SECURITE EN MOBILITE.....	100
6.7.1	Sécurité des équipements de mobilité.....	100
6.7.2	Sécurisation des accès à distance	101
6.8	SUPPORTS AMOVIBLES.....	101
6.8.1	Supports amovibles au sein du système d'information classifié.....	101
6.8.2	Supports amovibles entre un système d'information classifié et d'autres systèmes.....	101
6.9	AUDIT DES SYSTEMES D'INFORMATION.....	102
7	GESTION DES INFORMATIONS ET SUPPORTS CLASSIFIES TOUT AU LONG DE LEUR CYCLE DE VIE.....	104
7.1	ÉLABORATION DES INFORMATIONS ET SUPPORTS CLASSIFIES	104
7.1.1	Règles de classification	104
7.1.2	Marquage.....	107

7.2	TRAÇABILITE DES INFORMATIONS ET SUPPORTS CLASSIFIES AU SEIN DE L'ORGANISME DETENTEUR	110
7.2.1	<i>Organisation de la gestion des informations et supports classifiés</i>	<i>110</i>
7.2.2	<i>Enregistrement.....</i>	<i>113</i>
7.2.3	<i>Conservation.....</i>	<i>114</i>
7.2.4	<i>Reproduction.....</i>	<i>114</i>
7.2.5	<i>Gestion des éléments constitutifs d'un système d'information classifié.....</i>	<i>116</i>
7.3	DIFFUSION DES INFORMATIONS ET SUPPORTS CLASSIFIES	116
7.3.1	<i>Envoi d'informations et supports classifiés.....</i>	<i>116</i>
7.3.2	<i>Transport.....</i>	<i>117</i>
7.3.3	<i>Réception.....</i>	<i>120</i>
7.4	INVENTAIRE	121
7.4.1	<i>Principes généraux.....</i>	<i>121</i>
7.4.2	<i>Inventaire au niveau Secret.....</i>	<i>122</i>
7.4.3	<i>Inventaire au niveau Très Secret.....</i>	<i>122</i>
7.5	FIN D'EXPLOITATION DES INFORMATIONS ET SUPPORTS CLASSIFIES	123
7.5.1	<i>Procédure de destruction</i>	<i>123</i>
7.5.2	<i>Mise au rebut ou réaffectation sécurisée du matériel informatique classifié.....</i>	<i>123</i>
7.5.3	<i>Évacuation et destruction d'urgence.....</i>	<i>124</i>
7.5.4	<i>Versement aux archives.....</i>	<i>124</i>
7.5.5	<i>Accès aux informations et supports ayant fait l'objet d'une mesure de classification versés dans un service public d'archives.....</i>	<i>125</i>
7.6	EXPIRATION DE LA CLASSIFICATION.....	127
7.6.1	<i>Mention d'échéance de la classification</i>	<i>127</i>
7.6.2	<i>Réexamen de la classification des informations et supports classifiés détenus par les services publics d'archives.....</i>	<i>128</i>
7.6.3	<i>Procédure de déclassification</i>	<i>128</i>
	LISTE DES ANNEXES	131

RÉFÉRENCES

Constitution du 4 octobre 1958 : articles 5, 20 et 21.

Conseil constitutionnel, décision n° 2011-192 QPC du 10 novembre 2011, décision n° 2015-713 DC du 23 juillet 2015 et décision n° 2016-738 DC du 10 novembre 2016.

Convention de Vienne du 18 avril 1961 sur les relations diplomatiques.

Loi du 18 mars 1918 réglementant la fabrication et la vente des sceaux, timbres et cachets officiels.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, et notamment son article 26.

Code civil : articles 22 et 1837.

Code de la commande publique : articles L. 2141-1 et suivants, R. 2300-1, R. 2332-8, R. 2343-4, R. 2343-5, R. 2343-13, R. 2351-14, R. 2396-6, R. 3123-3.

Code de commerce : article L. 210-3.

Code de la défense : articles L. 1131-1, L. 1332-1 et suivants, L. 2311-1, L. 2312-1 à L. 2312-8, L. 2362-1, L. 4121-2, R.* 1132-1 à R.* 1132-3 ; R. 1143-1, R. 1143-2, R. 1143-5, R. 1143-6, R. 1143-8, R. 2311-1 à R. 2311-9-1, R. 2311-10 à R. 2311-11, D.* 2311-12, R. 2312-1, R. 2312-2.

Code de justice militaire : article L. 332-2.

Code du patrimoine : articles L. 211-1, L. 212-2, L. 212-3 et L. 213-1 à L. 213-7.

Code pénal : articles 121-2, 226-13, 411-6 à 411-8, 413-7, 413-9 à 413-12, 414-5 à 414-9, 434-4, R. 413-1 à R. 413-5 et 444-1 à 444-9.

Code des postes et des communications électroniques : articles L. 36-5, R. 1-2-1 et R. 1-2-6.

Code de procédure pénale : article 56-4.

Code des relations entre le public et l'administration : articles L. 211-2 et L. 311-1 à 8.

Code de la sécurité intérieure : articles L. 114-1, L. 114-2 et L. 234-1.

Code du travail : L. 8112-1, L. 8113-10 à 11, L. 8114-1, L. 8114-2, L. 8123-1, L. 8123-4, L. 8123-5.

Décret n° 2005-850 du 27 septembre 2005 relatif aux délégations de signature des membres du Gouvernement.

Décret n° 2009-834 du 7 septembre 2009 modifié portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».

GLOSSAIRE

Accord de sécurité : accord intergouvernemental conclu entre la France et au moins un État ou une organisation internationale. Ces accords, qui doivent être obligatoirement entrés en vigueur avant tout échange d'information ou support classifiés avec l'État ou l'organisation internationale considéré, définissent les mesures de protection à appliquer dans le cadre de ces échanges, selon un principe d'équivalence entre les niveaux de classification français et ceux du partenaire, identifient les autorités nationales de sécurité compétentes, posent généralement le principe de la reconnaissance mutuelle des habilitations délivrées de part et d'autre, et précisent les modalités de transmission et de protection des informations et supports classifiés. Deux catégories d'accord de sécurité sont à distinguer : les accords applicables à l'ensemble des domaines de l'action gouvernementale, qualifiés d'« accords généraux de sécurité », et les accords limités à un domaine donné (généralement celui de la défense), alors qualifiés d'« accords de sécurité spécifiques ».

Action d'administration d'un système d'information classifié : action d'installation, de suppression, de modification et de consultation de la configuration d'un composant du système d'information.

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 classifié contenant des informations et supports classifiés aux niveaux *Secret* ou *Très Secret*.

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

Agrément d'un produit de sécurité : décision délivrée à l'issue d'une procédure par laquelle l'agence nationale de la sécurité des systèmes d'information reconnaît que le produit de sécurité évalué est apte à protéger des informations et supports sensibles ou classifiés au niveau et selon les conditions d'emploi spécifiées dans la décision d'agrément.

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.

Archives : ensemble des documents, y compris les données, 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 (cf. article L. 211-1 du code du patrimoine).

Auteur d'une information ou d'un support classifié : autorité qui, conformément aux modalités de classification arrêtées par l'autorité émettrice, prend la décision d'apposer le timbre de classification sur une information ou un support au niveau requis par son contenu.

Autorité d'emploi du système : autorité à l'origine du besoin du système d'information. Elle décide de sa mise en service (après son homologation par l'autorité d'homologation). Disposant d'un niveau hiérarchique suffisant, elle met à disposition des moyens de la sécurité des systèmes d'information au profit des utilisateurs, conformément aux directives de l'autorité qualifiée en sécurité des systèmes d'information (AQSSI). Le responsable de l'organisme peut être l'autorité d'emploi.

Autorité d'habilitation : autorité compétente pour diligenter une enquête administrative dans le cadre de l'habilitation au secret de la défense nationale et prendre la décision d'habilitation ou de refus d'habilitation.

Autorité d'homologation : personne physique qui, après instruction du dossier d'homologation, prononce l'homologation de sécurité du système d'information, c'est-à-dire, prend la décision d'accepter les risques résiduels identifiés sur le système. Elle est désignée à un niveau hiérarchique suffisant pour assumer les responsabilités qui lui incombent.

Autorité émettrice : autorité étatique nationale ou étrangère, ou supranationale, sous la responsabilité de laquelle un timbre de classification est apposé sur une information ou un support. C'est elle qui prend la décision de classification.

Autorité nationale de sécurité (ANS) : autorité nationale chargée d'assurer la protection des informations classifiées étrangères confiées aux organismes relevant de la juridiction de son État et d'assurer la liaison avec les autorités nationales de sécurité étrangères sur tout sujet relative à la protection des informations et supports classifiés. En France, l'autorité nationale de sécurité est le secrétaire général de la défense et de la sécurité nationale.

Autorité qualifiée en sécurité des systèmes d'information (AQSSI) : au titre de la présente instruction, autorité chargée de définir les lignes directrices relatives à la sécurité des systèmes d'information classifiés pour les organismes relevant de ses attributions et d'en contrôler l'application.

Autorité de sécurité déléguée (ASD) : autorité ayant reçu délégation pour exercer les missions dévolues à l'autorité nationale de sécurité dans un domaine spécifique et selon les modalités précisées dans la décision de délégation prise par l'autorité nationale de sécurité.

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, il ne lie pas l'autorité d'habilitation.

Avis de sécurité provisoire : avis de sécurité rendu à titre provisoire par le service enquêteur, visant à éclairer la décision de l'autorité d'habilitation dans le cadre de la procédure d'urgence prévue par la présente instruction. Cet avis prend fin lors de la délivrance de l'avis de sécurité définitif ou au plus tard six mois après avoir été accordé.

Avis technique d'aptitude physique (ATAP) : appréciation rendue par le service enquêteur portant sur la capacité physique des locaux à conserver et traiter des informations et supports classifiés au niveau requis selon les modalités définies par la présente instruction. Cet avis prend en compte la conformité aux exigences de sécurité du système d'information chargé du contrôle d'accès.

Besoin d'en connaître : nécessité impérieuse de prendre connaissance d'une information dans le cadre de l'exercice d'une fonction ou l'accomplissement d'une mission.

Bureau de protection du secret : bureau chargé de l'élaboration, du marquage, de la conservation, de l'acheminement, de l'enregistrement, du suivi et de la destruction des informations et supports classifiés au sein de l'organisme. Il est obligatoirement créé et dispose d'une zone réservée pour les organismes détenant des informations et supports classifiés au niveau *Très Secret*. Sa création est recommandée pour les organismes détenant des informations et supports classifiés au niveau *Secret*.

Catalogue des emplois : établi pour chaque niveau de classification, il permet d'identifier *via* l'octroi d'un numéro de poste, chaque fonction ou mission impliquant nécessairement l'accès à des informations et supports classifiés au niveau de classification considéré, ainsi que les nom et prénom des personnes physiques les occupant. Un organisme peut ainsi détenir plusieurs catalogues des emplois.

Certificat de sécurité : document attestant de l'habilitation d'une personne à accéder à des informations et supports classifiés à un niveau donné.

Compromission : destruction, détournement, soustraction, reproduction non autorisée ou divulgation d'une information ou d'un support classifié à une ou plusieurs personnes non qualifiées au sens de la présente instruction.

Compte administrateur : droits attribués à une personne exerçant les fonctions d'administrateur permettant l'accès privilégié à un système d'information dans le but exclusif d'y réaliser des actions d'administration.

Compte utilisateur : droits attribués à une personne permettant l'accès à un système d'information dans le but d'y réaliser les actions attendues.

Contrat sensible : contrat, quel que soit son régime juridique ou sa dénomination, qui n'implique pas l'accès à des informations ou supports classifiés mais dont l'exécution nécessite l'accès à un lieu abritant des éléments couverts par le secret de la défense nationale.

Décision d'habilitation : acte administratif autorisant, au terme d'une procédure d'habilitation, le titulaire (personne physique ou morale), en fonction de son besoin d'en connaître, à accéder aux informations et supports classifiés à un niveau inférieur ou égal au niveau mentionné sur la décision.

Décision d'habilitation provisoire : autorisation exceptionnelle et temporaire prise au vu d'un avis de sécurité provisoire délivré dans le cadre de la procédure d'urgence prévue par la présente instruction et permettant l'accès d'une personne aux informations et supports classifiés. Cette décision prend fin lors de la délivrance de la décision définitive ou au plus tard six mois après avoir été accordée.

Décision d'homologation : décision prise par l'autorité d'homologation à l'issue de la démarche d'homologation par laquelle l'autorité d'homologation assume les risques résiduels pesant sur le système d'information considéré et atteste de la capacité de ce système à traiter des informations classifiées pour un niveau de classification donné.

Décision d'habilitation temporaire : décision d'habilitation à accéder à des informations ou supports classifiés au niveau *Très Secret*, à l'exception des informations et supports faisant l'objet d'une classification spéciale, valable pour une durée maximale de trois mois et non renouvelable, délivrée à une personne faisant, par ailleurs, l'objet d'une habilitation au niveau *Secret* conformément au catalogue des emplois de son organisme.

Décision de sécurité convoyeur : autorisation accordée pour assurer, durant le transport, la garde des informations et supports classifiés. Cette décision est délivrée après une enquête administrative effectuée par le service enquêteur compétent.

Déclassement : modification, par abaissement, du niveau de classification d'une information ou d'un support classifié.

Déclassification : suppression de la classification d'une information ou d'un support classifié. Elle intervient automatiquement, sans qu'une décision de déclassification, ni l'apposition d'un timbre de déclassification ne soit nécessaire pour les informations et supports mentionnant la date à partir de laquelle la classification devient caduque, ni pour les informations et supports devenus communicables de plein droit en application de l'article L. 213-2 du code du patrimoine. Pour les informations et supports classifiés dont les délais de communicabilité de plein droit ne sont pas échus, la déclassification n'est effective qu'après l'adoption d'une décision formelle de déclassification par l'autorité émettrice compétente matérialisée par un timbre de déclassification.

Directives techniques particulières : chaque ministre peut en complément de l'instruction ministérielle et sur son fondement, élaborer des directives techniques particulières destinées à préciser, pour un domaine d'activité spécifique, les mesures de protection du secret complémentaires à mettre en œuvre. Chaque directive particulière contient un guide de

classification spécifique au domaine considéré permettant à chaque organisme d'évaluer le niveau de classification des informations et supports qu'il produit et d'en déduire les mesures d'organisation et de protection à mettre en œuvre.

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

Dossier d'habilitation d'une personne physique : dossier constitué en vue de l'habilitation d'une personne. Il comporte la demande d'habilitation établie par l'autorité demandeuse et attestant le besoin d'en connaître, la notice individuelle renseignée par le candidat et une photographie d'identité récente.

Dossier d'habilitation d'une personne morale : dossier permettant d'apprécier les garanties offertes par la personne morale 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 et supports classifiés.

Dossier sécurité d'une personne morale : ensemble des pièces administratives liées à l'exécution des prestations du contrat nécessitant l'accès à des informations et supports classifiés.

Élément constitutif d'un système d'information classifié : tout élément actif relié physiquement ou logiquement à un système d'information. Sont notamment entendus comme des éléments constitutifs au système d'information les supports de stockage dédiés au système d'information (internes ou externes), les écrans et les dispositifs d'affichage et de projection, les commutateurs, routeurs, pare-feu ou autres équipements réseau distribuant les flux, les unités centrales ou les boîtiers de serveurs et de postes de travail, tout équipement du système d'information fourni à l'utilisateur et les imprimantes, claviers et autres périphériques d'entrée et de sortie. Les supports amovibles ne sont pas considérés comme tels.

Engagement de responsabilité : document en deux volets signés par le titulaire de la décision d'habilitation par lequel il reconnaît avoir été informé que les manquements aux obligations liées à son habilitation sont susceptibles d'engager sa responsabilité pénale. Le premier volet est signé lors de la notification de la décision d'habilitation, le second lors de sa cessation de fonction ou, le cas échéant, en cas d'abrogation explicite de la décision d'habilitation, lors de la notification de la décision d'abrogation.

Exigences de sécurité relative à la sécurité des systèmes d'information classifiés : mesures de protection organisationnelles, physiques, logiques et environnementales, conformes aux lignes directrices définies par l'autorité qualifiée en sécurité des systèmes d'information, visant à garantir la sécurité d'un système d'information classifié. Ces exigences sont intégrées à la politique de protection du secret des organismes utilisant un système d'information classifié et sont précisées pour chaque système d'information classifié dans la politique de sécurité du système d'information classifié versée au dossier d'homologation.

Enquête administrative : procédure destinée à vérifier que le comportement des personnes physiques ou morales intéressées n'est pas incompatible avec l'exercice de la fonction ou l'accomplissement de la mission envisagée (Art. L. 114-1 du code de la sécurité intérieure).

Équipement de mobilité : matériel informatique non-fixe conçu pour permettre le traitement ou la consultation d'informations classifiées dématérialisées (ordinateur portable, téléphone portable, etc.).

Fonctionnaire de sécurité de défense (FSD) : personne placée auprès du haut fonctionnaire de défense et de sécurité, chargée d'accompagner les responsables d'organisme dépendant du champ d'attribution de son ministère dans l'animation de leur chaîne fonctionnelle de protection du secret.

Fonctionnaire de sécurité des systèmes d'information (FSSI) : personne placée auprès du HFDS, chargée d'accompagner les responsables d'organisme dépendant du champ d'attribution de son ministère dans l'animation de leurs chaînes fonctionnelles de sécurité des systèmes d'information et de sécurité des articles contrôlés de la sécurité des systèmes d'information.

Haut fonctionnaire de défense et de sécurité (HFDS) : autorité 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 défense et de sécurité (HFCDS) ou haut fonctionnaire de défense (HFD).

Homologation d'un système d'information : démarche visant à s'assurer, sur la base d'une analyse de risques globale, prenant en compte tous les éléments, y compris environnementaux, indispensables au fonctionnement et à la sécurité du système d'information considéré, que l'ensemble des risques a été identifié et fait l'objet d'un traitement approprié et que les risques résiduels sont acceptés. Cette démarche est sanctionnée par une décision d'homologation par laquelle l'autorité d'homologation atteste de la capacité du système d'information à traiter des informations classifiées pour un niveau de classification donné.

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

Information d'authentification : donnée visant à établir l'identité de l'utilisateur d'un système d'information au moyen d'un identifiant attribué individuellement et d'un authentifiant (code secret ou mot de passe).

Informations et supports classifiés : information, document, support, matériel, procédé, réseau informatique, donnée informatisée ou fichier, quels qu'en soient la forme, la nature ou le mode de transmission, qu'ils soient élaborés ou en cours d'élaboration, auxquels un niveau de classification a été attribué et qui, dans l'intérêt de la défense nationale et conformément aux procédures, lois et règlements en vigueur, nécessitent une protection contre toute violation, toute destruction, tout détournement, toute divulgation, toute perte ou tout accès par toute personne non autorisée ou tout autre type de compromission. Pour avoir accès à ce type d'information, il faut être habilité au niveau requis et avoir le besoin d'en connaître.

Inspection : mission consistant à s'assurer que les objectifs fixés par la présente instruction et ses déclinaisons ministérielles sont compris et appliqués. Le résultat d'une inspection est adressé aux autorités concernées.

Intégrité : propriété assurant qu'une information n'a pas été modifiée ou détruite de façon non autorisée.

Interconnexion : dispositif rendant possible le transfert d'information entre deux systèmes d'information par une continuité de signaux électromagnétiques entre les deux systèmes d'information (exemple : câble réseau, diode optique, etc.).

Journalisation des événements : processus consistant à enregistrer dans un format donné les événements fonctionnels ou techniques consécutifs à des actions réalisées sur une ressource du système d'information considéré.

Lieu abritant des éléments couverts par le secret de la défense nationale : pièce dans laquelle sont conservés des informations et supports classifiés, quel qu'en soient le niveau et le volume, répertoriée dans la liste des lieux abritant fixée chaque année par arrêté du Premier ministre conformément à l'article 56-4 du code de procédure pénale.

Lignes directrices relatives à la sécurité des systèmes d'information classifiés : lignes directrices fixées pour l'autorité qualifiée en sécurité des systèmes d'information dans la

politique de sécurité des systèmes d'information, auxquelles les organismes relevant de son champ d'attribution et utilisant un système d'information classifié doivent se conformer. Ces lignes directrices sont déclinées dans les exigences de sécurité relatives à la sécurité des systèmes d'information intégrées dans la politique de sécurité des informations et supports de l'organisme et dans les politiques de sécurité de chaque système d'information classifié.

Marquage : opération consistant à apposer sur un support classifié les mentions précisant son niveau de protection ou de classification, l'échéance de la 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 portant un timbre de classification et nécessitant une protection conforme à son niveau de classification.

Mécanismes d'importation ou d'exportation : mécanismes utilisés pour importer ou exporter des informations, classifiées ou non, vers ou depuis un système d'information classifié tel que, notamment, les guichets des diodes, les stations associées à leur durcissement, les moyens logiciels ou la solution logicielle employée.

Mise en éveil : démarche engagée par l'autorité d'habilitation auprès de la personne à habilitier pour la sensibiliser à ses vulnérabilités découvertes au cours de l'enquête administrative.

Mise en garde : démarche engagée par l'autorité d'habilitation visant à sensibiliser l'officier de sécurité du service employeur ou l'autorité hiérarchique du candidat à l'habilitation sur l'existence d'éléments pouvant présenter un risque de vulnérabilité pour le secret de la défense nationale.

Notice individuelle de sécurité : formulaire destiné à recueillir les renseignements nécessaires à l'habilitation d'une personne. Elle est renseignée par le candidat à l'habilitation et l'autorité sollicitant l'habilitation. Elle constitue un élément majeur du dossier d'habilitation et est exploitée par l'autorité d'habilitation et le service enquêteur.

Organisme : au titre de la présente instruction, tout service de l'État (services centraux, services déconcentrés, services à compétence nationale, organismes extérieurs), personne morale ayant accès, même à titre provisoire, à des informations et supports classifiés.

Passerelle d'interconnexion : dispositif ou ensemble de dispositifs permettant le transfert d'information entre deux systèmes d'information.

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 ou à détenir un support classifié et a le besoin d'en connaître.

Plan contractuel de sécurité : document attaché à une convention ou à un contrat énumérant, les engagements pris par la personne morale cocontractante de l'État pour protéger les informations et supports classifiés auxquelles elle aura accès dans le cadre de la convention ou du contrat. Ce document fait partie intégrante de la convention ou du contrat.

Plan d'urgence : document établi par un organisme détenteur d'informations et supports classifiés, prévoyant, en cas de circonstances exceptionnelles, les modalités d'évacuation ou de destruction des supports d'information.

Politique des informations et supports classifiés : document définissant l'ensemble des mesures de protection mises en œuvre par l'organisme pour protéger les informations et supports classifiés auquel il a accès. Ce document est élaboré par l'officier de sécurité de l'organisme, en lien avec l'officier de sécurité des systèmes d'information pour les organismes utilisant un système d'information classifié. Il est conforme à la présente

instruction, ainsi qu'à l'instruction ministérielle et le cas échéant aux directives techniques particulières applicables. Il prend en compte les obligations souscrites par l'organisme dans le cadre des plans contractuels de sécurité qui lui sont applicables.

Politique de sécurité des systèmes d'information : politique, applicable à l'ensemble des organismes relevant de l'autorité qualifiée en sécurité des systèmes d'information, définissant les mesures de sécurité des systèmes d'information dans leur ensemble. Les lignes directrices pour la sécurité des systèmes d'information constituent un sous-ensemble de cette politique générale.

Politique de sécurité d'un système d'information classifié : document, versé au dossier d'homologation, déclinant pour un système d'information donné les exigences de sécurité relatives à la sécurité des systèmes d'information intégrées dans la politique de protection du secret de l'organisme.

Principe du moindre privilège : principe consistant à attribuer à un utilisateur d'un système d'information les seuls droits d'accès à une information ou une ressource strictement nécessaire à son besoin légitime.

Primo-contractant : personne physique ou morale 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 ou sous-contractants.

Procédure d'habilitation : procédure visant à s'assurer qu'une personne peut, sans risque pour la défense et la sécurité nationale ou pour sa propre sécurité, connaître des informations et supports classifiés dans l'exercice de ses fonctions.

Reclassement : modification, par relèvement, du niveau de classification d'une information ou d'un support classifié.

Refus d'habilitation : décision prise par l'autorité d'habilitation, au vu de l'avis de sécurité ou de tout autre élément recueilli sur une personne, de ne pas habilitier cette personne.

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 d'évaluer l'opportunité de renouveler l'habilitation de la personne.

Responsable d'organisme : au sens de la présente instruction, pour les services de l'État (services centraux, services déconcentrés, services à compétence nationale, organismes extérieurs), le responsable d'organisme est le chef du service ayant accès à des informations et supports classifiés (directeur de cabinet ministériel, secrétaire général d'un ministère, directeur d'administration centrale, chef de service, chef d'établissement, etc.). Pour les personnes morales autres que l'État, le responsable d'organisme est le représentant légal de la personne morale. Le responsable d'organisme est pénalement responsable de la protection du secret de la défense nationale au sein de son organisme et par ses personnels.

Sensibilisation : instruction périodiquement prodiguée aux personnes habilitées ou susceptibles d'être habilitées, destinée à leur faire prendre conscience des enjeux de la protection du secret de la défense nationale et des informations sensibles, à les familiariser avec leur obligation de signalement de tout incident dans le respect des règles associées, à les mettre en capacité d'identifier les tentatives d'approche et à leur rappeler les sanctions judiciaires et administratives encourues en cas de manquement aux règles.

Service enquêteur : au sens de la présente instruction, service du ministère de la défense ou du ministère de l'intérieur chargé de procéder aux enquêtes administratives d'habilitation, d'évaluer l'aptitude physique des lieux abritant. Ces services rendent leurs conclusions sous forme d'avis.

Spécial France : mention complémentaire visant à restreindre la divulgation d'une information ou d'un support aux seuls ressortissants français. Une information ou un support portant cette mention ne peut-être communiqué, en tout ou partie, à un État étranger ou à l'un de ses ressortissants, organisation internationale ou personne morale de droit étranger, même s'il existe un accord de sécurité, général ou spécifique, entre la France et l'État ou l'organisation internationale considéré, sous réserve, lorsque cette mention est apposée sur des informations et supports protégés par la mention *Diffusion Restreinte*, des exigences résultant du code du patrimoine et du code des relations entre le public et l'administration.

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 d'administration : système d'information comprenant les ressources nécessaires pour administrer un système d'information considéré.

Système d'information classifié : système d'information homologué pour traiter, stocker ou transmettre des informations classifiées.

Timbre : mention figurant sur un support d'information précisant son niveau de classification et, le cas échéant, une mention de protection complémentaire. Le timbre respecte les caractéristiques définies par la présente instruction (dimensions, emplacement, aspect).

Travail à distance : toute forme d'organisation dans laquelle des fonctions exercées habituellement dans les locaux de l'employeur sont réalisées hors de ces locaux, soit de façon régulière et volontaire (télétravail), soit de façon occasionnelle ou ponctuelle (nomadisme).

Visite d'aptitude : évaluation de la conformité d'un lieu destiné à abriter des informations et supports classifiés conformément aux obligations fixées par la présente instruction et, le cas échéant, par l'instruction ministérielle, les directives techniques qui s'attachent à chaque niveau de classification.

Vulnérabilité : élément relatif à la situation d'une personne, d'un système d'information ou d'un local et qui amoindrit les garanties qu'il présente face aux menaces sur la protection des informations et supports classifiés.

Zone protégée : zone créée par arrêté du ministre déterminant le besoin de protection 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 créé par le responsable d'organisme, au sein d'une zone protégée, qui fait l'objet de mesures de protection matérielle particulières et dont l'accès est réglementé et subordonné à des conditions spéciales.

INTRODUCTION

La présente instruction vise à renforcer la rigueur avec laquelle il est fait recours au secret de la défense nationale, selon un principe de stricte nécessité. Elle clarifie les règles relatives au maniement des informations et supports classifiés dans un contexte de dématérialisation accélérée et de besoin d'échange accru avec les acteurs privés et les partenaires étrangers.

Tirant par ailleurs pleinement les conséquences de la récente modification législative du code du patrimoine, elle s'inscrit plus largement dans la volonté gouvernementale de faciliter, partout où cela est possible, le libre accès aux archives publiques.

Fondée sur le principe d'une conciliation au plus juste des impératifs constitutionnels de sauvegarde des intérêts fondamentaux de la Nation et d'obligation, pour tout Gouvernement, de rendre compte de son administration, elle s'articule autour du diptyque : « *Mieux classifier pour mieux protéger* ».

MIEUX CLASSIFIER...

Visant à protéger les informations et supports dont la divulgation ou auxquels l'accès est de nature à nuire à la défense et à la sécurité nationale, le secret de la défense nationale participe de la sauvegarde des intérêts fondamentaux de la Nation¹.

Le secret de la défense nationale est invoqué dans les domaines de l'action publique, et notamment, politique, militaire, diplomatique, scientifique, économique et industrielle, dès lors que les informations et supports qu'il entend protéger ont fait l'objet d'une mesure de classification.

La décision de classification, matérialisée par l'apposition du timbre de classification correspondant, constitue ainsi la pierre angulaire de la protection du secret de la défense nationale. C'est elle qui confère son caractère de secret de la défense nationale à une information ou à un support à protéger. C'est également elle qui justifie, en cas de violation de la réglementation applicable, la mise en œuvre des sanctions pénales associées.

Décider de classer une information ou un support est un acte important, tant par les mesures de protection contraignantes qui en découlent, que par les conséquences judiciaires que cette décision peut entraîner.

La décision de classification est ainsi à manier au plus juste :

- utilisée de façon abusive, la classification nuit, de par les mesures de protection qu'elle impose, à l'exigence de réactivité et d'agilité de l'action publique. Elle se traduit par une dévaluation du secret de la défense nationale et une érosion progressive du respect des règles associées ;
- sous-employée, elle facilite l'accès des services de renseignement étrangers, des groupements hostiles ou des individus cherchant à déstabiliser l'État ou la société, à des informations et supports dont la divulgation est de nature à nuire aux intérêts fondamentaux de la Nation.

La sur-classification, comme la sous-classification, sont ainsi porteuses de risques pour la sécurité de la Nation.

Dans ce contexte, la présente instruction précise les règles relatives à la protection du secret de la défense nationale pour permettre à l'ensemble des personnes, physiques et morales,

¹ Conseil constitutionnel, décision n° 2011-192 QPC du 10 novembre 2011, décision n° 2015-713 DC du 23 juillet 2015 et décision n° 2016-738 DC du 10 novembre 2016.

amenées à accéder, produire, détenir, échanger des informations et supports classifiés, de mieux classifier pour mieux protéger.

Cet objectif n'est pas nouveau, mais il gagne aujourd'hui en acuité face à la nécessité paradoxale d'ouvrir l'accès au secret de la défense nationale à de nouveaux publics dans un contexte d'internationalisation accélérée des politiques de sécurité et de nécessaire implication accrue des acteurs publics et privés dans leur mise en œuvre.

Pour y répondre, le décret n° 2019-1271 du 2 décembre 2019 relatif aux modalités de classification et de protection du secret de la défense nationale a substitué aux trois niveaux de classification *Confidentiel Défense*, *Secret Défense* et *Très Secret Défense*, les niveaux *Secret* et *Très Secret*. Ce recentrement du dispositif de protection du secret de la défense nationale procède d'une double préoccupation :

- éviter la tendance à un recours irraisonné au plus bas niveau de classification et, par suite, endiguer la prolifération d'informations et supports classifiés ;
- réaligner les standards de protection des niveaux de classification français sur les standards de protection des niveaux de classification des partenaires internationaux, afin de mieux protéger les informations et supports classifiés échangés avec ces derniers.

Dans ce cadre réglementaire rénové, la présente instruction définit par chacun des niveaux de classification *Secret* et *Très Secret*, une protection proportionnée au risque encouru en cas de divulgation des informations et supports qu'il couvre. Le niveau *Secret* protège les informations et supports dont la divulgation ou auxquels l'accès est de nature à porter atteinte à la défense et à la sécurité nationale, tandis que le niveau *Très Secret* concerne ceux dont la divulgation ou auxquels l'accès aurait des conséquences exceptionnellement graves pour la défense et la sécurité nationale. Elle organise également les règles relatives au maniement des informations et supports portant la mention *Diffusion Restreinte* qui n'est pas un niveau de classification mais une mention de protection assortie de règles propres².

Elle réaffirme également l'obligation, pour chaque ministre, de préciser par arrêté pour les services relevant de son autorité, les établissements publics placés sous sa tutelle, les opérateurs d'importance vitale dont il est le ministre coordonnateur et les personnes morales avec lesquelles il est lié par une convention ou un contrat, les modalités de classification et de protection aux niveaux *Secret* et *Très Secret*.

Elle renforce l'obligation de réexaminer le niveau de classification à toutes les étapes du cycle de vie d'un document classifié. De même, afin de faciliter l'accès aux archives publiques dans le respect de l'impératif de sauvegarde des intérêts fondamentaux de la Nation, cette nouvelle instruction tire, d'une part, pleinement les conséquences de l'article 25 de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement en rappelant que tout document ayant fait l'objet d'une mesure de classification au sens de l'article 413-9 du code pénal est automatiquement déclassifié, sans autre formalité nécessaire, dès lors qu'il devient librement communicable au sens de l'article L. 213-2 du code du patrimoine et même dès cinquante ans après son émission pour les documents frappés du délai de communicabilité de soixante-quinze ans. Elle met, d'autre part, en place des dispositions nouvelles visant à favoriser la déclassification des informations et supports classifiés avant l'échéance des délais de communicabilité prévus au code du patrimoine.

² Cf. Annexe 1.

... POUR MIEUX PROTEGER

Tirant également les conséquences de l'accroissement des coopérations internationales, ainsi que de l'ouverture à la concurrence européenne des marchés publics de défense ou de sécurité, la présente instruction aligne les standards de classification et de protection nationaux sur les standards internationaux afin de faciliter les échanges, tout en garantissant le respect de mesures de sécurité suffisantes. Elle clarifie les règles applicables dans le cadre des coopérations internationales et des contrats internationaux, ainsi que la procédure d'habilitation des ressortissants français appelés à accéder à des informations et supports classifiés au profit d'États étrangers ou d'organisations internationales.

Elle prend davantage en compte la dématérialisation croissante des informations classifiées. À cette fin, elle précise l'articulation entre la chaîne fonctionnelle de protection du secret et la chaîne fonctionnelle de sécurité des systèmes d'information et énonce les règles relatives à la sécurité des systèmes d'information homologués pour traiter des informations classifiées, afin de garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité des informations traitées par leur biais.

Enfin, elle explicite les règles applicables à l'ensemble des organismes amenés à accéder, même à titre provisoire, à des informations et supports classifiés, indépendamment de leur forme juridique et des finalités justifiant qu'ils y aient accès.

La présente instruction est applicable aux services de l'État, ainsi qu'à toute personne physique ou morale, indépendamment de son statut juridique, ayant accès, même à titre provisoire, au secret de la défense nationale ou à des informations ou supports portant la mention de protection *Diffusion Restreinte*.

Les termes les plus couramment utilisés dans la présente instruction sont définis dans le glossaire.

1 PRINCIPES GENERAUX

1.1 FONDEMENT DU SECRET DE LA DEFENSE NATIONALE

Le secret de la défense nationale vise, au travers de mesures de sécurité physiques, logiques ou organisationnelles à protéger les informations et supports dont la divulgation ou auxquels l'accès est de nature à nuire à la défense et à la sécurité nationale. Protégeant la Nation contre l'espionnage des services de renseignement étrangers et les tentatives de déstabilisation par des groupements terroristes, criminels, subversifs ou des individus isolés, la protection du secret de la défense nationale participe de la sauvegarde des intérêts fondamentaux de la Nation.

Le secret de la défense nationale est invoqué dans les domaines de l'action publique, et notamment, politique, militaire, diplomatique, scientifique, économique et industrielle, dès lors que les informations et supports qu'il entend protéger ont fait l'objet d'une mesure de classification.

La décision de classer une information ou un support au titre de la protection du secret de la défense nationale est une prérogative du pouvoir exécutif qui repose sur plusieurs fondements constitutionnels³.

Le secret de la défense nationale constitue ainsi un outil essentiel à l'exercice par l'État de ses missions régaliennes, et repose, à ce titre, sur un régime spécifique. Il est, parmi les différents secrets protégés par la loi, celui dont la répression pénale est la plus sévère et l'opposabilité, y compris au juge et à la représentation nationale, est la plus stricte, même si elle connaît quelques exceptions (cf. 1.2.2).

Corollaire de cette spécificité, le secret de la défense nationale impose une extrême rigueur dans son maniement et la mise en œuvre des mesures de protection qu'il induit. Il ne doit jamais être convoqué de façon arbitraire ou illégitime. En particulier, le recours indu au secret de la défense nationale en vue de faire obstacle à la manifestation de la vérité expose son auteur aux sanctions prévues à l'article 434-4 du code pénal⁴. La défense et la sécurité nationale sont et doivent être les seuls motifs présidant à la décision de classification.

1.2 ACCES AU SECRET DE LA DEFENSE NATIONALE

1.2.1 Principes généraux

Conformément aux articles 413-10 et suivants du code pénal, l'accès au secret de la défense nationale par des personnes non qualifiées est prohibé.

1.2.1.1 Principes régissant l'accès des personnes physiques au secret de la défense nationale

En application des articles R. 2311-7 à R. 2311-7-2 du code de la défense, deux critères cumulatifs doivent être réunis pour qu'une personne physique puisse accéder au secret de la défense nationale : l'habilitation et le besoin d'en connaître.

Sont ainsi considérées comme des personnes qualifiées au sens du code pénal, les personnes physiques :

- habilitées au niveau de classification requis conformément à l'une des procédures d'habilitation détaillées aux parties 3.2 et 3.3 ou habilitées *ès qualités* de par la loi ou leur statut constitutionnel (cf. 3.1.4) ;

³ Articles 5, 20 et 21 de la Constitution.

⁴ Article 56-4 du code de procédure pénale.

- justifiant, pour l'exercice de leur fonction ou l'accomplissement de leur mission, du besoin de connaître d'une information ou d'un support classifié tel qu'attesté par le catalogue des emplois établi par l'autorité d'emploi ou l'autorité administrative conformément aux dispositions détaillées au paragraphe 3.1.2.

1.2.1.2 Principes régissant l'accès des personnes morales au secret de la défense nationale

En application des articles R. 2311-7 à R. 2311-7-2 du code de la défense, sont considérées comme des personnes qualifiées au sens du code pénal :

- les services de l'État et les établissements publics sous sa tutelle dans la limite du besoin d'en connaître et du respect des modalités prescrites par la présente instruction, l'instruction ministérielle et, le cas échéant, les directives techniques particulières applicables ;
- les opérateurs désignés opérateurs d'importance vitale dans la limite du besoin d'en connaître en raison de leur désignation en tant qu'opérateurs d'importance vitale et du respect des modalités prescrites, d'une part, par la présente instruction, l'instruction ministérielle et, le cas échéant, les directives techniques particulières applicables, ainsi que, d'autre part, par le plan de sécurité d'opérateur ou le plan particulier de protection ;
- les collectivités territoriales, leurs établissements publics et les personnes morales de droit privé autorisées par l'État à accéder à des informations et supports classifiés pour un besoin précis défini dans le cadre d'une convention et sous réserve du respect des modalités prescrites, d'une part, par la présente instruction, l'instruction ministérielle et, le cas échéant, les directives techniques particulières applicables et, d'autre part, le plan contractuel de sécurité attaché à ladite convention ;
- les personnes morales habilitées au niveau requis au titre d'un contrat de la commande publique, d'un contrat de sous-traitance ou d'un sous-contrat à un contrat de la commande publique, d'un contrat de subvention ou dans le cadre d'un contrat exécuté au profit d'une entité étrangère ou d'une organisation internationale, dans les limites du besoin d'en connaître défini dans l'objet du contrat, selon les modalités prescrites, d'une part, par la présente instruction, l'instruction ministérielle et, le cas échéant, les directives techniques particulières applicables, et, d'autre part, par le plan contractuel de sécurité attaché au contrat.

1.2.2 Cas spécifiques

1.2.2.1 Personnes morales et ressortissants de droit étranger

Les conditions préalablement énoncées sont indépendantes de la nationalité de la personne physique ou du droit applicable à la personne morale considérée.

Ainsi, conformément aux dispositions détaillées au paragraphe 3.2.5, un ressortissant étranger peut, sous réserve de son habilitation préalable au niveau requis et dans la stricte limite du besoin d'en connaître, accéder à des informations et supports classifiés aux niveaux *Secret* et *Très Secret*.

De même, une personne morale de droit étranger peut être qualifiée pour accéder à des informations et supports classifiés aux niveaux *Secret* et *Très Secret*, dès lors qu'il existe, un accord de sécurité, général ou spécifique, entre la France et l'État ou l'organisation internationale dont relève l'organisme et que les exigences fixées par cet accord sont remplies (cf. 7.2.1.3).

Dans les deux cas, l'autorité nationale de sécurité ou l'autorité de sécurité déléguée mentionnées aux articles R. 2311-10 et R. 2311-10-1 du code de la défense peut décider, si le

ressortissant ou la personne morale a déjà été habilité(e) par l'État dont il(elle) relève et si l'accord de sécurité général ou spécifique conclu avec cet État le permet, de reconnaître l'habilitation délivrée par l'autorité étrangère sans que la délivrance d'une nouvelle décision d'habilitation par l'autorité nationale de sécurité ou l'autorité de sécurité déléguée soit nécessaire.

En revanche, conformément à l'article R. 2311-4 du code de la défense, aucun État, aucun ressortissant étranger, aucune organisation internationale, aucune institution, organe ou organisme de l'Union européenne, ni aucune personne morale de droit étranger ne peut se voir communiquer d'informations ou supports classifiés ou protégés comportant la mention *Spécial France*.

1.2.2.2 Personnes dans l'exercice de prérogatives juridictionnelles

a) Les juridictions n'ont pas accès au secret de la défense nationale

Le principe constitutionnel de séparation des pouvoirs interdit aux magistrats aussi bien judiciaires qu'administratifs et aux membres du Conseil d'État agissant dans le cadre de leurs prérogatives juridictionnelles d'accéder à des informations et supports couverts par le secret de la défense nationale⁵. La seule exception à ce principe concerne les membres de la formation spécialisée du Conseil d'État chargée du contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et de l'exercice du droit d'accès aux fichiers intéressant la sûreté de l'État (cf. 2.1.3.3)⁶.

Afin de concilier le principe de séparation des pouvoirs avec le droit à un recours effectif et l'objectif à valeur constitutionnelle de recherche des auteurs d'infraction, le code de la défense a cependant prévu une procédure spécifique qui permet à toute juridiction française, qu'elle soit administrative⁷ ou judiciaire, de demander les déclassifications qui lui sont nécessaires à la conduite de la procédure engagée devant elle⁸.

L'autorité administrative compétente doit alors saisir la commission du secret de la défense nationale, autorité administrative indépendante chargée de rendre un avis public sur la déclassification sollicitée par le juge. Cette procédure s'impose pour toutes les informations et supports portant un marquage de classification français⁹.

La procédure de déclassification est la même pour les deux ordres juridictionnels (cf. 1.2.2.2 a) i.). En revanche, les pouvoirs d'enquête particuliers dont disposent les magistrats en charge

⁵ En revanche, des magistrats, judiciaires ou administratifs ou des membres du Conseil d'État, peuvent, hors l'exercice de ces prérogatives, accéder au secret de la défense nationale. Ils sont alors habilités soit *ès qualités* si la loi en dispose ainsi (cas des magistrats membres d'autorités administratives indépendantes autorisées à accéder au secret de la défense nationale, cf. 3.1.4) soit selon l'une des procédures d'habilitation détaillées aux parties 3.2 et 3.3 (cas des magistrats détachés sur une fonction ou pour l'accomplissement d'une mission administratives).

⁶ Cf. articles L. 841-1 et L. 841-2-2 du code de la sécurité intérieure et article L. 773-2 du code de justice administrative.

⁷ Y compris les juridictions administratives spécialisées, à l'image de la Cour des comptes et des chambres régionales et territoriales des comptes lorsqu'elles statuent en matière juridictionnelle. En revanche, cette procédure n'est pas ouverte aux autorités administratives indépendantes, qui ne sont pas des juridictions.

⁸ Dans les procédures où les magistrats français agissent en exécution d'une demande de coopération d'une juridiction étrangère ou internationale, et sauf le cas des décisions d'enquêtes européennes, l'autorité administrative décide seule du maintien ou de la mainlevée de la classification pour répondre à la juridiction, sans demande d'avis préalable à la commission du secret de la défense nationale.

⁹ Pour ceux qui relèvent d'une autorité étrangère, d'une organisation internationale, d'une institution, d'un organe ou organisme de l'Union européenne, le magistrat saisit les autorités étrangères d'une demande de déclassification sans que la procédure impliquant la commission du secret de la défense nationale trouve à s'appliquer. Le secrétaire général de la défense et de la sécurité nationale, en sa qualité d'autorité nationale de sécurité, peut, en tant que de besoin, l'accompagner dans cette démarche.

du contentieux pénal, procureurs de la République et juridictions d'instruction notamment¹⁰, justifient des règles spécifiques de perquisition et de saisie prévues au code de procédure pénale et qui s'imposent à peine de nullité (cf. 1.2.2.2 a) ii.).

i. Déclassification pour les besoins d'une procédure contentieuse

Lorsqu'une juridiction décide de solliciter la déclassification d'informations et supports classifiés pour les besoins de la procédure, le processus de déclassification se déroule alors en trois phases successives¹¹.

La juridiction adresse d'abord une requête motivée à l'autorité administrative compétente, à savoir l'autorité émettrice, qui saisit sans délai la commission du secret de la défense nationale. Cette saisine est obligatoire, même si cette autorité est *a priori* favorable à la déclassification des informations et supports pour lesquels la demande est formulée¹².

La motivation de la requête permet à la commission de vérifier l'adéquation des recherches documentaires et l'intérêt d'une déclassification au regard des besoins de la juridiction compétente. Les critères de la délibération de la commission sont, d'une part, les missions du service public de la justice, autrement dit la recherche de la manifestation de la vérité, le respect de la présomption d'innocence et les droits de la défense et, d'autre part, le respect des engagements internationaux de la France, la nécessité de préserver les capacités de défense et la sécurité des personnes.

Ensuite, la commission du secret de la défense nationale émet, dans le délai de deux mois à compter de sa saisine, un avis qui peut être favorable, favorable à une déclassification partielle ou défavorable. Elle le transmet à l'autorité administrative compétente. Le sens de l'avis est publié au Journal officiel de la République française.

Enfin, dans un délai de quinze jours francs à compter de la réception de l'avis de la commission, ou de l'expiration du délai de deux mois à compter de la saisine à défaut d'avis rendu, l'autorité administrative compétente décide de lever la classification ou bien de la maintenir sur toute ou partie des informations et supports classifiés sans être liée par l'avis de la commission. Elle notifie sa décision à la juridiction ayant demandé la déclassification. Cette décision, qui est dispensée de l'obligation de motivation¹³, est insusceptible de recours.

Chaque élément déclassifié est revêtu du timbre de déclassification précisant la date de la décision du ministre : il peut alors être joint au dossier de la procédure dans le respect du principe du contradictoire. Le versement à la procédure, même par erreur, d'une pièce classifiée, doit conduire à prendre immédiatement toute mesure pour faire cesser la diffusion et limiter ses conséquences, tout en préservant, autant que possible, les éléments utiles à la matérialisation du délit. En effet, cette situation fait encourir les sanctions pénales prévues pour la compromission, à celui qui en est à l'origine et à ceux qui relaient l'information compromise. Les dispositions de l'article 40 du code de procédure pénale relatives à la dénonciation du délit au procureur de la République trouvent par ailleurs à s'appliquer¹⁴.

¹⁰ Les juridictions de jugement procèdent parfois à des suppléments d'information et agissent alors comme des juges d'instruction.

¹¹ Cf. articles L. 2312-4 et suivants du code de la défense.

¹² L'expression « sans délai » doit être entendue comme le temps strictement nécessaire à la collecte des éléments sollicités avec la préoccupation constante de permettre à la juridiction d'obtenir une réponse le plus rapidement possible. En outre, au-delà de la notion de promptitude que cette expression contient, elle signifie que l'autorité responsable de la classification a "compétence liée" pour saisir la commission du secret de la défense nationale (rapport n° 337 au projet de loi n° 98-567 du 8 juillet 1998 instituant une commission consultative du secret de la défense nationale).

¹³ Article L. 211-2 du code des relations entre le public et l'administration.

¹⁴ Cf. alinéa 2 de l'article 40 du code de procédure pénale : « toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit, est tenu

ii. Perquisition et saisie de documents classifiés par les magistrats judiciaires

Acte préalable à une saisie par lequel l'autorité judiciaire recherche des éléments de preuve d'une infraction, la perquisition peut viser expressément des informations ou supports protégés par le secret de la défense nationale, ou bien amener l'autorité judiciaire à la découverte incidente de tels documents dans des lieux où leur présence n'était pas préalablement prévue.

Le code de procédure pénale distingue en effet expressément ces deux hypothèses selon que les lieux investis auront été préalablement identifiés comme « abritant » des informations et supports classifiés, ou bien n'en comportent pas *a priori* et sont donc considérés comme « neutres »¹⁵.

Pour faire connaître ces dispositions et faciliter le déroulement d'une perquisition en préservant les éléments protégés par le secret de la défense nationale de toute compromission, chaque responsable d'organisme détenant des informations et supports classifiés informe son personnel de la conduite à tenir en cas de perquisition conformément à l'instruction ministérielle dont son organisme relève.

- Perquisition dans un lieu abritant des informations et supports classifiés

La commission du secret de la défense nationale joue un rôle essentiel pour éviter la compromission d'informations et supports classifiés dans cette procédure qui exige du magistrat de vérifier au préalable si tout ou partie des lieux objet de son intérêt figure sur la liste des lieux abritant (cf. 2.3.2.2). Dans l'affirmative, il ne peut déléguer la perquisition aux officiers de police judiciaire et doit se déplacer lui-même pour y procéder. Surtout, n'ayant pas accès au secret de la défense nationale (cf. 1.2.2.2 a)), le magistrat ne peut réaliser une perquisition qu'après avoir adressé une décision écrite au président de la commission du secret de la défense nationale lui indiquant les informations utiles à l'accomplissement de sa mission. Les opérations ne peuvent débuter qu'en présence du président de la commission ou de son représentant dûment habilité, qui se transporte sur les lieux sans délai et sans que nul ne puisse s'opposer à son action pour aucun motif que ce soit.

Dès le début de la perquisition, le magistrat informe le président de la commission et le responsable de l'organisme ou son représentant, de la nature de l'infraction objet de ses investigations, des motifs justifiant la perquisition et des lieux concernés. Fort de ces éléments, c'est le président de la commission ou son représentant, assisté de toute personne habilitée à cet effet, qui prend connaissance des éléments classifiés, trie et sélectionne pour saisie ceux qui sont relatifs aux faits sur lesquels portent les investigations. Il dresse un inventaire de chaque élément saisi et placé sous scellés fermés¹⁶. Le détail des éléments saisis n'est pas communiqué au magistrat qui, dans la pratique, ne se voit communiquer que le nombre de pièces saisies et, le cas échéant, le nombre de pages et de supports.

Deux procès-verbaux rendant compte des opérations de perquisition sont dressés à l'issue des opérations : l'un, non protégé, établi par le magistrat, est versé au dossier de la procédure pénale. L'autre, rédigé par le président de la commission du secret de la défense nationale, ou son représentant dûment habilité, contient l'inventaire des documents classifiés saisis et est conservé par le président de la commission qui est institué gardien des scellés.

d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs ».

¹⁵ Cf. article 56-4 du code de procédure pénale, dans sa rédaction résultant de la décision du Conseil constitutionnel n° 2011-192 QPC du 10 novembre 2011.

¹⁶ Si l'enquête l'exige, les documents sont saisis en original, contre copie remise au détenteur.

Il appartient ensuite au magistrat de demander, le cas échéant, la déclassification des informations et supports classifiés saisis suivant le processus décrit au point i. Dans ce cas, les scellés sont remis à l'autorité administrative compétente par la commission du secret de la défense nationale en même temps que son avis¹⁷. Dans le cas où aucune requête en déclassification n'est émise par le magistrat, le devenir des scellés classifiés se résout par l'application des dispositions du droit commun de la procédure pénale relatives à la restitution des scellés à l'autorité émettrice¹⁸.

Le cas de l'accès, par le magistrat qui opère une perquisition, à un système d'information classifié, doit être traité selon la même logique que l'accès aux informations et supports classifiés, les modalités techniques de constitution des scellés exigeant simplement d'être adaptées. Seul un représentant de la commission du secret de la défense nationale est autorisé à accéder au système.

- Perquisition dans un lieu non déclaré comme lieu abritant révélant la présence d'informations et supports classifiés

Cette hypothèse peut matérialiser l'existence d'une compromission de plus ou moins grande ampleur et est susceptible de déclencher l'ouverture d'une procédure judiciaire incidente visant expressément ce délit. Dès la découverte de supports classifiés, le magistrat présent ou immédiatement prévenu par l'officier de police judiciaire opérant la perquisition, informe le président de la commission du secret de la défense nationale.

Les informations et supports classifiés sont placés sous scellés par le magistrat ou l'officier de police judiciaire qui les a découverts, sans qu'il soit pris connaissance de leur contenu. Le ou les scellés sont transmis à la commission du secret de la défense nationale ou lui sont remis directement au cas où le président ou son représentant se sont rendus sur place. Le président de la commission en devient gardien.

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 commission qui établit un inventaire des pièces ou documents saisis et en informe le magistrat et la ou les autorités émettrices. Ces dernières sont ainsi à même de prendre la mesure de leur sensibilité, de la gravité de l'atteinte portée au secret de la défense nationale du fait de leur compromission et de mener les actions qui s'imposent. L'évaluation de la gravité de l'atteinte portée au secret du fait de la compromission bénéficie également à l'autorité judiciaire qui apprécie les suites pénales opportunes, nonobstant sa possibilité de demander une déclassification des éléments ainsi placés sous scellés selon la procédure décrite au point i.

Le cas échéant, la déclassification ultérieure pour communication à l'autorité judiciaire des éléments ainsi placés sous scellés relève elle aussi de la procédure décrite au point i.

- Cas particulier des auditions

Une personne habilitée ne peut en aucun cas être déliée de ses obligations de protection du secret de la défense nationale par quiconque, y compris son autorité hiérarchique, tant que l'information ou le support n'est pas déclassifié(e). Si elle est interrogée sur des informations classifiées, il lui appartient d'opposer au magistrat ou aux enquêteurs les dispositions des articles 413-10 et suivants du code pénal qui énoncent les sanctions applicables au délit de compromission.

¹⁷ Article L. 2312-5 du code de la défense.

¹⁸ Article 41-4 du code de procédure pénale s'agissant des scellés constitués pendant l'enquête initiale ou lorsqu'il n'a pas été statué sur leur restitution par une juridiction de jugement, articles 99 et 212 du même code s'agissant des scellés constitués au cours de l'information judiciaire, articles 479 et suivants et 373 pour les juridictions de jugement correctionnelle et criminelle.

b) Par exception, les membres de la formation du Conseil d'État spécialisée dans le contentieux des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État ont accès au secret de la défense nationale

Le contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État et la défense relève de la compétence en premier et dernier ressort d'une formation spécialisée du Conseil d'État, dans les conditions prévues aux articles L. 841-1 et L. 841-2 du code de la sécurité intérieure et L. 773-1 et suivants du code de justice administrative, dont les membres peuvent accéder, dans la mesure nécessaire à l'exercice du contrôle juridictionnel, à des informations et supports classifiés.

Cet accès dérogatoire est justifié par le fait que l'essentiel des informations et supports maniés par les services de renseignement est couvert par le secret de la défense nationale, eu égard à la sensibilité et à la nécessaire discrétion qui sont inhérentes à la mission de recueil de renseignements qui leur incombe, et par l'impossibilité, de ce fait, d'organiser un contrôle juridictionnel effectif en se conformant aux règles de procédure de droit commun.

En vertu de l'article L. 5 du code de justice administrative, les exigences de la contradiction sont adaptées à celles du secret de la défense nationale. Il en résulte que, par dérogation au principe du contradictoire, le requérant ne reçoit pas communication des informations et supports classifiés qui sont portés à la connaissance de la formation spécialisée. Par ailleurs, lorsqu'est en cause le secret de la défense nationale, le président de la formation de jugement ordonne le huis clos. Enfin, les décisions rendues par la formation spécialisée, qui sont publiques, ne font état d'aucun élément protégé par le secret de la défense nationale.

Par suite, lorsque la formation de jugement constate une illégalité susceptible de constituer, de surcroît, une infraction au regard des règles qui gouvernent la matière, elle en informe la personne concernée ou la juridiction, ainsi que le procureur de la République. De plus, elle transmet à la commission du secret de la défense nationale l'ensemble des éléments du dossier au vu duquel elle a statué, afin que celle-ci donne au Premier ministre son avis sur la possibilité de déclassifier tout ou partie de ces éléments en vue de leur transmission au procureur de la République¹⁹.

La procédure devant la formation spécialisée garantit également le droit à un procès équitable et le droit au recours eu égard aux pouvoirs dont elle est investie pour instruire les requêtes, relever d'office toutes les illégalités qu'elle constate et enjoindre à l'administration de prendre toutes mesures utiles afin de remédier aux illégalités constatées²⁰.

1.2.2.3 Parlementaires

a) Les parlementaires n'ont pas accès au secret de la défense nationale

Eu égard au principe constitutionnel de séparation des pouvoirs, les parlementaires ne peuvent pas, dans le cadre de l'exercice de leur mission de membres du Parlement²¹, accéder au secret de la défense nationale, à l'exception des membres de la délégation parlementaire au renseignement selon les modalités définies au b).

Les présidents des commissions chargées des affaires de sécurité intérieure, de la défense ou des finances de l'Assemblée nationale et du Sénat peuvent en revanche demander la

¹⁹ Article L. 773-7 du code de justice administrative

²⁰ CE, formation spécialisée, 8 fév. 2017, n° 396550, B ; CE, formation spécialisée, 8 fév. 2017, n° 396567, B.

²¹ En revanche, des parlementaires peuvent, dans le cadre de fonctions ou dans l'accomplissement d'une mission sans lien avec l'exercice de leur mandat parlementaire, accéder au secret de la défense nationale. Ils sont alors habilités soit en qualité si la loi en dispose ainsi (cas des parlementaires-membres d'autorités administratives indépendantes autorisées à accéder au secret de la défense nationale, cf. 2.1.3.2 ou selon les modalités prévues à la partie 3.2 (cas de parlementaires en mission pour le Gouvernement par exemple).

déclassification de tout document nécessaire à l'exercice des missions de la commission qu'ils président. Ils adressent alors une demande motivée à l'autorité administrative compétente, qui saisit sans délai la commission du secret de la défense nationale²². L'avis de la commission du secret de la défense nationale et la décision de l'autorité émettrice sont rendus selon les mêmes modalités que celles décrites au 1.2.2.2 a) i.

b) Par exception, les membres de la délégation parlementaire au renseignement ont accès au secret de la défense nationale

Conformément à l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, les membres de la délégation parlementaire au renseignement, commune à l'Assemblée nationale et au Sénat, sont destinataires des informations utiles à l'accomplissement de leur mission de contrôle de l'action du Gouvernement en matière de renseignement et d'évaluation de la politique publique en ce domaine. À ce titre, ils sont autorisés à accéder aux informations et supports classifiés nécessaires à l'accomplissement de leurs missions, à l'exclusion des documents, informations et éléments d'appréciation portant sur les opérations en cours de ces services, sur les instructions données par les pouvoirs publics à cet égard, sur les procédures et méthodes opérationnelles, ou sur les échanges avec les services étrangers ou des organismes internationaux compétents dans le domaine du renseignement, et des données dont la communication pourrait mettre en péril l'anonymat, la sécurité ou la vie d'une personne relevant ou non d'un service de renseignement²³, ainsi que les modes opératoires propres à l'acquisition du renseignement. Les agents des assemblées parlementaires désignés pour les assister doivent, pour leur part, être habilités selon l'une des procédures détaillées aux parties 3.2 et 3.3.

1.2.3 Règles de communication des documents classifiés

Les dispositions qui suivent définissent, conformément au code des relations entre le public et l'administration et au code du patrimoine, les règles de communication et de consultation des documents classifiés, y compris les données, 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.

Conformément à l'article L. 311-2 du code des relations entre le public et l'administration, lorsqu'une administration mentionnée à l'article L. 300-2 du même code ou la commission d'accès aux documents administratifs est saisie d'une demande de communication d'un document administratif susceptible de relever de plusieurs des régimes d'accès mentionnés aux articles L. 342-1 et L. 342-2, il lui appartient de l'examiner d'office au regard de l'ensemble de ces régimes, à l'exception du régime organisé par l'article L. 213-3 du code du patrimoine.

Dès lors, lorsqu'une personne habilitée mais ne disposant pas du besoin d'en connaître pour l'exercice de sa fonction ou l'accomplissement de sa mission, ou bien lorsqu'une personne non habilitée, souhaite accéder à un document classifié, deux situations sont à distinguer :

a) Le caractère classifié du document est le seul motif faisant obstacle à sa libre communication.

Le service qui le détient informe le demandeur qu'il peut, par son intermédiaire, en solliciter la déclassification. Dans le cas où le demandeur souhaite poursuivre en ce sens, le service

²² Article L. 2312-4 du code de la défense.

²³ Cf. services mentionnés à l'article L. 811-2 du code de la sécurité intérieure et ceux désignés par le décret en Conseil d'État mentionné à l'article L. 811-4 du même code.

détenteur relaie sa demande à l'autorité émettrice compétente *via* le service du haut fonctionnaire de défense et de sécurité de cette dernière.

En cas de refus explicite ou résultant du silence gardé par l'autorité émettrice sur la demande, le service détenteur est lié par la décision de cette dernière et le document demeure non communicable²⁴.

Dans le cas où l'autorité émettrice donne une suite favorable à la demande de déclassification, il y est procédé selon les modalités prévues au 7.6.3. Le document devient alors librement communicable.

b) Outre le caractère classifié du document, un autre motif fait obstacle à sa libre communication.

Le service qui le détient instruit la demande au regard des dispositions respectives des articles L. 311-5 du code des relations entre le public et l'administration et L. 213-2 et L. 213-3 du code du patrimoine, et sollicite parallèlement la déclassification du document.

En cas de refus explicite ou résultant du silence gardé par l'autorité émettrice sur la demande de déclassification, le service détenteur est lié par la décision de cette dernière et le document demeure non communicable²⁵. Ce refus est notifié par le service détenteur.

Dans le cas où l'autorité émettrice donne une suite favorable à la demande de déclassification, il est procédé à la déclassification du document selon les modalités prévues au 7.6.3. Cette décision ne préjuge pas du sens de la décision prise par l'administration dans le cadre de la demande d'accès.

Les règles de communication des documents déclassifiés sont détaillées au 7.6.3.7.

1.3 PORTEE DES TIMBRES DE CLASSIFICATION *SECRET* ET *TRES SECRET* ET DE LA MENTION *DIFFUSION RESTREINTE*

1.3.1 Portée des timbres de classification *Secret* et *Très Secret*

Conformément à l'article 413-9 du code pénal, seuls les informations et supports ayant fait l'objet d'une mesure de classification en application des articles R. 2311-2 et R. 2311-3 du code de la défense présentent un caractère de secret de la défense nationale.

Ainsi, l'apposition d'un timbre de classification, matérialisant la décision de classification et le niveau de classification retenu, constitue le seul moyen de conférer à des informations et supports la protection pénale liée au secret de la défense nationale.

Deux niveaux de classification sont désormais prévus par le code de la défense :

- le niveau *Secret* qui protège les informations et supports dont la divulgation ou auxquels l'accès est de nature à porter atteinte à la défense et à la sécurité nationale ;

²⁴ Cf. CE, 1^{er} octobre 2015, n° 373019, B : « il appartient à l'administration de laquelle émane les documents classifiés d'examiner l'opportunité de procéder à leur déclassification. Dans le cas où elle estime que la classification demeure justifiée, il lui appartient d'informer l'administration chargée des archives qu'elle s'oppose, pour cette raison, à leur consultation anticipée. À défaut d'accord de l'autorité de laquelle émanent les documents dont la consultation est demandée, l'administration chargée des archives est tenue de rejeter la demande de consultation anticipée dont elle est saisie. » » En outre, « la satisfaction de l'intérêt légitime du demandeur doit être concilié avec le respect de la défense nationale (...) il en résulte qu'il appartient à l'administration de laquelle émanent les documents classifiés d'examiner l'opportunité de procéder à leur déclassification ». Enfin, si le refus de l'autorité émettrice « ne constitue pas une décision susceptible de recours, sa régularité et son bien-fondé peuvent être contestés à l'appui d'un recours dirigé contre la décision opposant un refus à la demande de consultation anticipée ».

²⁵ Cf. Articles L. 311-1 et suivants du code des relations entre le public et l'administration et L. 213-3 et L. 213-4 du code du patrimoine.

- le niveau *Très Secret* qui protège ceux dont la divulgation ou auxquels l'accès aurait des conséquences exceptionnellement graves pour la défense et la sécurité nationale.

Les informations et supports classifiés au niveau *Très Secret* concernant des priorités gouvernementales en matière de défense et de sécurité nationale font de surcroît l'objet d'une classification spéciale (article R. 2311-3 du code de la défense).

La différence entre ces deux niveaux de classification ne réside pas dans l'obligation de protéger les informations et supports dont le caractère est toujours impératif, mais dans la profondeur des mesures de sécurité physiques, logiques ou organisationnelles, qu'ils induisent. Pour autant, les sanctions pénales encourues en cas de compromission d'une information ou d'un support classifié sont les mêmes, quel que soit le niveau de classification de l'information ou du support compromis.

Pierre angulaire de la protection du secret de la défense nationale, l'apposition du timbre de classification est également un critère essentiel pour garantir la protection des informations et supports classifiés étrangers confiés à la France. En effet, conformément à l'article 414-9 du code pénal, la protection que confère le code pénal aux informations et supports classifiés nationaux s'applique également aux informations et supports échangés avec un État étranger, une organisation internationale, une institution, un organe ou un organisme de l'Union européenne en vertu d'un accord de sécurité, général ou spécifique, régulièrement approuvé et publié, dont l'objet ou l'un des objets est de prévoir une équivalence entre les niveaux de protection français et étrangers.

1.3.2 Portée de la mention de protection *Diffusion Restreinte*, qui n'est pas un timbre de classification

La mention *Diffusion Restreinte* n'est pas un timbre de classification mais une mention de protection. Elle vise à protéger des informations et supports qu'il n'y a pas lieu de classer mais qui présentent une sensibilité particulière, en ce que notamment ils sont susceptibles de comporter des éléments dont la consultation ou la communication porterait atteinte à l'un des secrets, autres que le secret de la défense nationale, mentionnés au 2° de l'article L. 311-5 du code des relations entre le public et l'administration.

Son objectif principal est de sensibiliser l'utilisateur à la nécessaire discrétion dont il doit faire preuve dans la manipulation des informations et supports couverts par cette mention. Ceux-ci ne peuvent être communiqués qu'aux personnes ayant besoin d'en connaître dans le respect des mesures de protection définies à l'Annexe 1.

La circonstance que ces informations et supports soient couverts par la mention *Diffusion Restreinte* ne saurait toutefois, par elle-même, constituer pour l'administration saisie d'une demande tendant à accéder à ces informations et supports un motif de refus d'accès sur le fondement des dispositions des articles L. 311-1 et suivants du code des relations entre le public et l'administration ou L. 213-1 du code du patrimoine.

1.4 RESPONSABILITE DES DEPOSITAIRES DU SECRET DE LA DEFENSE NATIONALE

1.4.1 Responsabilité de l'autorité émettrice et de l'auteur d'information classifiée

Sous la responsabilité du Premier ministre au titre de l'article 21 de la Constitution et, par délégation, de chaque ministre dans son champ d'attribution, la préservation du secret de la défense nationale doit être une préoccupation constante de toute personne physique ou morale intervenant dans l'élaboration et le maniement d'informations et supports classifiés.

Cette préoccupation intervient avant la décision de classification. En effet, la décision de classification est un acte important tant par les mesures de protection contraignantes qui en découlent, que par les conséquences judiciaires que cette décision peut entraîner. Alors que l'efficacité des politiques de protection nécessite l'intervention d'un nombre et d'une

typologie d'acteurs de plus en plus variés (ensemble des ministères, collectivités territoriales, acteurs privés, partenaires étrangers), il convient d'éviter toute classification excessive et injustifiée au regard de l'objectif de sauvegarde des intérêts fondamentaux de la Nation, qui aurait pour effet contraire de restreindre à outrance la nécessaire circulation de l'information. La classification au titre du secret de la défense nationale est, en effet, la forme ultime de protection qu'une information ou un support peut recevoir. Il existe d'autres secrets protégés par la loi permettant de limiter la divulgation non autorisée d'informations et de supports.

À cet égard, l'autorité émettrice et l'auteur d'une information ou d'un support classifié exercent une responsabilité première dans la mise en œuvre de la protection du secret de la défense nationale.

En effet, l'autorité émettrice est l'autorité étatique ou supranationale sous la responsabilité de laquelle un timbre de classification est apposé sur une information ou un support. C'est elle qui prend la décision de classification. Sont ainsi autorités émettrices :

- sur le plan national :
 - le Président de la République ;
 - le Premier ministre pour les informations et supports classifiés au niveau *Très Secret* faisant l'objet d'une classification spéciale ou pour les informations et supports classifiés aux niveaux *Secret* et *Très Secret* dont l'élaboration est nécessaire à l'exercice des missions directement exercées par le Premier ministre, son cabinet ou dévolues aux services du Premier ministre et aux administrations placées sous sa responsabilité ;
 - chaque ministre dans le champ de ses attributions (cf. 2.1.2.1) ;
 - dans les limites fixées par la loi, la formation spécialisée du Conseil d'État, la délégation parlementaire au renseignement et les autorités administratives indépendantes autorisées par la loi à accéder au secret de la défense nationale ;
 - dans l'exercice de ses attributions non juridictionnelles, la Cour des comptes.
- sur le plan international : les États, organisations internationales, institutions, organes ou organismes de l'Union européenne sous la responsabilité desquelles des informations et supports relevant de leurs attributions respectives sont classifiés.

L'auteur d'une information ou d'un support classifié est celui qui, conformément aux modalités de classification arrêtées par l'autorité émettrice, prend la décision d'apposer le timbre de classification sur une information ou un support au niveau requis par son contenu. C'est donc lui qui confère matériellement sa protection juridique à l'information ou au support concerné.

Lorsque l'information ou le support est classifié, c'est l'ensemble de la chaîne de sécurité (cf. 2.2) qui est responsable de son intégrité, et pas simplement la personne appelée à le manier et le détenir. Tout responsable d'un organisme ayant accès à des informations et supports protégés par le secret de la défense nationale, indépendamment de son statut, peut lui-même être poursuivi pour compromission lorsqu'une information détenue par l'un de ses collaborateurs est compromise, dès lors qu'il n'a pas procédé aux diligences nécessaires pour l'empêcher et la prévenir (cf. 1.4.2.1 et 1.4.2.2).

1.4.2 Répression pénale des atteintes au secret de la défense nationale

La nature particulière du secret de la défense nationale et son rôle essentiel dans la protection des intérêts fondamentaux de la Nation expliquent une répression pénale sévère de ses atteintes ainsi que certaines particularités procédurales.

Ainsi, le délit de compromission du secret de la défense nationale, prévu aux articles 413-10 et suivants du code pénal, s'insère dans un titre expressément consacré à la protection des

intérêts fondamentaux de la Nation et partage avec les autres crimes et délits de ce panel infractionnel, des quantum de peines encourues très élevés²⁶, sans rapport avec ceux prévus pour la violation d'autres secrets protégés par la loi tels que, par exemple, le secret professionnel, le secret des correspondances ou encore le secret de l'identité de certains personnels dont l'anonymat est protégé²⁷.

Par ailleurs, et à l'instar d'autres atteintes portées à la défense nationale en temps de guerre, les peines encourues pour la compromission sont aggravées en temps de guerre jusqu'à vingt ans de réclusion criminelle²⁸.

Enfin, l'instruction et le jugement des auteurs de compromission et des infractions connexes relèvent de la compétence de juridictions de droit commun spécialisées en matière militaire prévues et organisées aux articles 697 et 698-6 du code de procédure pénale²⁹.

1.4.2.1 Caractérisation du délit

Comme précisé à l'article 413-10 du code pénal, l'élément matériel du délit de compromission consiste en la destruction, le détournement, la soustraction ou la reproduction non autorisée d'une information ou d'un support classifié au regard des règles prescrites par la présente instruction, ainsi que 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 ou de le porter à la connaissance d'une ou plusieurs personnes non qualifiées, voire du public.

Ainsi que prévu par l'article 413-11 du même code, l'infraction peut être le fait d'un tiers au secret, ou bien d'une personne qualifiée, c'est-à-dire celle 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.

Toute personne légitimement détentrice d'éléments couverts par le secret de la défense nationale en est « responsable » ce qui met à sa charge des obligations positives et exige une vigilance particulière dont le défaut est également sanctionné : la personne qualifiée peut ainsi être poursuivie alors qu'elle a agi par simple imprudence ou négligence. Elle doit donc s'assurer que les informations et supports ne sont pas détruits, détournés, soustraits, reproduits dans des conditions autres que celles autorisées par la présente instruction, ni communiqués à une personne non qualifiée. Enfin, la personne qualifiée n'est pas déliée de ses obligations parce qu'elle n'est plus habilitée : elle y reste tenue tant que l'information reste classifiée.

L'information qui peut faire l'objet de la compromission s'entend de toute information ou système d'information classifié, quelle que soit la nature du support, ayant fait l'objet d'une mesure de classification toujours effective (cf. 7.5.5.3). Ainsi, il convient de vérifier que le timbre de classification matérialisant cette mesure, à l'exclusion de toute autre mention de restriction à la diffusion ou à la manipulation³⁰, n'a pas perdu sa valeur. Certains documents

²⁶ Ainsi des crimes de trahison et d'espionnage (articles 411-1 à 411-11), de l'attentat et du complot (articles 412-1 et 412-2), du mouvement insurrectionnel (articles 412-3 à 412-6), ou encore de l'usurpation de commandement, de la levée des forces armées ou de la provocation à s'armer illégalement (articles 412-7 et 412-8).

²⁷ Les articles 226-13 et 226-15 du code pénal font encourir à l'auteur de violation du secret professionnel et du secret des correspondances, une peine d'emprisonnement de un an, outre des peines d'amende s'élevant respectivement à 15 000 et 45 000 euros ; les articles 413-3 et 413-14 prévoient des peines de cinq ans d'emprisonnement, outre des peines d'amende, pour les atteintes à l'anonymat de certains personnels militaires et membres des services de renseignement.

²⁸ Article L. 332-2 du code de justice militaire.

²⁹ Articles 701 et 702 du code de procédure pénale ; En temps de guerre, cette compétence est dévolue aux juridictions des forces armées selon les règles définies par le code de la justice militaire.

³⁰ Ainsi en est-il des mentions telles que « confidentiel personnel », ou « Diffusion Restreinte » dont la protection ne relève pas du régime juridique de la compromission.

peuvent en effet avoir perdu leur protection au titre du secret de la défense nationale de façon automatique, sans pour autant avoir fait l'objet d'une décision formelle de déclassification (cf. 7.5.5.1 et premier paragraphe du 7.5.5.2).

Enfin, la répression de la compromission est étendue aux actes commis au préjudice des partenaires étrangers et européens :

- puissances signataires du Traité de l'Atlantique Nord ou de son organisation³¹ ;
- État étranger ou organisation internationale en vertu d'un accord de sécurité relatif à la protection des informations classifiées conclu entre la France et un État étranger ou une organisation internationale, régulièrement approuvé et publié ;
- Institution, organe ou organisme de l'Union européenne en vertu des règlements de sécurité de ces derniers qui ont fait l'objet d'une publication au Journal officiel de l'Union européenne³².

1.4.2.2 Répression du délit

La compromission, ou sa simple tentative, est punie de sept ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle est le fait d'une personne qualifiée, quantums réduits à trois ans et 45 000 euros d'amende quand elle résulte d'une imprudence ou d'une négligence. Les peines prévues pour une personne non qualifiée sont de cinq ans et 75 000 euros³³. Les personnes physiques s'exposent également à des peines complémentaires d'interdiction d'exercice professionnel (fonction publique ou activité à l'occasion de laquelle les faits ont été commis)³⁴. Quant aux personnes morales³⁵, responsables des infractions commises, pour leur compte, par leurs organes ou représentants, elles peuvent être poursuivies seules ou en même temps que ces derniers, et condamnées à une amende portée à un montant maximum cinq fois supérieur à celui prévu pour les personnes physiques, outre les peines habituelles qui s'appliquent à elles pouvant aller jusqu'à leur dissolution³⁶.

Les agissements susceptibles de caractériser une compromission du secret de la défense nationale sont divers et peuvent révéler une démarche plus ou moins active, une intention délictueuse plus ou moins grave de la part de l'auteur : non-respect des instructions et consignes administratives relatives à la manipulation du secret, confiance à un collègue habilité mais n'ayant pas qualité pour connaître d'une information, défaillance dans l'administration d'un réseau informatique conduisant à des « fuites » d'information vers des tiers, révélations à la presse, etc.

L'orientation de la procédure judiciaire lors d'une compromission dénoncée ou constatée relève de la compétence du procureur de la République selon le principe de l'opportunité des poursuites. Il prend alors en compte la gravité de l'atteinte portée au secret de la défense nationale à raison de la compromission commise. L'autorité émettrice lui transmet tout élément susceptible de l'éclairer à cette fin. Mais, que ce soit au stade des poursuites ou du jugement, la gravité du comportement que la compromission révèle, est appréciée par l'autorité judiciaire.

Les conséquences d'une compromission, même en l'absence de poursuites, peuvent être particulièrement lourdes pour une personne qualifiée. En effet, et outre les éventuelles suites administratives et disciplinaires qui pourront être mises en œuvre indépendamment de la

³¹ Article 414-8 du code pénal.

³² Article 414-9 du code pénal.

³³ Articles 413-10, 413-11 et 413-12 du code pénal.

³⁴ Article 414-5 du code pénal.

³⁵ Pour mémoire, l'État n'est pas responsable pénalement.

³⁶ Articles 414-7 et, par renvoi, 131-8 et 131-9 du code pénal.

procédure judiciaire, la seule mention d'un antécédent judiciaire, peut subsister dans les fichiers de police et empêcher la délivrance d'une nouvelle habilitation ou l'exercice de certaines professions³⁷.

1.4.2.3 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 et supports classifiés compromis.

Il est rendu compte immédiatement de toute découverte de compromission possible à l'autorité compétente et à la personne exerçant la fonction d'officier de sécurité de l'organisme concerné. Qu'il y ait une compromission avérée ou une simple suspicion, sont informés directement et dans les plus brefs délais :

- soit le service compétent de la direction générale de la sécurité intérieure, chargé de centraliser les cas et de procéder à l'enquête sous le contrôle de l'autorité judiciaire ;
- soit le service compétent de la direction du renseignement et de la sécurité de la défense ou de la direction générale de la sécurité extérieure dans son domaine d'attribution, qui avise lui-même le service compétent de la direction générale de la sécurité intérieure ;
- dans le cadre d'un contrat, sous-traité ou sous-contrat conformément à la partie 4.4 de la présente instruction, l'autorité publique contractante ;
- le haut fonctionnaire de défense et de sécurité du ministère intéressé qui avise lui-même le secrétariat général de la défense et de la sécurité nationale de chaque cas de compromission ;
- et, le cas échéant, l'émetteur du document, l'officier de sécurité des systèmes d'information (le responsable de la sécurité du système d'information éventuellement) ou l'autorité d'emploi du système classifié ;
- la chaîne fonctionnelle de sécurité des systèmes d'information classifiés pour toute perte ou vol d'un élément constitutif d'un système d'information classifié ou d'un support amovible.

L'autorité compétente prend immédiatement, en liaison avec l'officier de sécurité, les mesures adéquates pour prévenir la réitération de tels faits. Une personne qui ne signale pas de tels actes favorisant la divulgation d'une information ou d'un support classifié est susceptible d'encourir des sanctions administratives ou professionnelles, voire pénales dès lors qu'une telle abstention crée les conditions de nouvelles compromissions.

Lorsque la compromission porte sur des informations classifiées étrangères, le secrétariat général de la défense et de la sécurité nationale, ou, le cas échéant, l'autorité de sécurité déléguée compétente après information de ce dernier, informe dans les plus brefs délais l'autorité nationale de sécurité étrangère. Lorsque la compromission concerne des informations de niveau *Très Secret*, l'autorité de sécurité déléguée rend compte au secrétariat général de la défense et de la sécurité nationale qui informe lui-même l'autorité nationale de sécurité étrangère.

L'ensemble de ces procédures s'exécute sans préjudice de l'obligation générale faite à tout officier public ou fonctionnaire et à toute autorité constituée de dénoncer au procureur de la

³⁷Voir les articles 230-6 et suivants du code de procédure pénale pour les fichiers judiciaires d'antécédents et les articles L. 234-1 et, par renvoi, L. 114-1 du code de la sécurité intérieure pour la consultation de ces fichiers dans le cadre de certaines enquêtes administratives.

République compétent l'existence d'un délit suffisamment étayé³⁸. S'agissant de compromission, cette obligation est mise en œuvre dans des conditions protectrices du secret de la défense nationale auquel les magistrats n'ont pas accès dans le cadre de la conduite des procédures judiciaires. Le cas échéant, un dialogue avec le procureur de la République peut être utilement engagé. La direction générale de la sécurité intérieure étant le service d'enquête saisie de manière privilégiée par l'autorité judiciaire, elle joue un rôle important dans l'articulation entre les mesures administratives de prise en compte et de résolution des dysfonctionnements et la procédure judiciaire éventuellement mise en œuvre.

1.4.2.4 Réponses aux incidents liés à la sécurité des systèmes d'information classifiés

Lorsqu'un organisme détient un système d'information pour le traitement des informations classifiées qu'il échange ou détient, il se dote d'un dispositif technique et humain de gestion des incidents afin de détecter et d'analyser les attaques et de réagir face à des événements susceptibles d'affecter la sécurité du système d'information classifié.

Ce dispositif s'appuie notamment sur des systèmes de détection conformes au paragraphe 6.6.4.5.

Les chaînes fonctionnelles de protection du secret et de sécurité des systèmes d'information évaluent les conséquences de ces incidents de sécurité et prennent les décisions adaptées en réaction. En particulier, l'officier de sécurité informe de l'incident l'officier de sécurité de l'organisme émetteur de l'information classifiée. L'ensemble des actions entreprises à la suite d'un incident de sécurité ou d'une compromission est répertorié par l'organisme émetteur dans un registre dédié.

L'agence nationale de la sécurité des systèmes d'information et le service enquêteur compétent sont tenus informés des incidents de sécurité et de leurs caractéristiques techniques affectant les systèmes d'information classifiés.

1.4.3 Sanction de la divulgation non autorisée d'informations et supports portant la mention de protection *Diffusion Restreinte*

La mention *Diffusion Restreinte* n'est pas un niveau de classification mais une mention de protection et n'a ainsi pas pour effet de conférer la protection pénale propre au secret de la défense nationale. Pour autant, la divulgation d'informations et supports portant la mention *Diffusion Restreinte* à des personnes physiques ou morales n'ayant pas le besoin d'en connaître est susceptible d'exposer son auteur à des sanctions disciplinaires, administratives, et éventuellement pénales notamment au titre de la violation du secret professionnel.

³⁸ Article 40 alinéa 2 du code de procédure pénale.

2 STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

La protection du secret de la défense nationale est une responsabilité du Premier ministre. À ce titre, avec l'appui du secrétaire général de la défense et de la sécurité nationale, il :

- définit et coordonne la mise en œuvre des mesures générales nécessaires à la protection des informations et supports classifiés, quel que soit leur niveau de classification ;
- détermine les critères de classification et modalités de protection des informations et supports classifiés au niveau *Très Secret* faisant l'objet de classifications spéciales et en contrôle la mise en œuvre ;
- assure l'interface avec les autorités nationales de sécurité étrangères et s'assure de la sécurité des informations classifiées échangées en vertu d'un accord de sécurité conclu entre la France et un État étranger ou une organisation internationale.

Chaque ministre est chargé de décliner ces mesures dans son champ d'attribution et d'en contrôler la mise en œuvre par les personnes physiques et les organismes, publics ou privés, entrant dans son champ de compétence.

La mise en œuvre de la protection du secret s'appuie sur une chaîne fonctionnelle, dite « chaîne de protection du secret », et sur la chaîne de sécurité des systèmes d'information qui assure la sécurité de tous les systèmes d'information utilisés par l'organisme et est renforcée lorsque l'organisme dispose, par ailleurs, des systèmes d'information classifiés (cf. Annexe 2).

Des outils de pilotage, de contrôle et de suivi sont mis en place aux niveaux interministériel et ministériel, pour s'assurer du respect des règles relatives à la protection du secret de la défense nationale (instructions ministérielles, directives techniques particulières, inspection, rapport annuel, bases interministérielles de données pour la gestion des habilitations, des lieux abritant, des décisions de déclassification, etc.) et prendre, le cas échéant, les mesures correctrices nécessaires.

2.1 AUTORITES CHARGEES DU PILOTAGE DE LA PROTECTION DU SECRET DE LA DEFENSE NATIONALE

2.1.1 Au niveau interministériel

2.1.1.1 Le Premier ministre

Conformément à l'article 21 de la Constitution, le Premier ministre dirige l'action du Gouvernement et est responsable de la défense nationale.

Il est, à ce titre, chargé de définir, par arrêté, les mesures nécessaires à la protection du secret de la défense nationale suivant lesquelles chaque ministre détermine, dans son champ d'attribution, les informations et supports qu'il y a lieu de classer aux niveaux *Secret* et *Très Secret*, hors classifications spéciales, et les modalités de leur protection³⁹.

Le Premier ministre définit, en outre, les informations et supports classifiés de niveau *Très Secret* portant sur des priorités gouvernementales en matière de défense et de sécurité nationale et devant, par suite, faire l'objet d'une classification spéciale⁴⁰. À cette fin, il

³⁹ Article R. 2311-5 du code de la défense.

⁴⁰ Article R. 2311-3 du code de la défense.

détermine les critères de classification et les modalités particulières de protection des informations et supports de niveau *Très Secret* faisant l'objet d'une classification spéciale au travers d'une réglementation spécifique complémentaire à la présente instruction⁴¹. Il prend les décisions d'habilitation en précisant les classifications spéciales auxquelles la personne habilitée a accès⁴².

Il établit, par arrêté, sur proposition des ministres intéressés, la liste des lieux abritant des éléments couverts par le secret de la défense nationale et définit les conditions d'accès sécurisé à cette liste⁴³.

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

2.1.1.2 Le secrétaire général de la défense et de la sécurité nationale

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 nationale⁴⁴, y compris en matière de sécurité des systèmes d'information.

a) Sur le plan national

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

Il veille également à la mise en œuvre des mesures relatives aux classifications spéciales. Il définit et organise les réseaux de sécurité correspondant aux classifications spéciales et autorise les organismes, en fonction de leur besoin d'en connaître, à accéder à des informations et supports classifiés au niveau *Très Secret* faisant l'objet de classifications spéciales. Il prend, par délégation du Premier ministre, les décisions d'habilitation à connaître des informations et supports classifiés couverts par une classification spéciale.

Enfin, il assume les missions dévolues par la présente instruction aux hauts fonctionnaires de défense et de sécurité pour les organismes relevant de ses attributions (cf. 2.1.3.1).

b) Sur le plan international

Le secrétaire général de la défense et de la sécurité nationale est l'autorité nationale de sécurité (ANS) pour le secret de la défense nationale⁴⁵. À ce titre, il :

- négocie, en accord avec le ministre des affaires étrangères, en concertation avec l'ensemble des ministères, les accords intergouvernementaux encadrant l'échange d'informations classifiées et protégées avec des États partenaires ou des organisations internationales (cf. 7.2.1.3) ;
- supervise, en lien avec le ministère des affaires étrangères, la négociation par le ministère compétent, des accords intergouvernementaux encadrant l'échange d'informations classifiées et protégées avec des États partenaires ou des organisations internationales dans un domaine spécifique (cf. 7.2.1.3) ;
- est l'interlocuteur des autorités nationales de sécurité étrangères ;

⁴¹ Articles R. 2311-5 et R. 2311-6 du code de la défense.

⁴² Article R. 2311-8 du code de la défense.

⁴³ Article R. 2311-9-1 du code de la défense.

⁴⁴ Article R. 2311-10 du code de la défense.

⁴⁵ Article R. 2311-10-1 du code de la défense.

- assure, en application des accords internationaux régulièrement approuvés et publiés, la sécurité des informations et supports classifiés confiés à la France, détermine les procédures d'habilitation requises pour permettre l'accès à ces informations et organise, dirige et contrôle les réseaux correspondant ;
- participe, avec ses partenaires étrangers, à l'élaboration des règles de sécurité au sein des organisations internationales, y représente la France sur ces sujets et en contrôle la mise en œuvre au plan national.

En sa qualité d'autorité nationale de sécurité, le secrétaire général de la défense et de la sécurité nationale peut nommer des autorités de sécurité déléguées, chargées de mettre en œuvre les missions dévolues à l'autorité nationale de sécurité dans un domaine particulier⁴⁶. Il définit alors les missions déléguées à l'autorité de sécurité déléguée et les modalités de mise en œuvre de cette délégation dans une décision de délégation. L'autorité de sécurité déléguée est responsable devant l'autorité nationale de sécurité.

c) Services à disposition du secrétaire général de la défense et de la sécurité nationale

Pour l'exercice de ses missions aux plans national et international, le secrétaire général de la défense et de la sécurité nationale dispose d'un service de sécurité de défense en charge de la protection du secret⁴⁷.

Dans le domaine de la sécurité des systèmes d'information, il est assisté de l'agence nationale de la sécurité des systèmes d'information (ANSSI)⁴⁸, service à compétence nationale rattaché au secrétaire général de la défense et de la sécurité nationale.

2.1.2 Au niveau ministériel

2.1.2.1 Les ministres

En vertu de l'article R. 2311-6 du code de la défense, chaque ministre est responsable de la protection du secret de la défense nationale dans son champ d'attribution, y compris pour les informations et supports classifiés étrangers confiés à la France en vertu d'un accord général ou spécifique de sécurité.

Relèvent du champ d'attribution ministériel, au titre de la présente instruction :

- les services centraux, services déconcentrés, services à compétence nationale et organismes extérieurs relevant de son autorité ;
- les établissements publics placés sous sa tutelle ;
- les opérateurs d'importance vitale dont il est le ministre coordonnateur ;
- les collectivités territoriales et les personnes morales de droit privé avec lesquelles il a conclu une convention conformément à la partie 4.3 ;
- les personnes morales, publiques ou privées, avec lesquelles le ministre a conclu un contrat de commande publique ou un contrat de subvention conformément à la partie 4.4, ainsi que les sous-traitants ou sous-contractants de ces personnes morales ayant également besoin d'accéder à des informations ou supports classifiés pour l'exécution des prestations du contrat nécessitant l'accès à des informations et supports classifiés réalisés en appui du contrat principal ;

⁴⁶ Article R. 2311-10-1 du code de la défense.

⁴⁷ Article D*. 2311-12 du code de la défense.

⁴⁸ Décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».

- les personnels qui, au sein de ces différents organismes, ont besoin, pour l'exercice de leur fonction ou l'accomplissement de leur mission, d'accéder à des informations ou supports classifiés.

Dans le respect de la présente instruction, chaque ministre précise, dans une instruction ministérielle approuvée par arrêté, les modalités de classification et de protection des informations et supports aux niveaux *Secret* et *Très Secret* (cf. Annexe 3), hors classifications spéciales. Conformément aux dispositions détaillées au chapitre 4, ces modalités s'appliquent à tous les organismes relevant de son champ d'attribution, ainsi qu'à leur personnel.

Chaque ministre prend également, dans son champ d'attribution, les décisions d'habilitation pour les niveaux *Secret* et *Très Secret*, hors classifications spéciales, en application des dispositions de la présente instruction (cf. 3.2, 3.3 et 4.4.1.4)⁴⁹.

Pour l'exercice de ses responsabilités, chaque ministre est assisté d'un haut fonctionnaire de défense et de sécurité (HFDS)⁵⁰.

2.1.2.2 Les hauts fonctionnaires de défense et de sécurité

Le haut fonctionnaire de défense et de sécurité supervise, anime et coordonne l'application de l'ensemble des dispositions relatives à la protection du secret de la défense nationale pour les personnes physiques et morales relevant du champ d'attribution du ministre dont il dépend (cf. 2.1.2.1). Il anime également la politique de sécurité des systèmes d'information et contrôle l'application de celle-ci⁵¹.

Le haut fonctionnaire de défense et de sécurité prend, par délégation du ministre⁵², sous réserve des autres délégations organisées par le code de la défense⁵³, les décisions d'habilitation pour les niveaux *Secret* et *Très Secret*, hors classifications spéciales.

Il tient à jour le registre des personnes physiques et morales relevant de son champ d'attribution habilitées ou en cours d'habilitation (cf. 2.3.2.1 et 3.1.2).

Le haut fonctionnaire de défense et de sécurité dispose d'un service spécialisé de défense ou de défense et de sécurité (désigné dans la présente instruction « service du haut fonctionnaire de défense et de sécurité »)⁵⁴, comprenant, pour l'exercice de ses missions relatives à la protection du secret de la défense nationale :

- un fonctionnaire de sécurité de défense (FSD), chargé d'accompagner les responsables d'organisme dépendant du champ d'attribution de son ministère dans l'animation de leur chaîne fonctionnelle de protection du secret (cf. 2.2.2) ;
- un fonctionnaire de sécurité des systèmes d'information (FSSI), chargé d'accompagner les responsables d'organisme dépendant du champ d'attribution de son ministère et détenant un ou des systèmes d'information classifiés dans l'animation de leurs chaînes fonctionnelles de sécurité des systèmes d'information classifiés et de sécurité des articles contrôlés de la sécurité des systèmes d'information (cf. 2.2.3).

⁴⁹ Article R. 2311-8 du code de la défense.

⁵⁰ 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 leur champ d'attribution respectif, d'un haut fonctionnaire correspondant de défense et de sécurité (HFCDS), le ministre de l'intérieur, d'un haut fonctionnaire de défense (HFD).

⁵¹ Article R. 1143-5 du code de la défense.

⁵² Décret n° 2005-850 du 27 juillet 2005 relatif aux délégations de signature des membres du Gouvernement.

⁵³ Articles R. 2311-8 à R. 2311-8-2 du code de la défense.

⁵⁴ Article R. 1143-2 du code de la défense.

2.1.3 Cas spécifiques

Certaines entités disposent, en vertu de la Constitution ou la loi, d'un statut particulier justifiant la mise en place de procédures adaptées.

2.1.3.1 Services du Premier ministre

En application du décret n° 2012-383 du 20 mars 2012 relatif aux attributions du haut fonctionnaire de défense et de sécurité auprès du Premier ministre, le secrétaire général du Gouvernement exerce les missions dévolues par la présente instruction aux hauts fonctionnaires de défense et de sécurité au profit du cabinet et des services du Premier ministre et cabinet des secrétariats d'État rattachés, à l'exception des entités suivantes pour lesquelles ces fonctions sont assumées par le secrétaire général de la défense et de la sécurité nationale :

- le secrétariat général de la défense et de la sécurité nationale, y compris l'agence nationale de la sécurité des systèmes d'information, l'opérateur des systèmes d'information interministériels classifiés et le service de vigilance et de protection contre les ingérences numériques étrangères ;
- l'institut des hautes études de la défense nationale ;
- le groupement interministériel de contrôle (à l'exception des décisions d'habilitations de ses agents aux niveaux *Secret* et *Très Secret*, hors classifications spéciales)⁵⁵ ;
- l'académie du renseignement.

2.1.3.2 Autorités administratives indépendantes autorisées, par la loi, à accéder au secret de la défense nationale dans l'accomplissement de leur mission

Certaines autorités administratives indépendantes peuvent être autorisées par la loi, pour l'accomplissement de leur mission, à accéder au secret de la défense nationale.

Elles peuvent être assistées, pour la mise en œuvre des règles relatives à la protection du secret de la défense nationale, par le haut fonctionnaire de défense et de sécurité du ministère dont elles dépendent administrativement ou du secrétaire général du Gouvernement lorsqu'elles sont rattachées pour leur gestion administrative ou budgétaire au Premier ministre.

2.1.3.3 Formation spécialisée du Conseil d'État

Conformément à l'article L. 773-2 du code de justice administrative, les membres de la formation spécialisée du Conseil d'État et les personnes qui les assistent, peuvent avoir besoin, dans l'accomplissement de leur mission, d'accéder à des informations ou supports classifiés.

Le haut fonctionnaire de défense et de sécurité du ministère de la justice accompagne la formation spécialisée dans la mise en œuvre des règles relatives à la protection du secret de la défense nationale. À ce titre notamment, il délivre les habilitations aux agents qui assistent les membres de la formation spécialisée selon les modalités prévues aux parties 3.2 et 3.3, tandis que les membres de la formation spécialisée et son rapporteur public sont autorisés ès qualités par la loi, à accéder à des informations et supports classifiés sans que la délivrance d'une décision d'habilitation soit nécessaire (cf. 3.1.4)⁵⁶.

⁵⁵ Décret du 20 décembre 2016 portant délégation de signature du Premier ministre au directeur du groupement interministériel de contrôle.

⁵⁶ Article L. 773-2 du code de justice administrative.

2.1.3.4 Cour des comptes

Dans l'exercice de ses attributions non juridictionnelles, la Cour des comptes peut être appelée à accéder à des informations ou supports classifiés, ainsi qu'à en émettre.

Conformément au décret n° 2012-383 du 20 mars 2012 relatif aux attributions du haut fonctionnaire de défense et de sécurité auprès du Premier ministre, le secrétaire général du Gouvernement peut assister la Cour des comptes dans la mise en œuvre des règles relatives à la protection du secret de la défense nationale. À ce titre, il délivre les décisions d'habilitation des membres et du personnel de la Cour qui ont besoin d'accéder à des informations et supports classifiés dans l'accomplissement de leurs attributions non juridictionnelles en relation avec le Gouvernement.

La déclassification des informations et supports classifiés émis par la Cour des comptes est décidée par le président de la Cour des comptes, après avis du Premier ministre.

2.1.3.5 Délégation parlementaire au renseignement

Conformément à l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, les membres de la délégation parlementaire au renseignement, ainsi que les agents des assemblées parlementaires qui les assistent, peuvent, pour l'exercice du contrôle parlementaire de l'action du Gouvernement en matière de renseignement et l'accomplissement de sa mission d'évaluation de la politique publique en ce domaine, avoir besoin d'accéder à des informations ou supports classifiés.

Alors que les parlementaires membres de la délégation parlementaire au renseignement sont habilités *ès qualités* (cf. 1.2.2.3 b) et 3.1.4), les agents des assemblées parlementaires qui les assistent font l'objet d'une décision d'habilitation selon les modalités prévues aux 3.2 et 3.3.

L'autorité d'habilitation est déterminée par les présidents des assemblées en application de l'article 3 de l'ordonnance du 17 novembre 1958.

2.2 CHAINES DE SECURITE ENCADRANT, SOUS LA RESPONSABILITE DU RESPONSABLE D'ORGANISME, LA MISE EN ŒUVRE DE LA PROTECTION DU SECRET DE LA DEFENSE NATIONALE

2.2.1 Responsabilité première du responsable d'organisme

Le responsable d'un organisme ayant accès, même à titre provisoire, à des informations et supports classifiés est responsable de la protection du secret de la défense nationale au sein de son organisme et par son personnel.

À ce titre :

- il met en place, selon les modalités prévues par la présente instruction, complétées, le cas échéant, par l'instruction ministérielle, les directives techniques particulières et les dispositions contractuelles applicables, l'organisation et les procédures nécessaires pour garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité des informations et supports classifiés au sein de son organisme ;
- il approuve la politique de protection du secret de son organisme qui intègre, le cas échéant, les exigences relatives à la sécurité des systèmes d'information classifiés. Ces exigences sont cohérentes avec la politique de sécurité des systèmes d'information applicables à l'organisme lorsqu'elle existe ;
- il veille à l'application de cette politique au sein de son organisme et désigne à cet effet un officier de sécurité et, le cas échéant, un officier de sécurité des systèmes d'information ;

- il peut, lorsque l'activité de son organisme le justifie, décider de mettre en place un bureau de protection du secret chargé d'appuyer l'officier de sécurité dans ses missions. Il peut être dirigé par l'officier de sécurité. La mise en place d'un tel bureau est obligatoire lorsque l'organisme détient des informations de niveau *Très Secret* (cf. 7.2.1.2).

Pour les organismes privés ou les organismes publics autres que les établissements publics de l'État, le responsable d'organisme est également chargé de désigner une autorité qualifiée en sécurité des systèmes d'information (cf. 2.2.3.1) dès lors que son organisme détient un système d'information classifié.

Pour exercer ses missions, le responsable d'organisme s'appuie sur une chaîne de sécurité, articulée autour de la chaîne fonctionnelle de sécurité de protection du secret, complétée, le cas échéant, par la chaîne de sécurité des systèmes d'information.⁵⁷

2.2.2 Chaîne fonctionnelle de protection du secret

La chaîne fonctionnelle de protection du secret est organisée de façon à veiller à la mise en œuvre de l'ensemble des dispositions relatives à la protection du secret de la défense nationale au sein de l'organisme. Elle est structurée de façon à :

- veiller à la bonne mise en œuvre des mesures de sécurité applicables aux personnes physiques et morales conformément aux chapitres 3 et 4 ;
- garantir la protection physique et logique des informations et supports classifiés, y compris les systèmes d'information classifiés conformément aux chapitres 5 et 6 ;
- assurer la gestion des informations et supports classifiés conformément au chapitre 7 ;
- être en capacité de détecter dans les meilleurs délais toute compromission avérée ou suspectée du secret de la défense nationale (cf. 1.4.2).

Elle est placée sous la responsabilité du responsable d'organisme et est animée par l'officier de sécurité qu'il désigne à cet effet.

2.2.2.1 L'officier de sécurité

a) Critère de désignation et rôle de l'officier de sécurité

Le responsable de l'organisme ayant accès à des informations et supports classifiés désigne, parmi son personnel, une personne chargée d'exercer la fonction d'officier de sécurité (désignée dans la présente instruction « officier de sécurité ») ainsi que, dans la mesure du possible, un adjoint ou un suppléant.

L'officier de sécurité, son adjoint, son suppléant, doivent :

- être habilités au niveau requis par la fonction ;
- être subordonnés au responsable d'organisme et disposer d'un niveau hiérarchique suffisant pour le conseiller ;
- disposer de l'autorité fonctionnelle nécessaire à l'égard du personnel de l'organisme et entretenir une relation étroite avec le fonctionnaire de sécurité de défense du ministère dont il relève ;
- disposer de tous les moyens nécessaires à l'accomplissement de sa mission ;

⁵⁷ Outre la protection du secret, ces chaînes fonctionnelles sont susceptibles d'être impliquées dans la mise en œuvre d'autres politiques de protection comme la sécurité des activités d'importance vitale (SAIV) ou la protection du potentiel scientifique et technique (PPST).

- appartenir de façon suffisamment stable à l'organisme ;
- être formés à la législation et à la réglementation, relatives à la protection du secret de la défense nationale.

Lorsque l'organisme est appelé à traiter des informations et supports classifiés portant la mention de protection *Spécial France*, l'officier de sécurité doit avoir la nationalité française.

Il revient au responsable d'organisme de communiquer au fonctionnaire de sécurité de défense le nom et les coordonnées de l'officier de sécurité, de son adjoint ou suppléant, et de l'informer de tout changement.

La fonction d'officier de sécurité, adjoint ou suppléant, ainsi que le cas échéant, les missions dévolues au bureau de protection du secret, ne peuvent en aucun cas être externalisées.

b) Rôle de l'officier de sécurité

Outre les missions qui lui sont dévolues par la ou les instructions ministérielles et, le cas échéant, directives techniques particulières, dont il relève, l'officier de sécurité a notamment pour mission, sous l'autorité du responsable d'organisme, de :

- rédiger la politique de protection du secret de son organisme et veiller à son application ;
- s'assurer, en lien avec l'officier de sécurité des systèmes d'information, du niveau de sécurité des systèmes d'information classifiés ;
- tenir à jour le(s) catalogue(s) des emplois de son organisme en identifiant avec les autorités compétentes les fonctions ou missions nécessitant l'accès à des informations et supports classifiés, engager les procédures d'habilitation (cf. 3.3.1) en référence au catalogue des emplois et notifier les décisions ;
- gérer les dossiers d'habilitation du personnel et assurer la liaison avec le fonctionnaire de sécurité de défense et les services enquêteurs ;
- instruire et sensibiliser le personnel en matière de protection du secret de la défense nationale avec, le cas échéant, l'appui de l'officier de sécurité des systèmes d'information ;
- diligenter les enquêtes administratives en matière d'accès en zone protégée (cf. 5.3.1.1) ;
- s'assurer lorsque son organisme est lié par une convention ou un contrat prévoyant l'accès à des informations et support classifiés que les stipulations contractuelles en matière de protection du secret de la défense nationale sont appliquées ;
- réaliser ou faire réaliser des contrôles internes et des audits de sécurité portant sur la gestion des informations et supports classifiés, la sécurité des systèmes d'information classifiés et l'aptitude physique des lieux abritant des éléments couverts par le secret de la défense nationale ;
- assurer un suivi de l'activité liée aux habilitations, aux lieux abritant des éléments couverts par le secret de la défense nationale, aux informations et supports classifiés et aux systèmes d'information classifiés et en rendre compte au fonctionnaire de sécurité de défense ;
- rendre compte, le cas échéant avec l'officier de sécurité des systèmes d'information, via leur chaîne fonctionnelle respective (cf. partie 2.2) des compromissions du secret avérées ou supposées ;

- diriger, lorsque le responsable de l'organisme le décide, le bureau de protection du secret.

Pour les questions relatives à la sécurité des systèmes d'information, l'officier de sécurité est assisté de l'officier de sécurité des systèmes d'information.

Lorsque l'officier de sécurité dispose d'un adjoint ou d'un suppléant, la répartition des missions entre le titulaire et son adjoint ou suppléant est approuvée par le responsable d'organisme.

c) Officier de sécurité de groupe ou de holding, officier central de sécurité, officier de sécurité d'établissement, de correspondants de sécurité

i. Officier de sécurité de groupe ou de *holding*

Un officier de sécurité de groupe ou de *holding* peut être désigné respectivement au sein d'un groupe de sociétés lorsqu'au moins une société a accès au secret de la défense nationale ou d'une société holding si une de ses filiales a accès au secret de la défense nationale afin d'assurer une cohérence entre la gouvernance du groupe ou de la société holding et les enjeux de la protection du secret.

ii. Officier central de sécurité, officier de sécurité d'établissement, correspondants de sécurité

Lorsque l'organisme dispose d'un ou plusieurs établissements abritant des informations et supports classifiés, le responsable d'organisme peut désigner un officier de sécurité par établissement abritant. Ces derniers sont placés sous la supervision de l'officier de sécurité placé directement aux côtés du responsable d'organisme, alors désigné « officier central de sécurité ».

L'officier de sécurité d'établissement est habilité au niveau requis par sa fonction. Il dispose d'un positionnement hiérarchique suffisant pour conseiller et entretenir une relation étroite avec le directeur d'établissement et les dirigeants de la personne morale. Il dispose de tous les moyens nécessaires pour accomplir ses missions. Cette fonction ne peut en aucun cas être externalisée.

Le responsable d'organisme peut, en outre, en dehors des établissements abritant des informations ou supports classifiés, désigner des correspondants de sécurité placés sous le contrôle opérationnel de l'officier de sécurité ou de l'officier central de sécurité au sein de chaque subdivision physique ou opérationnelle de la personne morale.

2.2.3 Chaîne fonctionnelle de sécurité des systèmes d'information

La chaîne fonctionnelle de sécurité des systèmes d'information est organisée de manière à veiller à la sécurité de l'ensemble des systèmes d'information détenus par l'organisme, tout au long de leur cycle de vie. Le rôle de cette chaîne fonctionnelle, qui n'est pas spécifique aux systèmes d'information classifiés, est renforcé dès lors qu'un organisme dispose d'un ou plusieurs systèmes classifiés. Elle contrôle alors l'application de la réglementation en matière de protection du secret sur ces systèmes.

Elle s'appuie sur les autorités qualifiées en sécurité des systèmes d'information, les personnes exerçant la fonction d'officier de sécurité des systèmes d'information (OSSI), les responsables de la sécurité des systèmes d'information (RSSI), les autorités d'homologation et les autorités responsables de l'exploitation des systèmes conformément aux modalités arrêtées par le ministre dont elles relèvent.

Sous la responsabilité du responsable d'organisme, la chaîne de sécurité des systèmes d'information contribue au déploiement et à la traçabilité des articles contrôlés de la sécurité des systèmes d'information (ACSSI).

2.2.3.1 L'autorité qualifiée en sécurité des systèmes d'information

L'autorité qualifiée en sécurité des systèmes d'information (AQSSI) a pour mission de garantir la sécurité des systèmes d'information classifiés. Elle doit avoir un niveau hiérarchique suffisant et disposer de tous les moyens nécessaires à l'accomplissement de ses missions.

a) Modalité de désignation de l'autorité qualifiée en sécurité des systèmes d'information

Chaque ministre désigne pour les services centraux, déconcentrés, les services à compétence nationale relevant de sa responsabilité, les organismes extérieurs ainsi que pour les établissements publics dont il assure la tutelle, la ou les autorités qualifiées en sécurité des systèmes d'information.

S'agissant des autres personnes morales (organisme ayant accès à des informations et supports classifiés en raison de leur désignation en tant qu'opérateur d'importance vitale ou en vertu d'une convention ou d'un contrat conformément aux parties 4.1, 4.2, 4.3 et 4.4), il appartient au responsable de l'organisme de désigner, en son sein, une personne ayant la fonction d'autorité qualifiée en sécurité des systèmes d'information. Il en informe le fonctionnaire de sécurité des systèmes d'information du ministère dont il relève.

b) Missions de l'autorité qualifiée en sécurité des systèmes d'information

L'autorité qualifiée en sécurité des systèmes d'information définit les lignes directrices relatives à la sécurité des systèmes d'information classifiés pour les organismes relevant de ses attributions et en contrôle l'application⁵⁸.

À ce titre, elle approuve les exigences de sécurité relatives à la sécurité des systèmes d'information classifiés intégrées dans la politique de protection des organismes relevant de ses attributions (cf. 2.3.1.3).

Les missions en matière de sécurité des systèmes d'information confiées aux officiers de sécurité des systèmes d'information, aux responsables de la sécurité des systèmes d'information, aux autorités d'homologation, aux autorités d'emploi ou, plus généralement, aux organismes, sont réalisées sous l'autorité et la responsabilité de leur autorité qualifiée en sécurité des systèmes d'information.

Afin de lui permettre de maîtriser les systèmes d'information placés sous sa responsabilité et d'améliorer la capacité de réaction en cas d'incident, chaque autorité qualifiée en sécurité des systèmes d'information élabore, avec, le cas échéant, l'appui du ou des officiers de sécurité des systèmes d'information qui lui sont fonctionnellement rattachés, la cartographie de l'ensemble des systèmes d'information classifiés dont elle est responsable. L'autorité qualifiée en sécurité des systèmes d'information s'assure que cette cartographie, établie suivant les recommandations de l'agence nationale de la sécurité des systèmes d'information, est régulièrement actualisée.

L'accès à cette cartographie respecte le besoin d'en connaître. Son éventuelle classification est déterminée par l'autorité qualifiée en sécurité des systèmes d'information.

⁵⁸ Article R. 2311-6-2 du code de la défense.

2.2.3.2 L'officier de sécurité des systèmes d'information (OSSI)

Le responsable d'organisme utilisant des systèmes d'information classifiés désigne, parmi son personnel, une personne exerçant la fonction d'officier de sécurité des systèmes d'information ainsi que, dans la mesure du possible, un adjoint ou un suppléant répondant aux exigences suivantes, complétées le cas échéant par l'instruction ministérielle :

- être habilité au niveau requis par cette fonction ;
- avoir un niveau hiérarchique suffisant ;
- disposer de tous les moyens nécessaires à l'accomplissement de ses missions ;
- appartenir de façon suffisamment stable à l'organisme ;
- être formé à la législation et à la réglementation, relatives à la protection du secret, à la sécurité des systèmes d'information, y compris classifiés.

Lorsque l'organisme est appelé à traiter des informations et supports classifiés portant la mention de protection *Spécial France*, l'officier de sécurité des systèmes d'information doit avoir la nationalité française.

Sous réserve de ces exigences complétées, le cas échéant, par l'instruction ministérielle, l'officier de sécurité des systèmes d'information :

- est le correspondant local du fonctionnaire de sécurité des systèmes d'information et des services enquêteurs selon les modalités définies dans l'instruction ministérielle ;
- conçoit et met en œuvre le management de la sécurité des systèmes d'information au sein de son organisme. À ce titre, il définit les exigences de sécurité applicables au sein de son organisme et relatives à l'usage des systèmes d'information classifiés utilisés au sein de son organisme et les soumet à la validation de l'autorité qualifiée en sécurité des systèmes d'information ;
- s'assure que les politiques de sécurité de chaque système d'information classifié utilisé par l'organisme sont conformes aux exigences de sécurité qui s'y appliquent ;
- participe à l'instruction et à la sensibilisation du personnel en matière de protection du secret de la défense nationale ;
- recense les besoins de communications sécurisées et s'assure de la traçabilité et de l'intégrité des articles contrôlés de la sécurité des systèmes d'information au sein de son organisme ;
- travaille en collaboration quotidienne et étroite avec l'officier de sécurité.

Il revient au responsable d'organisme de communiquer au fonctionnaire de sécurité des systèmes d'information le nom et les coordonnées de l'officier de sécurité des systèmes d'information, de son adjoint ou suppléant, et de l'informer de tout changement.

Lorsque l'officier de sécurité des systèmes d'information dispose d'un adjoint ou d'un suppléant, la répartition des missions entre le titulaire et son adjoint ou suppléant est approuvée par le responsable d'organisme.

Lorsque plusieurs établissements de l'organisme utilisent des systèmes d'information classifiés, le responsable d'organisme désigne un officier de sécurité des systèmes d'information par établissement utilisateur. Ces derniers sont placés sous la supervision de l'officier de sécurité des systèmes d'information placé directement aux côtés du responsable d'organisme et désigné « officier central de sécurité des systèmes d'information ».

2.2.3.3 Le responsable de la sécurité du système d'information (RSSI)

Dans le cadre du développement et de l'exploitation d'un système d'information classifié, une personne exerçant la fonction de responsable de la sécurité du système d'information est désignée pour piloter la démarche d'intégration de la sécurité du système d'information classifié durant la phase du projet, jusqu'à l'homologation initiale incluse, qu'il est chargé d'instruire sous la responsabilité de l'autorité d'homologation.

Après l'homologation initiale et dès que le système est opérationnel, le responsable de la sécurité du système d'information assure le suivi de la sécurité du système d'information en service. Il est notamment chargé d'instruire les renouvellements d'homologation. Pour le système dont il a la charge et dans le domaine de la sécurité des systèmes d'information, il conseille, recommande et propose à l'autorité d'emploi du système d'information des règles spécifiques. Il est garant de la cohérence des mécanismes et des procédures de sécurité ainsi que du maintien du niveau de sécurité dans le temps.

Il assure principalement les fonctions opérationnelles liées à la sécurité des systèmes d'information classifiés relevant de son périmètre de responsabilité.

2.3 OUTILS DE PILOTAGE, DE MISE EN ŒUVRE ET DE SUIVI

2.3.1 Instructions ministérielles et documents d'application

La protection du secret de la défense nationale repose sur un corpus de textes schématisé en Annexe 4, dont le code pénal, le code de la défense et la présente instruction constituent le socle. Ce socle est ensuite décliné par un ensemble de textes réglementaires (instructions interministérielles particulières, instructions ministérielles, directives techniques particulières) et infra-réglementaires (politique de sécurité des systèmes d'information), internes aux organismes (politique de protection du secret, plan de sécurité d'opérateur, plan particulier de protection) ou contractuels (plan contractuel de sécurité).

2.3.1.1 Instructions ministérielles

a) Élaboration de l'instruction ministérielle

Conformément au 2.1.2.1, chaque ministre précise, pour son champ d'attribution, dans une instruction approuvée par arrêté, les modalités de classification et de protection encadrant la classification des informations et supports aux niveaux *Secret* et *Très Secret*, hors classifications spéciales.

L'instruction ministérielle se conforme à la réglementation en vigueur en matière de protection du secret de la défense nationale et, en particulier, aux dispositions fixées par la présente instruction. Elle comporte un guide de classification (cf. Annexe 3).

Le haut fonctionnaire de défense et de sécurité rédige le projet d'instruction ministérielle qu'il transmet, pour avis, au secrétaire général de la défense et de la sécurité nationale. Cet avis est réputé favorable s'il n'est pas intervenu dans le délai de deux mois à compter de la réception du projet. Une copie de l'instruction ministérielle signée est adressée au secrétaire général de la défense et de la sécurité nationale.

Chaque ministre peut en complément de l'instruction ministérielle et sur son fondement, élaborer des directives techniques particulières destinées à préciser, pour un domaine d'activité spécifique, les mesures de protection du secret complémentaires à mettre en œuvre. Chaque directive particulière contient un guide de classification spécifique au domaine considéré permettant à chaque organisme d'évaluer le niveau de classification des informations et supports qu'il produit et d'en déduire les mesures d'organisation et de protection à mettre en œuvre.

b) Revue de l'instruction ministérielle

L'instruction ministérielle fait l'objet d'une revue à intervalles réguliers ou en cas de nécessité afin de garantir la pertinence, l'efficacité et l'adéquation des mesures.

Toute modification est soumise, pour avis, au secrétaire général de la défense et de la sécurité nationale dans les mêmes conditions que celles définies au a).

2.3.1.2 Politique de sécurité des systèmes d'information

Chaque autorité qualifiée en sécurité des systèmes d'information s'assure de l'existence d'une politique de sécurité des systèmes d'information applicable aux organismes relevant de sa compétence et, à défaut, l'élabore.

Cette politique qui porte sur la sécurité des systèmes d'information au sens large comporte des lignes directrices en matière de sécurité des systèmes d'information classifiés (cf. 2.2.3.1 b))⁵⁹.

Ces lignes directrices sont déclinées dans la politique de protection du secret des organismes utilisant des systèmes d'information classifiés.

Ces exigences sont ensuite intégrées dans le dossier d'homologation de chaque système d'information (cf. 2.3.1.2).

2.3.1.3 Politique de protection du secret

Chaque responsable d'organisme ayant accès au secret de la défense nationale élabore une politique de protection du secret en déclinaison de l'instruction ministérielle et, le cas échéant, des directives techniques particulières applicables à son organisme. S'agissant de la sécurité des systèmes d'information classifiés, cette politique se conforme aux recommandations de l'agence nationale de la sécurité des systèmes d'information.

Cette politique peut être plus restrictive que la réglementation sous réserve qu'elle ne s'y oppose pas. Elle :

- précise la déclinaison au sein de l'organisme de la chaîne fonctionnelle de protection du secret, et, le cas échéant, des chaînes de la sécurité des systèmes d'information classifiés et de la sécurité des articles contrôlés de la sécurité des systèmes d'information ;
- définit les exigences en ce qui concerne l'habilitation, ainsi que la formation et la sensibilisation à la protection du secret et la sécurité des systèmes d'information et des articles contrôlés de la sécurité des systèmes d'information ;
- précise les mesures de protection et de gestion des informations et supports classifiés, des systèmes d'information classifiés, des articles contrôlés de la sécurité des systèmes d'information et des lieux abritant des éléments couverts par le secret de la défense nationale. À ce titre, la politique de protection du secret comprend les mesures de contrôle nécessaires pour limiter l'accès des personnes non qualifiées aux emprises de l'organisme abritant des informations et supports classifiés et comprend, pour les organismes utilisant des systèmes d'information classifiés, les exigences relatives à leur sécurité. Ces exigences sont élaborées par l'officier de sécurité des systèmes d'information ;
- prend en compte, le cas échéant, les exigences propres, à la protection des informations classifiées étrangères ou relevant d'une organisation internationale. En

⁵⁹ Article R. 2311-6-2 du code de la défense.

particulier, elle intègre les exigences relatives à la protection des informations classifiées de l'OTAN et de l'Union européenne ;

- fixe les obligations en matière de contrôle et de suivi de l'activité liée aux habilitations, aux lieux abritant des éléments couverts par le secret de la défense nationale, aux informations et supports classifiés, aux systèmes d'information classifiés et aux articles contrôlés de la sécurité des systèmes d'information ;
- établit les procédures de remontée de l'information et les mesures de protection à mettre en œuvre en cas de compromission avérée ou supposée du secret de la défense nationale ou d'articles contrôlés de la sécurité des systèmes d'information.

Pour les opérateurs d'importance vitale, cette politique est conforme aux engagements pris dans le cadre du plan de sécurité d'opérateur ou du plan particulier de protection.

Pour les organismes accédant à des informations et supports classifiés au titre d'une convention ou d'un contrat selon les modalités définies aux parties 4.3 et 4.4, cette politique est conforme aux stipulations du ou des plans contractuels de sécurité applicables à l'organisme.

La politique de protection du secret fait l'objet d'une révision à intervalles réguliers ou en cas de nécessité afin de garantir la pertinence, l'efficacité et l'adéquation des mesures. En particulier, elle est revue lorsqu'un incident de sécurité a abouti à divulguer ou rendre possible la divulgation d'un secret de la défense nationale.

2.3.2 Outils et mesures de suivi de l'activité « protection du secret »

2.3.2.1 Traitement automatisé relatif à la gestion des habilitations au secret de la défense nationale

Chaque ministère met en place et tient à jour, dans les conditions fixées par voie réglementaire, un traitement automatisé des dossiers d'habilitation en cours d'instruction et de suivi des habilitations en cours de validité pour les personnes physiques et morales relevant de son champ d'attribution.

Le secrétaire général de la défense et de la sécurité nationale met en place et tient à jour, dans les mêmes conditions, un traitement automatisé des dossiers d'habilitation en cours d'instruction et de suivi des habilitations en cours de validité pour les domaines relevant de sa compétence.

2.3.2.2 Base de données des lieux abritant des éléments couverts par le secret de la défense nationale

Les lieux abritant des éléments couverts par le secret de la défense nationale sont les pièces dans lesquelles sont conservés des informations et supports classifiés. Les mesures de protection et les règles régissant l'accès à ces lieux sont encadrées par les dispositions du code pénal, du code de procédure pénale, du code de la défense, du code de la sécurité intérieure, du code du travail, des accords généraux ou spécifiques de sécurité (cf. 7.2.1.3) et selon les modalités précisées, pour les opérateurs d'importance vitale, dans le plan de sécurité d'opérateur ou le plan particulier de protection (cf. 4.2) et, pour les autres personnes morales liées à l'État pour une convention ou un contrat, dans le plan contractuel de sécurité (cf. 4.3 et 4.4).

Afin de garantir l'intégrité de ces lieux et de s'assurer qu'aucune personne non qualifiée ne puisse, même par inadvertance, y avoir accès, une base de données interministérielle recensant l'ensemble des lieux abritant est mise en place. Cette base de données est tenue à jour. Ainsi, l'officier de sécurité informe le service du haut fonctionnaire de défense et de sécurité de tout changement (création, modification, suppression) affectant les lieux abritant

placés dans son domaine de compétence. La base de données est vérifiée annuellement au plus tard le 15 novembre par les services des hauts fonctionnaires de défense et de sécurité compétents, au sens des paragraphes 2.1.2.2 et 2.1.3.

Sur la base des informations contenues dans la base de données interministérielle sur les lieux abritant, une liste des lieux abritant des éléments couverts par le secret de la défense nationale est établie annuellement par arrêté du Premier ministre, sur proposition des ministres intéressés⁶⁰. Elle précise, pour chaque lieu, l'organisme concerné, les pièces clairement déterminées⁶¹ et l'adresse du site où sont conservés les informations et supports classifiés.

La liste est accessible au ministre de la justice et à la commission du secret de la défense nationale.

2.3.3 Inspections, contrôles et audits

Conformément aux dispositions législatives et réglementaires relatives à la protection du secret de la défense nationale, des inspections, contrôles ou audits⁶² des organismes ayant accès à des informations ou supports classifiés sont organisés périodiquement par le haut fonctionnaire de défense et de sécurité compétent, avec l'appui, si nécessaire, des services compétents en matière de protection physique et de sécurité des systèmes d'information, afin de s'assurer du respect des règles relatives à la protection des informations et supports classifiés aux niveaux *Secret* et *Très Secret*, hors classifications spéciales.

Par dérogation à l'alinéa précédent, pour les organismes relevant du champ d'attribution du ministre des armées, ces audits, contrôles et inspections, sont organisés conformément à l'instruction ministérielle dans les organismes ayant conclu une convention ou un contrat classifiés à son profit.

Chaque inspection, contrôle ou audit donne lieu à un rapport adressé au responsable de l'organisme contrôlé et au haut fonctionnaire de défense et de sécurité dont il relève. Ce rapport identifie, par ordre de priorité, les mesures propres à améliorer les conditions générales de sécurité.

Le secrétariat général de la défense et de la sécurité nationale peut également inspecter tout organisme ayant accès à des informations et supports classifiés, en liaison avec le haut fonctionnaire de défense et de sécurité compétent, notamment au regard du compte rendu annuel d'évaluation de la protection du secret adressé par le haut fonctionnaire de défense et de sécurité dont l'organisme dépend. Le secrétariat général de la défense et de la sécurité nationale peut, si nécessaire, se faire assister par l'agence nationale de la sécurité des systèmes d'information ou la diligenter.

Le secrétariat général de la défense et de la sécurité nationale procède, par ailleurs, aux inspections, contrôles ou audits permettant de s'assurer du respect de la réglementation spécifique applicable aux classifications spéciales. À l'issue de chaque inspection, contrôle ou audit, le secrétariat général de la défense et de la sécurité nationale adresse un rapport au responsable d'organisme contrôlé et au haut fonctionnaire de défense et de sécurité dont il relève. Ce rapport identifie, par ordre de priorité, les mesures propres à améliorer les conditions générales de sécurité.

⁶⁰ Article R. 2311-9-1 du code de la défense.

⁶¹ Conformément à l'article 56-4 de code de procédure pénale, un lieu abritant est un « *lieu précisément identifié* » et se limite, ainsi que l'a rappelé le Conseil constitutionnel dans sa décision n° 2011-192 QPC du 10 novembre 2011, à une pièce clairement déterminée.

⁶² Article R. 2311-9 du code de la défense.

En cas d'anomalies graves constatées à l'occasion d'une inspection, d'un audit ou d'un contrôle réalisé par le secrétariat général de la défense et de la sécurité nationale, celui-ci en informe sans délai le haut fonctionnaire de défense et de sécurité compétent et, en cas de compromission avérée ou suspectée, saisit la direction générale de la sécurité intérieure qui concourt à la prévention et à la répression des actes portant atteinte au secret de la défense nationale sous le contrôle et la direction de l'autorité judiciaire, sans préjudice de la dénonciation de l'infraction au procureur de la République sur le fondement de l'article 40 du code de procédure pénale.

2.3.4 Rapport annuel sur la protection du secret de la défense nationale

Le secrétaire général de la défense et de la sécurité nationale contrôle l'application des mesures de protection du secret. Afin de lui permettre d'assurer ce contrôle et de disposer de la vision la plus précise possible de la mise en œuvre de la réglementation, chaque haut fonctionnaire de défense et de sécurité lui remet, avant le 31 mars de chaque année, un compte rendu d'évaluation de la protection du secret de la défense nationale dans son champ d'attribution. Ce rapport est classifié au niveau *Secret* et marqué *Spécial France*. Il est établi sur la base d'un questionnaire transmis par le secrétariat général de la défense et de la sécurité nationale au plus tard le 30 novembre de chaque année.

Ce compte rendu porte sur l'ensemble du champ d'attribution du ministre concerné. Ainsi, pour chaque ministère, ce compte rendu porte à la fois sur la mise en œuvre de la protection du secret par les services centraux, déconcentrés, services à compétence nationale et établissements publics relevant de son ministère, mais également sur les opérateurs d'importance vitale qui lui sont rattachés, ainsi que sur les autres personnes morales avec lesquelles le ministère a conclu une convention ou un contrat nécessitant l'accès à des informations ou supports classifiés.

Ces comptes rendus comportent des données précises sur l'organisation, la gestion et la sensibilisation à la protection du secret dans le champ d'attribution du ministère concerné. Ils contiennent également des données sur le nombre d'incidents de sécurité recensés, sur le volume d'habilitations en cours de validité, le nombre de demandes en cours d'instruction, le nombre de refus et d'abrogation de décisions d'habilitation prononcés, ainsi que sur les contentieux en cours ou clos au cours de l'année écoulée. Les données relatives à l'activité des services enquêteurs sont intégrées dans les comptes rendus des ministères dont ils dépendent. Elles comportent notamment un bilan annuel des compromissions établi par les services enquêteurs et l'état d'avancement des procédures et des suites données.

Ce compte rendu fait également état des carences relevées dans le dispositif de protection du secret et des actions correctrices envisagées et engagées.

Sur la base des comptes rendus établis par les hauts fonctionnaires de défense et de sécurité, le secrétariat général de la défense et de la sécurité nationale adresse chaque année au Premier ministre un rapport d'évaluation de la protection du secret de la défense nationale.

3 MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES

Conformément à l'article R. 2311-7 du code de la défense, « *sauf exceptions prévues par la loi, nul n'est qualifié pour connaître d'informations et supports classifiés s'il n'a fait au préalable l'objet d'une décision d'habilitation et s'il n'a besoin, au regard du catalogue des emplois justifiant une habilitation, établi dans les conditions définies par arrêté du Premier ministre, de les connaître pour l'exercice de sa fonction ou l'accomplissement de sa mission* ».

Le présent chapitre définit chaque étape du processus d'habilitation des personnes physiques et rappelle les exceptions prévues par la loi.

3.1 PORTEE ET FONDEMENT DE LA PROCEDURE D'HABILITATION

3.1.1 Portée de l'habilitation et besoin d'en connaître

Conformément aux articles 413-10 et suivants du code pénal, l'accès par des personnes non qualifiées à des informations ou supports protégés par le secret de la défense nationale est prohibé.

Pour qu'une personne physique puisse être considérée comme qualifiée au sens du code pénal, elle doit répondre à deux exigences cumulatives :

- avoir été dûment habilitée au niveau de classification requis, à l'issue d'une enquête administrative destinée à évaluer les vulnérabilités qu'elle est susceptible de présenter pour le secret de la défense nationale (cf. 3.3) ou être habilitée *ès qualités* de par la loi ou son statut constitutionnel (cf. 3.1.4) ;
- justifier du besoin d'en connaître.

En effet, l'habilitation ne permet pas d'accéder sans limite à toute information ou support classifié. D'une part, elle ne permet d'accéder qu'aux informations et supports portant un timbre de classification de niveau inférieur ou égal au niveau mentionné sur la décision d'habilitation. D'autre part, une personne habilitée ne peut ni ne doit accéder à une information ou un support classifié que si l'autorité ayant sollicité son habilitation estime absolument nécessaire qu'elle ait accès à l'information ou au support considéré.

La procédure d'habilitation ne peut être lancée que pour les fonctions et missions figurant au catalogue des emplois de l'organisme concerné, justifiant la nécessité pour le candidat à l'habilitation d'accéder à des informations et supports classifiés au niveau requis.

3.1.2 Justification de la demande d'habilitation au regard du catalogue des emplois

3.1.2.1 Autorités compétentes pour l'établissement et la mise à jour des catalogues des emplois

En application de l'article R. 2311-7 du code de la défense, nul ne peut faire l'objet d'une demande d'habilitation si la fonction ou la mission justifiant son besoin d'accéder à des informations ou supports classifiés ne figure sur un catalogue des emplois établi par une autorité compétente.

Chaque ministre précise pour les services centraux, les services déconcentrés, les services à compétence nationale, les organismes extérieurs relevant de son autorité, ainsi que les établissements publics placés sous sa tutelle et les opérateurs d'importance vitale relevant d'un secteur d'activités dont il est le coordonnateur, les autorités chargées d'établir, en lien avec leur officier de sécurité, les catalogues des emplois.

3.1.2.2 Contenu et actualisation annuelle du catalogue des emplois

Un catalogue des emplois est établi pour chaque niveau de classification. Il identifie, *via* l'octroi d'un numéro de poste, chaque fonction ou mission impliquant nécessairement l'accès à des informations et supports classifiés au niveau de classification considéré, ainsi que les noms et prénoms des personnes physiques occupant les postes inscrits au catalogue des emplois. Chaque catalogue des emplois est mis à jour par l'officier de sécurité.

Dès l'ouverture d'un catalogue des emplois, l'officier de sécurité en adresse une copie au haut fonctionnaire de défense et de sécurité, sauf dispositions contraires prévues par l'instruction ministérielle.

Il lui adresse par ailleurs chaque année une version mise à jour en date du 31 décembre au plus tard le 1^{er} février de l'année suivante. À cette occasion, il vérifie auprès des titulaires des postes répertoriés s'ils ont effectivement eu accès à des informations et supports classifiés pour le niveau concerné et inscrit les postes qui requièrent un accès au secret de la défense nationale. Le cas échéant, l'officier de sécurité, en lien avec l'autorité compétente, réévalue le niveau d'habilitation requis par les fonctions ou missions. Dans le cas où elles ne nécessitent plus d'accéder au secret de la défense nationale, il les supprime du catalogue des emplois, notifie aux titulaires des emplois concernés que leur décision d'habilitation est abrogée et leur fait signer le second volet de l'engagement de responsabilité (cf. 3.5.2).

3.1.2.3 Référence au catalogue des emplois dans les demandes d'habilitation et mise à jour éventuelle

Les demandes d'habilitation sont établies en référence au catalogue des emplois et précisent le numéro de poste du catalogue des emplois auquel correspond la demande.

Lorsqu'une demande d'habilitation porte sur une fonction ou une mission nouvelle, ou sur une fonction ou une mission non préalablement inscrite sur un catalogue des emplois, et que la fonction ou la mission considérée nécessite sans conteste que son titulaire accède à des informations et supports classifiés, l'officier de sécurité met à jour le catalogue des emplois en concertation avec l'autorité d'habilitation.

3.1.3 Responsabilité de l'autorité hiérarchique ou administrative sollicitant l'habilitation

De même qu'une habilitation ne doit pas être sollicitée pour une personne appelée à exercer une fonction ou à accomplir une mission qui ne figure pas sur un catalogue des emplois, il appartient au responsable d'organisme de s'assurer, avec l'appui de l'officier de sécurité, que toute personne occupant un poste ou accomplissant une mission figurant dans le ou l'un des catalogues des emplois de son organisme a été dûment habilitée selon les modalités définies dans la présente instruction.

Dans le cas contraire, la personne est écartée des fonctions ou missions nécessitant l'accès aux informations et supports classifiés dans l'attente de son habilitation au niveau requis. Toute personne occupant ou visant un poste pour lequel le besoin d'habilitation est avéré et qui refuserait de se soumettre à la procédure d'habilitation est définitivement écartée du poste.

À titre exceptionnel, un service de l'État peut solliciter l'inscription à l'un de ses catalogues des emplois d'une personne physique ou d'un ensemble de personnes physiques non rattachées à lui, ni hiérarchiquement, ni fonctionnellement, ni sous couvert d'une convention ou d'un contrat au titre des parties 4.3 et 4.4. À cet effet, il adresse une demande motivée, justifiant précisément son besoin, au haut fonctionnaire de défense et de sécurité dont il dépend. Ce dernier rend sa décision après consultation du secrétariat général de la défense et de la sécurité nationale.

3.1.4 Personnes physiques habilitées ès qualités

Compte tenu de leur statut constitutionnel, le chef de l'État, le Premier ministre et les membres du gouvernement sont habilités ès qualités à connaître d'informations et supports couverts par le secret de la défense nationale.

Il en va de même des personnes dont la loi détermine qu'elles sont habilitées ès qualités pour l'exercice de leurs fonctions ou l'accomplissement de leurs missions et dans ces seules limites. Sont uniquement concernés :

- les membres de la délégation parlementaire au renseignement⁶³ ;
- les membres de la formation spécialisée du Conseil d'État⁶⁴ ;
- les membres de la commission du secret de la défense nationale⁶⁵ ;
- les membres de la commission nationale de contrôle des techniques de renseignement⁶⁶.

En revanche, les personnes susceptibles de les assister dans l'exercice de leur fonction ou dans l'accomplissement de leur mission font l'objet d'une procédure d'habilitation conforme aux dispositions des parties 3.2 et 3.3.

3.2 DIFFERENTS TYPES DE PROCEDURE

La demande d'habilitation déclenche une procédure destinée à vérifier que le candidat à l'habilitation peut, sans risque pour la défense et la sécurité nationale ou pour sa propre sécurité, accéder à des informations et supports classifiés dans l'exercice de sa fonction ou l'accomplissement de sa mission.

3.2.1 Balance des risques dans le choix de la procédure

Plusieurs cas de figure peuvent justifier la mise en œuvre de procédures d'habilitation dérogatoires que sont les procédures simplifiée (cf. 3.2.3) et d'urgence (cf. 3.2.4). L'autorité qui sollicite l'habilitation doit avoir à l'esprit que ces procédures offrent des garanties de sécurité moindres que la procédure de droit commun. Il revient ainsi au responsable d'organisme sollicitant l'habilitation, par le biais de son officier de sécurité, de procéder systématiquement à une balance « coût-avantage » avant de solliciter l'enclenchement d'une procédure dérogatoire.

En tous les cas, le recours à la procédure simplifiée ou à la procédure d'urgence est prohibé pour l'habilitation des agents des services spécialisés de renseignement visés à l'article R. 811-1 du code de la sécurité intérieure, à l'exception de ceux nommés conformément à l'article 13 de la Constitution ou relevant du chapitre Ier du titre II du décret n° 2019-1594 du 31 décembre 2019 relatif aux emplois de direction de l'État. Par ailleurs, conformément aux règles propres à leur service, les agents des services de renseignement peuvent faire l'objet d'une procédure d'habilitation plus approfondie que celle décrite dans la présente instruction.

⁶³ IV de l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires.

⁶⁴ Article L. 773-2 du code de justice administrative.

⁶⁵ Article L. 2312-5 du code de la défense.

⁶⁶ Article L. 832-5 du code de la sécurité intérieure.

3.2.2 Procédure d'habilitation de droit commun

Cette procédure (cf. Annexe 5) concerne toutes les personnes appelées à occuper un poste pour lequel le besoin d'habilitation au niveau *Secret* ou *Très Secret*, y compris pour les classifications spéciales de ce dernier niveau, est avéré.

Une habilitation temporaire peut être délivrée à l'issue de cette procédure selon les conditions définies au paragraphe 3.4.1.1.

Une procédure d'habilitation en urgence peut être engagée selon les conditions détaillées au paragraphe 3.3.2.

3.2.3 Procédure simplifiée

Distincte de l'enquête réalisée par le service enquêteur dans le cadre de la procédure d'habilitation de droit commun, cette procédure, uniquement applicable aux demandes d'habilitation au niveau *Secret* et réservée aux seuls agents publics (fonctionnaires ou agents non-titulaires, civils ou militaires), permet de délivrer une décision d'habilitation sur le fondement d'une enquête administrative réalisée au moment du recrutement, de la nomination ou de l'affectation, conformément aux articles L. 114-1 et L. 114-2 du code de la sécurité intérieure (cf. Annexe 6), sous réserve, pour le candidat à l'habilitation, de remplir une notice individuelle de sécurité comportant une attestation sur l'honneur de l'exactitude des informations mentionnées.

La décision d'habilitation délivrée dans le cadre d'une procédure simplifiée est valide pour une durée limitée ne dépassant pas la durée maximale déterminée par l'instruction ministérielle du ministère dont relève la personne habilitée.

L'autorité ayant sollicité l'habilitation par procédure simplifiée peut, à tout moment, solliciter une enquête administrative auprès du service enquêteur compétent conformément au II de l'article L. 114-1 du code de la sécurité intérieure.

La procédure simplifiée n'est pas applicable aux agents des services spécialisés de renseignement visés à l'article R. 811-1 du code de la sécurité intérieure, à l'exception des agents nommés conformément à l'article 13 de la Constitution ou relevant du chapitre Ier du titre II du décret n° 2019-1594 du 31 décembre 2019 relatif aux emplois de direction de l'État.

3.2.4 Procédure d'urgence

Distincte de la procédure simplifiée, cette procédure exceptionnelle, applicable quel que soit le niveau de l'habilitation, *Secret* ou *Très Secret*, sollicitée, permet de délivrer une habilitation à une personne dans des délais très brefs selon les modalités détaillées au 3.3.2 afin que cette dernière puisse avoir accès à des informations et supports classifiés dès sa prise de fonction.

La procédure d'urgence s'applique aux seuls cas exceptionnels de personnes affectées dans des conditions ne permettant pas le respect des délais mentionnés au 3.3.1.3 c) et exerçant des fonctions exigeant un accès immédiat à des informations et supports classifiés.

La procédure d'urgence n'est pas applicable aux agents des services spécialisés de renseignement visés à l'article R. 811-1 du code de la sécurité intérieure, à l'exception des agents nommés conformément à l'article 13 de la Constitution ou relevant du chapitre Ier du titre II du décret n° 2019-1594 du 31 décembre 2019 relatif aux emplois de direction de l'État.

3.2.5 Habilitation des ressortissants étrangers

Les ressortissants étrangers⁶⁷ occupant une fonction ou accomplissant une mission nécessitant l'accès à des informations ou supports classifiés, dans la limite du strict besoin d'en connaître, peuvent être habilités au niveau *Secret* ou *Très Secret*, à la condition qu'il existe un accord de sécurité, général ou spécifique, entre la France et l'État dont l'intéressé est ressortissant.

Par dérogation au paragraphe précédent, lorsqu'il n'existe aucun accord de sécurité entre la France et l'État dont l'intéressé est ressortissant, à titre exceptionnel, si le besoin d'en connaître est avéré, le responsable de l'organisme dont il relève saisit, en motivant sa demande, *via* le haut fonctionnaire de défense et de sécurité compétent, le secrétaire général de la défense et de la sécurité nationale qui apprécie l'opportunité de l'habilitation et définit, le cas échéant, la procédure à suivre⁶⁸.

3.2.5.1 Attestation d'habilitation ou de sécurité dans le cadre d'une coopération étatique

Lorsque, dans le cadre d'une coopération étatique, un ressortissant d'un État étranger ou relevant d'un organisme de droit international public avec lequel la France a conclu un accord de sécurité, général ou spécifique applicable au cas d'espèce, est envoyé en mission ou détaché dans un organisme français, l'attestation d'habilitation ou le certificat de sécurité délivré(e) par l'autorité étrangère ou internationale compétente suffit à permettre la délivrance d'une décision d'habilitation au niveau requis conformément au tableau d'équivalence de l'accord de sécurité applicable, sans qu'il soit nécessaire de diligenter une enquête administrative au préalable.

3.2.5.2 Procédure d'habilitation hors coopération étatique

Lorsqu'un ressortissant étranger d'un État avec lequel la France a conclu un accord de sécurité général ou spécifique applicable au cas d'espèce, présente sa candidature à un emploi en France nécessitant l'accès à des informations et supports classifiés, la procédure d'habilitation est engagée par le responsable de l'organisme français concerné avec l'appui de son officier de sécurité, selon les modalités suivantes :

- le responsable d'organisme adresse la demande d'habilitation à l'autorité d'habilitation dont il dépend, après avoir vérifié que le dossier remplit toutes les exigences fixées au 3.3.1.1 ;
- l'autorité d'habilitation saisit le service enquêteur compétent selon les procédures habituelles détaillées à la partie 3.3 ;
- parallèlement, l'autorité d'habilitation saisit le secrétaire général de la défense et de la sécurité nationale, en sa qualité d'autorité nationale de sécurité. Cette saisine est transmise *via* le haut fonctionnaire de défense et de sécurité compétent quand l'autorité d'habilitation est distincte de celui-ci (cf. 3.3.1.2) ;
- le secrétaire général de la défense et de la sécurité nationale assure la liaison avec les autorités nationales de sécurité étrangères afin d'obtenir l'assurance qu'il n'existe aucune information défavorable sur l'intéressé de nature à constituer une vulnérabilité

⁶⁷ Conformément à l'article 22 du code civil : « *La personne qui a acquis la nationalité française jouit de tous les droits et est tenue à toutes les obligations attachées à la qualité de Français, à dater du jour de cette acquisition.* ». Tout binational, quelle que soit son autre nationalité, est considéré en France comme jouissant de la seule nationalité française.

⁶⁸ Article R. 2311-11 du code de la défense.

pour le secret de la défense nationale, sans pour autant que ces éléments soient liant pour la délivrance de la décision d'habilitation ;

- le secrétaire général de la défense et de la sécurité nationale transmet les éléments reçus de son homologue étranger au haut fonctionnaire de défense et de sécurité compétent, qui les retransmet à l'autorité d'habilitation lorsque l'autorité d'habilitation est distincte de celui-ci.

Dans le cas particulier où l'autorité d'habilitation est autorité de sécurité déléguée, et sous réserve des dispositions de l'accord de sécurité applicable, cette dernière peut saisir directement son homologue étranger. L'autorité de sécurité déléguée peut, en outre, au besoin, solliciter une démarche analogue du secrétaire général de la défense et de la sécurité nationale vers l'autorité nationale de sécurité étrangère.

La décision d'habilitation n'est prise par l'autorité française d'habilitation qu'à l'issue de cette procédure.

3.2.6 Habilitation des ressortissants français au profit d'une organisation internationale, d'une institution, d'un organisme ou d'un organe de l'Union européenne ou d'une personne morale de droit étranger

Les ressortissants français, occupant une fonction ou accomplissant une mission au sein d'une organisation internationale, d'une institution, d'un organisme ou d'un organe de l'Union européenne ou d'un organisme de droit étranger et nécessitant l'accès à des informations et supports classifiés étrangers peuvent être habilités au niveau requis selon les modalités ci-après détaillées.

3.2.6.1 Procédure d'habilitation pour les ressortissants français mis à disposition ou envoyés en mission dans le cadre d'une coopération étatique ou détachés par la France dans une organisation internationale, une institution, un organisme ou un organe de l'Union européenne

Lorsque, dans le cadre d'une coopération étatique, un ressortissant français est envoyé en mission ou détaché dans un organisme étranger ou relevant du droit international public, l'officier de sécurité de l'organisme français dont il ressort délivre, sur demande de l'autorité d'accueil, une attestation d'habilitation ou un certificat de sécurité conformément au tableau d'équivalence de l'accord de sécurité conclu entre la France, l'État partenaire ou l'organisation internationale, l'institution, l'organe ou l'organisme de l'Union européenne concerné.

Dans le cas où le ressortissant français ne dispose pas d'une habilitation en cours de validité, une demande d'habilitation est transmise par le responsable de l'organisme français dont le ressortissant français relève, selon les mêmes modalités que pour tout autre candidat à l'habilitation relevant de son organisme.

3.2.6.2 Procédures applicables aux ressortissants français candidats à un poste ou employés, sans lien avec l'État français, par un organisme étranger ou relevant du droit international public

Lorsqu'un ressortissant français candidate à un poste ou est employé, sans lien avec l'État français, par une personne morale de droit étranger, la procédure d'habilitation est engagée par l'autorité étrangère compétente.

L'autorité de sécurité étrangère compétente en vertu de l'accord de sécurité applicable ou des règles de sécurité de l'organisation internationale concernée saisit le secrétaire général de la défense et de la sécurité nationale, en sa qualité d'autorité nationale de sécurité ou, le cas échéant, l'autorité de sécurité déléguée compétente, afin d'obtenir l'assurance qu'il n'existe

aucune information défavorable sur l'intéressé de nature à constituer une vulnérabilité pour la protection du secret.

Le secrétaire général de la défense et de la sécurité nationale ou, le cas échéant, l'autorité de sécurité déléguée compétente, saisit le service enquêteur compétent pour vérifier si l'intéressé dispose d'un avis de sécurité en cours de validité ou procéder à l'enquête.

Dès le retour du service enquêteur, le secrétaire général de la défense et de la sécurité nationale, ou, le cas échéant, l'autorité de sécurité déléguée compétente, répond à l'autorité étrangère à l'origine de la demande conformément aux modalités définies dans l'accord de sécurité applicable ou par les règles de sécurité de l'organisation internationale concernée.

Indépendamment de la forme que prend la réponse française (acte préparatoire à la décision d'habilitation de l'autorité étrangère ou décision d'habilitation au profit de cette dernière), cette dernière peut, lorsqu'elle fait grief, faire l'objet de recours administratifs ou contentieux (cf. 3.4.2.2).

3.3 DEROULEMENT DES PROCEDURES D'HABILITATION

Sauf cas particulier, la procédure d'habilitation n'est engagée qu'au profit de la personne effectivement nommée dans l'emploi afin d'éviter toute surcharge inutile des services chargés d'en assurer la conduite. Elle doit toutefois être anticipée, sans attendre la prise effective de fonction, de façon à permettre à la personne de prendre connaissance d'informations et supports classifiés au plus tôt à sa prise de fonction. Ainsi, le dossier d'habilitation dûment constitué (cf. 3.3.1.1) doit être transmis à l'autorité d'habilitation compétente avant toute prise de poste.

S'agissant des personnes candidates à un poste au sein des services spécialisés de renseignement définis à l'article R. 811-1 du code de la sécurité intérieure, à l'exception des personnes nommées conformément à l'article 13 de la Constitution ou relevant du chapitre Ier du titre II du décret n° 2019-1594 du 31 décembre 2019 relatif aux emplois de direction de l'État, la procédure d'habilitation est conduite dès la phase de recrutement et doit être finalisée avant la prise de fonction dans le service concerné. Si cette procédure débouche sur un refus d'habilitation, conformément à l'article L. 114-1 du code de la sécurité intérieure, la personne candidate n'est pas recrutée.

Tout candidat à l'habilitation est informé par l'officier de sécurité, lors de sa demande, des obligations induites par l'habilitation ainsi que des dispositions relatives à sa responsabilité pénale en cas de compromission.

3.3.1 Procédures de droit commun

3.3.1.1 Constitution du dossier

Le dossier d'habilitation (cf. Annexe 7) a pour objet de réunir les éléments nécessaires à la conduite de l'enquête administrative⁶⁹. Il est constitué de :

- la demande d'habilitation formulée par l'autorité compétente attestant le besoin de connaître des informations et supports classifiés à un niveau donné, pour une personne nommément désignée à un poste donné ;
- la notice individuelle de sécurité, renseignée intégralement et signée par le candidat et vérifiée par l'officier de sécurité de l'organisme dont il relève.

⁶⁹ Le traitement de données à caractère personnel est notamment encadré par la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

L'officier de sécurité adresse le dossier d'habilitation à l'autorité d'habilitation et en conserve une copie datée et signée au plus tard jusqu'à un an après la durée de l'avis de sécurité en cours de validité. La transmission du dossier par voie électronique est privilégiée à condition que le système d'information employé garantisse l'identification et l'authentification de l'émetteur comme du destinataire, assure la confidentialité et l'intégrité des données et permette de tracer les actions effectuées. Dans le cas contraire, le dossier d'habilitation est établi en trois exemplaires (un original et deux photocopies, datées et revêtues de la signature originale du candidat) et accompagné de trois photographies d'identité originales, identiques et récentes.

3.3.1.2 Autorité d'habilitation

L'autorité d'habilitation est :

- le ministre pour les organismes relevant de son champ d'attribution (cf. 2.1.2.1) ou, par délégation, le haut fonctionnaire de défense et de sécurité, ainsi que toute autre personne désignée par arrêté⁷⁰ ;
- le secrétaire général de la défense et de la sécurité nationale :
 - par délégation du Premier ministre pour les demandes d'habilitation au niveau *Très Secret* faisant l'objet d'une classification spéciale ;
 - pour les personnes relevant des organismes entrant dans son champ de compétence au titre du décret n° 2012-383 du 20 mars 2012 relatif aux attributions du haut fonctionnaire de défense et de sécurité auprès du Premier ministre, à l'exception des agents du groupement interministériel de contrôle⁷¹ ;
- dans les limites des compétences définies par la décision de délégation mentionnée à l'article R. 2311-10-1 du code de la défense, l'autorité de sécurité déléguée pour les ressortissants français candidats à un poste ou employés, sans lien avec l'État français, par une personne morale de droit étranger ;
- les autorités endossant la fonction de haut fonctionnaire de défense et de sécurité selon les modalités décrites au 2.1.3.

L'autorité d'habilitation vérifie que le dossier d'habilitation est complet et le transmet au service enquêteur compétent afin qu'il diligente une enquête administrative. La transmission du dossier par voie électronique est privilégiée à condition que le système d'information employé soit conforme aux conditions détaillées au 3.3.1.1.

Le secrétaire général de la défense et de la sécurité nationale est également autorité d'habilitation des ressortissants français candidats à un poste ou employés, sans lien avec l'État français, par une personne morale de droit étranger sous réserve des compétences des autorités de sécurité déléguées.

3.3.1.3 Enquête administrative

a) Finalité de l'enquête administrative préalable à la décision d'habilitation

Cette 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

⁷⁰ Décret n° 2005-850 du 27 juillet 2005 relatif aux délégations de signature des membres du Gouvernement.

⁷¹ Décret du 20 décembre 2016 portant délégation de signature du Premier ministre au directeur du groupement interministériel de contrôle.

trouve exposé à un risque de chantage ou de pressions pouvant mettre en péril les intérêts de l'État, chantage ou pressions exercés notamment par un service étranger de renseignement, un groupe terroriste, une organisation ou une personne se livrant à des activités subversives.

b) Service enquêteur chargé de diligenter l'enquête administrative

Sont services enquêteurs :

- la direction du renseignement et de la sécurité de la défense (DRSD) pour le personnel civil ou militaire relevant du ministère de la défense⁷², le personnel militaire de la gendarmerie, les organismes relevant du champ d'attribution de ce ministère ainsi que leur personnel à l'exception de ceux travaillant au profit de la direction générale de la sécurité extérieure, les auditeurs de l'institut des hautes études de défense nationale ;
- la direction générale de la sécurité extérieure (DGSE) pour son personnel, les organismes travaillant à son profit et leur personnel ;
- la direction générale de la sécurité intérieure (DGSI) pour le personnel civil, y compris pour le personnel civil travaillant pour la gendarmerie, les organismes et leur personnel travaillant dans le domaine civil.

c) Durée et priorisation des enquêtes par les services enquêteurs

La durée de l'enquête administrative est en principe de trois mois pour un dossier d'habilitation au niveau *Secret* et six mois au niveau *Très Secret*, à compter de sa réception par le service chargé de la réaliser. Dans le cadre d'une procédure d'urgence (cf. 3.2.4 et 3.3.2), ce dernier peut délivrer, sur demande de l'autorité compétente, un avis de sécurité provisoire qui ne prolonge pas la durée de l'enquête. Cet avis de sécurité provisoire est valable jusqu'à réception de l'avis de sécurité définitif ou, au plus tard, six mois après sa date d'émission.

Les enquêtes administratives relatives aux agents des services spécialisés de renseignement mentionnés à l'article R. 811-1 du code de la sécurité intérieure sont diligentées en priorité.

d) Clôture de l'instruction et avis de sécurité

L'enquête administrative donne lieu à un avis de sécurité dans lequel le service chargé de la réaliser adresse ses conclusions à l'autorité d'habilitation.

Cet avis permet à l'autorité d'habilitation d'apprécier l'opportunité d'habiliter le candidat, au regard des éléments communiqués, des garanties qu'il présente et du niveau d'habilitation requis.

Les conclusions de l'avis de sécurité sont de trois types⁷³ :

- « avis sans objection » : l'instruction n'a révélé aucune vulnérabilité de nature à constituer un risque pour la sécurité des informations et supports classifiés ni pour celle de l'intéressé ;
- « avis restrictif » : le candidat présente certaines vulnérabilités constituant des risques directs ou indirects pour la sécurité des informations et supports classifiés auxquels il aurait accès, mais que des mesures de sécurité spécifiques prises par l'officier de

⁷² Les dossiers des personnels militaires qui ont fait l'objet d'un avis de sécurité émis par les services enquêteurs du ministère de la défense leur restent attachés, dans l'hypothèse d'une nouvelle enquête administrative, pendant un délai de cinq ans après la cessation de leurs fonctions.

⁷³ Chaque ministère peut décliner, dans l'instruction ministérielle, chacune de ces trois catégories pour l'adapter à ses besoins propres.

sécurité et, le cas échéant, une sensibilisation particulière du candidat, permettraient de maîtriser. Dans ce cas, le service ayant réalisé l'enquête recommande une procédure de mise en garde de l'employeur ou de mise en éveil de l'intéressé, ou qu'il soit recouru à ces deux procédures (cf. 3.4.1.2) ;

- « avis défavorable » : des informations précises font apparaître que le candidat présente des vulnérabilités faisant peser sur le secret de la défense nationale des risques tels qu'aucune mesure de sécurité ne permettrait de maîtriser.

L'avis de sécurité est émis pour un niveau donné d'habilitation. L'avis « sans objection » est valable pour le niveau pour lequel il a été requis et, le cas échéant, pour le niveau inférieur. Sa durée de validité ne dépasse pas celle de l'avis initial. Sauf précision contraire du service enquêteur, l'avis restrictif ou défavorable vaut pour le niveau d'habilitation concerné et le niveau inférieur.

Les avis restrictifs et défavorables sont assortis d'une fiche confidentielle classifiée indiquant les motifs de l'avis. Cette fiche distingue clairement :

- les éléments classifiés qui ne sont communiqués qu'à l'autorité d'habilitation et, de façon strictement nécessaire, dans le cas où :
 - une procédure de mise en garde est recommandée, aux autorités chargées de procéder à la mise en garde de l'autorité compétente ou de l'officier de sécurité dont relève le candidat à l'habilitation ainsi que, le cas échéant, à ladite autorité ou au dit officier de sécurité ;
 - une procédure de mise en éveil est recommandée, à l'autorité chargée de procéder à la mise en éveil du candidat selon les modalités définies par l'autorité d'habilitation, en liaison avec le service enquêteur conformément aux dispositions du paragraphe b).
- les éléments communicables, y compris au candidat.

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. L'autorité d'habilitation peut, en tant que de besoin, demander à nouveau communication des éléments qu'elle contient, en particulier, lorsqu'elle est chargée de mettre en garde l'autorité d'emploi, en cas de changement de comportement ou de situation de l'intéressé, à l'occasion de l'instruction d'une nouvelle demande d'habilitation le concernant ou pour l'instruction des recours gracieux ou contentieux dont la décision qu'elle a prise sur la base de l'avis de sécurité du service enquêteur peut faire l'objet.

La durée de validité de l'avis de sécurité dépend du niveau d'habilitation demandé. Elle ne peut excéder :

- sept ans pour le niveau *Secret* ;
- cinq ans pour le niveau *Très Secret*.

L'avis de sécurité constitue un acte préparatoire à la décision d'habilitation. Il 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 l'ensemble des éléments recueillis pendant l'instruction du dossier.

3.3.2 Procédure d'urgence

La procédure d'urgence est engagée dans les seuls cas prévus au 3.2.4. Le dossier d'habilitation est identique à celui prévu au 3.3.1.1. Il est constitué selon la procédure de droit commun, à la différence près que l'autorité compétente doit, dans la demande, préciser et motiver l'urgence de l'habilitation et l'impossibilité de procéder autrement. Pour les

classifications spéciales, seul le secrétaire général de la défense et de la sécurité nationale peut, en sa qualité d'autorité d'habilitation, engager une telle procédure au regard des éléments transmis par l'autorité d'emploi.

Dans les quinze jours ouvrables suivant sa saisine, le service enquêteur émet un avis de sécurité provisoire. La procédure de droit commun se poursuit après l'émission de l'avis de sécurité provisoire.

Au vu de ce dernier, l'autorité d'habilitation peut prendre une décision d'habilitation provisoire qui expire :

- soit lorsqu'à réception de l'avis de sécurité définitif, la décision d'habilitation ou de refus d'habilitation est prise ;
- soit au plus tard six mois après sa date d'émission.

3.4 DECISION D'HABILITATION OU DE REFUS D'HABILITATION

3.4.1 Typologie des décisions

3.4.1.1 Décision d'habilitation

La décision d'habilitation est l'autorisation donnée à une personne, sous réserve de son besoin d'en connaître, d'accéder à des informations et supports classifiés au niveau précisé dans la décision, ainsi qu'au niveau inférieur (cf. Annexe 8).

Elle est prononcée par l'autorité d'habilitation⁷⁴ au regard notamment des conclusions du service enquêteur, quel que soit le sens de l'avis de sécurité. L'autorité d'habilitation informe le service enquêteur de sa décision.

L'autorité d'habilitation peut également décider d'accorder une décision d'habilitation temporaire⁷⁵, à l'issue d'une procédure d'habilitation de droit commun (cf. 3.3.1) à un agent de l'État ou d'un de ses établissements publics lorsque l'intéressé fait l'objet d'une habilitation au niveau *Secret* pour lequel il est inscrit au catalogue des emplois et qu'il a besoin, de façon ponctuelle, d'accéder à des informations et supports classifiés au niveau *Très Secret*, hors classification spéciale. Cette décision, non renouvelable, est valable pour une durée maximale de trois mois, à l'exception des décisions délivrées aux militaires pour l'accomplissement de leur mission en opération intérieure ou extérieure, qui sont valables la durée de la projection.

L'autorité d'habilitation est tenue d'en informer le service enquêteur.

3.4.1.2 Décision d'habilitation assortie de mesures particulières

L'autorité d'habilitation peut décider, lorsque l'enquête a mis en évidence des éléments de vulnérabilité, d'accorder l'habilitation après avoir pris des précautions particulières. Les deux procédures sont éventuellement cumulables.

a) Procédure de mise en garde

L'autorité d'habilitation peut décider d'accorder l'habilitation à l'intéressé sous réserve de la mise en garde de l'autorité compétente ou de l'officier de sécurité de l'organisme ayant fait la demande d'habilitation dont relève le candidat à l'habilitation.

⁷⁴ Article R. 2311-8 du code de la défense.

⁷⁵ Une personne morale de droit privé ayant accès à des informations et supports classifiés dans le cadre d'un contrat ou d'une convention, et les personnes physiques travaillant pour son compte ne peuvent bénéficier d'une habilitation temporaire.

Cette procédure permet à ces derniers de mettre en œuvre des mesures de sécurité ou de prendre des précautions particulières à l'égard de l'intéressé, si besoin avec le conseil de l'autorité d'habilitation ou du service enquêteur.

A l'issue de l'entretien de mise en garde, une attestation (cf. Annexe 9) est signée par l'autorité compétente ou l'officier de sécurité dont relève l'intéressé et conservée par l'autorité d'habilitation. La décision d'habilitation n'est rendue qu'à l'issue de la procédure. L'autorité d'habilitation en informe le service enquêteur.

b) Procédure de mise en éveil

L'autorité d'habilitation peut décider d'accorder l'habilitation après une mise en éveil de l'intéressé, qui consiste à sensibiliser ce dernier sur les éléments communicables de vulnérabilité révélés par l'enquête⁷⁶.

L'autorité d'habilitation définit conjointement avec l'officier de sécurité de l'organisme ayant demandé l'habilitation les modalités de la mise en éveil. Elle consulte à cette fin le service enquêteur et peut solliciter sa présence lors de l'entretien avec l'intéressé. L'officier de sécurité étudie avec le service enquêteur les mesures de sécurité complémentaires à mettre en œuvre au regard de la situation lorsque cela s'avère justifié.

À l'issue de l'entretien de mise en éveil, une attestation (cf. Annexe 10) est signée par l'autorité d'habilitation ou son représentant, par l'officier de sécurité et par l'intéressé. Elle est conservée par l'autorité d'habilitation. La décision d'habilitation n'est prise qu'à l'issue de la procédure. L'autorité d'habilitation en informe le service enquêteur.

3.4.1.3 Décision de refus d'habilitation

La décision de refus d'habilitation est prononcée par l'autorité d'habilitation au regard notamment des conclusions du service enquêteur, quel que soit le sens de l'avis de sécurité.

3.4.2 Notification de la décision

L'officier de sécurité qui a fait la demande d'habilitation est informé par l'autorité d'habilitation de la décision prise par cette dernière. La décision ou, à défaut, le sens de la décision est communiqué à l'officier de sécurité. À réception, ce dernier notifie au candidat à l'habilitation la décision individuelle prise à son endroit, qu'elle soit favorable ou non.

3.4.2.1 Décision favorable

L'officier de sécurité notifie la décision d'habilitation à l'intéressé en le sensibilisant aux obligations particulières imposées par l'accès à des informations et supports classifiés, aux risques liés à la sécurité des systèmes d'information classifiés lorsque des droits d'accès à un tel système lui sont accordés ainsi qu'aux sanctions prévues par le code pénal en cas d'inobservation de la réglementation protégeant le secret de la défense nationale. L'intéressé signe le premier volet de l'engagement de responsabilité (cf. Annexe 11) par lequel il reconnaît avoir connaissance de ces obligations.

L'intéressé est également avisé de ce qu'il est tenu d'informer sans délai l'officier de sécurité, pendant toute la durée de son habilitation, de tout changement affectant sa vie personnelle (concubinage, pacte civil de solidarité, mariage, séparation, etc.), professionnelle ou géographique (lieu de domicile ou de résidence). Il lui est également signifié qu'il doit l'informer de toute relation suivie, dépassant le cadre professionnel, avec un ou plusieurs ressortissants étrangers et de le consigner dans une notice individuelle de sécurité transmise à l'autorité d'habilitation. De tels changements de situation peuvent justifier un réexamen du

⁷⁶ Il peut s'agir par exemple de ses attaches avec l'étranger ou de diverses particularités de son environnement.

dossier d'habilitation et, le cas échéant, la saisine ou l'auto-saisine du service enquêteur, qui émet un nouvel avis de sécurité.

3.4.2.2 Refus d'habilitation

La décision par laquelle l'autorité d'habilitation refuse d'habiliter une personne au titre de la protection du secret de la défense nationale (cf. Annexe 12), est notifiée à l'intéressé par l'officier de sécurité. Cette décision est dispensée de l'obligation de motivation⁷⁷.

Lors de cet entretien, l'officier de sécurité remet à l'intéressé la décision de refus d'habilitation ainsi qu'un récépissé de notification de décision de refus d'habilitation (cf. Annexe 13) qui comporte la mention des voies et délais de recours et dont un exemplaire, daté et signé par l'intéressé, est conservé par l'autorité d'habilitation. Le refus d'habilitation ou l'avis défavorable à l'habilitation d'un ressortissant français pour l'exercice d'une fonction ou l'accomplissement d'une mission au profit d'une personne morale de droit étranger suit le même formalisme (cf. 3.2.6.2).

3.4.3 Obligation de discrétion de la personne habilitée

Une personne titulaire d'une décision d'habilitation ne peut en faire état ni révéler son niveau d'habilitation sauf si la communication de ces informations est nécessaire à l'exercice de ses fonctions ou de l'accomplissement d'une mission à raison desquelles elle a été habilitée.

3.4.4 Portée de la décision en matière internationale

Toute décision d'habilitation émise au niveau national pour un ressortissant français peut, sous réserve du besoin d'en connaître, donner accès, de manière exceptionnelle, aux informations et supports classifiés du niveau correspondant et des niveaux inférieurs échangés dans un cadre international en application de l'accord de sécurité conclu entre les États membres de l'OTAN et des dispositions mises en place dans le cadre de l'Union européenne.

Un certificat de sécurité peut être émis par l'autorité d'habilitation.

3.5 CYCLE DE VIE DE LA DECISION D'HABILITATION

3.5.1 Durée de validité

La décision d'habilitation cesse de produire ses effets :

- soit à la fin de validité figurant sur la décision qui peut être au plus égale à celle de l'avis de sécurité (cf. 3.3.1.3 d) ;
- soit lorsque la fonction ou la mission l'ayant justifié disparaît, y compris si la date de fin de validité figurant sur la décision est postérieure.

Ainsi, la décision d'habilitation est implicitement abrogée au terme de la durée de validité de la décision ou lorsque la fonction ou la mission cesse, quand bien même la date de fin de validité inscrite sur la décision d'habilitation n'est pas échue.

3.5.2 Abrogation explicite d'une décision d'habilitation

Une décision d'habilitation peut être abrogée à tout moment ou ne pas être renouvelée si l'intéressé ne remplit plus les conditions nécessaires à sa délivrance.

L'abrogation fait l'objet d'une décision explicite, notifiée à l'intéressé selon les modalités prévues au 3.4.2.2. Lors de la notification, l'intéressé signe le second volet de l'engagement

⁷⁷ Article L. 211-2 du code des relations entre le public et l'administration.

de responsabilité (cf. Annexe 11). L'officier de sécurité met alors en œuvre les mesures du 3.5.8. L'autorité d'habilitation informe le service enquêteur de la décision d'abrogation.

3.5.3 Enquêtes administratives pendant la durée de l'habilitation

Afin de s'assurer que le comportement de la personne habilitée n'est pas devenu incompatible avec les exigences relatives à la protection du secret de la défense nationale, l'autorité d'habilitation peut, d'elle-même ou après signalement par l'officier de sécurité ou l'autorité d'emploi dont la personne habilitée relève, d'un changement de comportement ou de situation, diligenter une nouvelle enquête administrative conformément au II de l'article L. 114-1 du code de la sécurité intérieure.

Si des vulnérabilités sont apparues, l'autorité d'habilitation peut décider d'abroger la décision d'habilitation selon les modalités décrites au 3.5.2.

3.5.4 Conservation des décisions

Pendant leur durée de validité, les décisions d'habilitation sont conservées par l'officier de sécurité ou par l'autorité compétente désignée dans l'instruction ministérielle. Ces documents ne sont en aucun cas remis aux intéressés, ni reproduits.

3.5.5 Certificat de sécurité

Afin d'attester de son habilitation, il peut être remis à l'intéressé un certificat de sécurité (cf. Annexe 14) d'une durée de validité limitée à un an au maximum et pour une mission déterminée. Ce certificat de sécurité est délivré par l'autorité d'habilitation ou par l'officier de sécurité de l'organisme de l'intéressé.

L'intéressé procède ou fait procéder à sa destruction avant la fin de validité mentionnée sur le certificat.

3.5.6 Renouvellement

Afin d'éviter une interruption inopportune des conditions d'emploi, dans l'exercice de la fonction ou l'accomplissement de la mission du titulaire d'une décision d'habilitation lorsque la durée d'habilitation, qui ne peut excéder celle de l'avis de sécurité, est inférieure à celle de la fonction ou de la mission la justifiant, la validité de la décision initiale est tacitement prorogée d'une durée maximale de douze mois après la fin de validité de la décision initiale sous réserve qu'une demande de renouvellement, pour la même fonction ou la même mission, soit engagée dans un délai d'un an minimum et, au plus tard, trois mois avant la date d'expiration de l'habilitation en cours.

Cette demande de renouvellement s'accompagne d'un nouveau dossier de demande d'habilitation (cf. 3.3.1.1).

Si la procédure de renouvellement n'est pas engagée dans les délais impartis, aucune prorogation tacite n'est, en revanche, possible. Le titulaire doit quitter sans délai les fonctions ou cesser la mission ayant justifié son habilitation à expiration de la décision initiale.

3.5.7 Portabilité de l'avis de sécurité en cas de changement de fonction ou de mission nécessitant une nouvelle habilitation

En cas de changement de fonction ou de mission de la personne habilitée, l'habilitation détenue à ce titre devient caduque⁷⁸. Si l'intéressé exerce une nouvelle fonction ou accomplit

⁷⁸ À l'exception d'une décision d'habilitation couvrant expressément plusieurs postes, conformément à l'article R. 2311-8 du code de la défense.

une nouvelle mission pour laquelle une habilitation est requise, une nouvelle procédure est engagée.

Lorsque l'avis de sécurité ayant fondé l'habilitation précédente est toujours en cours de validité et qu'aucun changement de situation justifiant sa révision (cf. 3.5.3) n'est survenu, la nouvelle décision d'habilitation est délivrée sur la base de l'avis de sécurité en cours et n'excède pas la durée de validité de ce dernier.

Afin de garantir la portabilité de l'avis de sécurité en cas de changement d'autorité d'habilitation, l'officier de sécurité de l'organisme quitté ou l'autorité compétente renvoie la décision d'habilitation et l'engagement de responsabilité à l'autorité ayant décidé l'habilitation. La précédente autorité d'habilitation transmet à la nouvelle autorité d'habilitation une attestation d'avis de sécurité (cf. Annexe 15) assortie de sa durée de validité. Parallèlement, afin d'éclairer sa décision, la nouvelle autorité d'habilitation peut demander au service enquêteur que l'avis de sécurité lui soit renvoyé, ainsi que les motifs l'ayant justifié.

3.5.8 Cessation ou modification des droits associés à l'habilitation

Le service des ressources humaines collabore avec l'autorité d'emploi et l'officier de sécurité afin de gérer les aspects liés au départ ou au changement de fonction de la personne habilitée (sensibilisation, retrait des droits d'accès au site et aux systèmes d'information classifiés, etc.). En outre, l'officier de sécurité s'assure du retrait immédiat des différents droits d'accès. Il en informe l'officier de sécurité des systèmes d'information concernés qui veille au retrait des droits et moyens d'accès aux systèmes d'information classifiés.

Un inventaire des informations et supports classifiés dont l'intéressé a été le détenteur est établi dans les conditions énumérées à la partie 7.4.

Les obligations relatives à la protection des informations classifiées auxquelles il a pu être donné accès, perdurent au-delà du terme mis aux fonctions ou à l'habilitation de l'intéressé. Ce dernier en est informé lorsqu'il signe le second volet de l'engagement de responsabilité. Une fois signé, ce document est retourné à l'autorité d'habilitation.

3.6 FORMATION ET SENSIBILISATION DE LA PERSONNE HABILITEE

Lors de la notification de sa décision d'habilitation, la personne habilitée est sensibilisée aux enjeux de la protection du secret. À cette occasion, elle est informée qu'elle ne peut se prévaloir de sa décision d'habilitation en dehors de l'exercice de ses fonctions ou de l'accomplissement de sa mission (cf. 3.4.3).

La personne habilitée est formée de manière adaptée à ses fonctions, à la protection du secret, de façon à développer les compétences nécessaires pour traiter des informations et supports classifiés. Ces actions de formation sont renforcées pour les personnes ayant des responsabilités particulièrement sensibles au regard de la protection du secret⁷⁹.

La formation, organisée par l'officier de sécurité et l'officier de sécurité des systèmes d'information, porte notamment sur :

- les risques d'investigations ou d'approches par des individus ou des organisations étrangers ;

⁷⁹ Officier de sécurité, officier de sécurité des systèmes d'information, personnel servant dans les bureaux de protection du secret, personnes en charge de l'administration de la sécurité des systèmes d'information classifiés ou disposant de droits d'accès privilégiés à ces systèmes.

- les dispositions législatives et réglementaires en vigueur (code pénal, code de la défense, présente instruction, instruction ministérielle), ainsi que les accords et règles internationales applicables ;
- la politique de protection du secret, y compris celle des systèmes d'information de l'organisme ;
- les bonnes pratiques à mettre en œuvre dans l'environnement de travail et celles relatives à la sécurité informatique appliquées aux systèmes d'information⁸⁰ ;
- les mesures à prendre en cas de compromission, ainsi qu'en cas d'incident affectant la sécurité d'un système d'information.

Lorsque la personne habilitée est amenée à se rendre hors du territoire national, elle en avertit l'officier de sécurité qui, le cas échéant, peut organiser une action de sensibilisation spécifique avant son déplacement et éventuellement, à son retour.

L'officier de sécurité et l'officier de sécurité des systèmes d'information ou toute autre personne désignée par eux, dans leur domaine respectif de compétence, sont chargés de veiller à l'application de la présente instruction et, le cas échéant, de l'instruction ministérielle, ainsi qu'à la sensibilisation du personnel sur les nécessités de garantir la protection du secret.

⁸⁰ Conformément aux recommandations de l'ANSSI.

4 MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES

Toute personne morale peut être qualifiée pour accéder à des informations et supports couverts par le secret de la défense nationale si son besoin d'en connaître est reconnu par l'État.

Les exigences à remplir par la personne morale pour être alors considérée comme qualifiée au sens des articles 413-10 et suivants du code pénal varient selon la nature juridique de la personne morale considérée et selon les finalités justifiant cet accès.

Ces exigences sont détaillées au sein du présent chapitre et synthétisées en Annexe 16.

4.1 ÉTABLISSEMENTS PUBLICS DE L'ÉTAT

Tout établissement public sous tutelle de l'État peut accéder à des informations et supports classifiés sous réserve :

- de disposer d'un besoin d'en connaître reconnu par le ministre dont il relève ;
- du respect des mesures définies par la présente instruction, complétée de l'instruction ministérielle de son ministre de tutelle et, le cas échéant, des directives techniques particulières applicables à son secteur d'activité.

Le responsable de l'établissement est, en sa qualité de responsable d'organisme, responsable du respect des règles de la protection du secret en son sein et par son personnel (cf. 2.2.1), sous le contrôle de son ministre et, par délégation, du haut fonctionnaire de défense et de sécurité, de tutelle.

À ce titre, notamment, le responsable de l'établissement s'assure de l'aptitude de ses locaux à abriter des éléments couverts par le secret de la défense nationale au regard de la présente instruction, complétée de l'instruction ministérielle de son ministre de tutelle et, le cas échéant, des directives techniques particulières applicables à son secteur d'activité. En cas d'utilisation d'un système d'information, il s'assure, de la même façon, que ce système est apte à traiter et protéger les informations et supports classifiés qu'il héberge.

Lorsqu'un établissement public candidate à un appel d'offres ou un appel à projet international nécessitant l'accès à des informations et supports classifiés, il se conforme aux exigences de l'autorité contractante étrangère et suit, le cas échéant, la procédure décrite au 4.4.1.4 g).

4.2 OPERATEURS D'IMPORTANCE VITALE

Les opérateurs d'importance vitale⁸¹ ayant accès, en cette qualité, à des informations et supports classifiés n'ont pas à faire l'objet d'une habilitation « personne morale » mais se conforment aux dispositions de la présente instruction, complétée de l'instruction ministérielle du ministre coordonnateur dont ils relèvent, des directives techniques particulières, le cas échéant, applicables, ainsi qu'aux dispositions spécifiques détaillées dans le plan de sécurité d'opérateur et le plan particulier de protection⁸².

En dehors des activités liées à sa désignation en tant qu'opérateur d'importance vitale, un tel opérateur ne peut accéder au secret de la défense nationale sauf s'il est partie à une convention ou un contrat nécessitant l'accès au secret de la défense nationale, conformément aux dispositions des parties 4.3 et 4.4.

⁸¹ Articles L. 1332-1 et suivants du code de la défense.

⁸² Article R. 2311-9 du code de la défense.

Le délégué pour la défense et la sécurité, prévu par la réglementation relative à la sécurité des activités d'importance vitale, exerce la fonction d'officier de sécurité. Le cas échéant, cette fonction peut être exercée par son adjoint.

4.3 AUTRES PERSONNES MORALES ASSOCIEES A LA PROTECTION DES INTERETS FONDAMENTAUX DE LA NATION

La recrudescence de l'espionnage par les services de renseignements étrangers, les évolutions de la menace non-étatique et les tentatives accrues de captation du patrimoine scientifique et technologique de la Nation nécessitent d'associer pleinement les collectivités territoriales et les acteurs privés à la protection des intérêts fondamentaux de la Nation.

Lorsqu'il est justifié par cette association, fondée sur le volontariat de la collectivité territoriale ou de la personne morale de droit privé, l'accès à des informations ou supports classifiés est autorisé sous réserve d'être encadré par une convention précisant l'objet et l'objectif de cette association et comportant un plan contractuel de sécurité énumérant, conformément aux exigences décrites au paragraphe 4.4.2.3 a) et en Annexe 17, les engagements pris par la personne morale pour protéger ces informations et supports classifiés.

L'État peut décider de suspendre ou de mettre fin unilatéralement à la convention à tout moment. En cas de fin de la convention, les informations et supports classifiés transmis à la collectivité territoriale ou à la personne morale de droit privé sont restitués ou détruits conformément aux stipulations du plan contractuel de sécurité.

Lorsque la coopération le justifie, l'État peut exiger que l'exécution de la convention soit conditionnée à l'habilitation préalable de la personne morale selon les modalités décrites à la partie 4.4. Cette exigence est stipulée dans le plan contractuel de sécurité adossé à la convention.

Les conventions conclues au titre du présent paragraphe sont élaborées selon le modèle établi par le secrétaire général de la défense et de la sécurité nationale et conclues après avis favorable du haut fonctionnaire de défense et de sécurité dont l'autorité étatique contractante relève. Le haut fonctionnaire de défense et de sécurité en contrôle la mise en œuvre, adresse une copie de chaque convention signée au secrétaire général de la défense et de la sécurité nationale et en dresse le bilan qualitatif dans le compte rendu annuel sur la protection du secret (cf. 2.3.4).

4.4 MESURES APPLICABLES DANS LE CADRE D'UN CONTRAT DE LA COMMANDE PUBLIQUE, D'UN CONTRAT DE SOUS-TRAITANCE OU D'UN SOUS-CONTRAT A UN CONTRAT DE LA COMMANDE PUBLIQUE OU D'UN CONTRAT DE SUBVENTION

Les dispositions de la présente partie s'appliquent, selon les modalités définies ci-après, aux personnes morales (y compris les autoentrepreneurs), candidates ou parties à un contrat de la commande publique, à un contrat de sous-traitance, à un sous-contrat à un contrat de la commande publique, à un contrat de subvention, ci-après désigné sous le terme générique de « contrat », ou à un contrat exécuté au profit d'une entité étrangère impliquant l'accès du contractant à des informations et supports classifiés (cf. Annexe 18).

L'État doit pouvoir, y compris dans l'exercice de ses missions en matière de défense et de sécurité nationale, s'appuyer sur des compétences extérieures, en particulier dans les domaines technique, technologique, industriel ou pour l'optimisation des fonctions de soutien. Il doit alors être en mesure d'échanger en toute confiance avec ses cocontractants et leurs sous-traitants, y compris des informations et supports couverts par le secret de la défense nationale.

Ainsi, la procédure d'habilitation propre à la personne morale vise un double objectif :

- à travers les vérifications effectuées dans son cadre sur l'actionnariat de la personne morale, son équipe dirigeante, ses modes de financement, sa stratégie, ses relations contractuelles, elle permet à l'État de prendre des garanties sur la fiabilité de ses co-contractants et leur chaîne de sous-traitance, indépendamment de celle qu'offre la procédure d'habilitation du représentant légal de la personne morale et de ses seuls préposés susceptibles d'accéder à des informations et supports classifiés ;
- à travers les vérifications faites sur l'organisation de la chaîne de sécurité mise en place par la personne morale (cf. 4.4.1.2), elle permet de s'assurer que la personne morale dispose de la structure de sécurité nécessaire à la protection des informations et supports classifiés auxquels elle est susceptible d'avoir accès et d'engager pénalement son représentant légal en cas de défaillance de cette structure de sécurité.

L'habilitation de la personne morale impose des exigences plus ou moins étendues, selon qu'elle autorise :

- uniquement l'accès de la personne morale à des informations et supports classifiés, sans détention de ces informations et supports par la personne morale dans ses locaux ou au sein d'un système d'information qu'elle détient ;
- l'accès de la personne morale à des informations et supports classifiés avec détention physique de tout ou partie de ces informations et supports au sein d'au moins l'un de ses établissements ;
- la détention par la personne morale d'informations et supports classifiés au sein d'un système d'information qu'elle détient.

4.4.1 Avant signature du contrat

4.4.1.1 Obligation d'information par l'autorité publique contractante

a) Information relative à l'obligation d'habilitation

Le responsable légal est informé, dans la mesure du possible dès la pré-information et au plus tard dès l'avis d'appel public à la concurrence ou, à défaut de mise en concurrence, dès le début de la procédure de passation, de son obligation d'obtenir, pour lui-même et pour la personne morale qu'il représente, des habilitations de même niveau, préalablement à la signature du contrat, voire dès le dépôt de leur candidature⁸³.

L'autorité publique contractante l'informe des délais impartis pour fournir les éléments constitutifs des dossiers de demande d'habilitation. Elle lui adresse les formulaires nécessaires ou, à défaut, lui indique les modalités pour se les procurer ainsi que, le cas échéant, le service compétent pour traiter le dossier. Dans le cadre d'un contrat de sous-traitance ou d'un sous-contrat à un contrat de la commande publique impliquant également l'accès à des informations ou supports classifiés, le primo-contractant⁸⁴ est tenu à la même obligation d'information à l'égard de ses sous-traitants et sous-contractants.

⁸³ Conformément à l'article R. 2343-5 du code de la commande publique, l'autorité contractante peut en effet exiger des candidats qu'ils soient habilités au moment du dépôt de leur candidature, c'est-à-dire qu'ils soient en mesure de présenter une attestation d'habilitation et, dans le cadre d'un contrat impliquant la détention d'informations et supports classifiés, qu'ils produisent un avis technique d'aptitude physique délivré par le service enquêteur compétent justifiant de leur capacité à traiter, conserver et transmettre ces informations et supports classifiés au niveau de protection nécessaire.

⁸⁴ Primo-contractant : 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 ou sous-contractants.

b) Informations relatives à l'obligation de mise en conformité physique en cas de détention d'informations ou supports classifiés

Lorsque le contrat ou sa procédure de passation ou de conclusion impliquent la détention au sein d'un ou plusieurs établissements de la personne morale d'informations et supports classifiés, l'autorité publique contractante informe la personne morale des normes physiques que cette détention implique et dont la conformité aux exigences de la présente instruction est sanctionnée par l'obtention d'un avis d'aptitude physique délivré par le service enquêteur compétent.

c) Informations relatives à l'obligation d'homologation des systèmes d'information appelés à traiter des informations classifiées et aux procédures de sécurité à mettre en place pour la gestion des articles contrôlés de la sécurité des systèmes d'information

Si l'utilisation d'un système d'information classifié est requise pour l'exécution du contrat, voire dans le cadre de sa passation ou de sa conclusion, l'autorité publique contractante précise que ce système doit faire l'objet, préalablement à son emploi, d'une décision d'homologation⁸⁵ et que la mise en œuvre ou l'accès à des articles contrôlés de la sécurité des systèmes d'information (ACSSI) impliquent le respect des mesures de sécurité requises par la présente instruction.

4.4.1.2 Préfiguration de la chaîne de sécurité de la personne morale

Pour toutes les démarches engagées avant la signature du contrat, le représentant légal de la personne morale désigne, parmi son personnel, la personne qui exercera la fonction d'officier de sécurité (cf. Annexe 19) et, le cas échéant, celle qui exercera la fonction d'officier de sécurité des systèmes d'information, répondant aux exigences définies aux 2.2.2.1 et 2.2.3.2 pour être les correspondants de l'autorité publique contractante et de l'autorité d'habilitation.

4.4.1.3 Communication d'informations et supports classifiés en phase précontractuelle

Sauf si l'autorité publique contractante exige l'habilitation dès la candidature⁸⁶, lorsqu'en phase précontractuelle d'un contrat de la commande publique ou d'un contrat de subvention, l'accès à des informations et supports classifiés par les candidats admis est nécessaire, l'habilitation des personnes physiques employées par la personne morale candidate 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 engagée et que les lieux destinés à abriter les informations et supports classifiés soient aptes à les conserver conformément aux dispositions mentionnées au chapitre 5, à moins que l'autorité publique contractante ou le pouvoir adjudicateur lui permette de disposer d'un accès aux informations et supports classifiés dans ses propres locaux.

Le candidat désigne parmi son personnel, au plus tard lorsque sa candidature a été retenue pour établir une offre, les personnes qui accèderont aux informations et supports classifiés dans le strict besoin de l'élaboration de l'offre. Si les personnes désignées ne sont pas titulaires d'une habilitation ou si la décision d'habilitation les concernant n'est pas appropriée aux besoins du contrat, le candidat dépose simultanément une demande d'habilitation pour chacune d'elles. Cette demande est instruite en procédure d'urgence (cf. 3.3.2). La délivrance d'une décision d'habilitation provisoire des personnes qui accèderont aux informations et

⁸⁵ Article R. 2311-6-1 du code de la défense.

⁸⁶ Article R. 2343-5 du code de la commande publique.

supports classifiés dans le strict besoin de l'élaboration de l'offre ne préjuge pas de l'habilitation de la personne morale pour exécuter ledit contrat.

Le candidat dont l'offre n'est pas retenue détenant des informations et supports classifiés est tenu de les restituer à l'autorité contractante dès la notification du rejet de son offre et selon les modalités définies par l'autorité publique contractante. Il remet à l'autorité publique contractante une attestation par laquelle il certifie ne conserver aucune information ni support classifié. Dans le cas où des informations ou supports classifiés ont été transmis sous forme dématérialisée, il fournit une attestation précisant que les documents ont été effacés conformément aux dispositions de la présente instruction. Si les systèmes d'information classifiés et les articles contrôlés de la sécurité des systèmes d'information utilisés pour consulter les informations dématérialisées ne sont plus utilisés dans le cadre d'autres conventions ou contrats, ils sont détruits selon les dispositions de la présente instruction.

4.4.1.4 Procédure d'habilitation de la personne morale

À l'exception des établissements publics de l'État pour les contrats conclus avec une autorité publique contractante française, les personnes morales souhaitant conclure un contrat nécessitant pour son exécution l'accès à des informations et supports classifiés doivent être habilitées. La personne morale doit pouvoir justifier de son habilitation, ainsi que de celle de son responsable légal dès la candidature si l'autorité publique contractante l'exige⁸⁷ ou au plus tard au moment de la signature du contrat (cf. 4.4.1.4 d)).

a) Constitution du dossier d'habilitation

Afin d'enclencher la procédure d'habilitation, la personne morale constitue un dossier d'habilitation (cf. Annexe 20). Ce dossier comprend également les éléments nécessaires au lancement de la procédure d'habilitation de son responsable légal conformément à la procédure détaillée à la partie 3.3.

Si la personne morale a déjà fait l'objet d'une décision d'habilitation à l'occasion d'un précédent contrat, elle est tenue de présenter :

- une attestation d'avis de sécurité (cf. Annexe 21) produite par l'autorité d'habilitation mentionnant la fin de validité de l'avis de sécurité délivré par le service enquêteur compétent ou, dans le cas où l'autorité d'habilitation est identique à celle ayant délivré la précédente habilitation, une attestation d'habilitation (cf. Annexe 22) ;
- une attestation précisant qu'aucun changement dans la direction ou les statuts de la personne morale n'est intervenu depuis la délivrance de la précédente habilitation.

b) Envoi du dossier d'habilitation

Le dossier d'habilitation est transmis par l'officier de sécurité de la personne morale à l'autorité publique contractante.

Dans le cadre d'un contrat de sous-traitance ou de sous-contrat à un contrat de la commande publique ou à un contrat de subvention, le dossier constitué par le sous-traitant ou le sous-contractant est transmis soit par l'officier de sécurité du primo-contractant à l'autorité publique contractante, après vérification par ce dernier, de la complétude du dossier, soit directement à l'autorité publique contractante. Cette transmission est assortie d'une justification par le primo-contractant du besoin d'habilitation de son sous-traitant ou sous-contractant et d'une copie du plan contractuel de sécurité du contrat que le primo-contractant prévoit de conclure avec le sous-traitant ou le sous-contractant, afin que l'autorité publique

⁸⁷ Article R. 2343-5 du code de la commande publique.

contractante puisse apprécier sa conformité avec la réglementation applicable et le plan contractuel de sécurité du contrat principal.

L'envoi du dossier d'habilitation par voie dématérialisée est privilégié.

c) Instruction du dossier d'habilitation

L'autorité publique contractante vérifie la complétude des dossiers d'habilitation. Lorsque le dossier est incomplet, elle informe la personne morale des pièces manquantes et du délai imparti pour les fournir. À expiration de ce délai, la personne morale n'ayant pas fourni les documents nécessaires à la complétude de son dossier est réputée avoir renoncé au contrat.

Le dossier d'habilitation est ensuite vérifié :

- dans le cadre d'un contrat de la commande publique ou d'un appel à projet : par l'autorité publique contractante. Seuls les dossiers des candidats retenus sont ensuite transmis à l'autorité d'habilitation. L'autorité publique contractante informe l'autorité d'habilitation des candidats écartés aux différents stades de la compétition. Elle lui transmet le projet de plan contractuel de sécurité. Seuls les candidats retenus se voient délivrés une décision d'habilitation ;
- dans le cadre d'un contrat de sous-traitance ou d'un sous-contrat : par l'autorité d'habilitation du primo-contractant.

Après cette première phase d'instruction, l'autorité d'habilitation transmet les dossiers d'habilitation au service enquêteur compétent conformément au 3.3.1.3 b).

Le service enquêteur mène les investigations nécessaires sur chaque personne morale pour évaluer l'absence de vulnérabilité pour la défense et la sécurité nationale.

Le service enquêteur émet un avis de sécurité qui est ensuite transmis à l'autorité d'habilitation. Sauf changement dans la situation de fait ou de droit de la personne morale, la durée de validité de l'avis de sécurité émis est fixée conformément au 3.3.1.3 d).

Au regard du principe de reconnaissance des habilitations entre autorités d'habilitation (cf. 4.4.1.4 e)), l'avis de sécurité ainsi que tous les éléments relatifs à l'habilitation de la personne morale détenue par l'autorité d'habilitation précédente sont transmis à la nouvelle autorité d'habilitation. À cet effet, la personne morale fait état des habilitations en cours ou précédemment détenues par la personne morale, ainsi que des autorités d'habilitation correspondantes (cf. Annexe 20).

d) Délivrance de la décision d'habilitation

La décision d'habilitation de la personne morale est une décision explicite délivrée par l'autorité d'habilitation (cf. Annexe 23), notamment sur le fondement de l'avis de sécurité émis par le service enquêteur compétent. L'autorité d'habilitation n'est pas liée par cet avis, qui n'est qu'un des éléments parmi les actes préparatoires à sa décision.

La décision d'habilitation comporte une durée de validité fixée par l'autorité d'habilitation ainsi que, s'il y a lieu, un domaine de validité. Cette durée ne peut excéder la durée de validité de l'avis de sécurité émis conformément au 3.3.1.3 d).

Dans le cas où le service enquêteur n'a pas encore rendu son avis, en cas d'urgence justifiée et après saisine du service enquêteur, l'autorité d'habilitation, peut exceptionnellement prendre sa décision au vu d'autres éléments utiles en sa possession. L'habilitation ainsi délivrée est provisoire.

Tout changement de fait ou de droit dans la situation de la personne morale de droit privé intervenant après la décision doit être signalé à l'autorité d'habilitation afin de lui permettre, le cas échéant, de reconsidérer sa décision.

La décision de refus d'habilitation (cf. Annexe 24) est notifiée au représentant légal de la personne morale (cf. Annexe 25) dans les conditions prévues au 3.4.2.2.

Une décision de refus ne préjuge pas de la conclusion de conventions ou de contrats de toute nature n'impliquant pas la mise en œuvre de mesures de protection du secret de la défense et de la sécurité nationale ou impliquant l'accès au secret de la défense nationale pour un besoin autre que celui résultant du contrat pour lequel l'habilitation est refusée.

e) Principe de reconnaissance de la décision d'habilitation d'une personne morale

Dans le cas où une personne morale a déjà fait l'objet d'une habilitation à l'occasion d'une convention ou d'un contrat, cette habilitation demeure valable, pour toute autre convention ou contrat passé avec cette même personne morale par le ministère ou le service de l'État dont l'autorité d'habilitation relève, dans les limites de date et de domaine de validité de l'habilitation initiale et sauf changement dans la situation de fait ou de droit de la personne morale.

Dans le cas où une personne morale a déjà fait l'objet d'une habilitation à l'occasion d'une convention ou d'un contrat par une autorité d'habilitation relevant d'un autre ministère ou d'un autre service de l'État et lorsque l'avis de sécurité émis à cette occasion est toujours valide, sauf changement dans la situation de droit ou de fait de la personne morale, une nouvelle décision d'habilitation est prise sur la base de l'avis de sécurité en cours. Cette décision ne peut excéder ni la durée de validité ni le domaine d'application de l'avis de sécurité initial.

f) Cas particulier des personnes morales de droit étranger soumissionnant à un contrat de droit français nécessitant l'accès à des informations ou supports classifiés

Seule une personne morale établie sur le territoire d'un État avec lequel la France dispose d'un accord général ou spécifique de sécurité (cf. 7.2.1.3) peut être habilitée dans le cadre d'un contrat de droit français prévoyant l'accès à des informations ou supports classifiés.

La personne morale de droit étranger souhaitant conclure un tel contrat est alors tenue, à l'appui de sa candidature, de produire une attestation justifiant de son habilitation, délivrée par l'autorité compétente de l'État dont elle relève. Si la personne morale de droit étranger n'est pas habilitée, l'autorité française d'habilitation saisit le secrétaire général de la défense et de la sécurité nationale, en sa qualité d'autorité nationale de sécurité, ou, le cas échéant, l'autorité de sécurité déléguée compétente afin de solliciter de l'autorité compétente de l'État, sous la juridiction de laquelle la personne morale de droit étranger se trouve, qu'elle procède à son habilitation.

Aucune personne morale de droit étranger ne peut candidater ou présenter une offre lorsque l'exécution du contrat implique la détention au sein d'un établissement de la personne morale d'un système d'informations, d'informations ou supports portant la mention *Spécial France*.

g) Cas des personnes morales de droit français soumissionnant dans un cadre international

Lorsqu'une personne morale de droit français, non préalablement habilitée, candidate à un marché ou à un appel à projet au profit d'une autorité contractante de droit étranger, en vue d'un contrat nécessitant l'accès à des informations ou supports classifiés étrangers, elle adresse un dossier d'habilitation au secrétaire général de la défense et de la sécurité nationale, en sa qualité d'autorité nationale de sécurité ou, le cas échéant, à l'autorité de sécurité déléguée compétente.

Le secrétaire général de la défense et de la sécurité nationale ou, le cas échéant, l'autorité de sécurité déléguée, transmet le dossier d'habilitation au service du haut fonctionnaire de défense et de sécurité compétent au regard du domaine d'activité de la personne morale ou du

contrat considéré, en vue de la délivrance d'une décision d'habilitation conformément à la procédure décrite au sein de la présente partie. Lorsque la procédure d'habilitation permet la délivrance d'une décision d'habilitation, le haut fonctionnaire de défense et de sécurité adresse une attestation d'habilitation (cf. Annexe 22) à l'officier de sécurité de la personne morale candidate à l'habilitation, directement ou *via* le secrétaire général de la sécurité et de la défense nationale ou, le cas échéant, l'autorité de sécurité déléguée compétente. Dans tous les cas, une copie de la décision d'habilitation ou du refus d'habilitation est transmise au secrétaire général de la sécurité et de la défense nationale et, le cas échéant, à l'autorité de sécurité déléguée compétente.

Une personne morale déjà habilitée et disposant d'un avis de sécurité en cours de validité s'adresse à son autorité d'habilitation pour une extension éventuelle de son domaine d'habilitation. L'autorité d'habilitation adresse une attestation d'habilitation à l'officier de sécurité de la personne morale candidate, directement ou *via* le secrétaire général de la défense et de la sécurité nationale ou, le cas échéant, l'autorité de sécurité déléguée compétente. Dans tous les cas, une copie de l'attestation d'habilitation est transmise au secrétaire général de la défense et de la sécurité nationale et, le cas échéant, à l'autorité de sécurité déléguée compétente.

4.4.1.5 Lancement de la procédure d'aptitude physique

a) Cas où la personne morale ne dispose pas d'avis technique d'aptitude des locaux et des systèmes d'information contribuant à la sécurité des locaux

Lorsque le contrat implique la détention par la personne morale d'informations et supports classifiés, la personne morale dépose, parallèlement au dossier d'habilitation et le cas échéant d'homologation du ou des systèmes d'information classifiés qui ont vocation à être utilisés pour l'exécution du contrat, un dossier d'aptitude pour chacun des établissements situés sur le territoire français dans lesquels elle envisage de conserver des informations et supports classifiés. Ce dossier est destiné à évaluer l'aptitude desdits établissements à assurer la protection des éléments couverts par le secret de la défense nationale.

Un contrôle initial d'aptitude portant sur les mesures prises par la personne morale pour assurer la sécurité des informations et supports classifiés et, le cas échéant, du système d'information chargé du contrôle d'accès, est effectué par le service enquêteur dans le ou les établissement(s) concerné(s), préalablement à la signature de la convention ou du contrat.

À l'issue du contrôle initial, l'avis technique d'aptitude physique délivré par le service enquêteur est transmis à l'autorité publique contractante et à l'autorité d'habilitation et notifié à la personne morale :

- si l'avis est sans réserve : le responsable légal de la personne morale établit une attestation de conformité physique certifiant la conformité aux normes des locaux du ou des établissements concernés (cf. Annexe 26) ;
- si l'avis fait état de carences dans le dispositif de sécurité mis en œuvre au sein de la personne morale : son responsable légal s'engage à mettre en œuvre toutes les mesures nécessaires à la mise en conformité de son établissement et des systèmes d'information contribuant à la sécurité des locaux, dans un délai défini en liaison avec le service enquêteur et l'autorité publique contractante et compatible avec la date de début des prestations du contrat nécessitant la détention d'informations et de supports classifiés.

À l'issue des travaux de mise aux normes et, au plus tard, à la date d'échéance du délai défini en liaison avec le service enquêteur, le responsable légal de la personne morale transmet le certificat de mise aux normes de sécurité physique (cf. Annexe 27) à l'autorité publique

contractante et à l'autorité d'habilitation. Cette dernière en informe le service enquêteur et peut, en lien avec l'autorité publique contractante, le solliciter pour diligenter un contrôle.

b) Cas où un avis technique d'aptitude des locaux et des systèmes d'information contribuant à la sécurité des locaux est déjà en cours de validité

Si les locaux où seront abrités les informations et supports classifiés dans le cadre de la convention ou du contrat considéré disposent d'un avis technique d'aptitude physique en cours de validité et qu'aucun changement des conditions qui ont présidé à sa délivrance n'est intervenu, cet avis suffit. Le responsable d'organisme le communique alors à l'autorité publique contractante et à l'autorité d'habilitation, accompagné d'une attestation de non-changement des conditions qui ont présidé à sa délivrance.

Il en va de même pour le système d'information chargé du contrôle d'accès.

4.4.1.6 Lancement de la démarche d'homologation

Lorsque l'exécution de la convention ou du contrat prévoit l'utilisation d'un système d'information classifié, la personne morale engage parallèlement à la procédure d'habilitation et à la démarche d'aptitude physique, une démarche d'homologation conformément aux modalités précisées à la partie 6.1.

Si la personne morale dispose déjà d'un système d'information classifié homologué au niveau requis, la décision d'homologation demeure valide. La personne morale adresse alors une copie de la décision d'homologation à l'autorité publique contractante, ainsi qu'à l'autorité d'habilitation.

4.4.2 Exécution du contrat

4.4.2.1 Décisions administratives préalables au lancement de l'exécution des prestations du contrat nécessitant l'accès à des informations ou supports classifiés

a) Finalisation du dossier d'aptitude physique

Si les attestations d'aptitude physique ne sont pas parvenues dans le délai prédéfini ou si des carences sont constatées lors des contrôles effectués par le service enquêteur conformément au 4.4.1.5 a), une mise en demeure de se conformer aux prescriptions de la présente instruction est effectuée par l'autorité publique contractante⁸⁸. Le défaut d'exécution des travaux de mise en conformité fait obstacle à l'exécution du contrat et engage la responsabilité du représentant légal de la personne morale.

b) Finalisation de la démarche d'homologation des systèmes d'information classifiés

Dans le cas où la procédure d'homologation du système d'information classifié devant être utilisé pour l'exécution du contrat n'a pas été finalisée avant la signature du contrat, l'homologation du système doit intervenir au plus tard avant le début des prestations du contrat nécessitant son utilisation selon un calendrier établi en liaison avec l'autorité publique contractante.

L'autorité publique contractante peut, en parallèle de la démarche d'homologation ou de confirmation de l'existence d'une décision d'homologation en cours de validité, solliciter auprès du service enquêteur compétent, un contrôle d'aptitude visant à vérifier la capacité du système d'information à traiter des informations et supports classifiés au niveau requis

⁸⁸ Article R. 2311-9 du code de la défense.

conformément aux exigences de la présente instruction et de l'instruction interministérielle n° 300 sur les signaux parasites compromettants.

c) Habilitation des personnes physiques participant à l'exécution du contrat prévoyant l'accès à des informations ou supports classifiés

Sont seules autorisées à connaître des informations et supports classifiés pour le compte d'une personne morale habilitée les personnes rattachées à cette dernière qui ont fait l'objet d'une décision d'habilitation délivrée à l'issue de l'une des procédures d'habilitation définies à la partie 3.3.

Cette décision doit intervenir avant le début d'exécution par la personne physique considérée de ses missions nécessitant l'accès à des informations ou supports classifiés.

Afin d'éviter tout retard dans le lancement de l'exécution des prestations du contrat nécessitant l'accès à des informations ou supports classifiés, les procédures d'habilitation des personnes non encore habilitées sont lancées dès la signature du contrat, ou en amont de celle-ci, si la conclusion du contrat avec la personne morale considérée est certaine.

Sauf exception relative aux administrateurs et auditeurs des systèmes d'information classifiés et internes à la personne morale (cf. 3.2.2), le niveau et la durée de validité de cette habilitation ne peuvent excéder ceux de l'habilitation de la personne morale.

Un catalogue des emplois, tenu par l'officier de sécurité de la personne morale, est établi et mis à jour selon les modalités définies au 3.1.2.2, complétées le cas échéant des dispositions de l'instruction ministérielle, des directives techniques particulières applicables et des stipulations du plan contractuel de sécurité.

Ce catalogue des emplois tient lieu de répertoire des postes nécessitant l'accès à des informations ou supports classifiés. Il indique le niveau, les dates de délivrance et de fin de validité des décisions d'habilitation du personnel. Une mise à jour annuelle est réalisée et, à cette occasion, le représentant légal de la personne morale vérifie que les personnes habilitées ont effectivement eu accès à des informations et supports classifiés pour le niveau concerné et supprime, le cas échéant, les fonctions et missions ne nécessitant plus d'accéder au secret de la défense nationale.

Dès lors qu'une personne physique est susceptible, dans l'exécution de son contrat de travail, de connaître ou de détenir des informations et supports classifiés, son contrat de travail comporte, dans la mesure du possible, une clause de protection du secret de la défense nationale conforme à la clause-type figurant à l'Annexe 17. 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.

4.4.2.2 Obligations du titulaire

a) Devoir de discrétion de la personne morale habilitée

La personne morale et son personnel titulaire d'une décision d'habilitation ne peut publiquement en faire état ni s'en prévaloir. Elle ne peut communiquer à des tiers cette décision, ni aucune information résultant des informations et supports auxquels elle a accès pour l'exécution des prestations du contrat nécessitant l'accès à des informations et supports classifiés, sauf autorisation expresse de l'autorité publique contractante ou en réponse à des procédures contractuelles qui l'exigeraient.

b) Obligations du responsable légal

En sa qualité de responsable d'organisme (cf. 2.2.1), le responsable légal de la personne morale s'engage, sous sa responsabilité pénale et contractuelle et celle de la personne morale, à assurer la protection des informations et supports classifiés dont son organisme et son personnel ont à connaître, selon les dispositions réglementaires applicables (cf. Annexe 4) et le plan contractuel de sécurité qu'il a conclu avec l'autorité publique contractante.

À ce titre, il approuve la politique de sécurité des systèmes d'information et la politique de protection du secret de son organisme (cf. 2.3.1.3) et met en place la chaîne de sécurité détaillée à la partie 2.2.

c) Obligations spécifiques des primo-contractants

En cas de recours à des sous-traitants ou sous-contractants pour l'exécution de son contrat qui ont besoin, à cet effet, d'accéder à des informations et supports classifiés, le primo-contractant en informe l'autorité publique contractante au moment de la signature du contrat, sauf impossibilité caractérisée, et justifie leur besoin d'en connaître pour exécuter le contrat.

Lorsque l'autorité publique contractante reconnaît ou identifie le besoin du sous-traitant ou du sous-contractant d'accéder à des informations et supports classifiés, le primo-contractant informe le sous-traitant ou le sous-contractant pressenti.

Le sous-traitant ou le sous-contractant pressenti constitue alors un dossier de demande d'habilitation de la personne morale selon les modalités décrites au 4.4.1.4. Ce dossier est transmis à l'autorité d'habilitation selon les modalités définies au 4.4.1.4 b).

L'accès à des informations et supports classifiés par un sous-traitant ou un sous-contractant ne peut se faire que sous couvert d'un contrat comportant un plan contractuel de sécurité approuvé par l'autorité publique contractante de référence et sous réserve de l'habilitation préalable du sous-traitant ou du sous-contractant et de ses employés appelés à en connaître. Cet accès est strictement limité au besoin d'en connaître de sous-traitants ou sous-contractants, eu égard aux prestations définies par le sous-traité ou le sous-contrat.

Dans le cas où l'autorité publique contractante reconnaît ou identifie le besoin du sous-traitant ou du sous-contractant d'accéder à des informations et supports classifiés, le primo-contractant informe le sous-traitant ou le sous-contractant pressenti.

4.4.2.3 Mesures de sécurité liées à la détention d'informations et supports classifiés

Durant l'exécution du contrat, le titulaire est tenu de mettre en œuvre les mesures de sécurité requises pour assurer la protection des informations et supports classifiés. Ces mesures sont détaillées dans un plan contractuel de sécurité partie intégrante au contrat.

a) Plan contractuel de sécurité

Toute convention ou tout contrat nécessitant l'accès à des informations ou supports classifiés comporte un plan contractuel de sécurité qui énumère les exigences de sécurité relatives à la convention ou au contrat et détermine le besoin d'en connaître. Il stipule que des inspections, contrôles ou audits peuvent être organisés dans les établissements de la personne morale abritant des informations et supports classifiés aux fins de s'assurer de leur condition de protection.

Le plan contractuel de sécurité répond aux exigences mentionnées en Annexe 28. Celles-ci peuvent être adaptées par l'autorité publique contractante en liaison avec le titulaire sans pouvoir leur être contraires. Il doit mentionner, entre autres, la classification suivant le niveau retenu (*Secret*, *Très Secret*) et la nature (France, OTAN, UE, autres) des informations et supports classifiés.

Lorsque son contenu le justifie, le plan contractuel de sécurité est classifié en tout ou partie. Il peut être modifié en cours d'exécution de la convention ou du contrat à l'initiative de l'autorité publique contractante ou sur proposition de la personne morale.

L'autorité publique contractante valide le plan contractuel de sécurité des éventuels sous-traités et des sous-contrats au contrat principal.

Le plan contractuel de sécurité du primo-contrat intègre la liste des sous-traités et des sous-contrats concernés identifiés lors de la rédaction du plan contractuel de sécurité, les travaux réalisés, 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.

Le suivi des plans contractuels de sécurité des sous-traités ou des sous-contrats est effectué par le contractant principal sous la responsabilité et le contrôle de l'autorité publique contractante de référence. Les modalités de ce contrôle peuvent être définies dans des clauses particulières ou dans le plan contractuel de sécurité du contrat principal.

b) Inspections, contrôles et audits

Conformément aux stipulations du plan contractuel de sécurité, la personne morale se soumet à des inspections, contrôles et audits périodiques de l'autorité publique contractante ou du service enquêteur, tout au long de l'exécution du contrat et après son exécution si elle continue à détenir des informations et supports classifiés.

Des contrôles d'aptitude sont diligentés périodiquement dans ses locaux pour vérifier le respect de la protection du secret pour l'exécution de chaque convention et contrat.

Ces inspections, contrôles et audits incluent les systèmes d'information s'ils traitent d'informations classifiées ou s'ils contribuent à la sécurité des locaux abritant des éléments couverts par le secret de la défense nationale.

Lorsqu'une inspection, un contrôle ou un audit fait apparaître que les locaux ou les systèmes d'information de la personne morale ne sont plus conformes à la réglementation et aux normes fixées par le(s) plan(s) contractuel(s) de sécurité actif(s), le service enquêteur informe la personne morale, l'autorité publique contractante et le haut fonctionnaire de défense et de sécurité du ministère compétent de la non-conformité de ses locaux. Le responsable légal de la personne morale fait procéder à leur mise en conformité et prend toutes les mesures nécessaires pour assurer la sécurité des informations et supports classifiés pendant les travaux de réaménagement.

Après chaque mise en conformité, un contrôle donnant lieu à un nouvel avis d'aptitude des locaux concernés est effectué par le service enquêteur. Lorsqu'il apparaît que des informations et supports classifiés sont conservés dans des lieux qui ne sont pas de nature à garantir leur protection, le service enquêteur en informe l'autorité d'habilitation ainsi que l'autorité publique contractante. Cette dernière peut mettre en demeure la personne morale d'effectuer les travaux nécessaires à leur mise en sécurité dans un délai de trois mois à compter de la notification de la mise en demeure. À l'issue d'une mise en demeure infructueuse, l'autorité d'habilitation peut abroger la décision d'habilitation de la personne morale⁸⁹.

Tout refus de mise en conformité ou tout retard pour se mettre en conformité peut être considéré comme un non-respect des engagements conventionnels ou contractuels en matière

⁸⁹ Article R. 2311-9 du code de la défense.

de protection du secret et entraîner le prononcé des sanctions prévues par la convention ou le contrat, sans préjudice d'éventuelles sanctions pénales.

4.4.3 Résiliation et terme du contrat

4.4.3.1 Fin de l'habilitation de la personne morale

Si la décision d'habilitation arrive à expiration au cours de l'exécution d'un contrat visé par les présentes dispositions, une demande de renouvellement est déposée auprès de l'autorité d'habilitation dans l'année et, au plus tard, six mois avant cette date d'expiration. La durée de validité de la décision est alors prorogée dans les conditions définies au paragraphe 3.5.6.

L'habilitation peut être abrogée en cours de validité ou peut ne pas être renouvelée si la personne morale de droit privé ne remplit plus les conditions nécessaires à sa délivrance.

L'abrogation de la décision d'habilitation (cf. Annexe 24) est notifiée au représentant légal de la personne morale dans les mêmes formes que le refus d'habilitation (cf. 3.4.2.2).

L'abrogation de la décision d'habilitation n'entraîne pas nécessairement la résiliation du contrat, en particulier si l'accès aux informations et supports classifiés n'est plus nécessaire à son exécution. Les conséquences d'une telle décision doivent ainsi être examinées au cas par cas.

4.4.3.2 Mesures particulières en fin d'exécution du contrat

Lorsque les prestations du contrat nécessitant l'accès à des informations et supports classifiés ont été réalisées, la personne morale en informe dans le délai d'un mois l'autorité publique contractante qui lui précise la destination à donner aux informations et supports classifiés qu'elle détenait jusqu'alors. À cet effet, les modalités de destruction, d'archivage ou de restitution des informations et supports classifiés ainsi que celles portant sur le démantèlement des systèmes d'information classifiés sont définies par l'autorité publique contractante de référence en liaison avec les services concernés dans une fiche de clôture du plan contractuel de sécurité. Le plan contractuel de sécurité du contrat est clôturé sauf s'il a donné lieu à un ou plusieurs sous-traités ou sous-contrats. Dans ce cas, il ne peut être clôturé qu'après la clôture des plans contractuels de sécurité de chaque sous-contrat.

Si la personne morale conserve des informations et supports classifiés après la clôture du plan contractuel de sécurité, elle est tenue de :

- maintenir la chaîne fonctionnelle de protection du secret, complétée, le cas échéant, de la chaîne fonctionnelle de la sécurité des systèmes d'information ;
- disposer d'une décision d'habilitation pour elle-même, valide et cohérente avec les informations et supports classifiés conservés ;
- maintenir les habilitations de son personnel ayant le besoin d'en connaître ;
- entretenir les aptitudes physiques des locaux abritant des informations et supports classifiés ;
- tenir à jour les dossiers d'homologation des systèmes d'information classifiés et maintenir l'homologation de ces systèmes.

Un suivi de ces obligations est assuré par le service enquêteur compétent.

4.5 MESURES DE SECURITE APPLICABLES EN CAS DE CESSATION D'ACTIVITE OU DE DISSOLUTION DE LA PERSONNE MORALE

Le plan contractuel de sécurité précise les modalités de destruction, d'archivage ou de restitution des informations et supports classifiés détenus par la personne morale, en cas de cessation d'activité ou de dissolution de cette dernière.

5 SECURITE DES LIEUX

5.1 PRINCIPE DE DEFENSE EN PROFONDEUR ET ANALYSE DE RISQUES

La protection du secret de la défense nationale appelle la mise en place de mesures de sécurité plus ou moins élevées selon qu'il s'agit de :

- lieux dit « abritant », c'est-à-dire de lieux ayant vocation à conserver des informations et supports classifiés, quels qu'en soient le niveau et le volume⁹⁰ ;
- ou de lieux, telles que les salles de réunion, où des informations et supports classifiés sont communiqués, échangés ou manipulés mais où ces informations et supports n'ont pas vocation à être conservés.

Dans les deux cas, le système de protection déployé est destiné à protéger les informations et supports classifiés contre toute menace, interne ou externe, qui pourrait mettre en cause leur disponibilité, leur intégrité, leur confidentialité et leur traçabilité et à empêcher qu'une personne non qualifiée puisse y accéder. Il s'appuie sur une analyse de risques et s'inscrit dans une logique de défense en profondeur qui repose sur des barrières successives répondant aux critères suivants :

- être multifonctions, c'est-à-dire 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 homogènes, c'est-à-dire garantir la même efficacité en tous points, l'atteinte aux informations et supports classifiés se mesurant toujours dans la zone de moindre résistance et la valeur d'un système équivalant à celle de son élément le plus faible ;
- être dissuasives, c'est-à-dire contribuer à réduire le risque d'une tentative d'atteinte aux informations et supports classifiés ;
- être contrôlées, c'est-à-dire être testées fréquemment afin de vérifier qu'elles sont en état opérationnel ;
- être traçables, c'est-à-dire fournir tout moyen pouvant apporter un historique du fonctionnement des différents composants.

La sécurité des lieux résulte de l'articulation des différentes mesures de protection définies à l'Annexe 29. La sécurité des lieux abritant repose sur une articulation de l'ensemble de ces mesures, conforme au niveau de classification des informations et supports qu'ils conservent. Les lieux où des informations et supports classifiés sont communiqués ou manipulés sans y être conservés garantissent *a minima* le respect des règles relatives à la classe du bâtiment et/ou de l'emprise, ainsi qu'à la classe du local (cf. 2. a) et b) de l'Annexe 30). Il est à noter qu'un lieu où est installé ou conservé un système d'information classifié est considéré comme un lieu abritant⁹¹.

⁹⁰ Conformément à l'article 56-4 du code de procédure pénale, la liste des lieux visés abritant est établie de façon précise et limitative par arrêté du Premier ministre. Cet arrêté est actualisé chaque année (cf. 2.3.2.2).

⁹¹ Conformément à l'article 413-9 du code pénal, les réseaux informatiques et données informatisées qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès présentent un caractère de secret de la défense nationale. Il en découle que les lieux dans lesquels sont conservés ces réseaux informatiques et données informatisées sont des lieux abritant.

5.2 PROTECTION PHYSIQUE

5.2.1 Règles générales

Conformément au principe de défense en profondeur, la sécurité des informations et supports classifiés est assurée par un ensemble de mesures destinées à garantir l'intégrité des bâtiments, des lieux qui abritent les meubles dans lesquels ils sont conservés ou dans lesquels un système d'information classifié est déployé, ainsi que par la fiabilité des meubles dans lesquels ils sont conservés. Ces mesures ont pour objet d'éviter toute dégradation, compromission ou risque de compromission des informations et supports classifiés.

Le degré de sécurité physique à appliquer pour assurer la protection des lieux abritant dépend des niveaux de classification et, le cas échéant, de protection logique des informations et supports classifiés qu'ils abritent et des menaces auxquelles ils sont exposés.

Le dispositif global de protection et la solution technique retenue reposent sur les conclusions rendues par l'autorité compétente qui s'appuient sur l'évaluation des menaces et des contraintes inhérentes à l'environnement du site, ainsi que sur les méthodes de travail et de gestion des informations et supports classifiés concernés (par exemple, en fonction de la circulation de ces informations et supports dans le site et du nombre de personnes y ayant accès).

La sécurisation physique des accès d'énergie, des locaux techniques et des moyens de communication participe également de la protection physique des informations et supports classifiés.

Les informations et supports classifiés qui ne sont plus sous la surveillance de l'utilisateur font l'objet, selon les risques liés à leur environnement, de mesures de protection adaptées, déterminées par l'autorité compétente.

5.2.2 Dispositif global de protection

Le dispositif de protection physique des informations, supports et systèmes d'information classifiés est constitué de plusieurs barrières successives, que sont :

- l'emprise du bâtiment et/ou le bâtiment lui-même ;
- les locaux qui contiennent le meuble ou les éléments du système d'information ;
- le meuble dans lequel sont conservés les informations et supports classifiés ;
- et, pour les systèmes d'information, la sécurité logique à l'égard des utilisateurs du système et éventuellement, à l'égard des ressources du système d'information.

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. Les types de mesures de sécurité physique, leur articulation selon le type de barrière et les mesures spécifiques aux niveaux supérieurs de classification sont détaillés de l'Annexe 29 à l'Annexe 32.

Compte tenu de leur environnement particulier, les lieux dans lesquels sont conservés des informations et supports classifiés et, le cas échéant, des systèmes d'information classifiés, peuvent faire l'objet de dispositions de sécurité adaptées.

Sur un territoire étranger et compte tenu de leur environnement particulier, les organismes détenteurs d'informations et supports classifiés français relevant administrativement ou contractuellement de la juridiction de l'État français, doivent, sauf urgence ou contrainte majeure (opérationnelle, etc.), appliquer les mesures de protection décrites dans la présente instruction.

Lorsque les circonstances imposent la détention et la production d'informations et supports classifiés mais ne permettent pas la mise en place des moyens adéquats de sécurité physique, des mesures compensatoires sont prises afin de conserver le même niveau de protection. Ces mesures de substitution procèdent d'une analyse précise des risques, réalisée par le responsable du site concerné ou, le cas échéant, par le service enquêteur compétent. Elles sont évaluées par le service enquêteur compétent. Le service du haut fonctionnaire de défense et de sécurité est destinataire de l'analyse de risques et de l'avis du service enquêteur. Le niveau de protection doit, en toute hypothèse, être suffisant pour permettre la prise en compte du délai réel d'intervention avant la compromission.

5.3 CONTROLE D'ACCES

5.3.1 Contrôle physique des accès

Le contrôle d'accès s'intègre dans un système de management de la sûreté qui comprend aussi bien des moyens de détection que de surveillance. Il combine des moyens techniques, organisationnels et humains et a 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. L'accès à un local technique d'un système d'information classifié fait l'objet de mesures de protection physique supplémentaires ;
- d'empêcher ou de limiter les déplacements de personnes non autorisées.

Il peut s'appuyer sur la création de zones protégées et réservées.

5.3.1.1 Zones protégées

La création d'une zone protégée est conseillée pour les lieux abritant des informations et supports classifiés au niveau *Secret* et obligatoire au niveau *Très Secret*.

Une zone protégée est un local ou un terrain clos rattaché à une entreprise, un service, un établissement, public ou privé, intéressant la défense nationale, auquel l'accès est soumis à autorisation afin de protéger les installations, les matériels, le secret des recherches, des études ou des fabrications ou les informations et supports classifiés qui s'y trouvent⁹².

Elle est créée par arrêté ministériel selon les modalités définies aux articles R. 413-1 à R. 413-5 du code pénal et permet d'assurer aux lieux abritant des informations et supports protégés par le secret de la défense nationale une protection juridique renforcée, et notamment pénale, contre les intrusions, que ces lieux soient rattachés à un service de l'État, à un établissement public ou à toute personne physique ou morale, publique ou privée, intéressant la défense nationale.

L'ensemble des accès est contrôlé et tracé en permanence afin d'éviter toute pénétration intentionnelle ou fortuite dans la zone protégée. Le système d'information permettant de contrôler et tracer les accès en zone protégée, homologué par l'autorité d'emploi, met en œuvre des mécanismes d'authentification et d'intégrité garantissant l'accès à ce système par les seules personnes autorisées. À défaut d'un tel système, un registre physique répondant aux mêmes objectifs, accessible aux seules personnes ayant le besoin d'en connaître, est utilisé.

Les limites de la zone protégée et les mesures d'interdiction d'accès dont elle fait l'objet sont rendues apparentes afin de ne pas être franchies par inadvertance. À cet effet, des panneaux sont disposés en nombre suffisant aux endroits appropriés.

⁹² Articles 413-7 et R. 413-1 et suivants du code pénal.

Par principe, l'autorisation de pénétrer dans une 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. Lorsque la zone est instituée pour protéger des recherches, études ou fabrications qui doivent être tenues secrètes dans l'intérêt de la défense nationale, l'autorisation est délivrée uniquement par le ministre qui a déterminé le besoin de protection.

Conformément à l'article L. 114-1 du code de la sécurité intérieure, l'autorité chargée de prendre la décision peut diligenter une enquête administrative afin de s'assurer que le comportement de la personne, physique ou morale, n'est pas incompatible avec l'accès à cette zone ou ne l'est pas devenu. L'officier de sécurité du site saisit alors le service compétent d'une demande d'enquête administrative (cf. Annexe 6) avant d'autoriser l'accès à la zone protégée. Après instruction du dossier et sur la base des éléments qu'il a pu réunir, le service compétent émet un avis qu'il adresse au demandeur. Cet avis peut être favorable, défavorable ou réservé. La durée de validité de cet avis est laissée à l'appréciation de chaque ministre.

L'autorisation d'accéder à une zone protégée est délivrée par écrit et peut être retirée à tout moment dans les mêmes formes.

Sans préjudice des sanctions disciplinaires, toute personne non autorisée s'introduisant ou tentant de s'introduire dans une zone protégée encourt la peine prévue à l'article 413-7 du code pénal.

5.3.1.2 Zones réservées

La création d'une zone réservée, par définition incluse dans une zone protégée et pouvant même lui correspondre, vise à apporter une protection complémentaire. Elle est obligatoire pour les lieux abritant des informations et supports classifiés, y compris les systèmes d'information classifiés, au niveau *Très Secret*.

Les zones réservées sont créées par décision du responsable d'organisme. Chaque ministre veille à ce que des zones réservées soient créées dans tous les organismes qui, de manière habituelle, élaborent, traitent, reçoivent ou détiennent des informations et supports classifiés au niveau *Très Secret*.

Les mesures de sécurité propres aux zones réservées sont définies en Annexe 32.

Lorsqu'un organisme est amené à traiter ou détenir de tels informations et supports au niveau *Très Secret* pour des raisons opérationnelles et de manière temporaire, le responsable d'organisme crée une zone réservée temporaire soumise aux mesures de sécurité détaillées en Annexe 32, y compris lorsque les conditions de création d'une zone protégée ne sont pas réunies⁹³.

5.3.2 Accès des personnes non habilitées dans le cadre de l'exécution d'un contrat « sensible »

5.3.2.1 Mesures de sécurité relatives au contrat sensible

Un contrat « sensible » est un contrat, quel que soit son régime juridique ou sa dénomination, qui n'implique pas l'accès à des informations ou supports classifiés mais dont l'exécution nécessite l'accès à un lieu abritant des éléments couverts par le secret de la défense nationale.

⁹³ Dans le cas des moyens mobiles (aéronefs, navires, etc.) conservant des informations et supports classifiés au niveau *Très Secret*, lorsque les conditions de création d'une zone protégée ne sont pas réunies, une zone réservée peut exceptionnellement y être créée et faire l'objet de modalités spécifiques de sécurité définies dans l'instruction ministérielle

Il s'agit notamment des contrats de gardiennage, d'entretien ou de maintenance de lieux abritant des éléments couverts par le secret de la défense nationale.

Sauf si un accord de sécurité ou des règles de sécurité d'une organisation internationale, d'une institution, d'un organe ou d'un organisme de l'Union européenne impose, au cas d'espèce, des règles plus strictes, il n'y a pas lieu de procéder à l'habilitation de la personne morale ni à celle de son personnel. En revanche, l'autorité publique contractante ou le primo-contractant dans le cadre d'un contrat sensible en sous-traitance ou sous-contrat à un contrat classifié (cf. 4.4) ou sensible fait figurer au contrat les stipulations nécessaires pour garantir que ses conditions d'exécution ne portent pas atteinte au secret de la défense nationale. Ces stipulations prennent la forme d'une clause de protection du secret sur le modèle de clause-type présenté en Annexe 33, complétée ou adaptée, le cas échéant, selon les spécificités du contrat considéré, sans toutefois être contraire ou moins disante que le modèle.

5.3.2.2 Mesures de sécurité relatives à la personne morale exécutant un contrat sensible

En application des dispositions des articles L. 114-1 et R. 114-4 du code de la sécurité intérieure, l'autorité contractante peut solliciter du service compétent que soit diligentée une enquête administrative à l'encontre d'une personne morale, ainsi que de ses éventuels sous-contractants et leur personnel, sur la base des éléments fournis à l'occasion de la procédure de passation du marché ou lors de la demande d'acceptation du sous-contractant.

Le service compétent adresse son avis, consigné sur une fiche navette (cf. Annexe 34), à l'autorité contractante et au service du haut fonctionnaire de défense et de sécurité concerné.

Lorsque l'avis révèle un fait constituant un motif d'exclusion au sens des articles L. 2141-1 à L. 2141-5 de la commande publique, l'autorité publique contractante écarte la candidature de la personne morale concernée⁹⁴, sauf si des raisons impérieuses imposent le recours à la dite personne morale, que le marché en cause ne peut être confié qu'à ce seul opérateur économique et qu'un jugement définitif d'une juridiction d'un État membre de l'Union européenne n'exclut pas expressément l'opérateur concerné des marchés.

Lorsque l'avis révèle un fait pouvant constituer un motif d'exclusion au sens des articles L. 2141-7 à L. 2141-10 de la commande publique, l'autorité publique contractante peut écarter la candidature de la personne morale concernée selon les modalités prévues à l'article L. 2141-11 du même code.

5.3.2.3 Mesures de sécurité relatives au personnel de la personne morale exécutant un contrat sensible

En application des dispositions des articles L. 114-1 et R. 114-4 du code de la sécurité intérieure, le personnel de la personne morale chargé d'exécuter la prestation prévue par le contrat sensible peut préalablement faire l'objet d'une enquête administrative par le service compétent.

Il est recommandé d'insérer une clause de protection du secret (cf. Annexe 17, point 5) dans les contrats de travail des personnes exécutant un contrat sensible. Lorsqu'un salarié exécutant un contrat de travail ordinaire se trouve soumis aux conditions applicables aux contrats sensibles, un avenant conforme aux présentes dispositions peut être introduit dans son contrat de travail.

⁹⁴ Articles L. 2141-1 et suivants du code de la commande publique.

Les parties contractantes peuvent compléter ou adapter la clause du contrat de travail mentionnée précédemment selon les spécificités dudit contrat sensible sans jamais lui être contraires.

5.3.2.4 Accès des personnes non habilitées à des lieux abritant des éléments couverts par le secret de la défense nationale, dans le cadre de la législation du travail

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.

En matière de législation sociale, les personnes morales de droit privé liées par un contrat prévoyant l'accès à des informations et supports classifiés (cf. chapitre 4) doivent concilier l'impératif de protection du secret de la défense nationale avec la nécessité d'appliquer les règles propres au droit du travail⁹⁵ relatives aux contrôles et inspections (par exemple les médecins ou les inspecteurs du travail, les ingénieurs de prévention, les instances représentatives du personnel). Lorsque la personne morale de droit privé détient des éléments couverts par le secret de la défense nationale conformément aux dispositions précédentes, seule l'autorité responsable du site auquel le lieu abritant est rattaché, après contrôle de la qualité et vérification de l'identité des contrôleurs ou inspecteurs⁹⁶, les autorise à pénétrer dans les zones où sont abrités des informations et supports classifiés.

Bien que les contrôleurs ou inspecteurs s'engagent à ne rien révéler des secrets de fabrication ou procédés d'exploitation qui pourraient leur être révélés à cette occasion⁹⁷, sous peine d'encourir des poursuites sur le fondement de la violation du secret professionnel⁹⁸, ils ne sont nullement autorisés, sauf à être dûment habilités et à justifier du besoin d'en connaître pour l'exercice de leur fonction ou l'accomplissement de leur mission, à accéder ou à prendre connaissance d'informations et supports classifiés, cet accès restant subordonné au respect des règles énoncées par la présente instruction.

Si, dans des circonstances exceptionnelles, l'un d'eux accède fortuitement à un secret de la défense nationale, il s'expose, en cas de divulgation, aux peines prévues à l'article 413-11 du code pénal.

5.3.2.5 Exception en cas de secours, de sécurité ou d'incendie

Le personnel d'intervention en matière de secours, de sécurité ou d'incendie, agissant dans des cas d'urgence avérée, est autorisé 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.

5.3.3 Vérification de la protection physique par les services enquêteurs

5.3.3.1 Règles générales

Les lieux abritant des informations et supports classifiés font l'objet d'un avis technique d'aptitude physique à un niveau au moins égal au niveau de classification des informations et supports qu'ils ont vocation à abriter.

⁹⁵ Articles L. 8112-1, L. 8123-1, L. 8123-4 du code du travail.

⁹⁶ Articles L. 8114-1 et 2 du code du travail : le refus du responsable du site de se prêter à ces opérations constitue le délit d'entrave.

⁹⁷ Articles L. 8113-10, L. 8113-11, L. 8114-2 et L. 8123-5 du code du travail.

⁹⁸ Article 226-13 du code pénal.

Cet avis est délivré par le service enquêteur compétent.

a) Au niveau Secret

- pour les services de l'État : cet avis est facultatif ;
- pour les établissements publics de l'État, les opérateurs d'importance vitale dans le cadre de leur accès à des informations et supports classifiés en raison de leur désignation en tant qu'opérateur d'importance vitale, les personnes morales, publiques ou privées, dans le cadre d'une convention au titre de la partie 4.3 : cet avis n'est pas obligatoire avant la détention et intervient au plus tard à l'occasion d'un contrôle organisé par le haut fonctionnaire de défense et de sécurité conformément au 2.3.3 ;
- pour les personnes morales, publiques ou privées, liées par un contrat au sens de la partie 4.4, cet avis est obligatoire préalablement à la détention (cf. 4.4.1.1 b)).

b) Au niveau Très Secret

Cet avis est obligatoire, pour tout organisme, indépendamment de son statut juridique et de la finalité de détention, préalablement à la détention, sauf en cas d'impossibilité majeure.

5.3.3.2 Évaluation de la sécurité physique

Le service enquêteur s'assure de la cohérence de l'analyse de risques et des moyens mis en œuvre pour contrer une atteinte aux informations et supports classifiés, notamment que les mesures de protection physique des locaux et de protection logique des systèmes d'information chargés de la sûreté, qu'elles soient réglementaires ou compensatoires, permettent de détecter une intrusion suffisamment tôt et de la freiner le temps nécessaire à une intervention (cf. Annexe 30). Cette évaluation figure dans l'avis technique d'aptitude physique. En raison de la diversité des dispositifs de protection disponibles sur le marché et de l'évolution constante des techniques utilisées, le responsable d'organisme peut, en cas de besoin, consulter les services enquêteurs sur les normes que doivent respecter les matériels et les systèmes de protection qu'ils désirent mettre en place.

Lorsque les moyens techniques et, le cas échéant, logiques ne permettent pas de contrer une atteinte à la protection des informations et supports classifiés, le service enquêteur émet un avis technique d'inaptitude physique. Il peut également émettre un avis technique avec réserve si la mise aux normes est envisageable sous réserve de la réalisation de travaux de sécurité physique dans un délai défini en liaison avec l'officier de sécurité de l'organisme concerné.

L'avis technique d'aptitude physique précise le niveau de classification des informations et supports classifiés qui peuvent être traités et conservés dans le local.

En cas de changement affectant l'aptitude physique du lieu abritant pour lequel un avis technique d'aptitude physique a été délivré ou à l'occasion d'une inspection, d'un contrôle ou d'un audit réalisé par le service enquêteur ou par l'autorité administrative, une demande de réévaluation est formulée par l'officier de sécurité dans les plus brefs délais et avant l'échéance de l'avis, auprès du service enquêteur.

Les éléments de vulnérabilité décelés à l'occasion d'une évaluation technique sollicitée par l'officier de sécurité, lors d'une demande de renouvellement ou à l'occasion d'une inspection, d'un contrôle ou d'un audit peuvent entraîner une réévaluation des avis techniques précédemment émis par le service enquêteur.

5.4 SECURISATION DES SALLES, BUREAUX ET EQUIPEMENTS

5.4.1 Principe d'identification

Les informations et supports classifiés sont traités dans des locaux qui sont à l'abri des captations, réémissions ou enregistrements non autorisés de sons, d'images et d'informations.

Le niveau de classification des informations et supports qui peuvent être traités dans le local est indiqué à l'intérieur de celui-ci. Le contrôle du local est effectué de manière régulière sous la responsabilité de l'officier de sécurité.

5.4.2 Politique du bureau propre et de l'écran vide

En dehors des heures de travail ou lorsqu'une personne pénètre dans son espace de travail, tout détenteur d'information ou support classifié s'assure qu'aucune information ou support classifié n'est susceptible d'être accessible par une personne non qualifiée au sens de la présente instruction.

5.4.3 Organisation des réunions

La tenue d'une réunion de travail, d'une conférence, d'un exercice ou la présentation de matériels impliquant l'accès de ses participants à des informations et supports classifiés exige la mise en œuvre de mesures de sécurité. L'autorité organisatrice veille à la protection des informations et supports classifiés échangés au cours ou dans la suite d'une réunion de travail, d'une conférence, d'un exercice ou d'une présentation de matériels et s'assure notamment que :

- le local où se tient la réunion présente les garanties de sécurité prévues par la présente instruction complétées, le cas échéant, par l'instruction ministérielle, les directives techniques particulières et le plan contractuel de sécurité applicables ;
- les participants à la réunion sont habilités au niveau requis par la réunion et ont le besoin d'en connaître ;
- les informations et supports classifiés communiqués aux participants à l'issue de la réunion sont traités et gérés conformément à la réglementation applicable.

Les mesures de sécurité devant être mises en œuvre, avant, pendant et après la réunion, sont détaillées en Annexe 35.

5.5 PROTECTION CONTRE LES MENACES EXTERIEURES ET ENVIRONNEMENTALES

Selon le besoin en disponibilité des systèmes d'information classifiés et le résultat de l'analyse de risques, le responsable d'organisme détermine les mesures de protection physique contre les menaces extérieures et environnementales adéquates. Lorsque le site abrite des systèmes d'information classifiés, ces mesures figurent dans le dossier d'homologation (cf. 6.1.4).

Ces mesures concernent notamment les dispositifs contre les incendies, les dégâts des eaux, les risques liés à l'alimentation électrique et tout autre risque environnemental identifié.

6 SECURITE DES SYSTEMES D'INFORMATIONS CLASSIFIES

Comme pour les lieux abritant des éléments couverts par le secret de la défense nationale, les mesures de sécurité applicables aux systèmes d'information classifiés visent, conformément à l'article R. 2311-6-1 du code de la défense à prévenir toute menace, interne ou externe, qui pourrait mettre en cause la disponibilité, l'intégrité, la confidentialité et la traçabilité des informations et supports classifiés qu'ils contiennent, ainsi qu'à empêcher qu'une personne non autorisée puisse y accéder.

La sécurité d'un système d'information classifié repose avant tout sur une analyse de risques, à partir de laquelle un ensemble de mesures organisationnelles, physiques, logiques et environnementales sont mises en place. Une logique de défense en profondeur articulée autour de cinq axes en découle :

- prévenir : éviter la présence ou l'apparition de failles de sécurité ;
- bloquer : empêcher les attaques ;
- contenir : limiter les conséquences d'une attaque ;
- détecter : pouvoir identifier, en vue d'y réagir, les incidents et les attaques 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 attaque.

La sécurité d'un système d'information classifié repose sur deux grands types de barrières de sécurité : les mesures de sécurité physiques et environnementales et les mesures de sécurité logiques inhérentes au système lui-même.

L'ensemble de ces mesures sont prises en compte dans la démarche d'homologation préalable à la mise en service de tout système d'information classifié.

L'agence nationale de la sécurité des systèmes d'information tient à jour sur son site internet la liste des instructions et recommandations citées dans la présente instruction.

6.1 HOMOLOGATION DU SYSTEME D'INFORMATION CLASSIFIE

6.1.1 Démarche d'homologation

Conformément à l'article R. 2311-6-1 du code de la défense, tout système d'information classifié doit faire l'objet d'une décision d'homologation préalablement à son emploi.

La démarche d'homologation vise à s'assurer que l'ensemble des risques pesant sur le système a été identifié et a fait l'objet d'un traitement approprié afin de réduire la vraisemblance d'une attaque informatique, et en particulier, au titre de la protection du secret, d'une compromission des informations classifiées qu'il aura à traiter.

Cette démarche repose sur une analyse de risques globale et prend ainsi en compte tous les éléments, y compris environnementaux, indispensables au fonctionnement et à la sécurité du système. Le dossier d'homologation inclut ainsi les éléments fonctionnels, organisationnels et techniques mis en œuvre pour garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité des informations classifiées que le système d'information classifié est appelé à traiter, ainsi que le périmètre géographique et physique dans lequel le système est déployé.

La décision d'homologation, aboutissement de cette démarche, est une décision prise par l'autorité d'homologation. Elle atteste que les risques pesant sur la sécurité de ce système et sur les informations classifiées qu'il aura à traiter ont été identifiés et que les mesures nécessaires pour le protéger sont mises en œuvre. Le traitement d'informations dont le niveau

de classification est supérieur au niveau de classification prévu par la décision d'homologation du système d'information est interdit.

Le périmètre d'homologation d'un système d'information classifié inclut les éventuels supports amovibles mis à disposition par l'autorité d'emploi pour ce système d'information, que ceux-ci soient destinés à être utilisés exclusivement au sein du système d'information classifié (cf. 6.8.1) ou qu'ils soient destinés à réaliser des échanges avec d'autres systèmes d'information (cf. 6.8.2). Par la décision d'homologation, l'autorité d'homologation accepte les risques résiduels de sécurité, en pleine connaissance de cause.

En particulier, une grande attention est prêtée à :

- l'interconnexion avec d'autres systèmes ;
- l'usage de supports amovibles ;
- l'accès à distance par des utilisateurs en mobilité ;
- les moyens de visualisation et d'hébergement des informations classifiées ;
- les opérations de maintenance ou d'exploitation du système ou d'administration, en particulier lorsqu'elles sont effectuées par des prestataires externes.

6.1.2 Autorité d'homologation

L'autorité d'homologation est :

- le secrétaire général de la défense et de la sécurité nationale :
 - pour les systèmes d'information traitant d'informations classifiées au niveau *Très Secret* faisant l'objet d'une classification spéciale ;
 - pour les systèmes d'information amenés à traiter des informations classifiées de l'Union européenne ou de l'OTAN, ou toute autre autorité à laquelle il délègue cette responsabilité ;
 - pour les systèmes d'information classifiés utilisés par des organismes relevant de son périmètre au titre de l'article 2 du décret n° 2012-383 du 20 mars 2012 relatif aux attributions du haut fonctionnaire de défense et de sécurité auprès du Premier ministre.
- l'autorité qualifiée en sécurité des systèmes d'information ou la personne qu'elle désigne pour les systèmes d'information traitant d'informations classifiées au niveau *Secret* ou *Très Secret*, hors classifications spéciales.

Dans le cas où le système d'information classifié dépend de la responsabilité de plusieurs ministres, les autorités qualifiées en sécurité des systèmes d'information désignent une autorité d'homologation unique.

6.1.3 Commission d'homologation

L'autorité d'homologation met en place une commission d'homologation chargée de l'assister et de préparer la décision d'homologation. Cette commission comprend notamment des représentants de l'autorité d'emploi du système d'information, dont l'officier de sécurité des systèmes d'information et le responsable de la sécurité du système d'information, ainsi que des représentants du service du haut fonctionnaire de défense et de sécurité compétent. Des représentants du service enquêteur compétent peuvent être conviés à la commission et sont obligatoirement présents lorsque l'homologation est au profit d'une personne morale de droit privé. Dans le cadre de l'utilisation d'un système d'information classifié en exécution d'un contrat au sens de la partie 4.4, l'autorité contractante participe également à la commission.

En tant qu'autorité nationale en matière de sécurité des systèmes d'information, l'agence nationale de la sécurité des systèmes d'information peut participer à toute commission d'homologation d'un système d'information classifié. Afin de lui permettre d'apprécier la nécessité de sa participation, l'autorité d'homologation l'informe dans un délai raisonnable de la date de la commission et lui transmet, le cas échéant, les pièces nécessaires à l'instruction du dossier d'homologation. Les modalités de transmission des décisions et d'accès aux dossiers sont déterminées en accord avec le service du haut fonctionnaire de défense et de sécurité compétent.

L'agence nationale de la sécurité des systèmes d'information est membre de droit de la commission d'homologation lorsque le secrétaire général de la défense et de la sécurité nationale est autorité d'homologation.

6.1.4 Dossier d'homologation

Le dossier d'homologation est établi selon les recommandations de l'agence nationale de la sécurité des systèmes d'information. Le dossier d'homologation, initié dès la conception du système, est par la suite tenu à jour tout au long du cycle de vie du système d'information classifié.

La stratégie d'homologation précise, à partir de l'analyse de risques pesant sur le système d'information classifié et conformément à la politique de sécurité des systèmes d'information applicable, la constitution du dossier d'homologation.

La nécessité de verser au dossier d'homologation les documents listés ci-après est ainsi évaluée et justifiée au regard de l'analyse de risques et de la stratégie d'homologation. Si un document n'est pas versé au dossier d'homologation, la justification associée y figure.

Peuvent être versés au dossier d'homologation les documents suivants :

- la politique de sécurité du système d'information applicable ;
- les procédures d'exploitation sécurisée du système, y compris la documentation à destination des utilisateurs et des administrateurs ;
- les modalités de gestion des risques résiduels ;
- le plan d'amélioration continue de la sécurité ;
- les résultats des tests et des audits menés pour vérifier l'état de sécurité du système ;
- la documentation relative à la gestion des éléments cryptographiques mis en œuvre dans le système d'information ;
- la cartographie complète du système d'information qui comprend notamment la liste des équipements externes pouvant être connectés au système d'information (matériel de maintenance, d'audit, etc.) ;
- les schémas détaillés de l'architecture du système d'information ;
- les agréments des dispositifs de sécurité ;
- l'analyse de risques et les mesures de mitigation envisagées, lorsque, par dérogation, il est envisagé de recourir à des dispositifs de sécurité non agréés (cf. 6.5.2).

Une fois le système d'information classifié déployé, les documents relatifs aux lieux d'installation, et notamment les mesures de protection physique et les avis techniques d'aptitude physique, sont versés au dossier d'homologation.

Le dossier d'homologation est tenu à disposition :

- du service du haut fonctionnaire de défense et de sécurité ;

- de l'agence nationale de la sécurité des systèmes d'information.

6.1.5 Durée de la décision d'homologation

La décision d'homologation est prononcée pour une durée maximale :

- de trois ans pour un système d'information au niveau *Secret* ;
- de deux ans pour un système d'information au niveau *Très Secret*.

L'agence nationale de la sécurité des systèmes d'information est destinataire de toute décision d'homologation portant sur les systèmes d'information classifiés et peut demander le dossier d'homologation correspondant. Les modalités de transmission des décisions et d'accès aux dossiers sont déterminées en accord avec le service du haut fonctionnaire de défense et de sécurité de chaque ministère. Le service du haut fonctionnaire de défense et de sécurité et, le cas échéant, l'autorité contractante, sont également destinataires de la décision d'homologation. Le service enquêteur compétent est destinataire de la décision d'homologation prise au profit d'une personne morale de droit privé.

6.1.6 Contrôle et renouvellement de l'homologation

Conformément aux lignes directrices de l'autorité qualifiée en sécurité des systèmes d'information (cf. 2.2.3.1 b)), l'autorité d'homologation fixe les conditions du maintien de l'homologation de sécurité tout au long du cycle de vie du système d'information. Elle contrôle régulièrement que le système fonctionne effectivement selon les conditions qu'elle a approuvées.

L'autorité d'homologation procède au renouvellement de l'homologation avant le terme prévu. Elle s'assure de la complétude du dossier d'homologation et vérifie que les pièces nécessaires à son actualisation y figurent.

Une nouvelle décision d'homologation est nécessaire lorsque :

- les conditions d'emploi et d'exploitation du système ont été significativement modifiées ;
- de 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 significativement évolué ;
- de nouvelles vulnérabilités non corrigées ont été identifiées ;
- le système a fait l'objet d'un incident de sécurité significatif au regard de l'analyse de risques.

Si le système d'information classifié n'a pas connu de changements significatifs, une procédure simplifiée d'homologation est mise en œuvre.

6.1.7 Procédure dérogatoire en cas d'urgence opérationnelle

La décision d'homologation intervient avant la mise en service opérationnelle 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, l'autorité d'homologation délivre une autorisation provisoire d'emploi (APE) pour une durée courte et associée à un plan de mise en conformité.

6.2 HOMOLOGATION DES INTERCONNEXIONS D'UN SYSTEME D'INFORMATION CLASSIFIE

6.2.1 Interconnexion entre deux systèmes d'information classifiés de même niveau

Toute interconnexion entre systèmes d'information classifiés de même niveau doit être justifiée et faire l'objet d'une homologation spécifique à ce même niveau. L'ajout d'une interconnexion constitue, en effet, un changement structurel nécessitant une nouvelle homologation des systèmes d'information interconnectés.

L'autorité d'homologation est désignée après concertation entre les autorités d'homologation de chaque système d'information interconnecté.

L'autorité d'homologation est le secrétariat général de la sécurité et de la défense nationale, ou toute autorité à qui il en délègue la responsabilité, dans les cas suivants :

- pour les transferts d'informations entre des systèmes d'information classifiés de même niveau, dont l'un n'est pas sous maîtrise nationale ;
- pour les transferts d'informations entre des systèmes d'information classifiés de même niveau, dont l'un est amené à traiter des informations classifiées de l'Union européenne ou de l'OTAN ;
- lorsque l'utilisation de dispositifs de sécurité agréés est obligatoire mais impossible, notamment lorsqu'il n'existe pas de dispositif de sécurité agréé ou lorsqu'il n'est pas agréé au bon niveau.

L'interconnexion est obligatoirement réalisée à l'aide de dispositifs de sécurité agréés lorsqu'ils sont utilisés comme moyens essentiels de protection contre les accès non autorisés aux informations classifiées ou au système :

- pour les transferts d'informations entre des systèmes d'information classifiés de même niveau ou de niveaux équivalents, dont l'un n'est pas sous maîtrise nationale ;
- pour les transferts d'informations entre des systèmes d'information classifiés de même niveau ou de niveaux équivalents, dont l'un est amené à traiter des informations classifiées de l'Union européenne ou de l'OTAN.

Ces dispositifs de sécurité agréés sont déployés dans les conditions d'emploi associées aux décisions d'agrément pour cet usage.

6.2.2 Autres interconnexions

Les interconnexions entre systèmes d'information de niveaux de classification différents ou entre un système d'information classifié et un système d'information non-classifié sont par principe interdites.

Toute interconnexion de ce type dérogeant à l'interdiction de principe doit être justifiée par un besoin opérationnel strictement nécessaire. La justification est versée au dossier d'homologation.

Toute interconnexion d'un système d'information classifié avec un système d'information non classifié ou de niveau de classification différent est homologuée au niveau du système d'information le plus élevé. Cette interconnexion fait l'objet d'une homologation spécifique. L'ajout d'une interconnexion constitue un changement structurel nécessitant une nouvelle homologation des systèmes d'information interconnectés.

L'autorité d'homologation est par défaut l'autorité d'homologation du système d'information du niveau le plus élevé, mais elle peut être aussi désignée après concertation entre les autorités d'homologation de chaque système d'information interconnecté.

L'autorité d'homologation est le secrétariat général de la sécurité et de la défense nationale, ou toute autorité à laquelle il en délègue la responsabilité, dans les cas suivants :

- pour les transferts d'informations entre un système d'information classifié avec un système d'information non classifié ou de niveau de classification différent, dont l'un n'est pas sous maîtrise nationale ;
- pour les transferts d'informations entre un système d'information classifié avec un système d'information non classifié ou de niveau de classification différent, dont l'un est amené à traiter des informations classifiées de l'Union européenne ou de l'OTAN ;
- lorsque l'utilisation de dispositifs de sécurité agréés est obligatoire mais n'est pas possible, notamment lorsqu'il n'existe pas de dispositif de sécurité agréé ou lorsqu'il n'est pas agréé au bon niveau.

L'interconnexion est obligatoirement réalisée à l'aide de dispositifs de sécurité agréés lorsqu'ils sont utilisés comme moyens essentiels de protection contre les accès non-autorisés aux informations classifiées ou au système.

Ces dispositifs de sécurité agréés sont déployés dans les conditions d'emploi associées aux décisions d'agrément pour cet usage.

6.3 MESURES DE SECURITE APPLICABLES EN CAS DE SOUS-TRAITANCE DU DEVELOPPEMENT OU DE LA MAINTENANCE D'UN SYSTEME D'INFORMATION CLASSIFIE

Le développement ou le maintien en condition opérationnelle et de sécurité d'un système d'information classifié respecte les règles définies dans la présente instruction. Aucun sous-traitant ne peut accéder à un système d'information classifié s'il ne fait pas l'objet d'une décision d'habilitation (cf. partie 4.4).

Toute information spécifique liée au développement ou à la configuration d'un logiciel ou d'un système d'information classifié et dont la divulgation est susceptible de porter atteinte à la sécurité du système d'information classifié ou des informations classifiées qu'il contient est classifiée à un niveau équivalent ou supérieur à celui du système d'information classifié lui-même.

Lorsqu'ils sont considérés comme des documents administratifs au sens de l'article L. 300-2 du code des relations entre le public et l'administration, compte tenu du risque d'atteinte au secret de la défense nationale et à la sécurité des systèmes d'information susceptible de résulter de leur divulgation, les codes source et les éléments de configuration d'un système d'information classifié ne sont pas librement communicables et peuvent être classifiés en fonction de leur sensibilité.

Les besoins de protection du code source et des éléments de configuration d'un système d'information classifié sont définis dans le plan contractuel de sécurité du contrat correspondant.

6.4 MESURES DE SECURITE PHYSIQUES ET PRISE EN COMPTE DES SIGNAUX PARASITES COMPROMETTANTS

6.4.1 Lieu abritant le système d'information classifié

Comme tout lieu abritant des informations et supports classifiés, les lieux abritant des systèmes d'information classifiés doivent satisfaire aux règles énoncées au chapitre 5.

De surcroît, ils respectent la réglementation en matière de protection contre les signaux parasites compromettants, y compris en matière de câblage⁹⁹.

6.4.2 Matériel classifié laissé sans surveillance par son détenteur

La démarche d'homologation tient compte des risques liés à la protection physique des matériels classifiés, y compris lorsque des matériels classifiés peuvent être laissés sans surveillance par leur détenteur. À cette fin, différentes mesures de défense en profondeur sont combinées conformément aux dispositions de l'Annexe 30. Des mesures spécifiques sont également prises pour protéger l'accès aux éléments physiques des systèmes d'information classifiés hors équipements de mobilité. Le cas échéant, l'homologation du système d'information classifié prévoit des mesures de protection adaptées.

L'autorité d'emploi du système d'information met à disposition les moyens prescrits par l'officier de sécurité ou permet leur mise en œuvre.

6.5 MESURES DE SECURITE INHERENTES AU SYSTEME D'INFORMATION CLASSIFIE

Tout équipement constitutif d'un système d'information classifié est équipé de moyens de protection et doté d'une configuration durcie.

6.5.1 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 proposés par le responsable de la sécurité des systèmes d'information peuvent être développés pour un usage général ou pour un système particulier. Ils mettent en œuvre différents types de fonctions et de mécanismes de sécurité, comme :

- des fonctions cryptographiques permettant la protection en confidentialité ou en intégrité, l'authentification ou la signature des informations stockées sur des supports ou transmises sur des réseaux ;
- des fonctions ou des mécanismes destinés à protéger le dispositif lui-même, comme le contrôle, 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.

⁹⁹ Instruction interministérielle n° 300/SGDSN/ANSSI du 23 juin 2014 relative à la protection contre les signaux parasites compromettants.

6.5.2 Recours à des dispositifs de sécurité agréés

Un dispositif de sécurité mis en place dans un système d'information qui traite d'informations classifiées est agréé par l'agence nationale de la sécurité des systèmes d'information¹⁰⁰ 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.

À titre exceptionnel, et sur le fondement d'une analyse de risques réalisée par le responsable de la sécurité du système d'information dans le cadre de l'homologation, l'autorité d'homologation peut autoriser le recours à des matériels et logiciels agréés à un niveau inférieur, voire non agréés lorsqu'il n'existe pas de dispositif de sécurité agréé au bon niveau. La justification de cette autorisation est motivée dans le dossier d'homologation du système.

6.6 CONCEPTION ET EXPLOITATION DU SYSTEME D'INFORMATION

6.6.1 Administration des systèmes d'information classifiés

Les actions d'administration permettent de maintenir le système d'information classifié en condition de sécurité et en condition opérationnelle. Qu'il s'agisse d'actions liées à des évolutions du système d'information ou à l'exploitation courante, celles-ci nécessitent des privilèges. Elles constituent à ce titre une activité critique.

De manière générale, les principes suivants doivent être appliqués :

- les actions d'administration sont menées par du personnel spécialement formé et sensibilisé ;
- le système d'information d'administration est classifié au même niveau que le système d'information administré ;
- l'administration d'un système d'information classifié au niveau *Secret* est faite dans une zone protégée et au niveau *Très Secret* dans une zone réservée.

Les pratiques d'administration, en particulier pour la gestion des comptes privilégiés et la protection de leurs mécanismes d'authentification, sont établies suivant les recommandations de l'agence nationale de la sécurité des systèmes d'information. Toute non-conformité est justifiée et intégrée dans les risques résiduels présentés lors de la commission d'homologation après avoir été notifiée à l'autorité qualifiée en sécurité des systèmes d'information et au service du haut fonctionnaire de défense et de sécurité compétents. Au niveau *Très Secret*, les non-conformités sont également déclarées à l'agence nationale de la sécurité des systèmes d'information, au plus tard lors de la commission d'homologation.

L'autorité d'emploi d'un système d'information classifié applique les règles suivantes au système d'information d'administration et aux flux correspondants :

- les ressources matérielles, les ressources logicielles et les informations d'authentification sont strictement séparées selon leur usage. Ainsi, toute action d'administration est réalisée exclusivement par un administrateur depuis un compte administrateur individuel et dédié à cet usage. En outre, les actions d'administration sont conduites depuis des ressources d'administration dédiées (postes de travail, serveurs, ou autres équipements spécifiques). Les ressources d'administration, matérielles et logicielles, en particulier les postes d'administration, sont utilisées exclusivement pour les actions d'administration. Ces ressources sont gérées et

¹⁰⁰ Article 3 du décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».

configurées par l'autorité responsable de l'administration du système d'information classifié ou par le prestataire qu'elle a mandaté pour réaliser les actions d'administration ;

- les flux d'administration sont cloisonnés à l'égard des flux métier au niveau des ressources administrées. Les ressources d'administration accèdent aux ressources administrées au moyen d'une interface réseau dédiée à l'administration. Cette interface est physique ou, à défaut, logique. L'interface réseau utilisée pour les actions d'administration n'est accessible qu'aux seules ressources d'administration. En l'absence de mesure d'isolation physique de cette interface, un filtrage logique assure cette restriction d'accès. Quand des raisons techniques ou opérationnelles ne permettent pas l'administration des ressources administrées par des interfaces réseau dédiées, les actions d'administration sont faites par l'unique interface réseau de la ressource administrée. Ce cas de figure est justifié dans le dossier d'homologation ;
- les flux réseau entre les ressources administrées et les ressources d'administration sont filtrés. Afin de réduire le risque de compromission des ressources d'administration depuis les ressources administrées, les ressources d'administration sont déployées sur un réseau dédié à cet usage. Ce réseau portant les ressources d'administration est un réseau physiquement cloisonné de préférence ou, à défaut, un réseau logiquement cloisonné à l'aide de mécanismes de chiffrement et d'authentification réseau. Un filtrage strict des flux réseau entre les ressources administrées et les ressources d'administration est mis en place. Pour minimiser les possibilités de rebonds entre ressources administrées en cas de compromission de l'une d'entre-elles, un mécanisme de filtrage restreint les possibilités de communication sur ce réseau d'administration.

6.6.2 Maîtrise des logiciels en exploitation

L'autorité d'emploi du système d'information installe, sur un système d'information classifié, les seuls services et fonctionnalités qui sont indispensables au fonctionnement ou à la sécurité du système d'information. Le responsable de la sécurité des systèmes d'information s'assure que les services et les fonctionnalités qui ne sont pas indispensables, notamment ceux installés par défaut, sont désactivés et les fait désinstaller si cela est possible. Lorsque la désinstallation n'est pas possible, cela est mentionné dans le dossier d'homologation du système d'information classifié en précisant les services et fonctionnalités concernés, ainsi que les mesures de réduction du risque mises en œuvre.

L'autorité d'emploi du système prévoit des dispositifs pour empêcher l'installation de services et fonctionnalités hors de ces procédures. En cas d'impossibilité, il y est fait mention dans le dossier d'homologation.

6.6.3 Contrôle d'accès aux systèmes d'information classifiés

6.6.3.1 Gestion des droits d'accès sur la base du principe du moindre privilège, corolaire du respect du besoin d'en connaître

Par principe, toute personne habilitée accédant à des informations ou support classifiés depuis un système d'information classifié utilise, à cette fin, un compte utilisateur individuel assorti des droits d'accès correspondant à son profil et à son besoin d'en connaître. Ce compte ne dispose pas de droits d'administration sur le système d'information classifié. Ainsi, l'administrateur d'un système d'information classifié et l'administrateur de sécurité disposent de comptes individuels dédiés pour chacune de ces fonctions, distincts de leur compte utilisateur.

Par défaut, un administrateur est habilité au niveau d'habilitation correspondant au moins au niveau de classification du système d'information classifié administré. Lorsque les droits qui

lui sont octroyés sur le système d'information classifié sont étendus, lui permettant notamment d'outrepasser ses droits ou de masquer ses actions sur le système d'information classifié, l'administrateur doit être habilité au niveau *Très Secret*, sans incidence sur le niveau d'habilitation de la personne morale.

À titre dérogatoire, lorsque des raisons techniques ou opérationnelles ne permettent pas de créer de compte individuel, ni de restreindre les droits d'administration aux seules personnes autorisées, cela est justifié dans le dossier d'homologation et l'autorité qualifiée en sécurité des systèmes d'information et le service du haut fonctionnaire de défense et de sécurité compétents en sont informés. Le responsable de la sécurité du système d'information met alors en place les mesures nécessaires pour réduire le risque lié à l'utilisation de comptes partagés et assurer la traçabilité et l'imputabilité de l'utilisation de ces comptes. Ces mesures et les raisons justifiant le recours à des comptes partagés sont décrites dans le dossier d'homologation du système d'information classifié concerné.

Seule l'agence nationale de la sécurité des systèmes d'information peut autoriser cette dérogation pour les systèmes d'information classifiés au niveau *Très Secret*. L'autorité d'homologation sollicite son autorisation dès la phase de conception du système d'information classifié.

Les utilisateurs d'un système d'information classifié ont uniquement accès aux données, systèmes et services auxquels ils sont autorisés à accéder au regard de leur niveau d'habilitation et de leur besoin d'en connaître. Les éléments constitutifs du système d'information s'authentifient, dans la mesure du possible, auprès des réseaux et des services. Le principe de moindre privilège est pris en compte dans la mesure du possible.

La procédure relative au retrait des droits d'accès (cf. 3.5.8) est validée par l'autorité d'emploi du système. Elle est précisée dans la politique de sécurité du système d'information considéré (cf. 2.3.1.2 et 2.3.1.3).

a) Maîtrise de la gestion des accès des utilisateurs

L'autorité d'emploi du système d'information classifié met en place une politique de gestion des éléments d'authentification liés aux comptes utilisateurs et administrateurs suivant les recommandations de l'agence nationale de la sécurité des systèmes d'information et s'assure de son respect.

Dans le cas d'un système d'information classifié au niveau *Très Secret*, le mécanisme de contrôle d'accès permet également de tracer chaque accès (consultation, copie, modification, impression, etc.) à chaque information classifiée.

Le mécanisme de contrôle d'accès repose sur des mécanismes d'authentification forte établis selon le référentiel général de sécurité.

Si la mise en œuvre de tels mécanismes n'est pas possible pour des raisons techniques ou opérationnelles et après en avoir rendu compte à l'autorité qualifiée en sécurité des systèmes d'information et au service du haut fonctionnaire de défense et de sécurité compétents, des mesures organisationnelles sont prises pour pallier cette lacune et sont décrites dans le dossier d'homologation. Au niveau *Très Secret*, cette exception est soumise à l'autorisation de l'agence nationale de la sécurité des systèmes d'information dès la phase de conception du système d'information.

b) Revue des droits d'accès des comptes

Pour chaque système d'information classifié et système d'administration des systèmes d'information classifiés, une revue des droits d'accès des comptes est mise en place. La périodicité et les modalités de cette revue sont fixées par l'autorité d'homologation en

cohérence avec les besoins opérationnels et ne doit pas excéder un an. Les conditions précises de cette revue sont décrites dans le dossier d'homologation, ainsi que dans les exigences relatives à la sécurité des systèmes d'information intégrées dans la politique des informations et supports classifiés de l'organisme (cf. 2.3.1.2 et 2.3.1.3).

c) Mesures de sécurité logiques relatives aux mentions complémentaires de protection¹⁰¹

Les systèmes d'information susceptibles de traiter des informations portant une mention complémentaire de protection, notamment la mention *Spécial France*, font l'objet de mesures de sécurité particulières techniques ou organisationnelles pour garantir l'accès aux seules personnes ayant le besoin d'en connaître. Le processus d'homologation tient compte du fait que le système d'information est susceptible de traiter de telles informations.

Dans le cas d'un système devant traiter à la fois des informations portant la mention complémentaire de protection et d'autres ne la portant pas, et accessible à des personnes non autorisées à accéder à des informations portant la mention complémentaire de protection, le système d'information considéré et les mesures organisationnelles afférentes garantissent notamment que :

- pour chaque mention de protection, les informations classifiées en étant marquées sont stockées dans des zones du système d'information clairement identifiées et indiquées dans le dossier d'homologation ;
- les zones du système d'information ainsi identifiées sont cloisonnées du reste du système d'information avec des mesures conformes aux recommandations de l'agence nationale de la sécurité des systèmes d'information ;
- le contrôle d'accès du système d'information permet d'assurer la protection du besoin d'en connaître pour les informations classifiées marquées de la mention de protection considérée. Si nécessaire, un contrôle d'accès dédié est mis en place ;
- lorsque des données portant une mention de protection circulent hors des zones identifiées, elles sont chiffrées avec des moyens conformes aux recommandations de l'agence nationale de la sécurité des systèmes d'information ;
- l'accès aux informations portant une mention de protection complémentaire ou aux zones les contenant est tracé et indique explicitement les éventuelles mentions de protection.

6.6.3.2 Responsabilité des utilisateurs

Chaque utilisateur est responsable de la protection de ses informations d'authentification et du bon usage des outils associés (de type ACSSI, cartes à puce, etc.). L'autorité d'emploi du système d'information met à sa disposition des moyens de conservation sécurisés et adaptés de ces informations.

6.6.3.3 Articles contrôlés de la sécurité des systèmes d'information classifiés

Certains moyens, tels que les dispositifs de sécurité ou leurs composants, et certaines informations relatives à ces moyens (spécifications algorithmiques, documents de conception, clefs de chiffrement, rapports d'évaluation, etc.) nécessitent la mise en œuvre d'une gestion spécifique visant à assurer leur traçabilité et leur intégrité tout au long de leur cycle de vie. Ces moyens et informations, appelés « articles contrôlés de la sécurité des systèmes d'information », sont traités conformément à l'instruction interministérielle

¹⁰¹ Cf. 7.1.1.3 de la présente instruction.

6.6.4 Supervision logicielle de la sécurité et traçabilité

6.6.4.1 Synchronisation des horloges

Pour les besoins en traçabilité, les composantes d'un système d'information classifié sont synchronisées sur une source de temps unique. Lorsque des raisons techniques ou opérationnelles ne le permettent pas, cette impossibilité est mentionnée dans le dossier d'homologation et des mesures palliatives sont mises en place par le responsable de la sécurité des systèmes d'information.

6.6.4.2 Journalisation des événements

À des fins d'investigation, de suivi *a posteriori* des échanges, de traitement des incidents et d'archivage, une journalisation des événements est mise en place pour tracer et imputer les actions réalisées sur les systèmes d'information classifiés selon les recommandations de l'agence nationale de la sécurité des systèmes d'information.

Les événements enregistrés par le système de journalisation sont horodatés au moyen de sources de temps synchronisées entre elles. Ils sont, pour chaque système d'information classifié, centralisés et archivés pour une durée d'au moins trois ans pour le niveau *Secret* et d'au moins cinq ans pour le niveau *Très Secret*. Le format d'archivage des événements permet de réaliser des recherches automatisées sur ces événements. Si la mise en œuvre de tels mécanismes est impossible pour des raisons techniques ou organisationnelles et, après en avoir rendu compte à l'autorité qualifiée en sécurité des systèmes d'information et au service du haut fonctionnaire de défense et de sécurité compétents, des mesures palliatives sont prises et décrites dans le dossier d'homologation.

6.6.4.3 Protection de l'information journalisée

Les journaux des événements ne doivent pas être conçus pour contenir d'informations permettant de retrouver les informations d'authentification (de type mots de passe, codes PIN, clés privées, etc.).

Les journaux d'événements sont sauvegardés et protégés de manière à assurer leur intégrité et leur disponibilité.

6.6.4.4 Accès aux journaux

Pour chaque système d'information classifié, une procédure portant sur la manipulation des journaux est élaborée par le responsable de la sécurité des systèmes d'information. Elle précise les personnes autorisées à y accéder, leurs modes de traitement ainsi que les moyens techniques et opérationnels mis en œuvre pour assurer le respect du besoin d'en connaître et la traçabilité des accès.

Les données de traçabilité des accès sont archivées sur une durée d'au moins trois ans pour le niveau *Secret* et cinq ans pour le niveau *Très Secret*.

6.6.4.5 Systèmes de détection

Une procédure de détection des incidents de sécurité affectant le système d'information classifié est établie.

Cette procédure prévoit des mesures organisationnelles et techniques destinées à détecter les incidents de sécurité affectant le système d'information classifié. Les mesures organisationnelles comprennent les modalités d'exploitation des dispositifs de détection et décrivent la chaîne de traitement des événements de sécurité identifiés par ces dispositifs. Les mesures techniques précisent la nature et le positionnement des dispositifs de détection.

Des dispositifs de détection capables d'identifier des événements caractéristiques d'un incident de sécurité notamment d'une attaque en cours ou à venir et de permettre la recherche de traces d'incidents antérieurs sont mis en œuvre. À cet effet, ces dispositifs :

- collectent les données représentatives de l'activité du système d'information, issues du réseau, des systèmes et/ou des applications, à partir de capteurs positionnés de manière à optimiser la couverture du dispositif de supervision global ;
- analysent les données issues des capteurs notamment en recherchant des marqueurs techniques d'attaques connus ou des anomalies, dans le but d'identifier les événements de sécurité et de les caractériser ;
- archivent les métadonnées des événements identifiés afin de permettre une recherche *a posteriori* de marqueurs techniques d'attaques ou de compromission sur une durée d'au moins trois ans pour le niveau *Secret* et d'au moins cinq ans pour le niveau *Très Secret*.

Les stratégies de collecte et d'analyse sont élaborées par le responsable de la sécurité des systèmes d'information et approuvées par l'autorité qualifiée en sécurité des systèmes d'information.

Le recours à plusieurs sources de données pour détecter des activités malveillantes est encouragé. Un système de corrélation et d'analyse des journaux des événements doit être mis en œuvre et exploité.

L'architecture de déploiement des systèmes de détection ne doit pas remettre en cause la sécurité du système d'information classifié. Dans le cadre de systèmes de détection réseau, des dispositifs de type « TAP » qualifiés, qui concourent à l'atteinte de cet objectif de sécurité, sont utilisés.

Ces systèmes de détection sont exploités en s'appuyant sur les exigences du référentiel en matière de détection des incidents de sécurité pris conformément à l'article 10 du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.

Les systèmes de détection sont pris en compte dans le périmètre de l'homologation et les risques propres à ces systèmes font l'objet d'une attention particulière. Si les systèmes de détection sont communs à plusieurs systèmes d'information classifiés, ils font l'objet d'une homologation spécifique.

Si la mise en œuvre de tels systèmes de détection est impossible pour des raisons techniques ou organisationnelles et, après en avoir rendu compte à l'autorité qualifiée en sécurité des systèmes d'information et au service du haut fonctionnaire de défense et de sécurité compétents, des mesures palliatives sont prises et décrites dans le dossier d'homologation.

6.6.5 Maintenance et maintien en condition opérationnelle et en condition de sécurité

Les opérations de maintenance, qui incluent les opérations de maintien en condition opérationnelle et en condition de sécurité sur un système d'information classifié sont tracées et imputées à leur auteur sous la responsabilité de l'officier de sécurité des systèmes d'information. Elles sont réalisées par des personnes habilitées conformément à la partie 3.3.

Le matériel connecté au système d'information classifié pour sa maintenance et son maintien en condition opérationnelle ou de sécurité lui est dédié et est classifié au même niveau que le système d'information. Les équipements sont utilisés conformément aux parties 6.5 et 6.7.

Tout élément constitutif d'un système d'information traitant d'informations classifiées est maintenu en condition opérationnelle et en condition de sécurité.

L'autorité d'emploi du système d'information élabore, tient à jour et met en œuvre une procédure de maintien en condition de sécurité des ressources matérielles et logicielles de ses systèmes d'information classifiés.

Cette procédure prévoit :

- l'installation et la maintenance de toutes les ressources matérielles et logicielles des systèmes d'information classifiés dans des versions supportées par leurs fournisseurs ou leurs fabricants et mises à jour du point de vue de la sécurité, sauf en cas de difficultés techniques ou opérationnelles justifiées ;
- préalablement à l'installation de toute nouvelle version, la vérification de l'origine de cette version et de son intégrité, et l'analyse de l'impact, d'un point de vue technique et opérationnel, de cette version sur le système d'information classifié concerné ;
- une veille sur les vulnérabilités affectant le système d'information classifié afin de pouvoir mettre en œuvre, dès qu'une vulnérabilité est connue, des mesures palliatives en attente de la publication d'une mesure correctrice de sécurité ;
- l'installation sans délai sous le contrôle du responsable de la sécurité du système d'information, de toute mesure correctrice de sécurité concernant l'une de ses ressources, après s'être assuré de l'origine de cette mesure et de son intégrité.

Lorsque des raisons techniques ou opérationnelles le justifient, conformément aux instructions de l'autorité d'homologation, l'autorité d'emploi du système d'information peut décider, pour certaines ressources de ses systèmes d'information classifiés et des systèmes d'administration de systèmes d'information classifiés, de ne pas installer une version supportée par le fournisseur ou le fabricant de la ressource concernée ou de ne pas installer une mesure correctrice de sécurité. Dans ce cas, le responsable de la sécurité du système d'information met en œuvre des mesures techniques ou organisationnelles pour réduire les risques liés à l'utilisation d'une version obsolète ou comportant des vulnérabilités connues. Il documente ces mesures et les intègre au cycle de maintien en condition de sécurité de son système d'information.

6.6.6 Cloisonnement

Les systèmes d'information classifiés sont séparés physiquement des systèmes d'information de classification différente et des systèmes d'information non-classifiés. À défaut, des moyens agréés sont utilisés pour cloisonner logiquement ces systèmes d'information.

Lorsque sont concernés deux systèmes d'information classifiés au même niveau dont l'un n'est pas sous maîtrise nationale, les mêmes dispositions s'appliquent.

Tout système d'information classifié est découpé en zones fonctionnelles ayant des besoins de sécurité homogènes, cloisonnées entre elles suivant les recommandations de l'agence nationale de la sécurité des systèmes d'information.

6.6.7 Mécanismes de filtrage des flux de données

L'autorité d'emploi du système d'information classifié met en place des mécanismes de filtrage des flux de données circulant dans ou entre les systèmes d'information classifiés afin de bloquer la circulation des flux susceptibles de faciliter des attaques informatiques. Ces mécanismes respectent les règles suivantes :

- le responsable de la sécurité des systèmes d'information établit et tient à jour une liste des règles de filtrage mentionnant l'ensemble des règles en vigueur ou supprimées ;

- la circulation des flux de données est limitée autant que possible aux seuls flux nécessaires au fonctionnement et à la sécurité du système d'information classifié ;
- les flux entrants et sortants ainsi que les flux entre sous-systèmes du système d'information classifié sont filtrés au niveau de leurs interconnexions de manière à ne permettre que la circulation des seuls flux strictement nécessaires au fonctionnement et à la sécurité du système d'information. Les flux qui ne sont pas conformes aux règles de filtrage sont bloqués.

6.6.8 Gestion de la continuité et de la reprise de l'activité

Tout système d'information classifié le nécessitant fait l'objet d'un plan de continuité ou de reprise informatique (PCI/PRI).

Ce plan se conforme au plan de protection des sites, au plan de continuité ou de reprise d'activité (PCA/PRA) de l'organisme et ainsi que, le cas échéant, aux exigences du contrat au profit duquel le système d'information classifié est mis en œuvre.

Il est tenu à jour et régulièrement testé à l'occasion d'exercices.

L'absence de plan de continuité ou de reprise informatique est mentionnée et justifiée dans le dossier d'homologation.

6.7 SECURITE EN MOBILITE

6.7.1 Sécurité des équipements de mobilité

L'utilisation en mobilité d'équipements informatiques exploitant des informations classifiées est soumise à une analyse de risques dédiée qui est intégrée au dossier d'homologation. Des mécanismes et des fonctions de sécurité sont mis en place afin de protéger les informations classifiées.

Seuls les équipements mis à disposition et administrés par l'autorité d'emploi du système d'information classifié pour un usage en mobilité peuvent être utilisés.

De plus, si un équipement permet d'exploiter en mobilité des informations classifiées, il fait l'objet d'un agrément et est utilisé dans les conditions prévues par la décision d'agrément du produit.

Les règles minimales applicables aux équipements utilisés en mobilité sont :

- l'équipement est sous la surveillance permanente de l'utilisateur conformément aux conditions prévues par l'agrément de l'équipement ;
- l'utilisation d'un équipement contenant des informations classifiées n'est pas autorisée dès lors qu'une personne non habilitée ou n'ayant pas le besoin d'en connaître est susceptible d'en prendre connaissance directement ou indirectement ;
- la sortie du territoire national d'un équipement contenant des informations classifiées est soumise à autorisation de l'officier de sécurité des systèmes d'information qui fixe des règles particulières d'emploi et de l'officier de sécurité.

Ces règles sont, le cas échéant, complétées par l'officier de sécurité des systèmes d'information.

Lors de la remise d'un tel équipement, l'officier de sécurité des systèmes d'information informe l'utilisateur des règles spécifiques d'utilisation et le sensibilise aux risques liés à l'utilisation d'un tel équipement.

6.7.2 Sécurisation des accès à distance

Par principe, les systèmes d'information classifiés sont conçus et paramétrés pour interdire les accès à distance.

Lorsqu'un tel accès est absolument nécessaire pour des raisons opérationnelles, l'autorité d'homologation, s'appuyant sur le responsable de la sécurité du système d'information, protège l'accès à distance à ces systèmes d'information en ayant recours à des équipements mettant en œuvre des dispositifs de sécurité agréés au niveau de classification du système d'information auquel il donne accès.

6.8 SUPPORTS AMOVIBLES

La connexion ou l'installation d'équipements personnels à un système d'information classifié est strictement interdite.

La connexion d'un support amovible non classifié à un système d'information classifié est possible sous réserve de la mise en place de mesures techniques de protection, notamment des mesures de détection ou de protection contre l'introduction de codes malveillants ou d'exfiltration d'information.

Avant toute utilisation sur un système d'information traitant d'informations classifiées, l'innocuité de tout support est vérifiée.

Si l'utilisation de supports amovibles est autorisée, ceux-ci sont intégrés au périmètre d'homologation du système d'information classifié (cf. 6.1.1) lorsqu'ils sont gérés, administrés et mis à disposition par l'autorité d'emploi du système d'information classifié.

Tout support amovible susceptible de contenir ou d'avoir contenu de l'information classifiée d'un niveau donné est classifié au moins au même niveau et est soumis à ce titre aux obligations décrites au chapitre 7. En aucun cas, un support amovible classifié ne peut être connecté à un système d'information non-classifié ou de classification inférieure.

Lorsque des informations classifiées sont transportées à l'aide de supports amovibles, les supports amovibles respectent les exigences en matière de transport d'informations classifiées sur un support amovible (cf. 7.3.2.2).

L'officier de sécurité des systèmes d'information sensibilise les utilisateurs aux mesures de sécurité à respecter dans l'emploi des supports amovibles.

6.8.1 Supports amovibles au sein du système d'information classifié

Seuls les supports amovibles gérés, administrés et mis à disposition par l'autorité d'emploi du système d'information classifié sont autorisés à se connecter à ce système d'information classifié.

Des dispositifs de sécurité permettant de prévenir la connexion ou l'installation de supports amovibles non autorisés sont mis en place.

6.8.2 Supports amovibles entre un système d'information classifié et d'autres systèmes

Lorsque des supports amovibles sont utilisés pour importer et exporter des informations à partir d'un système d'information classifié, ce transfert d'information est réalisé exclusivement en connectant ces supports amovibles à des points de connexion appartenant au système d'information classifié. Ces points de connexion des supports amovibles sont dédiés à cet usage et garantissent notamment les exigences de sécurité suivantes :

- contrôle d'autorisation (approbation de la sortie d'information) ;

- rupture protocolaire : (rupture du flux transitant entre le support amovible et le système d'information émetteur ou destinataire) ;
- traçabilité et imputabilité du transfert.

Les exportations d'informations classifiées réalisées à partir de supports amovibles sont tracées par des moyens techniques ou organisationnels qui permettent notamment d'horodater le transfert et de l'imputer à un utilisateur du système d'information classifié.

Pour les systèmes d'information classifiés au niveau *Très Secret*, les mécanismes d'importation et d'exportation d'informations par support amovible permettent d'identifier l'émetteur et les destinataires de l'information classifiée.

L'utilisation de supports amovibles entre un système d'information classifié et un système d'information non classifié ou de classification différente est par principe interdite.

Toute dérogation à l'interdiction de principe doit être justifiée par un besoin opérationnel strictement nécessaire. La justification est versée au dossier d'homologation et les mesures de protection minimales suivantes s'appliquent :

- une analyse de risques est conduite pour identifier les mesures techniques et organisationnelles visant à prévenir tout risque de sortie incontrôlée d'information classifiée lié aux cas d'usage de ces supports amovibles ;
- les échanges d'information entre un système d'information classifié et un système d'information non classifié ou de classification différente s'effectuent au moyen de points de connexion des supports amovibles mettant en œuvre des dispositifs de sécurité utilisés comme moyens essentiels de protection contre les accès non-autorisés aux informations classifiées. Ces dispositifs de sécurité sont agréés (cf. 6.5.2). En absence de dispositifs agréés et après en avoir rendu compte à l'autorité qualifiée en sécurité des systèmes d'information et au service du haut fonctionnaire de défense et de sécurité compétents, des mesures palliatives sont prises et décrites dans le dossier d'homologation.

6.9 AUDIT DES SYSTEMES D'INFORMATION

En complément des tâches de maintien en condition de sécurité, l'autorité d'homologation réalise ou fait réaliser, en lien avec la chaîne fonctionnelle de la sécurité des systèmes d'information classifiés, des audits de sécurité périodiques des systèmes d'information classifiés, avant chaque homologation ou renouvellement d'homologation.

L'autorité d'emploi du système d'information visé précise les conditions du déroulement de l'audit, notamment de l'utilisation et de la restitution des équipements nécessaires à l'audit.

L'autorité d'homologation et l'autorité d'emploi du système d'information formalisent les conditions de réalisation de l'audit, le cas échéant, par une convention d'audit. Ces audits de sécurité doivent, au-delà de la conformité aux règles de la présente instruction, évaluer le niveau de robustesse des systèmes d'information eu égard aux évolutions de la menace informatique. Il s'agit de vérifier l'application de mesures de défense en profondeur, de les éprouver par des techniques et outils à l'état de l'art et de réaliser des tests complémentaires qui peuvent être conduits inopinément en fonction des relevés d'audit initiaux.

Les risques associés à l'utilisation des outils d'audit, des privilèges et de communication des relevés techniques nécessaires à la réalisation de l'audit de sécurité figurent dans le dossier d'homologation du système visé, quel que soit son niveau de classification et sans préjudice des dispositions de la présente instruction. Les rapports d'audit portant sur des systèmes d'information classifiés sont classifiés au moins au niveau *Secret*. Les relevés techniques d'audit sont classifiés au maximum au même niveau que le rapport.

L'autorité d'homologation et l'officier de la sécurité des systèmes d'information tiennent les rapports d'audit à disposition de l'agence nationale de la sécurité des systèmes d'information, du service du haut fonctionnaire de défense et de sécurité et du service enquêteur compétents. Les modalités de consultation des rapports d'audit sont déterminées en accord avec le service du haut fonctionnaire de défense et de sécurité.

En cas de recours, pour un audit d'un système d'information classifié, à un prestataire privé, la prestation d'audit doit être qualifiée par l'agence nationale de la sécurité des systèmes d'information¹⁰².

Par principe, les auditeurs doivent être habilités au niveau de classification du système d'information classifié audité selon les modalités détaillées à la partie 3.3. Toutefois, lorsque les droits qui leur sont octroyés initialement sur le système d'information classifié sont étendus, leur permettant notamment d'outrepasser leurs droits ou de masquer leurs actions sur celui-ci, les auditeurs doivent être habilités au niveau *Très Secret*.

¹⁰² Chapitre III du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.

7 GESTION DES INFORMATIONS ET SUPPORTS CLASSIFIES TOUT AU LONG DE LEUR CYCLE DE VIE

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 seules personnes qualifiées au sens des articles 413-10 et suivants du code pénal (cf. 1.2).

La classification est matérialisée par l'apposition d'un timbre de classification défini dans la présente instruction qui permet de caractériser l'infraction pénale en cas de compromission et détermine les mesures de protection à mettre en œuvre pour l'élaboration et la gestion de l'information et du support classifié tout au long de son cycle de vie.

7.1 ÉLABORATION DES INFORMATIONS ET SUPPORTS CLASSIFIES

7.1.1 Règles de classification

Classifier une information ou un support au titre du secret de la défense nationale a pour conséquence de le placer sous la protection des dispositions spécifiques du code pénal¹⁰³.

L'apposition d'un timbre de classification visible constitue le seul moyen de conférer cette protection particulière. Il est une marque de l'autorité publique¹⁰⁴ permettant de vérifier l'authenticité et l'intégrité du support.

7.1.1.1 Principes régissant la décision de classification

a) Articulation des rôles d'autorité émettrice et d'auteur d'informations et supports classifiés

La décision de procéder à la classification d'une information ou d'un support est une prérogative du Premier ministre exercée par le Premier ministre ou, par délégation, par chaque ministre dans son champ d'attribution (cf. 2.1.2.1), ainsi que par certaines autorités, du fait de leur statut constitutionnel ou du pouvoir qui leur a été conféré par la loi (cf. 2.1.3).

Ces différentes autorités sont qualifiées d'autorité émettrice, c'est-à-dire, l'autorité nécessairement étatique ou, dans le cas des organisations internationales ou de l'Union européenne, supra-étatique, sous la responsabilité de laquelle un timbre de classification ou de déclassification est apposé sur une information ou un support.

Le Premier ministre est seule autorité émettrice pour le niveau *Très Secret* faisant l'objet d'une classification spéciale.

L'auteur d'une information ou d'un support classifié est celui qui prend la décision d'apposer le timbre de classification sur une information ou un support au niveau requis par son contenu, conformément aux modalités de classification arrêtées par l'autorité émettrice. Ces modalités sont définies :

- pour le niveau *Très Secret* faisant l'objet d'une classification spéciale, dans les dispositions spécifiques prises par le secrétaire général de la défense et de la sécurité nationale ;
- pour les niveaux *Secret* et *Très Secret*, hors classifications spéciales : dans les guides de classification attachés aux instructions ministérielles du ministre sous l'autorité duquel l'information est classifiée, complétés, le cas échéant, des directives techniques particulières et, pour les personnes morales ayant accès à des informations ou supports

¹⁰³ Articles 413-9 et suivants du code pénal.

¹⁰⁴ Articles 444-1 à 444-9 du code pénal et loi du 18 mars 1918 réglementant la fabrication et la vente des sceaux, timbres et cachets officiels.

classifiés dans le cadre d'une convention ou d'un contrat, par le plan contractuel de sécurité attaché à la convention ou au contrat ;

- pour les informations et supports classifiés émis sous la responsabilité des autorités visées au paragraphe 2.1.3, par ces autorités, en conformité avec la présente instruction.

Avant de décider d'apposer un timbre de classification sur une information ou un support, l'auteur d'informations ou supports classifiés procède à l'analyse de l'importance de l'information¹⁰⁵ au regard de son contexte et eu égard aux directives de classification applicables.

Il veille ainsi, sous le contrôle de son autorité hiérarchique, ainsi que sous la responsabilité de son responsable d'organisme et de l'autorité émettrice pour laquelle il procède à la classification, à ce que le niveau de classification soit approprié à l'information ou au support concernés, c'est-à-dire à ce qu'il soit à la fois strictement nécessaire et suffisant.

Chaque échelon de la chaîne de responsabilité (cf. 1.4) doit être en mesure de justifier le timbre de classification apposé sur une information ou un support classifié et prévient les classifications abusives, qui génèrent des coûts de gestion, des charges de travail importantes et altèrent la valeur du secret de la défense nationale. Inversement, chaque échelon de la chaîne de responsabilité s'assure qu'aucune information ou support justifiant une classification n'échappe à la classification. Ne pas classer une information ou un support dont la divulgation ou auquel l'accès est de nature à porter atteinte à la défense et à la sécurité nationale constitue un manquement grave aux règles de la protection du secret de la défense nationale, dont chaque échelon de la chaîne de responsabilité est comptable. Cela caractérise une faute, qu'il revient à l'autorité compétente, le cas échéant, de sanctionner.

b) Le choix du niveau de classification

Ainsi que rappelé à la partie 1.3, il existe deux niveaux de classification¹⁰⁶ :

- *Secret* : réservé aux informations et supports dont la divulgation ou auxquels l'accès est de nature à porter atteinte à la défense et à la sécurité nationale ;
- *Très Secret* : réservé aux informations et supports dont la divulgation ou auxquels l'accès aurait des conséquences exceptionnellement graves pour la défense et la sécurité nationale. Des classifications spéciales sont créées, pour le niveau *Très Secret*, pour protéger les informations relatives aux priorités gouvernementales en matière de défense et de sécurité nationale.

Chaque ministre précise dans son instruction ministérielle les modalités de classification et de protection des informations et supports et souligne l'importance de ne classer que ce qui est réellement nécessaire (cf. Annexe 3).

Le niveau de classification est déterminé par la nature et le contexte de l'information ou du support classifié. La source de l'information peut également être prise en considération lorsque sa sensibilité justifie une protection¹⁰⁷. Les cas manifestes de sur-classification ou de sous-classification sont signalés par le(s) destinataire(s) à l'autorité émettrice ou à l'auteur de l'information ou du support classifié qui procède, si nécessaire, à la modification appropriée,

¹⁰⁵ Ou procédé, objet, document, réseau informatique, données informatisées ou fichier intéressant la défense nationale au sens de l'article 413-9 du code pénal.

¹⁰⁶ Articles R. 2311-2 et R. 2311-3 du code de la défense.

¹⁰⁷ Par source, il est ici entendu le(s) système(s) de renseignement ayant permis de produire une information.

en informe l'ensemble des destinataires et prend les mesures nécessaires pour éviter une compromission lorsque l'information change de niveau.

7.1.1.2 Principes de classification

a) Principe de classification d'un document

Tout ensemble (pages, paragraphes, annexes, appendices, pièces jointes) d'un document contenant des informations classifiées à des niveaux différents est classifié lui-même au niveau le plus élevé des informations qu'il contient.

Lorsqu'un document comprend diverses parties, les unes nécessitant une classification, les autres non, il convient de s'efforcer de préciser le niveau de classification en marge face aux parties ou paragraphes qu'il couvre (cf. Annexe 36). La diffusion des paragraphes non classifiés ou des paragraphes d'un niveau de classification inférieur est rendue possible par extraction des éléments non classifiés ou en rendant illisibles¹⁰⁸, de manière irréversible, les paragraphes classifiés ou classifiés au niveau supérieur.

Par principe, l'objet d'un document est classifié au même niveau que le document lui-même, sauf si son auteur en décide autrement et le précise.

b) Principe de classification d'un matériel et des informations qui lui sont relatives

Le niveau de classification des informations (notices, plans, etc.) concernant un matériel peut être différent du niveau de classification de ce dernier.

c) Principe de classification d'un agrégat

Un ensemble d'informations ou supports, dit « agrégat », peut être classifié si le regroupement des informations ou supports qui le composent le justifie, alors même qu'aucun de ses éléments, pris isolément, n'est classifié¹⁰⁹. Un agrégat d'informations ou supports classifiés peut également être classifié à un niveau supérieur.

d) Principe de transitivité du niveau de classification d'une information extraite d'une information classifiée

Un extrait d'information classifiée conserve le niveau de classification de l'information elle-même, sauf accord de l'autorité compétente désignée par l'autorité émettrice. En l'absence d'indication contraire, la diffusion séquentielle d'extraits non classifiés par découpage de l'information classifiée est interdite. 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 dispositions de la présente instruction.

e) Principe de classification des systèmes d'informations classifiés

Pour les systèmes d'information, la décision d'homologation du système vaut décision de classification.

f) Principe de rémanence du niveau de classification des supports informatiques traitant des informations classifiées

En raison de l'impossibilité technique de faire disparaître de manière fiable et irréversible des informations en principe effacées, un support informatique conserve toujours le niveau de classification le plus élevé qui lui a été attribué au cours de son cycle de vie. Il ne peut être

¹⁰⁸ Selon les recommandations de l'ANSSI lorsqu'il s'agit d'un support numérique.

¹⁰⁹ La somme des informations portant la mention de protection *Diffusion Restreinte* stockées sur un système d'information n'entraîne pas nécessairement la classification du système d'information.

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. Il peut être réaffecté dans les conditions prévues au paragraphe 7.5.2.

7.1.1.3 Mentions complémentaires à la marque de classification

a) Spécial France

La mention *Spécial France* n'est pas un timbre de classification. Elle est employée pour les informations et supports classifiés ou pour les informations et supports portant la mention *Diffusion Restreinte*, qui ne sauraient être communiqués, en tout ou partie, à un État étranger ou à l'un de ses ressortissants, à une organisation internationale, une institution, un organisme ou un organe de l'Union européenne, ni à une personne morale de droit étranger, même s'il existe un accord de sécurité entre la France et l'État ou la personne de droit international public considérée, sous réserve, lorsque cette mention est apposée sur des informations et supports protégés par la mention *Diffusion Restreinte*, des exigences résultant du code du patrimoine et du code des relations entre le public et l'administration. 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 niveau de classification, n'être transmises qu'à des personnes physiques ou morales françaises considérées comme qualifiées au regard du code pénal (cf. 1.2).

b) Autres mentions particulières

Les informations et supports classifiés devant faire l'objet de restrictions spécifiques de diffusion en raison de leur contenu portent, en plus de la marque éventuelle de leur niveau de classification, une mention particulière précisant les services, les États ou les organisations internationales, les institutions, organes ou organismes de l'Union européenne pouvant y avoir accès ou la classification spéciale dont ils font l'objet¹¹⁰. Les modalités d'emploi de ces mentions peuvent faire l'objet de directives d'application.

Cette mention, apposée par l'auteur d'informations ou supports classifiés sous la responsabilité de l'autorité émettrice, a pour effet de circonscrire expressément le périmètre de diffusion de ces informations et supports ainsi que d'attirer l'attention sur le strict besoin d'en connaître. Les mesures de sécurité du niveau de classification sont appliquées et leur acheminement est réalisé de façon à garantir le respect du périmètre de diffusion ainsi délimité.

7.1.2 Marquage

7.1.2.1 Visibilité du marquage

L'accès à une information ou un support classifié par une personne non qualifiée est prohibé par le code pénal. Aussi, une information doit pouvoir être identifiée comme étant classifiée avant même d'être consultée. Chaque information et support classifié porte ainsi la marque du niveau de classification des informations qu'il contient. Cette marque est qualifiée de « timbre de classification ».

Le marquage constitue une marque de l'autorité publique¹¹¹ dont l'usage est strictement réservé aux seules personnes autorisées dans le cadre de la présente instruction.

¹¹⁰ Article R. 2311-4 du code de la défense.

¹¹¹ Articles 444-1 à 444-9 du code pénal et loi du 18 mars 1918 réglementant la fabrication et la vente des sceaux, timbres et cachets officiels.

Des abréviations indiquant la classification peuvent être utilisées pour préciser le niveau de classification des paragraphes du texte d'une information ou d'un support classifié. Les abréviations employées sont les suivantes :

- *Secret* : S ;
- *Très Secret* : TS.

Ces abréviations ne remplacent pas la marque de classification inscrite en toutes lettres sur le support.

En cas de non-respect de ces consignes, la protection pénale qui s'attache aux informations classifiées ne s'applique pas¹¹².

7.1.2.2 Marquage des supports préparatoires

Les supports préparatoires servant à l'élaboration d'une information ou d'un support classifié portent un timbre de classification de niveau requis dès lors qu'ils contiennent des informations justifiant la classification de l'information ou du support final.

Dans le cas, à éviter, où la décision de classification ne peut intervenir qu'au moment de la finalisation de l'information ou du support classifié, les informations ou supports ayant servi à l'élaboration de l'information ou du support classifié (brouillons, documents de travail, impressions sur papier) qui ne sont pas marqués, sont détruits ou effacés, dans les conditions prévues au 7.5.1, le plus rapidement possible dès qu'ils sont devenus sans objet et, en tout état de cause, au plus tard lorsque l'information ou le support classifié est émis.

7.1.2.3 Marquage d'un support papier

Le marquage comprend à la fois le timbre, l'identification et la pagination.

a) Timbre

Il 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.

Il 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 (cf. Annexe 37). Le timbre, dont la dimension peut être adaptée à celle du support, est définitif et toujours visible.

Si l'information doit être divulguée aux seuls ressortissants français, le timbre *Spécial France*, de couleur bleue, est apposé en haut de chaque page, immédiatement à droite ou au-dessous du timbre de classification de l'information.

b) 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 :

- le timbre du niveau de classification (cf. Annexe 37) ;
- l'échéance de la classification ou, à titre exceptionnel, notamment, le cas échéant, pour les documents visés aux points a) à e) du 3° du I. de l'article L. 213-2 du code du patrimoine, lorsqu'une telle échéance ne peut être déterminée au moment de la

¹¹² Organisée notamment par les articles 413-9 à 413-12 du code pénal.

classification, la date ou le délai au terme duquel le niveau de classification doit être réévalué (cf. 7.6.1). Le cas échéant, la mention de déclassement ou de déclassification est apposée sur cette même page (cf. Annexe 38) ;

- les références de l'autorité émettrice et de l'auteur de l'information ou du support classifié ;
- la date d'émission ;
- le numéro d'enregistrement.

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 ou de protection, ou par une mise en page qui les détache sans ambiguïté du contexte général du document.

Au niveau *Très Secret*, chaque document est individualisé par son numéro d'exemplaire et le nombre total d'exemplaires est porté sur la première page. Chaque page porte également la référence du document.

c) Pagination

Chaque page du document est numérotée. Sur la première page sont précisés le nombre total de pages et les annexes ou plans qui le composent.

Les pages de chaque annexe sont numérotées de la pagination du document lui-même, et portent mention du nombre total de pages de l'annexe sur la première page de celle-ci.

Pour les documents classifiés au niveau *Très Secret*, les pages vierges et les feuilles intercalaires sont également numérotées. Toute page vierge porte en son centre la mention "PAS DE TEXTE".

7.1.2.4 Marquage d'un matériel classifié hors support amovible

Le marquage d'un matériel classifié hors support amovible est adapté au type de support, définitif et toujours visible. Il consiste en :

- un timbre de classification, spécifiant le niveau de classification ayant une dimension adaptée à celle du support et comporte la mention de ce niveau en toutes lettres. En cas de difficultés pratiques, les abréviations mentionnées au 7.1.2.1 évoquées peuvent y être substituées ;
- la référence de l'élément.

7.1.2.5 Marquage d'un support immatériel

Le marquage d'un support immatériel d'informations classifiées (message ou fichier électronique, base de données, etc.) est adapté au type de support et est toujours visible. Il consiste en :

- un timbre spécifiant le niveau de classification en toutes lettres et ayant une dimension adaptée à celle du support (abréviations). Il peut contenir la mention *Spécial France* si l'information doit être divulguée aux seuls ressortissants français ;
- la référence et, le cas échéant, le volume de chacune des informations enregistrées.

Dans la mesure du possible, les règles de marquage d'un support immatériel doivent respecter les règles de marquage d'un support papier (cf. 7.1.2.3).

S'il est matériellement impossible d'apposer le marquage sur le support classifié ou contenant une information classifiée, il convient de mettre en œuvre les mesures techniques et organisationnelles décrites dans le dossier d'homologation et la documentation utilisateur.

7.1.2.6 Marquage des éléments constitutifs d'un système d'information classifié

Le marquage des éléments constitutifs d'un système d'information classifié est adapté au type d'élément et toujours visible. Il consiste en :

- un timbre spécifiant le niveau de classification en toutes lettres et ayant une dimension adaptée à celle de l'élément ;
- une identification assurée par l'inscription des références de l'élément.

S'il est matériellement impossible d'apposer le marquage sur l'élément, il convient de mettre en œuvre les mesures techniques et organisationnelles décrites dans le dossier d'homologation et la documentation utilisateur.

Les claviers et autres périphériques d'entrée similaires peuvent être exemptés de marquage. Cette exemption doit être mentionnée dans le dossier d'homologation.

7.1.2.7 Marquage d'un support amovible

Le marquage d'un support amovible d'informations classifiées est adapté au type d'élément et toujours visible. Il consiste en :

- un timbre spécifiant le niveau de classification en toutes lettres et ayant une dimension adaptée à celle du support ;
- une identification assurée par l'inscription des références du support.

S'il est matériellement impossible d'apposer le marquage sur le support, il convient de mettre en œuvre les mesures techniques et organisationnelles décrites dans le dossier d'homologation et la documentation utilisateur.

Pour les supports amovibles agréés, le marquage est réalisé dans les conditions prévues par les instructions d'emploi du support, mentionnées dans la décision d'agrément.

7.2 TRACABILITE DES INFORMATIONS ET SUPPORTS CLASSIFIES AU SEIN DE L'ORGANISME DETENTEUR¹¹³

7.2.1 Organisation de la gestion des informations et supports classifiés

7.2.1.1 Recommandation au niveau *Secret*

Les personnes en charge de la gestion des informations et supports classifiés au niveau *Secret* doivent être habilitées au niveau au moins égal à ce niveau et sont fonctionnellement rattachées, pour l'accomplissement de ces missions, à l'officier de sécurité de leur organisme.

Il est par ailleurs recommandé aux responsables d'organisme ayant accès à des informations et supports classifiés au niveau *Secret* de créer un bureau de protection du secret, constitué de personnes identifiées au sein de son personnel, chargé de veiller à la bonne application de la réglementation relative à la gestion des informations et supports classifiés à ce niveau. Ces missions ne peuvent pas être externalisées.

7.2.1.2 Obligation au niveau *Très Secret*

La création d'un bureau de protection du secret est obligatoire dans les organismes ayant accès à des informations ou supports classifiés au niveau *Très Secret*.

¹¹³ Les critères et les modalités d'organisation de la protection des informations et supports classifiés *Très Secret* faisant l'objet d'une des classifications spéciales mentionnées à l'article R. 2311-3 du code de la défense relèvent de dispositions spécifiques prises par le Premier ministre.

Chaque ministre veille à la création de ces bureaux dans les organismes relevant de son champ d'attribution (cf. 2.1.2.1). Le bureau de protection du secret est composé exclusivement de personnes choisies parmi le personnel de l'organisme, habilitées au niveau *Très Secret*. Il dispose d'une zone réservée (cf. 5.3.1.2).

Le bureau de protection du secret assure le traitement, le marquage, la conservation et le suivi des informations et supports classifiés au niveau *Très Secret* jusqu'à leur destruction ou leur versement à un service d'archives. À ce titre, il est responsable de l'enregistrement, de l'expédition, de la réception et de la circulation des informations et supports classifiés à ce niveau, qui ne peuvent transiter que par son intermédiaire, hormis ceux comportant la mention « ACSSI »¹¹⁴ (cf. 2.2.3). Il dresse un inventaire annuel des informations et supports classifiés qu'il traite.

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 arrivée ou départ, autorité émettrice et auteur de l'information ou du support classifié, date de création, domaine, titre ou objet, nombre de pages, 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 de chaque exemplaire) ;
- recherche sur les supports d'information (détenteurs successifs d'un exemplaire, date de création, service émetteur, etc.) ;
- inventaire des informations et supports classifiés ;
- 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, etc.).

Aucun organisme ne peut élaborer, traiter, conserver, détruire ou acheminer des informations et supports classifiés au niveau *Très Secret* faisant l'objet d'une classification spéciale sans y avoir été préalablement autorisé par le secrétaire général de la défense et de la sécurité nationale.

7.2.1.3 Organisation des échanges d'informations et de supports classifiés avec des personnes physiques ou morales de droit étranger

Conformément à l'article 414-9 du code pénal, la France assure la même protection aux informations et supports classifiés étrangers, reçus ou produits en commun en vertu d'un accord de sécurité, général ou spécifique, régulièrement approuvé et publié, qu'aux informations et supports classifiés français de niveau équivalent.

Symétriquement, la communication d'informations ou supports classifiés français à une personne physique ou morale relevant de la juridiction d'un État étranger ou d'une organisation internationale n'est possible qu'en vertu d'un accord intergouvernemental conclu entre la France et l'État ou l'organisation internationale considéré ou conformément aux

¹¹⁴ Instruction générale interministérielle n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI).

règles de sécurité de l'organisation internationale, lorsque ces dernières sont directement applicables.

Les accords intergouvernementaux relatifs à l'échange et à la protection d'informations classifiées peuvent porter soit :

- sur un domaine spécifique (généralement celui de la défense) : l'accord est alors qualifié d'accord de sécurité dans le domaine considéré ;
- sur l'ensemble de l'action gouvernementale : l'accord est alors qualifié d'accord général de sécurité.

Plutôt que de définir, avec chaque partenaire, des mesures de protection *ad hoc*, ces accords fonctionnent sur la base d'un modèle-type et organisent la protection des informations et supports échangés sur la base d'un régime d'équivalence entre les niveaux de classification français et ceux du partenaire. Ce régime d'équivalence est établi après analyse de la législation du partenaire et présenté généralement sous la forme d'un tableau d'équivalence. La mention *Diffusion Restreinte* qui n'est pas, en France, une mention de classification conférant à ces informations la protection pénale propre au secret de la défense nationale, mais qui peut être un niveau de classification chez certains partenaires fait, par ailleurs, généralement l'objet d'un traitement spécifique au sein de ces accords.

Partant, sauf dispositions contraires dans l'accord ou des règles de sécurité applicables qu'il convient toujours de consulter avant tout échange d'information ou support classifié avec un partenaire étranger, la gestion (enregistrement, conservation, reproduction, diffusion, transport, expédition, réception, inventaire) des informations et supports classifiés étrangers confiés à la France suit des règles au moins aussi strictes que celles applicables aux informations classifiées nationales de niveau équivalent.

De la même façon, la protection des systèmes d'information traitant d'informations classifiées confiées à la France par des États étrangers ou par des organisations internationales, des institutions, organes ou organismes de l'Union européenne est assurée conformément à l'accord ou aux règles de sécurité applicables.

Symétriquement, lorsque des informations classifiées françaises sont transmises *via* et sur des systèmes d'information relevant de la responsabilité d'États étrangers ou d'organisations internationales, d'institutions, organes ou organismes de l'Union européenne, les mesures de protection sont fixées par l'accord ou les règles de sécurité applicables, qui assurent à ces informations un niveau de protection au moins équivalent à celui prévu dans la présente instruction.

Les accords et règles de sécurité font, le cas échéant, l'objet d'instructions complémentaires pour leur application en France. Notamment, dans le cadre des échanges avec les organisations internationales, des règles spécifiques peuvent s'ajouter aux règles nationales et imposer une supervision par l'autorité nationale de sécurité (rôle endossé en France par le secrétaire général de la défense et de la sécurité nationale ou l'autorité de sécurité déléguée (cf. 2.1.1.2 b)) des modalités de gestion des informations et supports classifiés émises dans le cadre de l'organisation internationale, quel que soit le niveau de classification des informations et supports considérés. Ainsi, le secrétariat général de la défense et de la sécurité nationale est notamment bureau d'ordre central pour les informations et supports classifiés de

l'OTAN et des institutions, organes ou organismes de l'Union européenne, dont les règles de gestion sont complétées par des instructions interministérielles spécifiques¹¹⁵.

Enfin, des règles complémentaires, si nécessaire plus restrictives, peuvent être stipulées dans le plan contractuel de sécurité attaché à des contrats internationaux nécessitant d'échanger ou de produire des informations ou supports classifiés avec un partenaire étranger.

À défaut d'instruction ou de stipulations complémentaires, les dispositions de la présente instruction s'appliquent.

7.2.2 Enregistrement

Tout support d'information classifiée est enregistré, dans l'ordre chronologique, dans un système d'enregistrement spécifique, manuel ou informatisé, dont l'accès est restreint aux personnes ayant le besoin d'en connaître¹¹⁶. Si ce système est classifié, les personnes y ayant accès sont habilitées au niveau requis.

Pour les informations classifiées dématérialisées, les obligations d'enregistrement sont assurées par les fonctions de traçabilité du système d'informations classifié les hébergeant.

L'enregistrement établit sans ambiguïté l'attribution du support à un détenteur, personne physique, clairement identifiée. Le détenteur assume alors la responsabilité de la protection du support. Cet enregistrement est la seule référence de cette attribution de responsabilité. Dans la mesure du possible, le numéro d'enregistrement est assorti d'une fiche où sont inscrites les références des informations contenues. Pour chaque support classifié, il est précisé dans le système d'enregistrement l'échéance de classification ou, à défaut, la date ou le délai de réévaluation impérative du niveau de classification (cf. 7.6.1) fixé par l'auteur de l'information. La mention de l'objet du document peut figurer dans le système d'enregistrement s'il porte le même niveau de protection ou de classification précisé par son auteur que le système ou si son auteur a précisé qu'il n'était pas protégé.

7.2.2.1 Au niveau *Secret*

Un système d'enregistrement est mis en place par le responsable d'organisme avec l'appui de l'officier de sécurité. Il est tenu, sous le contrôle de l'officier de sécurité, par les personnes en charge de la gestion des informations et supports classifiés ou, le cas échéant, par le bureau de protection du secret. Ce système peut être relié à une base de gestion du courrier sous réserve que l'accès à la base soit restreint aux seules personnes ayant le besoin d'en connaître et que cette base permette de tracer les documents jusqu'au détenteur final.

7.2.2.2 Au niveau *Très Secret*

Le bureau de protection du secret assure l'enregistrement des informations et supports classifiés sur un système d'enregistrement. Par principe, ce système est classifié au niveau *Très Secret*. Sa classification peut toutefois être limitée au niveau *Secret*, si les objets des informations et supports enregistrés n'y sont pas mentionnés ou si ces derniers ont tous été expressément déclassifiés ou déclassés par leur auteur conformément au dernier paragraphe du a) du 7.1.1.2.

¹¹⁵ Instruction interministérielle n° 2100 pour l'application en France du système de sécurité de l'OTAN et instruction générale interministérielle n° 2102 sur la protection en France des informations classifiées de l'Union européenne.

¹¹⁶ Un support amovible est enregistré comme un seul document même s'il contient plusieurs fichiers et ceux-ci sont inscrits dans le document d'enregistrement. La traçabilité intrinsèque du support dématérialisé permet de connaître les fichiers qu'il contient ou qu'il a contenus.

Chaque support d'informations classifiées au niveau *Très Secret* fait l'objet d'une double numérotation présentée sous la forme d'une fraction comportant le numéro d'enregistrement de l'auteur sur le numéro d'enregistrement du bureau de protection du secret chargé de leur traitement.

7.2.3 Conservation

Le responsable d'organisme met en place des moyens de conservation sécurisés et pérennes des informations et supports classifiés. Lorsque l'organisme dispose de plusieurs établissements, chaque établissement détenant des informations ou supports classifiés dispose des moyens sécurisés et pérennes nécessaires à leur conservation.

En dehors des périodes d'utilisation, les supports classifiés sont conservés dans un meuble de sécurité (coffre-fort ou armoire forte) répondant aux exigences énoncées dans la présente instruction (cf. Annexe 30). Le niveau de classification des documents contenus ne doit pas figurer à l'extérieur du meuble.

Des informations et supports classifiés de diverses origines peuvent être conservés à l'intérieur d'un même meuble de sécurité à condition d'en assurer le cloisonnement en séparant et précisant l'origine des supports et sous réserve que les personnes y ayant accès aient le même besoin d'en connaître. Dans le cas contraire, les informations et supports classifiés sont conservés dans des sous-coffres précisant leur origine.

La combinaison du meuble de sécurité, 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 ou l'armoire forte d'une autorité spécialement désignée, la clef de ce meuble étant elle-même placée dans un meuble distinct.

La combinaison est changée tous les ans et, à chaque fois, en cas de mutation des utilisateurs, d'identification d'un risque ou de suspicion de compromission.

Les clefs des lieux abritant des informations et supports classifiés 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 clef, à combinaison et à commande unique ou avec ouverture par lecture de badge, garde permanente avec système d'alarme, etc.). Il est formellement interdit d'emporter les clefs de ces lieux et des meubles de sécurité à l'extérieur des locaux de travail.

La responsabilité de la conservation des informations et supports classifiés incombe au détenteur auquel l'information ou le support classifié a été attribué, au chef du bureau de protection du secret ou aux personnes en charge de la gestion des informations et supports classifiés.

Les informations classifiées dématérialisées sont stockées sur un système d'information homologué au même niveau de classification ou au niveau supérieur. Les exigences de sécurité relatives à la sécurité du système d'information de l'organisme (cf. 2.3.1.2) prévoient des moyens et des procédures de sauvegarde et de conservation sécurisés et pérennes des informations classifiées contenues au sein des systèmes d'information classifiés utilisés. Ces moyens et procédures respectent le besoin d'en connaître. Le système de sauvegarde est du même niveau de classification que le système d'information traitant les données.

7.2.4 Reproduction

Chaque ministre définit dans son instruction ministérielle les consignes pour la reproduction et l'impression de supports classifiés de niveaux *Secret* et *Très Secret*. Ces consignes :

- désignent les personnes habilitées à autoriser la reproduction ;

- fixent les procédures et les mesures techniques garantissant la traçabilité des impressions, le contrôle du processus par le détenteur, de bout en bout, du lancement de l'impression jusqu'à la récupération de l'information classifiée imprimée.

Le détenteur de l'information ou du support classifié initial est responsable des reproductions et impressions qu'il entreprend jusqu'à leur attribution à un autre détenteur conformément aux modalités de la présente instruction, complétées, le cas échéant, par l'instruction ministérielle, les directives techniques particulières et le plan contractuel de sécurité applicables.

Les matériels utilisés pour la reproduction d'informations classifiées (photocopieuses, télécopieurs, systèmes informatiques, etc.) sont physiquement protégés afin d'en limiter l'emploi aux seules personnes autorisées. Si ces matériels sont connectés à un système d'information, ils sont intégrés dans le périmètre d'homologation du système d'information. 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 complétées, le cas échéant, par l'instruction ministérielle, les directives techniques particulières et le plan contractuel de sécurité applicables. Il en est de même pour leur mise au rebut qui doit garantir la destruction des mémoires de ces appareils (cf. 7.5.2).

La reproduction numérique d'informations classifiées dématérialisées est autorisée et se fait sous la responsabilité de l'utilisateur, qui est sensibilisé par l'officier de sécurité des systèmes d'information sur les bonnes pratiques en la matière. Il veille ainsi à limiter la diffusion de ces informations classifiées dématérialisées selon le strict besoin d'en connaître et s'assure que la convention de marquage de ces informations est respectée. Lorsque la reproduction numérique est réalisée sur un support amovible, elle respecte les exigences prévues par la présente instruction (cf. 6.8 et 7.3.1.1)

7.2.4.1 Au niveau *Secret*

La reproduction totale est effectuée par le détenteur, sous sa responsabilité, à condition de conserver sur un système d'enregistrement détenu par les personnes en charge de la gestion des informations et supports classifiés à ce niveau, les traces du nombre et des destinataires des exemplaires papiers reproduits.

Pour les informations classifiées dématérialisées, ce suivi est assuré par les fonctions de traçabilité du système d'information prévues par la présente instruction.

La reproduction partielle est possible dans les mêmes conditions que la reproduction totale. Les extraits d'informations classifiées ainsi reproduits sont classifiés au même niveau que le document dont ils sont extraits, sauf si l'autorité émettrice les a expressément classifiés à un niveau inférieur ou ne les a pas classifiés (cf. 7.1.2.3 b)).

7.2.4.2 Au niveau *Très Secret*

La reproduction des informations papier et supports classifiés n'est possible qu'avec l'autorisation écrite préalable de l'autorité émettrice.

Le détenteur de l'information papier ou du support classifié qui souhaite en effectuer une reproduction adresse une demande motivée (cf. Annexe 39) à cette autorité *via* son bureau de protection du secret, en précisant le nombre d'exemplaires. Si l'autorité émettrice consent à la reproduction (cf. Annexe 40), elle porte mention de cette reproduction sur l'exemplaire en sa possession. Le bureau de protection du secret du détenteur assure l'enregistrement de cet(ces) exemplaire(s) et le fait prendre en compte par les personnes citées dans la demande.

En cas d'urgence et à titre exceptionnel, le détenteur peut s'affranchir de cette procédure à la condition de prendre les dispositions suivantes *via* son bureau de protection du secret :

- limiter au minimum indispensable le nombre de reproductions ;
- procéder au marquage réglementaire en attribuant à chaque exemplaire un numéro individuel composé de deux nombres fractionnaires, en numérateur le numéro d'ordre de la copie dans la série des reproductions et en dénominateur le nombre total de reproductions ;
- porter, sur l'exemplaire reproduit, la destination qui en est faite ou établir une liste séparée des destinataires ;
- rendre compte sans délai à l'autorité émettrice du nombre de reproductions, des numéros de reproduction et de la destination des exemplaires. L'autorité émettrice porte mention de cette reproduction sur l'exemplaire en sa possession.

Pour les informations classifiées dématérialisées, ce suivi est assuré par les fonctions de traçabilité du système d'information prévues par la présente instruction décrites au 6.6.4.

7.2.5 Gestion des éléments constitutifs d'un système d'information classifié

La sortie d'éléments constitutifs d'un système d'information classifié de la zone dans laquelle ils se trouvent est soumise à une autorisation de l'officier de sécurité des systèmes d'information identifiant clairement les équipements concernés et désignant nominativement les personnes autorisées à sortir ces éléments. Cette autorisation peut avoir un caractère ponctuel ou permanent.

7.3 DIFFUSION DES INFORMATIONS ET SUPPORTS CLASSIFIES

7.3.1 Envoi d'informations et supports classifiés

Avant toute diffusion d'informations ou supports classifiés, son auteur établit la liste des destinataires en s'assurant qu'ils sont habilités au niveau de classification requis. Si cette liste est sensible, elle n'est pas jointe aux informations et supports classifiés.

7.3.1.1 Transmission dématérialisée d'informations classifiées

La transmission d'informations classifiées ne peut être réalisée que depuis ou vers un système d'information classifié.

Le transfert d'une information classifiée au travers d'un réseau non classifié ou d'un niveau de classification inférieur s'effectue à l'aide de moyens de chiffrement agréés.

7.3.1.2 Expédition d'informations et supports classifiés

Les procédures d'expédition doivent :

- permettre de respecter des délais compatibles avec le degré d'urgence de la transmission ;
- permettre le suivi des informations ou des supports transmis ;
- garantir leur intégrité physique grâce à un conditionnement adapté.

Les autorités d'expédition sont :

- au niveau *Secret*, les personnes en charge de la gestion des informations et supports classifiés à ce niveau (cf. 7.2.1.1) ;
- au niveau *Très Secret*, le bureau de protection du secret (cf. 7.2.1.2).

Au niveau *Très Secret*, le nombre et le numéro des supports attribués à chaque destinataire ainsi que le numéro des exemplaires conservés par l'émetteur sont précisés dans la liste de diffusion (deux exemplaires au moins, dont un original destiné à terme aux archives).

Après marquage et enregistrement de chaque support, il est procédé aux opérations suivantes :

a) Conditionnement

L'envoi de supports classifiés se fait sous double enveloppe. Chaque enveloppe présente des garanties de solidité suffisantes pour garantir au maximum son intégrité physique :

- l'enveloppe extérieure : renforcée, elle 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 du support qu'elle contient ;
- l'enveloppe intérieure de sécurité : opaque, toilée ou armée, elle interdit l'ouverture ou la 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 de l'organisme dans lequel il est affecté.

b) 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. Il comporte trois feuillets détachables A, B et B' (cf. Annexe 41), signés par le responsable de l'autorité expéditrice ou une personne désignée par lui :

- les feuillets A et B sont placés dans l'enveloppe intérieure et sont adressés au destinataire (cf. 7.3.1) qui conserve le premier comme élément de preuve et renvoie le second à titre d'accusé de réception ;
- le feuillet B' est conservé par l'expéditeur jusqu'à réception du feuillet B qui lui est alors substitué.

L'expéditeur s'assure de la date et de l'heure de livraison. Il en avise aussitôt le service destinataire 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. Tout retard anormal doit conduire à suspecter une compromission. Le bureau de protection du secret ou le service destinataire met alors en œuvre les dispositions du 1.4.2.3.

7.3.2 Transport

7.3.2.1 Supports classifiés

a) Sur le territoire national, à l'intérieur d'un site ou d'une même emprise

Les supports classifiés sont transportés par le détenteur lui-même, par une personne habilitée au niveau requis ou un convoyeur autorisé de l'organisme détenteur ou une personne du service de courrier interne de cet organisme.

La position des supports classifiés doit être suivie sans discontinuité, notamment dans le système d'enregistrement des supports classifiés.

Une fiche de suivi, établie pour chaque support classifié au niveau *Très Secret*, permet d'en contrôler la position et est émarginée par chaque personne qualifiée y ayant accès. La fiche de suivi est conservée par le bureau de protection du secret dans les mêmes conditions que pour un support classifié au niveau *Très Secret*.

b) Sur le territoire national, avec changement de site ou d'emprise

Le transport s'opère :

- aux niveaux *Secret* et *Très Secret*, par un porteur, qui est :
 - soit une personne habilitée de l'organisme détenteur ou d'un autre organisme ministériel ou d'un organisme lié par contrat (cf. 4.4) ;

- soit une personne ayant la qualité de convoyeur autorisé. Le convoyeur autorisé est une personne physique appartenant à l'organisme détenteur, titulaire d'une décision de sécurité convoyeur (cf. Annexe 42) délivrée par l'autorité d'habilitation après réalisation, par l'autorité compétente, d'une enquête administrative (cf. Annexe 6). Conformément à la demande de l'autorité d'habilitation, cette décision est valide soit pour une mission particulière, soit pour une durée nécessairement inférieure à trois ans. Cette décision peut être renouvelée par une demande qui est nécessairement effectuée avant l'expiration du délai fixé. Cette décision n'autorise en aucun cas à prendre connaissance d'informations et supports classifiés.

Le porteur ne peut se dessaisir des informations et supports classifiés jusqu'à leur remise au destinataire, sauf dérogation exceptionnelle accordée par le ministre dont il relève après consultation du secrétaire général de la défense et de la sécurité nationale.

- au niveau *Secret* et par dérogation au niveau *Très Secret*, par voie postale :
 - au niveau *Secret*, le transport par voie postale est autorisé à la condition impérative de confier le transport à un opérateur postal autorisé conformément aux dispositions du code des postes et des communications électroniques¹¹⁷ ;
 - au niveau *Très Secret*, le transport par voie postale est en principe prohibé. Toutefois, à défaut de porteur disponible dans des délais compatibles avec le degré d'urgence de transmission, degré d'urgence qui doit pouvoir être clairement justifié, le transport par un opérateur postal autorisé peut être permis à titre exceptionnel.

Conformément aux dispositions du code des postes et des communications électroniques, pour pouvoir être autorisé à acheminer des supports protégés par le secret de la défense nationale, l'opérateur postal doit notamment répondre aux exigences énoncées ci-dessous¹¹⁸ :

- jouir d'un établissement sur le territoire national ;
- disposer 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 ;
- être en capacité de fournir à l'expéditeur un justificatif de livraison sur le registre de signature et de pointage ou un reçu portant les numéros de colis ;
- garantir que la livraison sera effectuée dans un délai maximal de 24 heures, ou avant une date et une heure données.

L'instruction ministérielle peut imposer des conditions plus restrictives que celles prévues ci-dessus.

Le transport des supports marqués *Spécial France* est réalisé par les bureaux courriers nationaux de l'opérateur postal et emprunte exclusivement des voies nationales. La mention *Spécial France* est indiquée sur l'enveloppe intérieure de sécurité.

¹¹⁷ Autorisation délivrée par l'autorité de régulation des communications électroniques et des postes (ARCEP), articles L. 36-5 et suivants et R. 1-2-1 et suivants du code des postes et des communications électroniques.

¹¹⁸ Article R. 1-2-6 du code des postes et des communications électroniques.

c) *Vers ou depuis l'étranger*

Les 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. Les supports classifiés marqués *Spécial France* ne peuvent sortir des frontières du territoire que par la valise diplomatique ou, en cas d'urgence, par lettre de courrier délivrée par le ministère des affaires étrangères.

Le transport peut s'opérer :

- par 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 assuré par un porteur selon les règles édictées par le ministère des affaires étrangères. À défaut, il y a lieu de prévoir des mesures particulières en fonction des instructions de ce ministère. 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 valise diplomatique ne doit ni être ouverte, ni retenue¹¹⁹.

Le porteur doit seulement présenter sa « lettre de courrier » et faire appel, en cas de besoin, à l'assistance de l'agent diplomatique ou consulaire le plus proche. Si toutefois les autorités compétentes de l'État d'accueil demandent que la valise soit ouverte en leur présence, le porteur est en droit d'opposer un refus et de repartir avec la valise vers l'État d'origine.

- par porteur muni d'un certificat de courrier : lorsqu'un accord ou un règlement international de sécurité le prévoit, le transport est possible par porteur, dans les conditions déterminées au point b). Le porteur est alors muni d'un certificat de courrier pour un seul ou plusieurs voyages (cf. Annexe 43 et Annexe 44), délivré par le secrétaire général de la défense et de la sécurité nationale, en sa qualité d'autorité nationale de sécurité ou, le cas échéant, par l'autorité de sécurité déléguée compétente. Il est rappelé au porteur 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.
- par voie postale, pour les supports classifiés au niveau *Secret* envoyés vers les pays de l'Union européenne ou de l'OTAN, à la condition impérative de confier le transport à un opérateur postal autorisé conformément aux exigences définies au point b). Il est fait usage du service prioritaire « recommandé international », sous réserve que l'instruction de sécurité du programme l'autorise. À défaut, il convient de se référer à ce document pour connaître les modalités d'envoi de ces supports classifiés.

Pour les informations échangées dans le cadre d'un accord ou d'un programme international, il convient de se référer aux stipulations de l'accord ou du plan contractuel de sécurité applicable.

¹¹⁹ Article 27 point 3 de la Convention de Vienne du 18 avril 1961 sur les relations diplomatiques.

7.3.2.2 Transport d'informations classifiées sur un support amovible

Par principe, les informations classifiées stockées sur un support amovible en vue de leur transport sont chiffrées.

Lorsqu'elles sont chiffrées aux moyens d'un produit ou d'un mécanisme de chiffrement agréé par l'agence nationale de la sécurité des systèmes d'information au niveau de classification des informations transportées, le support amovible peut être transporté sans mesure de sécurité complémentaire.

En l'absence de solution agréée au niveau de classification requis ou lorsqu'à titre exceptionnel le chiffrement est impossible, le support amovible est transporté conformément aux dispositions du paragraphe 7.3.2.1.

7.3.2.3 Matériels classifiés

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 du transport.

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 de l'instruction interministérielle n° 3100¹²⁰.

Pour les autres matériels 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 convoi 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. À défaut, ils sont convoyés et toutes les dispositions sont prises pour que la sécurité soit assurée sans discontinuité pendant toute la durée du transport. Avant tout transport de matériel classifié, un certificat de courrier (cf. Annexe 43 et Annexe 44) est établi pour le porteur. Un plan de transport peut être exigé par le secrétaire général de la défense et de la sécurité nationale, en sa qualité d'autorité nationale de sécurité ou, le cas échéant, par l'autorité de sécurité déléguée compétente, en fonction du poids ou des dimensions du matériel.

7.3.3 Réception

La réception est assurée par le destinataire de l'envoi au niveau *Secret* ou, au niveau *Très Secret*, par le bureau de protection du secret de l'organisme destinataire, suivant la procédure suivante :

- l'intégrité de l'emballage est vérifiée afin de déceler une éventuelle compromission ;
- le destinataire fait procéder à son enregistrement :

¹²⁰ 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 directive interministérielle n° 312/SGDN/ANS/DR du 21 août 1981 sur la sécurité nucléaire dans le domaine de la défense.

- au niveau *Secret*, auprès du service en charge de la gestion des informations et supports classifiés à ce niveau ;
- au niveau *Très Secret*, par le bureau de protection du secret ;
- pour le support physique, le feuillet B du bordereau d'envoi est daté, signé et renvoyé à titre d'accusé de réception. Le bureau de protection du secret remet le support classifié *Très Secret* au destinataire.

Ces règles s'appliquent à la réception, par voie physique, des informations et supports devant faire l'objet d'un enregistrement (cf. 7.2.2). Dans le cas d'une information classifiée dématérialisée, la réception est attestée par les fonctions de traçabilité du système d'information classifié prévues par la présente instruction.

Dans le cas d'un acheminement à l'étranger, le destinataire appose son visa sur la liste d'inventaire présentée par le porteur (cf. Annexe 43 et Annexe 44).

7.4 INVENTAIRE

7.4.1 Principes généraux

Tout support classifié, y compris les supports de stockage d'informations classifiées dématérialisées, fait l'objet d'un suivi permanent afin d'assurer sa traçabilité et sa prise en compte par des détenteurs habilités.

À cette fin, un inventaire est réalisé chaque année par chaque détenteur avant le 31 décembre et avant toute prise et fin de fonction, sous le contrôle de l'officier de sécurité.

À l'occasion de l'inventaire, chaque détenteur procède à l'examen rigoureux de la pertinence de la conservation des supports qu'il détient, ainsi que du maintien de la classification des informations et supports dont il est l'auteur.

L'inventaire des informations classifiées dématérialisées contenues au sein d'un système d'information classifié n'est pas obligatoire, leur suivi étant assuré par la traçabilité interne du système d'information renforcée par les exigences organisationnelles et logiques prévues par la présente instruction.

7.4.1.1 Destruction des exemplaires inutiles

Lorsque plusieurs copies d'un même support initial sont détenues :

- si l'original est détenu, seul l'original est conservé ;
- si seules des copies sont détenues, une seule copie est conservée.

Les autres copies sont détruites conformément aux dispositions du 7.5.1.

7.4.1.2 Réexamen de la pertinence de la classification et de son échéance

La pertinence de la classification d'une information ou d'un support classifié évolue dans le temps.

Chaque détenteur réévalue, à l'occasion de l'inventaire, la pertinence du niveau de classification des informations et supports classifiés dont il est l'auteur et procède, chaque fois que possible, à leur déclassification, ou, à tout le moins, à leur déclassement. Dans les cas, rares, où du fait de circonstances particulières une information ou un support classifié dont il est l'auteur a, depuis sa classification, gagné en sensibilité, le détenteur procède, le cas échéant, à son reclassement, conformément aux directives de classification inscrites dans l'instruction ministérielle dont il relève.

Lorsque le détenteur décide le maintien en classification d'informations et de supports dont il est l'auteur, il procède alors au réexamen de la pertinence de l'échéance de classification

(cf. 7.6.1) et la revoit à la baisse chaque fois que possible. Le cas échéant, le cartouche mentionnant l'échéance de classification (cf. Annexe 36) est barré d'un trait rouge, oblique de haut en bas, de gauche à droite, et un nouveau cartouche, indiquant la nouvelle échéance, est placé sous le cartouche barré.

Dès la mise en service de la base interministérielle des décisions de déclassification mentionnée au 7.6.2, chaque organisme détenteur vérifie, en outre, au moment de l'inventaire, si les supports qu'il détient ont fait l'objet d'une déclassification et procède, le cas échéant, à leur démarquage conformément à l'Annexe 38.

7.4.1.3 Appréciation de l'utilité administrative courante

Lors de l'inventaire, chaque détenteur identifie les informations et supports classifiés ne présentant plus d'utilité administrative courante et procède à leur destruction, après accord de l'administration des archives, ou à leur versement aux archives selon les modalités respectivement définies aux 7.5.1, 7.5.2 et 7.5.4.

7.4.1.4 Banalisation d'une période dédiée à l'inventaire

Afin de permettre aux détenteurs d'informations et supports classifiés de procéder à cet examen rigoureux, chaque responsable d'organisme arrête une période ouvrée dédiée à l'inventaire, au cours de laquelle les détenteurs sont déchargés de leurs missions habituelles.

De même, le responsable d'organisme accorde à chaque personne détenant des informations et supports classifiés quittant ses fonctions une période lui permettant de procéder à son inventaire.

L'inventaire précise, pour chaque support classifié, l'échéance de classification fixée par son auteur pour le compte de l'autorité émettrice.

Si l'inventaire fait mention de documents dont l'objet est classifié, il est lui-même classifié au niveau de classification le plus élevé des documents qu'il inventorie.

Chaque ministre précise dans son instruction ministérielle, les modalités d'inventaire et de suivi des informations et supports classifiés *Secret* et *Très Secret*, hors classifications spéciales, détenus par les organismes relevant de son champ d'attribution.

7.4.2 Inventaire au niveau *Secret*

Un inventaire annuel est effectué sous la responsabilité de chaque détenteur qui doit être en mesure de le présenter aux personnes en charge de la gestion des informations et supports classifiés et à l'officier de sécurité.

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.

7.4.3 Inventaire au niveau *Très Secret*

Un inventaire annuel est effectué par chaque détenteur en liaison avec le bureau de protection du secret. Le procès-verbal d'inventaire annuel mentionne les références et l'identification de chaque support classifié *Très Secret* et est accompagné, le cas échéant¹²¹, de l'une ou l'autre des pièces administratives suivantes :

- un bordereau de prise en compte ;
- un procès-verbal de destruction (cf. Annexe 45) ;

¹²¹ Ces pièces ne sont 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.

- une fiche de suivi du support (cf. 7.3.2.1 a)) ;
- un procès-verbal de versement au service public d'archives compétent.

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.

7.5 FIN D'EXPLOITATION DES INFORMATIONS ET SUPPORTS CLASSIFIES

Toute autorité détenant des informations et supports classifiés, produits ou reçus, a pour obligation de faire assurer leur conservation et leur protection conformément aux dispositions législatives et réglementaires en vigueur.

À l'expiration de leur période d'utilisation courante, les informations et supports classifiés font l'objet d'un tri, selon la périodicité prévue par chaque ministre, visant à séparer les supports destinés à être conservés de ceux dépourvus d'utilité administrative ou d'intérêt historique ou scientifique :

- les supports présentant une utilité administrative ou un intérêt historique ou scientifique sont versés aux services publics d'archives compétents¹²² ;
- les autres supports sont détruits selon les principes développés au paragraphe suivant.

7.5.1 Procédure de destruction

Lorsque des informations et supports classifiés sont périmés ou devenus inutiles, il peut être procédé à leur destruction avec l'accord de l'administration des archives¹²³. La destruction ne peut être réalisée que par des personnes habilitées ou sous leur surveillance.

La destruction 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, dont les normes techniques sont arrêtées par le secrétaire général de la défense et de la sécurité nationale après expertise des services compétents. 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 est dressé. Ce procès-verbal de destruction porte la signature du détenteur et, en sus pour les documents *Très Secret*, celle d'un témoin habilité au niveau *Très Secret* (cf. Annexe 45).

Au niveau *Très Secret*, le détenteur du support informe par écrit l'autorité émettrice que, sauf avis contraire de sa part, elle procédera à sa destruction. Sans réponse dans un délai de deux mois, le détenteur procède à la destruction du support et en rend compte à l'autorité émettrice en lui adressant une copie du procès-verbal de destruction¹²⁴. Une copie de ce procès-verbal est transmise au bureau de protection du secret.

7.5.2 Mise au rebut ou réaffectation sécurisée du matériel informatique classifié

Un support classifié ou ayant contenu des informations classifiées ne peut être affecté à un nouvel utilisateur ou à un nouveau besoin qu'après effacement sécurisé de l'ensemble des

¹²² Articles L. 212-2, L. 212-3, L. 212-4 et R. 212-1 et suivants du code du patrimoine.

¹²³ Articles L. 212-2 et L. 212-3 du code du patrimoine.

¹²⁴ 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 service du haut fonctionnaire de défense et de sécurité du ministère compétent.

informations et supports classifiés qu'il contient et reste classifié à un niveau au moins égal au niveau de classification des informations et supports classifiés qu'il a préalablement contenus.

En l'absence d'une telle procédure d'effacement sécurisé, le support classifié n'est pas réaffecté.

Tout support de stockage électronique classifié mis au rebut est préalablement effacé selon les recommandations de l'agence nationale de la sécurité des systèmes d'information. À défaut, il est détruit physiquement, selon un procédé conforme aux recommandations du secrétariat général de la défense et de la sécurité nationale, qui rend impossible la reconstitution de tout ou partie de l'information classifiée qu'il a contenue.

7.5.3 Évacuation 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 et supports classifiés, des plans d'évacuation et de destruction d'urgence sont établis par chaque service ou organisme qui détient des informations et supports classifiés. Ces plans prévoient notamment les procédures d'accès, en toute circonstance, aux locaux et aux informations et supports classifiés.

Les modalités d'exécution pratiques de ces plans figurent sur des fiches placées dans chaque coffre par les personnes détenant des éléments couverts par le secret de la défense nationale. Elles précisent :

- les autorités désignées pour donner l'ordre de destruction ou d'évacuation ;
- la liste des informations et 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.

La mise en œuvre du dispositif ainsi établi est contrôlée par l'officier de sécurité, selon une périodicité définie par chaque ministère pour les niveaux *Secret* et *Très Secret*, qui ne peut excéder trois ans.

7.5.4 Versement aux archives

7.5.4.1 Préparation du versement par le service versant

a) Examen systématique de la pertinence de la classification par le service versant

- i. le service versant est l'auteur de l'information classifiée

Avant tout versement aux archives, le service versant s'assure que la classification, lorsqu'elle est toujours effective (cf. 7.6.3.1), demeure pertinente et procède, chaque fois que possible, à sa déclassification selon les modalités prévues au 7.6.3.2. Lorsqu'après examen, il s'avère que la déclassification n'est pas possible, le support est traité selon les modalités décrites dans les paragraphes suivants.

- ii. le service versant n'est pas l'auteur de l'information classifiée

Dans l'attente de la mise en service de la base interministérielle des décisions de déclassification mentionnée au. 7.6.3.5, le support est traité selon les modalités décrites au paragraphe 7.5.4.2.

Dès la mise en service de la base interministérielle des décisions de déclassification mentionnée au. 7.6.3.5, le service versant la consulte afin de vérifier si l'information ou le support est toujours classifié.

Dans le cas où l'information ou le support a fait l'objet d'une décision de déclassification, le service versant appose le timbre de déclassification conformément à l'Annexe 38.

Dans le cas où l'information ou le support n'a pas fait l'objet d'une décision de déclassification, lorsque le service versant est distinct du service ayant procédé à la classification, le support est traité selon les modalités décrites au paragraphe 7.5.4.2.

b) Identification et regroupement des supports classifiés

Avant chaque versement au service d'archives compétent, chaque support classifié contenu dans un dossier se voit attribuer un numéro d'ordre et fait l'objet d'un inventaire précisant, conformément à l'Annexe 46, la cote d'archives, le nom du service ayant procédé à la classification ou de l'auteur du support classifié, son numéro d'enregistrement, sa date d'émission, son titre ou objet, son niveau de classification et l'échéance de la classification. Ces supports et l'inventaire qui les décrits sont réunis, selon le niveau de classification et le volume représenté, dans une enveloppe scellée conforme à l'Annexe 46, rangée en tête du dossier auquel ils appartiennent, ou dans des articles clairement séparés des articles non classifiés de manière à faciliter leur protection au sein du service d'archives détenteur.

Les services publics d'archives compétents se chargent ensuite de porter sur chaque article matériel (carton, enveloppe ou dossier) sa référence archivistique (« cote »).

7.5.4.2 Versement et conservation aux services publics d'archives compétents

a) Responsabilité du service public d'archives compétent

Lorsque des informations ou supports classifiés sont versés au service public d'archives compétent, la responsabilité de leur protection incombe à ce dernier. Le ministère de tutelle (culture, défense, affaires étrangères) s'assure de la conformité aux exigences de la présente instruction des conditions de conservation des informations et supports classifiés.

Les services publics d'archives compétents peuvent recevoir des informations et supports classifiés jusqu'au niveau *Très Secret* hors classifications spéciales. Les informations et supports classifiés au niveau *Très Secret* faisant l'objet d'une classification spéciale ne peuvent être versés aux archives qu'après une procédure, obligatoire et préalable, de déassement ou de déclassification.

b) Conservation des informations et supports classifiés

Les supports classifiés versés aux services publics d'archives compétents sont conservés dans l'enveloppe scellée rangée en tête du dossier auquel ils appartiennent ou dans des articles clairement séparés et identifiés conservés dans les conditions de sécurité définies au chapitre 5, et comme prévu au 7.5.4.1 b). L'ensemble est conservé conformément aux exigences détaillées au chapitre 7.

7.5.5 Accès aux informations et supports ayant fait l'objet d'une mesure de classification versés dans un service public d'archives

Les dispositions qui suivent s'appliquent conformément à la volonté du Gouvernement et du législateur de garantir l'accès le plus large et le plus précoce possible aux archives publiques, dans le respect de l'impératif de sauvegarde des intérêts fondamentaux de la Nation.

7.5.5.1 Accès aux informations et supports ayant fait l'objet d'une mesure de classification devenus communicables de plein droit

Les informations et supports comportant un timbre de classification matérialisant une mesure de classification au sens de l'article 413-9 du code pénal sont automatiquement déclassifiés, sans qu'une décision formelle de déclassification (matérialisée par l'apposition d'un timbre de déclassification) ne soit nécessaire, dès lors qu'ils deviennent communicables de plein droit

en application de l'article L. 213-2 du code du patrimoine. Ils peuvent alors être librement communiqués.

Par exception, les mesures de classification dont font l'objet, le cas échéant, les documents mentionnés au 4° du I de l'article L. 213-2 du code du patrimoine, et notamment les documents relatifs aux enquêtes réalisées par les services de la police judiciaire et aux affaires portées devant les juridictions, prennent automatiquement fin dès l'expiration des délais prévus au 3° du I du même article L. 213-2 du code du patrimoine.

Dans la grande majorité des cas, la déclassification automatique intervient donc dans un délai de cinquante ans. Ce délai est, dans certains cas, porté à cent ans¹²⁵.

7.5.5.2 Accès aux informations et supports ayant fait l'objet d'une mesure de classification devenue caduque du fait de l'échéance de la date mentionnée dans leur timbre ou ayant fait l'objet d'une décision formelle de déclassification

Les informations et supports ayant fait l'objet d'une mesure de classification et qui, conformément aux dispositions de la présente instruction, comportent une date d'échéance de classification, sont automatiquement déclassifiés à cette date.

La déclassification à date d'une information ou d'un support ou après décision formelle ne signifie pas pour autant que cette information ou ce support devient librement communicable (cf. 7.6.3.7). Des délais de communicabilité définis par le code du patrimoine (article L. 213-2) peuvent en effet s'appliquer. Ainsi, le service public d'archives qui le détient s'assure qu'aucun autre motif d'incommunicabilité ne s'applique en vertu de l'article L. 213-2 du code du patrimoine, avant d'en permettre l'accès. Si un autre motif d'incommunicabilité s'applique, la demande est instruite conformément aux dispositions des articles L. 213-3 et L. 213-4 du code du patrimoine.

7.5.5.3 Accès aux informations et supports ayant fait l'objet d'une mesure de classification toujours effective

Est classifié toute information ou tout support ayant fait l'objet d'une mesure de classification mentionnée à l'article 413-9 du code pénal et qui n'a fait l'objet d'aucune mesure de déclassification formelle (cf. 7.6.3.2) ni automatique (cf. 7.6.3.1).

Seule une personne habilitée et qui dispose du besoin d'en connaître pour l'exercice de sa fonction ou l'accomplissement de sa mission peut accéder à une information ou à un support classifié détenu par un service public d'archives. Elle doit, pour ce faire, obtenir préalablement une autorisation de consultation anticipée par dérogation aux délais de communicabilité des archives publiques, conformément aux articles L. 213-3 et L. 213-4 du code du patrimoine. Cette autorisation peut être assortie de conditions spécifiques. Une telle autorisation n'est pas nécessaire pour les représentants de l'autorité dont émanent les documents, les agents des services des archives concernés et les représentants de leur autorité de tutelle.

Lorsqu'une personne habilitée mais ne disposant pas du besoin d'en connaître pour l'exercice de sa fonction ou l'accomplissement de sa mission, ou bien lorsqu'une personne non habilitée souhaite accéder à une information ou un support classifié détenu par un service public d'archives, sa demande est instruite selon la procédure définie au 1.2.3.

¹²⁵ Cf. article 5° du I de l'article L. 213-2 du code du patrimoine.

7.5.5.4 Incommunicabilité perpétuelle des informations et supports classifiés dont la communication est susceptible d'entraîner la diffusion d'informations permettant de concevoir, fabriquer, utiliser ou localiser des armes nucléaires, radiologiques, biologiques, chimiques ou toutes autres armes ayant des effets directs ou indirects de destruction d'un niveau analogue

Conformément au II. de l'article L. 213-2 du code du patrimoine, les informations et supports classifiés dont la communication est susceptible d'entraîner la diffusion d'informations permettant de concevoir, fabriquer, utiliser ou localiser des armes nucléaires, radiologiques, biologiques, chimiques ou toutes autres armes ayant des effets directs ou indirects de destruction d'un niveau analogue ne peuvent être communiqués ni ne peuvent, conformément au 7.6.1, être déclassifiés.

7.6 EXPIRATION DE LA CLASSIFICATION

7.6.1 Mention d'échéance de la classification

La sensibilité d'une information ou d'un support classifié évolue en fonction du temps ou des circonstances.

La protection qui lui est accordée initialement peut ainsi être réévaluée soit dans le sens d'un renforcement (reclassement au niveau supérieur), soit, dans la majorité des cas, dans le sens d'un abaissement prenant la forme d'un déclasserement ou d'une déclassification. De même, une information ou un support non protégé peut être classifié postérieurement à son émission si l'évolution de sa sensibilité au regard de la défense et de la sécurité nationale l'exige.

Afin de garantir le caractère dérogatoire du recours au secret de la défense nationale et de limiter les lourdeurs liées à la gestion des informations classifiées, l'auteur de l'information classifiée, apprécie, sous la responsabilité de l'autorité émettrice et selon les directives qu'elle a fixées dans son instruction ministérielle, la durée utile de classification.

Ainsi, l'auteur de l'information procède simultanément à deux opérations juridiques distinctes : la classification, qu'il matérialise par l'apposition d'un timbre de classification, et la déclassification à une date d'entrée en vigueur différée, qu'il matérialise par l'apposition d'une date d'échéance valant timbre de déclassification. Cette date est antérieure à l'échéance du délai de cinquante ans généralement prévu pour sa communicabilité et, pour faciliter l'accès des chercheurs aux archives publiques, lui est même largement antérieure dans la très grande majorité des cas. Pour autant, l'autorité émettrice conserve la possibilité à tout moment de rabaisser (cf. 7.4.1.2) ou, sous réserve des dispositions de l'article L. 213-2 du code du patrimoine, de prolonger le délai fixé, sous sa responsabilité, par l'auteur de l'information classifiée, ainsi que la possibilité de déclasser ou reclasser le support.

Lorsqu'à titre exceptionnel, notamment, le cas échéant, pour les documents visés aux points a) à e) du 3° du I. de l'article L. 213-2 du code du patrimoine, aucune date entraînant automatiquement la déclassification du support ne peut être déterminée, l'auteur de l'information classifiée indique la date ou le délai au terme duquel, en sus des réexamens annuels mentionnés au 7.4.1.2, le niveau de classification doit impérativement être réévalué. Cette date ou ce délai n'excède pas vingt ans à compter de la date de production du support.

Par dérogation aux dispositions précédentes, les informations classifiées dont la divulgation est susceptible d'entraîner la diffusion d'informations permettant de concevoir, fabriquer, utiliser ou localiser des armes nucléaires, radiologiques, biologiques, chimiques ou toutes autres armes ayant des effets directs ou indirects de niveau analogue ne comportent aucune échéance de classification et ne peuvent être déclassifiées.

7.6.2 Réexamen de la classification des informations et supports classifiés détenus par les services publics d'archives

Afin de faciliter l'accès aux archives publiques, le comité interministériel aux Archives de France, sur proposition des administrations des archives, identifie, parmi les ensembles d'archives versées et comportant un volume important de documents ayant fait l'objet d'une mesure de classification toujours effective (cf. 7.5.5.3), ceux qui sont fréquemment sollicités ou sont susceptibles de l'être, ou qui présentent un intérêt particulier pour la recherche historique ou scientifique. Il en fait rapport aux autorités émettrices compétentes, afin qu'elles puissent apprécier la pertinence du maintien de la classification des documents considérés et que soit, le cas échéant, entreprise, selon les modalités définies au 7.6.3.2, une déclassification anticipée et homogène de l'ensemble considéré, par exemple dans le contexte d'une décision d'ouverture anticipée de fonds d'archives publiques intégrant ces ensembles, décidée en application du II de l'article L. 213-3 du code du patrimoine.

Un point d'étape des déclassifications décidées dans ce cadre est réalisé à chaque réunion du comité.

Ces réunions du comité interministériel aux Archives de France en formation spécialisée sont également l'occasion pour les administrations des archives d'établir un bilan de la mise en œuvre des dispositions des points a) à e) du 3° du I. de l'article L. 213-2 du code du patrimoine et du traitement des demandes de consultation anticipée des documents entrant dans leur champ.

Les activités du comité interministériel aux Archives de France en formation spécialisée font l'objet d'un rapport annuel au Premier ministre

7.6.3 Procédure de déclassification

7.6.3.1 Déclassification automatique

Pour les informations et supports qui, conformément aux dispositions de la présente instruction, comportent une date d'échéance de classification, la déclassification intervient automatiquement à cette date, sans qu'une décision formelle de déclassification (matérialisée par l'apposition d'un timbre de déclassification) ne soit nécessaire.

De même, les informations et supports comportant un timbre de classification matérialisant une mesure de classification au sens de l'article 413-9 du code pénal sont automatiquement déclassifiés, sans qu'une décision formelle de déclassification (matérialisée par l'apposition d'un timbre de déclassification) ne soit nécessaire, dès lors qu'ils sont devenus communicables de plein droit en application de l'article L. 213-2 du code du patrimoine (cf. 7.5.5.1).

7.6.3.2 Déclassification nécessitant une décision formelle matérialisée par un timbre de déclassification

Les dispositions qui suivent s'appliquent aux seuls informations et supports classifiés qui ne comportent pas d'échéance de classification et pour lesquels les délais de communicabilité prévus à l'article L. 213-2 du code du patrimoine ne sont pas échus et qui ne peuvent, en conséquence, être déclassifiés qu'après une décision formelle de déclassification, matérialisée sur le document par l'apposition d'un timbre de déclassification.

7.6.3.3 Organisation de la fonction de déclassification

Conformément à l'article R. 2311-4 du code de la défense : « *Toute modification du niveau de classification, déclassification, modification ou suppression d'une mention particulière de protection d'une information ou d'un support classifié est décidée par l'autorité sous la responsabilité de laquelle il a été procédé à la classification.* ».

Ainsi, lorsque le support classifié ne comporte pas dans son timbre de classification de date à partir de laquelle il est automatiquement déclassifié – cas général pour les supports classifiés préalablement à l'entrée en vigueur de la présente instruction et cas dérogatoire et exceptionnel pour les supports classifiés après cette entrée en vigueur (cf. 7.6.1) – et que les délais de communicabilité prévus à l'article L. 213-2 du code du patrimoine ne sont pas échus, seule l'autorité émettrice (cf. 1.4) peut décider de reclasser, déclasser ou déclassifier le support.

Pour autant, chaque ministre peut, pour les informations et supports dont il est autorité émettrice, organiser dans son champ d'attribution, la fonction de déclassification comme il le souhaite et décider, s'il l'estime pertinent, de la centraliser, sans qu'il soit nécessaire de consulter, préalablement à l'adoption de la décision de déclassification, le service auteur ayant procédé à son marquage, ni, le cas échéant, le service successeur.

7.6.3.4 Matérialisation de la décision de déclassification sur le support classifié

Pour que la décision de déclassification des informations et supports classifiés, qui ne mentionnent pas dans leur timbre de classification de date à partir de laquelle ils sont automatiquement déclassifiés, produise pleinement ses effets et permette leur manipulation sans risque de compromission, elle doit être matérialisée sur le support par l'apposition d'un timbre de déclassification qui précise la date et la référence de la décision de déclassification, conformément au modèle de l'Annexe 38. Cette opération est appelée « démarquage ».

7.6.3.5 Information des destinataires et consignation des décisions de déclassification

L'autorité émettrice informe de sa décision de déclassification les destinataires à qui elle a transmis les informations et supports objet de la décision, afin qu'ils procèdent à leur démarquage.

En outre, le secrétariat général de la défense et de la sécurité nationale œuvre à la mise en place d'une base interministérielle regroupant les fac-similés des décisions de déclassification, afin de permettre à toute administration détenant des informations et supports classifiés de s'assurer qu'elle ne détient pas de support improprement marqué alors que l'information qu'il contient a fait l'objet d'une décision de déclassification et de permettre à tout citoyen d'accéder sans entrave aux supports déclassifiés, sous réserve des règles de communicabilité par ailleurs applicables (cf. 7.6.3.7). Cette base de données comprend toutes les décisions de déclassification émises à compter de sa mise en service. Afin de renforcer sa complétude, elle est progressivement complétée des décisions antérieures.

7.6.3.6 Déclassification des informations et supports classifiés d'origine étrangère

Pour les informations et supports classifiés d'origine étrangère, seule l'autorité étrangère émettrice peut procéder à leur déclassification ou leur déclassement. Le service du haut fonctionnaire de défense et de sécurité saisit le secrétariat général de la défense et de la sécurité nationale, en sa qualité d'autorité nationale de sécurité, afin d'obtenir des informations sur la procédure d'accès à de tels documents.

7.6.3.7 Règles de communication des documents déclassifiés

La déclassification formelle ou automatique d'un document ne le rend pas nécessairement communicable. En effet, d'autres motifs d'incommunicabilité prévus à l'article L. 311-5 du code des relations entre le public et l'administration et/ou d'autres délais de communicabilité au titre de l'article L. 213-2 du code du patrimoine peuvent s'appliquer.

Ainsi, lorsque le service détenteur d'un document déclassifié est saisi d'une demande de communication, il s'assure de sa communicabilité au regard des règles de l'article L. 311-5 du

code des relations entre le public et l'administration et L. 213-2 du code du patrimoine et instruit la demande en conséquence.

LISTE DES ANNEXES

ANNEXE 1 – REGLES DE PROTECTION DES INFORMATIONS ET SUPPORTS PORTANT LA MENTION <i>DIFFUSION RESTREINTE</i>	132
ANNEXE 2 – STRUCTURE ET PILOTAGE DE LA PROTECTION DU SECRET DE LA DEFENSE NATIONALE	134
ANNEXE 3 – RECOMMANDATIONS POUR L’ELABORATION DE L’INSTRUCTION MINISTERIELLE	135
ANNEXE 4 – HIERARCHIE DES NORMES RELATIVES A LA PROTECTION DU SECRET DE LA DEFENSE NATIONALE	136
ANNEXE 5 – SCHEMA PRESENTANT LA PROCEDURE D’HABILITATION AU SECRET DE LA DEFENSE NATIONALE D’UN RESSORTISSANT FRANÇAIS TRAVAILLANT EN FRANCE	137
ANNEXE 6 – MODELE DE DEMANDE D’ENQUETE ADMINISTRATIVE	138
ANNEXE 7 – MODELE DE DOSSIER DE DEMANDE D’HABILITATION D’UNE PERSONNE PHYSIQUE.....	139
ANNEXE 8 – MODELE DE DECISION D’HABILITATION D’UNE PERSONNE PHYSIQUE	150
ANNEXE 9 – MODELE D’ATTESTATION DE MISE EN GARDE.....	151
ANNEXE 10 – MODELE D’ATTESTATION DE MISE EN EVEIL	152
ANNEXE 11 – MODELE D’ENGAGEMENT DE RESPONSABILITE	153
ANNEXE 12 – MODELE DE DECISION DE REFUS D’HABILITATION OU D’ABROGATION D’UNE DECISION D’HABILITATION	154
ANNEXE 13 – MODELE DE RECEPISSE DE NOTIFICATION D’UNE DECISION DE REFUS D’HABILITATION OU D’ABROGATION D’UNE DECISION D’HABILITATION	155
ANNEXE 14 – MODELE DE CERTIFICAT DE SECURITE.....	156
ANNEXE 15 – MODELE D’ATTESTATION D’AVIS DE SECURITE	157
ANNEXE 16 – RECAPITULATIF DES OBLIGATIONS DES PERSONNES MORALES AYANT ACCES AU SECRET DE LA DEFENSE NATIONALE	158
ANNEXE 17 – CLAUSES-TYPES GENERALES CONTRACTUELLES DE PROTECTION DU SECRET DE LA DEFENSE NATIONALE A INSERER DANS LES CONVENTIONS ET LES CONTRATS	160
ANNEXE 18 – SCHEMA PRESENTANT LA PROCEDURE D’HABILITATION D’UNE PERSONNE MORALE FRANÇAISE.....	162
ANNEXE 19 – MODELE DE DESIGNATION D’UN OFFICIER DE SECURITE	163
ANNEXE 20 – MODELE DE DOSSIER DE DEMANDE D’HABILITATION D’UNE PERSONNE MORALE	164
ANNEXE 21 – MODELE D’ATTESTATION D’AVIS DE SECURITE D’UNE PERSONNE MORALE	172
ANNEXE 22 – MODELE D’ATTESTATION D’HABILITATION D’UNE PERSONNE MORALE	173
ANNEXE 23 – MODELE DE DECISION D’HABILITATION D’UNE PERSONNE MORALE	174
ANNEXE 24 – MODELE DE DECISION DE REFUS D’HABILITATION OU D’ABROGATION D’UNE DECISION D’HABILITATION D’UNE PERSONNE MORALE.....	175
ANNEXE 25 – MODELE DE RECEPISSE DE NOTIFICATION D’UNE DECISION DE REFUS D’HABILITATION OU D’ABROGATION D’UNE DECISION D’HABILITATION D’UNE PERSONNE MORALE	176
ANNEXE 26 – MODELE D’ATTESTATION DE CONFORMITE PHYSIQUE.....	177
ANNEXE 27 – MODELE DE CERTIFICAT DE MISE AUX NORMES DE SECURITE PHYSIQUE.....	178
ANNEXE 28 – PRESCRIPTIONS RELATIVES AUX PLANS CONTRACTUELS DE SECURITE, AUX PLANS DE SECURITE D’OPERATEURS ET AUX PLANS PARTICULIERS DE PROTECTION.....	179
ANNEXE 29 – TYPES DE MESURES DE PROTECTION PHYSIQUE	180
ANNEXE 30 – PROTECTION PHYSIQUE DES INFORMATIONS ET SUPPORTS CLASSIFIES : METHODE ET RECOMMANDATIONS ..	181
ANNEXE 31 – CONTROLE D’ACCES	191
ANNEXE 32 – MESURES APPLICABLES AUX ZONES RESERVEES	192
ANNEXE 33 – CLAUSES-TYPES CONTRACTUELLES DE PROTECTION DU SECRET DE LA DEFENSE NATIONALE POUR LES CONTRATS SENSIBLES	194
ANNEXE 34 – MODELE DE FICHE NAVETTE	195
ANNEXE 35 – GUIDE DES MESURES DE SECURITE APPLICABLES AU COURS D’UNE REUNION IMPLIQUANT DES INFORMATIONS ET SUPPORTS CLASSIFIES.....	196
ANNEXE 36 – EXEMPLE DE DOCUMENT CLASSIFIE.....	198
ANNEXE 37 – MODELES DE TIMBRES DE CLASSIFICATION ET DE PROTECTION	199
ANNEXE 38 – MODELES DE TIMBRES DE DECLASSEMENT ET DE DECLASSIFICATION.....	200
ANNEXE 39 – MODELE DE DEMANDE DE REPRODUCTION D’UN SUPPORT CLASSIFIE <i>TRES SECRET</i>	201
ANNEXE 40 – MODELE D’AUTORISATION DE REPRODUCTION D’UN SUPPORT CLASSIFIE <i>TRES SECRET</i>	202
ANNEXE 41 – MODELE DE BORDEREAU DE TRANSMISSION DE SUPPORTS CLASSIFIES	203
ANNEXE 42 – MODELE DE DECISION DE SECURITE CONVOYEUR	206
ANNEXE 43 – MODELE DE CERTIFICAT DE COURRIER	207
ANNEXE 44 – MODELE DE CERTIFICAT DE COURRIER MULTI-VOYAGES	216
ANNEXE 45 – MODELE DE PROCES-VERBAL DE DESTRUCTION DE SUPPORTS CLASSIFIES <i>SECRET</i> OU <i>TRES SECRET</i>	224
ANNEXE 46 – MODELE D’INVENTAIRE DES SUPPORTS CLASSIFIES.....	225

Annexe 1 – Règles de protection des informations et supports portant la mention *Diffusion Restreinte*

Comme rappelé au paragraphe 1.3.2 de la présente instruction, 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 et supports couverts par cette mention.

1. Condition d'emploi de la mention *Diffusion Restreinte*

Il appartient au Premier ministre et aux ministres de fixer les directives permettant de considérer que la diffusion d'une information doit être restreinte et d'identifier les organismes autorisés à apposer la mention de protection *Diffusion Restreinte*.

Ainsi, sous l'autorité de chaque ministre, sont autorisés à apposer sur des informations et supports la mention *Diffusion Restreinte* et à y accéder :

- les services centraux, services déconcentrés et services à compétence nationale relevant de son autorité ;
- les établissements publics placés sous sa tutelle ;
- les opérateurs d'importance vitale dont il est le ministre coordonnateur ;
- les collectivités territoriales et les personnes morales de droit privé avec lesquelles il a conclu une convention ;
- les personnes morales, publiques ou privées, avec lesquelles il a conclu un contrat de commande publique ou un contrat de subvention, ainsi que les sous-traitants ou sous-contractants de ces personnes morales ayant également besoin d'accéder à des informations ou supports protégés par la mention *Diffusion Restreinte* pour l'exécution de travaux réalisés en appui du contrat principal ;
- les personnels qui, au sein de ces différents organismes, ont besoin, pour l'exercice de leur fonction ou l'accomplissement de leur mission, d'accéder à des informations ou supports protégés par la mention *Diffusion Restreinte*.

Il revient à tout signataire d'un document émis pour le compte de l'une des autorités précitées d'apprécier, dans le respect des directives du Premier ministre et du ministre compétent, la sensibilité des informations qu'il contient et notamment d'apprécier si elles sont susceptibles de comporter des éléments dont la consultation ou la communication porterait atteinte à l'un des secrets, autres que le secret de la défense nationale, mentionnés au 2° de l'article L. 311-5 du code des relations entre le public et l'administration, et de décider, en conséquence, de l'opportunité d'y apposer la mention *Diffusion Restreinte*.

Il est recommandé de faire signer aux personnes susceptibles d'avoir accès à des informations *Diffusion Restreinte* un engagement de non-divulgateion.

L'utilisation de la mention complémentaire de protection *Spécial France*, en sus de la mention *Diffusion Restreinte*, reste soumise aux dispositions de la présente instruction.

2. Élaboration, marquage et enregistrement

L'élaboration des documents *Diffusion Restreinte* ne peut être effectuée que dans les lieux offrant des conditions de sécurité suffisantes interdisant l'accès de personnes non autorisées à ces documents.

Les documents *Diffusion Restreinte* sont identifiés sur la première page avec les références de l'autorité émettrice ou de l'organisme auteur, la date d'émission et le numéro d'enregistrement. Ils portent le marquage suivant :

DIFFUSION RESTREINTE

- sur chaque page, le timbre *Diffusion Restreinte* est apposé au milieu du haut de la page ;
- pour les messages et autres documents électroniques, la mention *Diffusion Restreinte* est rappelée en début de chaque page ;
- pour les documents reliés, le timbre *Diffusion Restreinte* est apposé au milieu de la page de garde et de la couverture ;
- sur un support non papier, la mention *Diffusion Restreinte* est adaptée au type de support, définitive et toujours visible.

Les documents *Diffusion Restreinte* sont enregistrés au départ et à l'arrivée.

3. Conservation, reproduction et destruction

Les documents *Diffusion Restreinte* doivent être conservés dans des meubles fermant à clef.

Leur reproduction doit rester limitée aux seuls besoins du service.

Leur destruction irréversible a lieu sous la responsabilité des détenteurs, sans mention particulière sur les documents d'enregistrement du courrier.

4. Diffusion

La diffusion interne de documents *Diffusion Restreinte* peut être effectuée :

- à l'intérieur :
 - d'un local, d'un bâtiment ou d'une emprise relevant d'un ministère, par toute personne de ce ministère ;
 - d'un organisme public ou privé dans le cadre d'un contrat de la commande publique, d'un contrat de sous-traitance ou d'un sous-contrat à un contrat de la commande publique, d'un contrat de subvention ou d'une convention, ou dans la cadre d'un plan contractuel de sécurité, d'un plan de sécurité d'opérateur ou d'un plan particulier de protection, sous enveloppe ou par personne désignée par le responsable d'organisme ;
- 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 en France métropolitaine, vers les départements, les collectivités territoriales ou vers l'étranger, par un moyen garantissant leur bonne réception de leur acheminement.

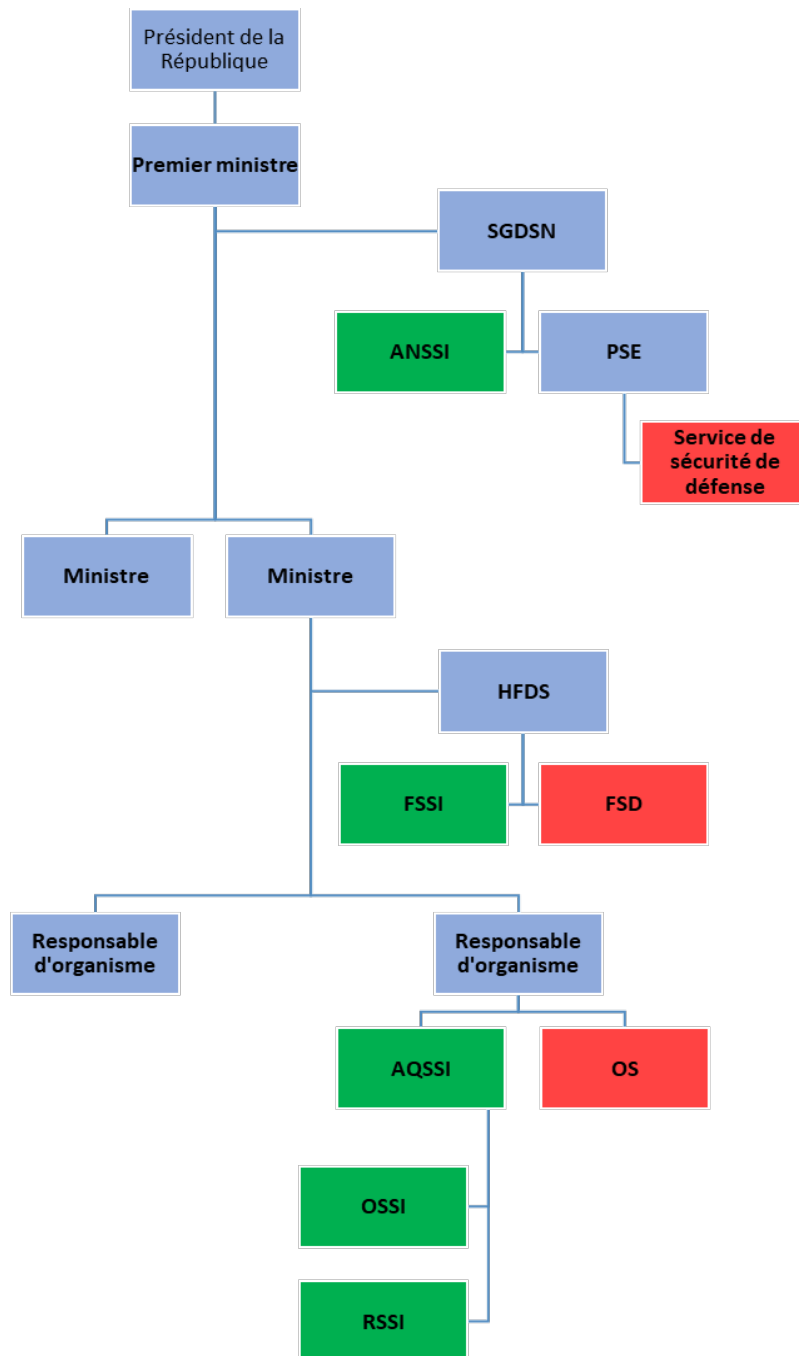
La transmission d'informations *Diffusion Restreinte* est interdite sur le réseau Internet ou sur tout autre système d'information non homologué *Diffusion Restreinte*, sauf à faire l'objet de mesures de protection particulières conformément à l'instruction interministérielle n° 901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles.

5. 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. L'instruction interministérielle n° 901/SGDSN/ANSSI précitée définit les règles applicables à ces systèmes d'information.

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 spécifique au *Diffusion Restreinte*. Ces cas exceptionnels sont notifiés au fonctionnaire de sécurité des systèmes d'information du service du haut fonctionnaire de défense et de sécurité du ministère concerné.

Annexe 2 – Structure et pilotage de la protection du secret de la défense nationale



Chaîne de protection du secret

Chaîne de sécurité des systèmes d'information

Annexe 3 – Recommandations pour l'élaboration de l'instruction ministérielle

Par délégation du Premier ministre, chaque ministre est responsable de la protection du secret de la défense nationale dans son champ d'attribution, y compris pour les informations et supports classifiés étrangers confiés à la France en vertu d'un accord général ou spécifique de sécurité régulièrement approuvé et publié.

Pour organiser cette protection, conformément à l'article R. 2311-6 du code de la défense, chaque ministre précise, dans une instruction approuvée par arrêté, les modalités de classification et de protection des informations et supports classifiés aux niveaux *Secret* et *Très Secret*, ainsi que des informations et supports classifiés étrangers échangés ou détenus en vertu d'un accord général ou spécifique de sécurité par les organismes relevant de son champ d'attribution.

Chaque ministre peut, par ailleurs, en complément de l'instruction ministérielle et sur son fondement, élaborer des directives techniques particulières destinées à préciser, pour un domaine d'activité spécifique, les mesures de protection du secret complémentaires à mettre en œuvre. Chaque directive particulière contient un guide de classification spécifique au domaine considéré permettant à chaque organisme d'évaluer le niveau de classification des informations et supports qu'il produit et d'en déduire les mesures d'organisation et de protection à mettre en œuvre (cf. chapitre 2).

Par souci de lisibilité et par suite de clarté juridique, il est recommandé que l'instruction ministérielle, qui constitue une déclinaison de la présente instruction, en reprenne, la structure d'ensemble.

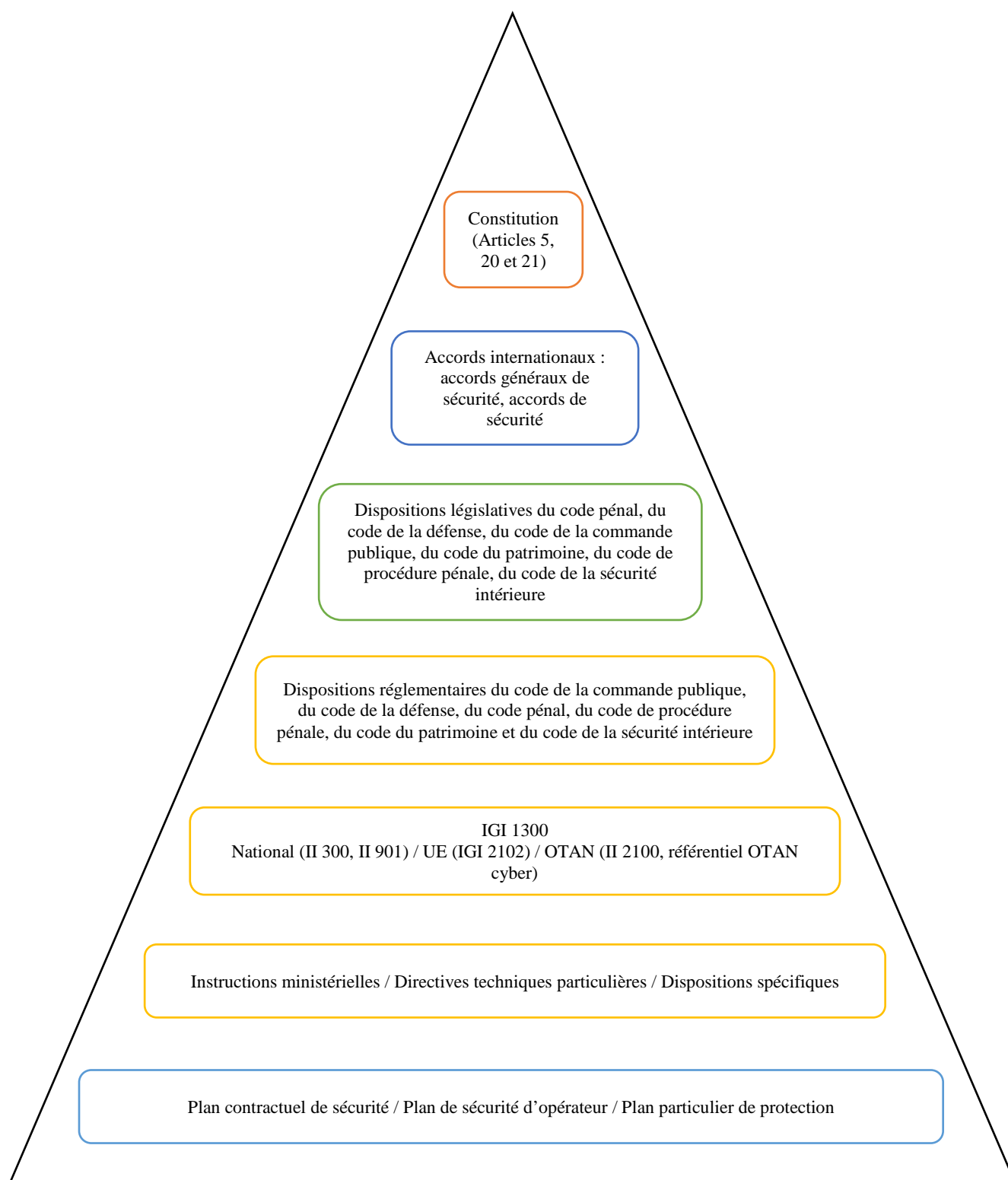
Il est également recommandé d'éviter de réécrire les dispositions de la présente instruction et d'opérer autant que possible par renvoi, afin que l'instruction ministérielle se concentre sur les mesures d'adaptation nécessaire à la spécificité ministérielle.

Sous réserve du respect de la hiérarchie des normes, l'instruction ministérielle peut être plus restrictive que la présente instruction, sans s'y opposer.

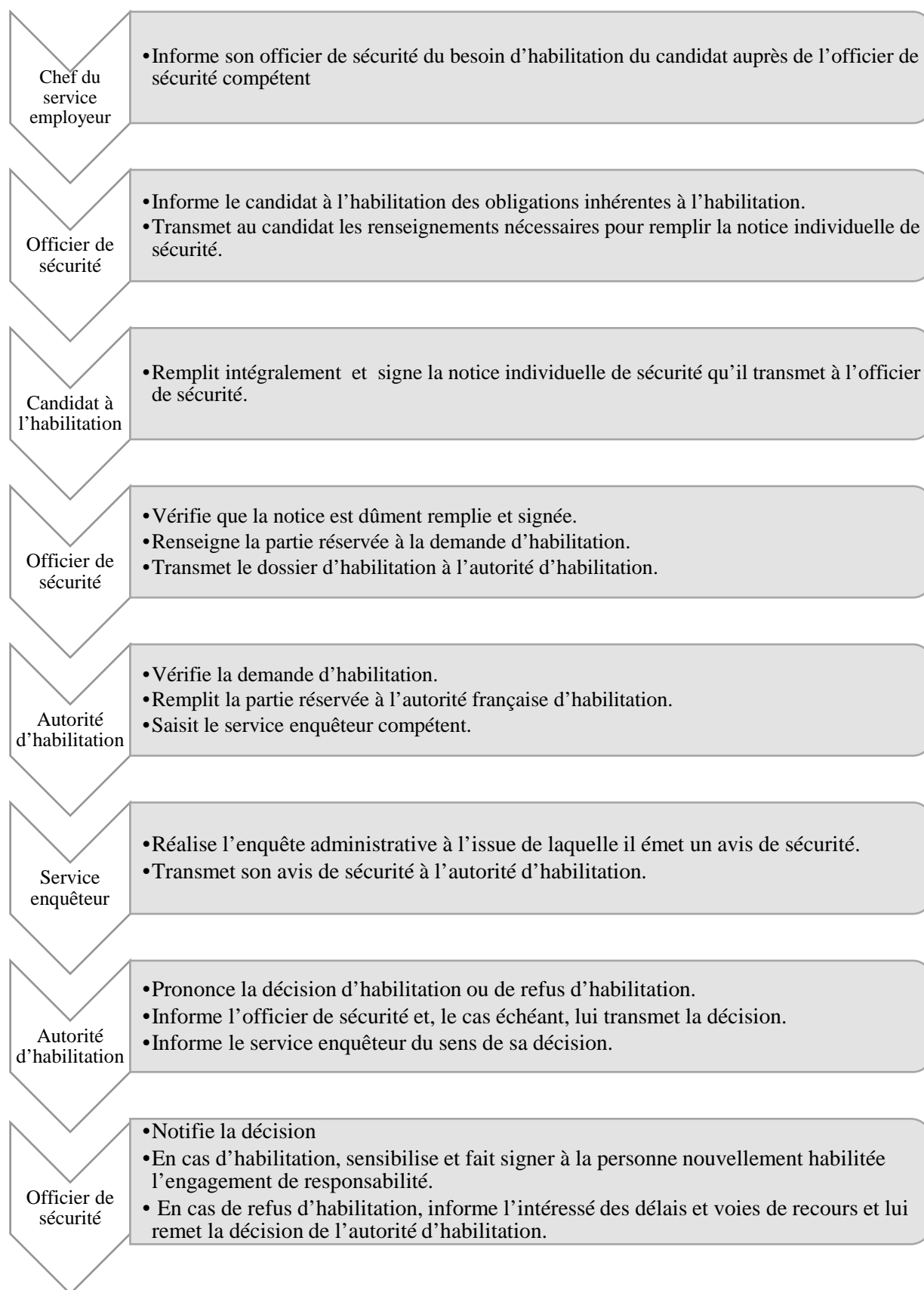
L'instruction ministérielle établit, en autres :

- un ou plusieurs guide(s) de classification définissant, par niveau de classification, les critères objectifs à considérer pour apprécier le caractère secret de l'information (par exemple : son importance au regard de l'organisation et de la politique de défense et de sécurité nationale, le domaine concerné, la nature de la source, etc. ; cf. chapitre 2), ainsi que la nomenclature des informations ou catégories d'informations à classifier ;
- les autorités sous la responsabilité desquelles, par délégation du ministre et conformément à ses directives, un timbre de classification peut être apposé sur un support ;
- les mesures de protection nécessaires pour chaque type de systèmes d'information ; les éléments permettant au sein de chaque service de l'État, organisme public ou privé, d'établir les catalogues des emplois identifiant les postes nécessitant d'accéder à des informations et supports classifiés.

Annexe 4 – Hiérarchie des normes relatives à la protection du secret de la défense nationale



Annexe 5 - Schéma présentant la procédure d'habilitation au secret de la défense nationale d'un ressortissant français travaillant en France



Annexe 6 – Modèle de demande d'enquête administrative

Ministère :

Organisme :

Date et numéro d'enregistrement :

DEMANDE D'ENQUETE ADMINISTRATIVE

Motifs de la demande :

Identité de la personne

Nom :

Prénom :

Date et lieu de naissance :

Nationalité(s) de naissance :

Nationalité(s) actuelle(s) :

Domicile actuel :

Domicile antérieur :

Renseignements

Grade ou titre :

Fonctions ou missions exercées :

Date d'expiration de la présente enquête administrative :

Nom, qualité, date, signature de l'autorité compétente¹²⁶
et cachet de l'organisme

¹²⁶ Autorité de décision ayant reçu délégation à cet effet.

Annexe 7 – Modèle de dossier de demande d’habilitation d’une personne physique



DEMANDE D’HABILITATION

À REMPLIR PAR L’AUTORITE D’EMPLOI/ADMINISTRATIVE DU CANDIDAT A L’HABILITATION

1. Organisme demandeur

Organisme :

N° de la demande :

Date d’enregistrement de la demande :

2. Personne en charge du suivi du dossier

Nom et prénom :

Fonctions :

3. Procédure d’habilitation engagée

Type de demande :

☐ ADMISSION

☐ RENOUVELLEMENT

☐ RÉVISION

Procédure d’urgence :

☐ Oui, le cas échéant, préciser et motiver la demande :

4. Habilitation demandée

Niveau d’habilitation :

☐ CONFIDENTIEL (uniquement UE et OTAN)

☐ SECRET

☐ TRÈS SECRET

☐ CLASSIFICATION SPECIALE

Nature des informations et supports classifiés :

☐ France

☐ UE

☐ OTAN

☐ Autres, préciser (ESA, OCCAr, etc.) :

5. Motif de la demande

Emploi et fonctions exercées (sans acronyme) :

Préciser, le cas échéant, le numéro de poste au catalogue des emplois :

Pour les ressortissants français employés par une personne morale de droit étranger À REMPLIR PAR L’AUTORITE ETRANGERE COMPETENTE (autorité nationale de sécurité, autorité de sécurité désignée/déléguée étrangère, autre)

Autorité compétente :

Date :

À REMPLIR PAR L’AUTORITE FRANÇAISE D’HABILITATION

Organisme :

Nom – prénom de la personne en charge du dossier :

Date :

NOTICE INDIVIDUELLE DE SECURITE

PARTIE 1 – INFORMATIONS SUR LE CANDIDAT A L'HABILITATION

1. Identité

Nom de famille (de naissance) :
Nom d'usage :
Prénoms (dans l'ordre d'état civil) :
Prénom usuel :
Sexe : ☐ M ☐ F
Surnom ou alias éventuels :

Insérer une
photographie
d'identité de
moins de 3 mois

2. Naissance

Date : Pays :
Commune : Code postal :

3. Nationalité(s)

Nationalité(s) :
Année d'acquisition de la nationalité française :
Année d'arrivée en France :

4. Document(s) d'identité

	Numéro	Date de délivrance	Autorité de délivrance
Carte nationale d'identité			
Passeport français			
Titre de séjour			
Autre pièce justificative d'identité			

5. Domicile actuel

N°, voie :
Commune : Code postal : Pays :
Depuis le :
Identité des personnes résidant au même domicile (autres que celles visées dans « situation de famille actuelle » page 3) :

6. Domicile précédent (si changement depuis moins de six mois)

☐ Cocher si sans objet

N°, voie :
Commune : Code postal : Pays :
Période :

7. Résidence secondaire ou occasionnelle, y compris à l'étranger si nécessaire, utiliser l'espace « renseignements complémentaires »

☐ Cocher si sans objet

N°, voie :
Commune : Code postal : Pays :
Depuis le : Téléphone domicile :

8. Coordonnées personnelles

Téléphone(s) portable(s) :
Téléphone(s) fixe(s) :
Email(s) :

9. Situation professionnelle actuelle

Fonction/profession : ☐ Civil ☐ Militaire
Organisme d'emploi : Depuis le :
Adresse professionnelle (N°, voie, code postal, commune, pays) :

Téléphone(s) professionnel(s) :

Email(s) professionnel(s) :

Le cas échéant, préciser :

- ministère d'origine :
- ministère d'emploi :
- grade :
- pour les militaires, armée/arme d'appartenance :

10. Emploi(s) successif(s) durant les cinq dernières années, si nécessaire, utiliser l'espace « renseignements complémentaires »

☐ Cocher si sans objet

Organisme d'emploi et adresse (n°, voie, code postal, commune, pays si étranger)

Emploi/fonction

Période
du au

11. Habilitation déjà détenue

☐ Cocher si sans objet

Niveau d'habilitation :

Depuis le :

12. Niveau d'études et culture générale

Diplômes obtenus ou niveau équivalent	Langues étrangères	
	Langues	Degré de connaissance

13. Situation de famille actuelle

- ☐ Célibataire ☐ En instance de mariage ☐ Marié(e) ☐ Veuf(ve) ☐ Séparé(e)
☐ Divorcé(e) ☐ En instance de remariage ☐ Remarié(e) ☐ Concubinage ☐ PACS
☐ Autre situation (en couple, avec ou sans cohabitation, en instance de séparation, etc.) :

Depuis le :

Commune :

Pays :

14. Parents du candidat (même si décédés)

		Père – Parent 1	Mère – Parent 2
Identité	Nom de famille (de naissance)		
	Nom d'usage		
	Prénom(s)		
	Sexe		
Naissance - décès	Date de naissance		
	Code postal de naissance		
	Commune de naissance		
	Pays de naissance		
	Date de décès		
Nationalité(s)	Nationalité(s)		
	Année d'acquisition de la nationalité française		
	Année d'arrivée en France		

	Type et numéro du document d'identité (obligatoire pour les ressortissants étrangers)		
Domicile actuel - dernier domicile	N° et voie		
	Code postal		
	Commune		
	Pays		
Employeur actuel - dernier employeur	Organisme d'emploi		
	Fonctions		
	Adresse de l'organisme d'emploi (n°, voie, code postal, commune, pays si étranger)		

☐ **Voyages et séjours à l'étranger durant les cinq dernières années (en partant du plus récent).** Si nécessaire, utiliser l'espace « renseignements complémentaires » ☐ Cocher si sans objet

Pays – adresse (uniquement séjours de plus de six mois)	Période (date de début et de fin)	Motif

PARTIE 2 – INFORMATIONS SUR LE CONJOINT DU CANDIDAT A L'HABILITATION (conjoint identifié au point 13 de la PARTIE 1)

☐ Identité

Nom de famille (de naissance) :

Nom d'usage :

Prénoms (dans l'ordre d'état civil) :

Prénom usuel :

Sexe : ☐ M ☐ F

Surnom ou alias éventuels :

15. Naissance

Date :

Pays :

Commune :

Code postal :

16. Nationalité(s)

Nationalité(s) :

Année d'acquisition de la nationalité française :

Année d'arrivée en France :

17. Document(s) d'identité

	Numéro	Date de délivrance	Autorité de délivrance
Carte nationale d'identité			
Passeport français			
Titre de séjour			
Autre pièce justificative d'identité			

18.Domicile actuel

☐ Si même domicile que le candidat, cocher et ne pas renseigner

N°, voie :

Commune :

Depuis le :

Code postal :

Pays :

19.Résidence secondaire ou occasionnelle, y compris à l'étranger si nécessaire, utiliser l'espace « renseignements complémentaires »

☐ Si sans objet ou si même résidence que le candidat, cocher et ne pas renseigner

N°, voie :

Commune :

Depuis le :

Code postal :

Téléphone domicile :

Pays :

20. Coordonnées personnelles

Téléphone(s) portable(s) :

Téléphone(s) fixe(s) :

Email(s) :

21.Situation professionnelle actuelle

Fonction/profession :

Organisme d'emploi :

Adresse professionnelle (N°, voie, code postal, commune, pays) :

☐ Civil
☐ Militaire

Depuis le :

Téléphone(s) professionnel(s) :

Email(s) professionnel(s) :

Le cas échéant, préciser :

- ministère d'origine :

- ministère d'emploi :

- grade :

- pour les militaires, armée/arme d'appartenance :

22. Niveau d'études et culture générale

Diplômes obtenus ou niveau équivalent	Langues étrangères	
	Langues	Degré de connaissance

23. Parents du conjoint du candidat (même si décédés)

		Père – Parent 1	Mère – Parent 2
Identité	Nom de famille (de naissance)		
	Nom d'usage		
	Prénom(s)		
	Sexe		
Naissance - décès	Date de naissance		
	Code postal de naissance		
	Commune de naissance		
	Pays de naissance		
	Date de décès		
Nationalité(s)	Nationalité(s)		

	Année d'acquisition de la nationalité française		
	Année d'arrivée en France		
	Type et numéro du document d'identité (obligatoire pour les ressortissants étrangers)		
Domicile actuel - dernier domicile	N° et voie		
	Code postal		
	Commune		
	Pays		
Employeur actuel - dernier employeur	Organisme d'emploi		
	Fonctions		
	Adresse de l'organisme d'emploi (n°, voie, code postal, commune, pays si étranger)		

24. Voyages et séjours à l'étranger durant les cinq dernières années (en partant du plus récent). Si nécessaire, utiliser l'espace « renseignements complémentaires » ☐ Cocher si sans objet

Pays – adresse (uniquement séjours de plus de six mois)	Période (date de début et de fin)	Motif.

PARTIE 3 – INFORMATIONS SUR LE(S) ENFANT(S) DU CANDIDAT A L'HABILITATION ET DE SON CONJOINT (identifié à la PARTIE 2)

25. Enfant(s) issu(s) de l'union entre le candidat et son conjoint ☐ Cocher si sans objet

Identité	Nom de famille (de naissance)	
	Nom d'usage	
	Prénom(s)	
	Sexe	
Naissance - décès	Date de naissance	
	Code postal de naissance	
	Commune de naissance	

	Pays de naissance	
	Date de décès	
Nationalité(s)	Nationalité(s)	
	Année d'acquisition de la nationalité française	
	Année d'arrivée en France	
	Type et numéro du document d'identité	
Domicile actuel (si différent du domicile du candidat) - dernier domicile)	N° et voie	
	Code postal	
	Commune	
	Pays	
Employeur actuel - dernier employeur	Organisme d'emploi	
	Fonctions	
	Adresse de l'organisme d'emploi (n°, voie, code postal, commune, pays si étranger)	

26. Enfant(s) du candidat issu(s) d'une précédente union		<input type="checkbox"/> Cocher si sans objet
Identité	Nom de famille (de naissance)	
	Nom d'usage	
	Prénom(s)	
	Sexe	
Naissance - décès	Date de naissance	
	Code postal de naissance	
	Commune de naissance	
	Pays de naissance	
	Date de décès	
Nationalité(s)	Nationalité(s)	
	Année d'acquisition de la nationalité française	
	Année d'arrivée en France	
	Type et numéro du document d'identité	
Domicile actuel (si différent du domicile du candidat) - dernier domicile)	N° et voie	
	Code postal	
	Commune	
	Pays	
Employeur actuel - dernier employeur	Organisme d'emploi	
	Fonctions	
	Adresse de l'organisme d'emploi (n°, voie, code postal,	

	commune, pays si étranger)	
--	----------------------------	--

27. Enfant(s) du conjoint du candidat issu(s) d'une précédente union		<input type="checkbox"/> Cocher si sans objet
Identité	Nom de famille (de naissance)	
	Nom d'usage	
	Prénom(s)	
	Sexe	
Naissance - décès	Date de naissance	
	Code postal de naissance	
	Commune de naissance	
	Pays de naissance	
	Date de décès	
Nationalité(s)	Nationalité(s)	
	Année d'acquisition de la nationalité française	
	Année d'arrivée en France	
	Type et numéro du document d'identité	
Domicile actuel (si différent du domicile du candidat) - dernier domicile)	N° et voie	
	Code postal	
	Commune	
	Pays	
Employeur actuel - dernier employeur	Organisme d'emploi	
	Fonctions	
	Adresse de l'organisme d'emploi (n°, voie, code postal, commune, pays si étranger)	

PARTIE 4 – ENVIRONNEMENT PERSONNEL COMPLEMENTAIRE

Cette partie concerne l'environnement proche du candidat et du conjoint du candidat (fratries, nouveau conjoint d'un parent, autre parent d'un enfant issu d'une précédente union et toute autre personne vivant sous le même toit). Si vous êtes concerné par une ou plusieurs situations, vous devez renseigner le document à partir des informations dont vous disposez.

Personne(s)		
Statut		
Identité	Nom de famille (de naissance)	
	Nom d'usage	
	Prénom(s)	
	Sexe	
Naissance - décès	Date de naissance	
	Code postal de naissance	
	Commune de naissance	

	Pays de naissance	
	Date de décès	
Nationalité(s)	Nationalité(s)	
	Année d'acquisition de la nationalité française	
	Année d'arrivée en France	
	Type et numéro du document d'identité	
Domicile actuel (si différent du domicile du candidat) - dernier domicile)	N° et voie	
	Code postal	
	Commune	
	Pays	
Employeur actuel - dernier employeur	Organisme d'emploi	
	Fonctions	
	Adresse de l'organisme d'emploi (n°, voie, code postal, commune, pays si étranger)	

PARTIE 5 – ENVIRONNEMENT NUMERIQUE

1) Utilisez-vous des réseaux sociaux ?

- ☐ OUI
☐ NON

2) Si oui, à quelle fréquence ?

- ☐ Rarement
☐ Occasionnellement
☐ Souvent
☐ Très souvent

3) Quel(s) réseau(x) utilisez-vous ?

Nom du réseau	Pseudo utilisé

PARTIE 6 – AUTRES RENSEIGNEMENTS DE SECURITE

1) Pensez-vous

- | | | |
|---|------------------------------|------------------------------|
| - avoir été sollicité(e) en dehors de vos attributions professionnelles pour fournir des informations à caractère sensible ? | <input type="checkbox"/> OUI | <input type="checkbox"/> NON |
| - que des pressions ont été exercées sur vous, ou sur des membres de votre famille, à la suite d'un incident survenu sur le territoire étranger ? | <input type="checkbox"/> OUI | <input type="checkbox"/> NON |
| - avoir été l'objet d'approches de la part d'un service de renseignement ou de sécurité étranger ? | <input type="checkbox"/> OUI | <input type="checkbox"/> NON |

En cas de réponse(s) positive(s), décrire les circonstances :

2) Etes-vous en relations suivies, à titre professionnel ou privé, avec des ressortissants étrangers ou des français résidant à l'étranger ? Si oui, préciser. ☐ Cocher si sans objet

Nom et prénom	Date et lieu de naissance	Nationalité(s)	Caractériser le lien	Commune et pays de résidence	Employeur

3) Des personnes interviennent-elle régulièrement, à titre professionnel ou privé, auprès de vos proches (garde d'enfant, entretien du domicile, etc.) ? ☐ Cocher si sans objet

Nom et prénom	Date et lieu de naissance	Nationalité(s)	Caractériser le lien

4) Si vous souhaitez communiquer un point particulier au service chargé de l'instruction de votre dossier, remplissez le champ suivant. ☐ Cocher si sans objet

ATTESTATION DU CANDIDAT A L'HABILITATION

Je soussigné(e)¹²⁷ :

- a) reconnais avoir été informé(e) de l'objet de l'habilitation à laquelle je suis candidat(e) et de sa portée. Ainsi, il m'a été indiqué que la décision d'habilitation, si elle est favorable, m'autorise, en fonction de mon besoin d'en connaître, à accéder à des informations et supports classifiés au(x) niveau(x) précisé(s) dans cette décision. Il m'a également été précisé que la présente demande d'habilitation déclenche une procédure destinée à vérifier qu'il m'est possible, sans risque pour la défense et la sécurité nationale ou pour ma propre sécurité, de connaître des informations et supports classifiés dans l'exercice de mes fonctions ou dans le cadre de l'accomplissement de ma mission ;
- b) reconnais être informé(e) :
- du caractère obligatoire des réponses qui me sont demandées ;
 - qu'en l'absence de réponse aux questions posées, aucune décision ne pourra être prise quant à mon éventuelle habilitation ;
 - que je dispose d'un droit d'accès et de rectification, en application de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés que je pourrais exercer auprès du service du haut fonctionnaire de défense et de sécurité du ministère dont ma procédure d'habilitation dépend ;
 - que les informations recueillies font l'objet d'un traitement informatique destiné à la gestion des habilitations au secret de la défense nationale ;
 - que les destinataires des données de ce traitement sont, en fonction de leurs attributions et dans la limite du besoin d'en connaître, le service du haut fonctionnaire de défense et de sécurité du ministère dont je dépends.
- c) certifie l'exactitude des renseignements que j'ai fournis dans la présente notice et admetts avoir été informé(e) que je m'expose, en cas d'altération frauduleuse de la vérité, à une peine de 3 ans d'emprisonnement et de 45 000 euros d'amende, en application des dispositions de l'article 441-1 du code pénal ;
- d) déclare avoir été dûment avisé(e) qu'en vertu des dispositions législatives et réglementaires relatives à la protection du secret, l'habilitation à laquelle je me porte candidat(e) engage ma responsabilité et fait naître à ma charge des obligations, parmi lesquelles celles de :
- garantir la sécurité des informations et supports classifiés auxquels je peux avoir accès par le strict respect de la réglementation applicable ;
 - répondre, pénalement et administrativement, de tout acte de malveillance, d'imprudence, de négligence ou d'inattention ayant pour résultat la destruction, le détournement, la soustraction, la reproduction ou la divulgation au public ou à une personne non qualifiée, d'une information ou d'un support classifié (article 413-10 du code pénal prévoyant et réprimant le délit de compromission du secret de la défense nationale).

A
Le
Signature du candidat

¹²⁷ Nom et prénom.

Annexe 8 – Modèle de décision d’habilitation d’une personne physique

Ministère :

Organisme :

Date et numéro d’enregistrement :

DECISION D’HABILITATION

Le¹²⁸ :

décide que

Madame/Monsieur¹²⁹ :

Date et lieu de naissance :

Grade ou titre :

Fonctions ou missions :

Est habilité(e) jusqu’au¹³⁰ :

Pour accéder à des informations et supports classifiés au(x) niveau(x)¹³¹ :

☐ TRÈS SECRET

☐ TRÈS SECRET UE/
EU TOP SECRET

☐ COSMIC TRÈS SECRET /
COSMIC TOP SECRET

☐ SECRET

☐ SECRET UE/
EU SECRET

☐ NATO SECRET/
NATO SECRET

☐ CONFIDENTIEL UE/
EU CONFIDENTIAL

☐ NATO CONFIDENTIEL/
NATO CONFIDENTIAL

A

Le

Signature et cachet de l’autorité d’habilitation

¹²⁸ Autorité d’habilitation ou autorité ayant reçu délégation à cet effet.

¹²⁹ Nom et prénom.

¹³⁰ Date d’expiration de la décision d’une durée égale ou moindre à celle de l’avis de sécurité.

¹³¹ Préciser le(s) niveau(x) de classification auquel (auxquels) il est donné accès.

Annexe 9 – Modèle d’attestation de mise en garde

Ministère :

Organisme :

Date et numéro d’enregistrement :

ATTESTATION DE MISE EN GARDE

Je¹³² soussigné(e)¹³³ :

certifie avoir été mis(e) en garde en présence de :

contre les risques que pourrait faire courir l’habilitation de¹³⁴ :

à connaître des informations et supports classifiés au(x) niveau(x)¹³⁵ :

- | | | |
|--------------------------------------|--|--|
| <input type="checkbox"/> TRÈS SECRET | <input type="checkbox"/> TRÈS SECRET UE/
EU TOP SECRET | <input type="checkbox"/> COSMIC TRÈS SECRET /
COSMIC TOP SECRET |
| <input type="checkbox"/> SECRET | <input type="checkbox"/> SECRET UE/
EU SECRET | <input type="checkbox"/> NATO SECRET/
NATO SECRET |
| | <input type="checkbox"/> CONFIDENTIEL UE/
EU CONFIDENTIAL | <input type="checkbox"/> NATO CONFIDENTIEL/
NATO CONFIDENTIAL |

A

Le

Signature de l’autorité compétente ou de
l’officier de sécurité

¹³² À remplir par l’autorité compétente ou l’officier de sécurité.

¹³³ Préciser les nom et prénom, grade ou titre, fonction.

¹³⁴ Nom et prénom, grade ou titre, fonction du candidat à l’habilitation.

¹³⁵ Préciser le(s) niveau(x) de classification auquel (auxquels) il est donné accès.

Annexe 10 – Modèle d’attestation de mise en éveil

Ministère :

Organisme :

Date et numéro d’enregistrement :

ATTESTATION DE MISE EN EVEIL

Je¹³⁶ soussigné(e)¹³⁷ :

reconnais avoir été mis(e) en éveil le :

en présence de¹³⁸ :

sur les risques que pourrait faire courir mon habilitation à connaître des informations et supports classifiés au(x) niveau(x) :¹³⁹

☐ TRÈS SECRET

☐ TRÈS SECRET UE/
EU TOP SECRET

☐ COSMIC TRÈS SECRET /
COSMIC TOP SECRET

☐ SECRET

☐ SECRET UE/
EU SECRET

☐ NATO SECRET/
NATO SECRET

☐ CONFIDENTIEL UE/
EU CONFIDENTIAL

☐ NATO CONFIDENTIEL/
NATO CONFIDENTIAL

Je m’engage à ne pas divulguer les informations et supports classifiés dont je pourrais avoir connaissance dans l’exercice de mes fonctions ou l’accomplissement de ma mission et à signaler immédiatement à mon officier de sécurité ou mon autorité d’emploi, toute tentative de pression dont je pourrais faire l’objet.

Intéressé(e)
signature

Officier de sécurité
signature

Autorité d’habilitation ou
représentant
signature

¹³⁶ À remplir par le candidat à l’habilitation.

¹³⁷ Nom et prénom, grade ou titre, fonction.

¹³⁸ Nom et prénom, grade ou titre, fonction.

¹³⁹ Cocher la case concernée.

Annexe 11 – Modèle d’engagement de responsabilité

Ministère :

Organisme :

Date et numéro d'enregistrement :

ENGAGEMENT DE RESPONSABILITE

VOLET 1

Je, soussigné(e)
déclare :

- avoir été informé(e) de la décision en date du m'autorisant l'accès à des informations et supports classifiés au(x) niveau(x):

<input type="checkbox"/> TRÈS SECRET	<input type="checkbox"/> TRÈS SECRET UE/ EU TOP SECRET	<input type="checkbox"/> COSMIC TRÈS SECRET / COSMIC TOP SECRET
<input type="checkbox"/> SECRET	<input type="checkbox"/> SECRET UE/ EU SECRET	<input type="checkbox"/> NATO SECRET/ NATO SECRET
	<input type="checkbox"/> CONFIDENTIEL UE/ EU CONFIDENTIAL	<input type="checkbox"/> NATO CONFIDENTIEL/ NATO CONFIDENTIAL
- avoir pris connaissance de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, ainsi que des dispositions du code pénal citées en références de l'instruction ;
- être pleinement conscient(e) de mes responsabilités en ce qui concerne la protection des informations et supports classifiés ;
- être informé(e) des conséquences prévues par les dispositions législatives (articles 121-2, 411-1 à 411-11, 413-9 à 413-12 et 414-7 à 414-9 du code pénal) et réglementaires, notamment pour le cas où, sciemment ou par négligence, je laisserais ces informations et supports classifiés parvenir à des personnes non qualifiées.

En conséquence, **je m'engage à ne pas divulguer**, même après la cessation de mes fonctions ou de ma mission, à des personnes non qualifiées les informations et supports classifiés dont j'aurais connaissance dans l'exercice de mes fonctions ou l'accomplissement de ma mission.

A _____, le _____

Nom et signature de l'officier de sécurité _____

Signature de l'intéressé(e) _____

VOLET 2

À compter de la date de cessation des fonctions ou de ma mission, pour lesquelles une décision d'habilitation à connaître d'informations et supports classifiés m'a été délivrée, **je m'engage à ne pas divulguer à des personnes non qualifiées** les informations et supports classifiés dont j'ai eu connaissance dans l'exercice de mes fonctions ou pendant l'accomplissement de ma mission et à **ne conserver par-devers moi aucun support classifié**.

Je reconnais être informé(e) des **conséquences** prévues par les dispositions législatives (articles 121-2, 411-1 à 411-11, 413-9 à 413-12 et 414-7 à 414-9 du code pénal) et réglementaires, notamment pour le cas où, sciemment ou par négligence, je porterais à la connaissance de personnes non qualifiées, ces informations et supports classifiés.

A _____, le _____

Nom et signature de l'officier de sécurité _____

Signature de l'intéressé(e) _____

Annexe 12 – Modèle de décision de refus d’habilitation ou d’abrogation d’une décision d’habilitation

Ministère :

Organisme :

Date et numéro d’enregistrement :

DECISION DE REFUS D’HABILITATION OU D’ABROGATION D’UNE DECISION D’HABILITATION

- ☐ Refus d’habilitation
- ☐ Abrogation de la décision d’habilitation¹⁴⁰

concernant

Madame/Monsieur¹⁴¹ :

Date et lieu de naissance :

Grade ou titre :

Organisme :

Fonctions ou missions :

La présente décision est notifiée à l’intéressé(e) conformément à l’instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

A

Le

Nom, qualité, signature de l’autorité d’habilitation
et cachet de l’organisme

¹⁴⁰ Référence et date de la décision d’habilitation.

¹⁴¹ Nom et prénom.

Annexe 13 – Modèle de récépissé de notification d’une décision de refus d’habilitation ou d’abrogation d’une décision d’habilitation

Ministère :

Organisme :

Date et numéro d’enregistrement :

RECEPISSE DE NOTIFICATION D’UNE DECISION DE REFUS D’HABILITATION OU D’ABROGATION D’UNE DECISION D’HABILITATION

Je soussigné(e) :

reconnais que l’officier de sécurité de¹⁴² :

m’a notifié et remis ce jour la décision¹⁴³ :

prise par¹⁴⁴ :

portant refus de délivrance ou d’abrogation de l’autorisation d’accéder aux informations et supports classifiés au(x) niveau(x) :

- | | | |
|--------------------------------------|--|--|
| <input type="checkbox"/> TRÈS SECRET | <input type="checkbox"/> TRÈS SECRET UE/
EU TOP SECRET | <input type="checkbox"/> COSMIC TRÈS SECRET /
COSMIC TOP SECRET |
| <input type="checkbox"/> SECRET | <input type="checkbox"/> SECRET UE/
EU SECRET | <input type="checkbox"/> NATO SECRET/
NATO SECRET |
| | <input type="checkbox"/> CONFIDENTIEL UE/
EU CONFIDENTIAL | <input type="checkbox"/> NATO CONFIDENTIEL/
NATO CONFIDENTIAL |

Je prends connaissance des voies et délais de recours relatifs à cette décision, indiqués ci-après.

Il est rappelé qu’aux termes de l’article L. 411-2 du code des relations entre le public et l’administration « *Toute décision administrative peut faire l’objet, dans le délai imparti pour l’introduction d’un recours contentieux, d’un recours gracieux ou hiérarchique qui interrompt le cours de ce délai. / Lorsque dans le délai initial du recours contentieux ouvert à l’encontre de la décision, sont exercés contre cette décision un recours gracieux et un recours hiérarchique, le délai du recours contentieux, prorogé par l’exercice de ces recours administratifs, ne recommence à courir à l’égard de la décision initiale que lorsqu’ils ont été l’un et l’autre rejetés* ».

A

Le

Signature de l’intéressé(e)

¹⁴² Organisme.

¹⁴³ Référence et date de la décision.

¹⁴⁴ Autorité d’habilitation ou autorité ayant reçu délégation à cet effet.

Annexe 14 – Modèle de certificat de sécurité

Ministère :
Organisme :
Date et numéro d'enregistrement :

CERTIFICAT DE SÉCURITÉ Attestation of personnel security clearance

Délivré par (ministère, organisme) :
Issued by (Ministry, entity)

Date et lieu de délivrance :
Date and place of issue

Numéro:
Number

valable jusqu'au¹⁴⁵ :
valid until

Objet / mission:
Object/mission

Il est certifié par le présent document que Madame/Monsieur
It is hereby certified that Ms/Mr

Nom et prénom :
Family name, given name

Grade et fonctions :
Rank and functions

Date et lieu de naissance :
Date and place of birth

Détenteur(trice) du passeport / de la carte d'identité n° :
Passport/identity card number

Délivré à :
Place of issue

en date du :
date of issue

a fait l'objet de la décision d'habilitation n° :
has been granted the personnel security clearance n°

valable jusqu'au :
until

pour accéder à des informations et supports classifiés au niveau¹⁴⁶ :
for access to classified information up to the level

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

Fin de validité :

¹⁴⁵ Certificat à détruire à l'expiration de sa date de validité.

¹⁴⁶ Niveau de classification maximum (maximum level of classification)

Annexe 15 – Modèle d’attestation d’avis de sécurité

Ministère :

Organisme :

Date et numéro d’enregistrement :

ATTESTATION D’AVIS DE SECURITE **Attestation of a positive clearance procedure**

Délivré par (ministère, organisme) :

Issued by (ministry, entity)

Date et lieu de délivrance :

Date and place of issue

Il est certifié par le présent document que Madame/Monsieur

It is hereby certified that Ms/Mr

Nom et prénom:

Family name, given name

Grade et fonctions :

Rank and functions

fait l’objet d’un avis de sécurité (sans objection, restrictif ou défavorable)¹⁴⁷ délivré par :

holds a security notice delivered by

valable jusqu’au :

expiring on DD/MM/AAAA

pour l’accès aux informations et supports classifiés au niveau¹⁴⁸ :

for access up to and including the level

Nom, qualité, signature de l’autorité d’habilitation
et cachet de l’organisme

¹⁴⁷ Rayer la mention inutile.

¹⁴⁸ Niveau de classification maximum (maximum level of classification).

Annexe 16 – Récapitulatif des obligations des personnes morales ayant accès au secret de la défense nationale

Obligations Situation	Habilitation			Mise en place des chaînes de sécurité		Obtention d'une attestation d'aptitude physique à détenir des ISC		Homologation des systèmes d'information classifiés en cas de détention d'un tel système	Vecteur juridique de référence
	Personne morale	Responsable de l'organisme ayant accès à des ISC ¹⁴⁹	Personnes physiques de l'organisme ayant accès à des ISC	ISC	Adaptation de la chaîne SSI ¹⁵⁰	Niveau <i>Secret</i>	Niveau <i>Très secret</i>		
Services de l'État	Non	Oui, sauf si besoin d'en connaître non avéré	Toute personne de l'organisme nécessitant, dans les limites du besoin d'en connaître, d'accéder à des informations ou supports classifiés dans l'exercice de sa fonction ou pour l'accomplissement de sa mission, conformément au catalogue des emplois de l'organisme	Oui, même en l'absence de détention au sein de l'organisme	Si hébergement ou exploitation d'un système d'information classifié	Non	Oui, préalablement à la détention	Oui, préalablement au déploiement et à l'exploitation du système	IGI 1300 Instruction ministérielle Le cas échéant, directives techniques particulières
Etablissements publics de l'État	Non	Oui, sauf si besoin d'en connaître non avéré				Oui, à l'occasion des contrôles organisés par le haut fonctionnaire de défense et de sécurité du ministre de tutelle	Oui, préalablement à la détention		
Opérateurs d'importance vitale	Non	Non, sauf si besoin d'en connaître avéré par le ministre coordonnateur	Délégué à la défense et à la sécurité Toute autre personne nécessitant d'accéder pour la réalisation par l'opérateur de ses missions d'importance vitale et conformément au catalogue des emplois de l'opérateur	Oui, même en l'absence de détention au sein de l'organisme	Si hébergement ou exploitation d'un système d'information classifié	Oui, à l'occasion des contrôles organisés par le haut fonctionnaire de défense et de sécurité du ministre coordonnateur	Oui, préalablement à la détention	Oui, préalablement au déploiement et à l'exploitation du système	Plan de sécurité d'opérateur ou Plan particulier de protection

¹⁴⁹ Informations et supports classifiés.

¹⁵⁰ Sécurité des systèmes d'information.

Obligations Situation	Habilitation			Mise en place des chaînes de sécurité		Obtention d'une attestation d'aptitude physique à détenir des ISC		Homologation des systèmes d'information classifiés en cas de détention d'un tel système	Vecteur juridique de référence
	Personne morale	Responsable de l'organisme ayant accès à des ISC ¹⁴⁹	Personnes physiques de l'organisme ayant accès à des ISC	ISC	Adaptation de la chaîne SSI ¹⁵⁰	Niveau <i>Secret</i>	Niveau <i>Très secret</i>		
Convention au sens de la présente instruction	Non, sauf si la convention en stipule autrement	Oui	Tout personnel de la collectivité territoriale ou de la personne morale de droit privée ayant besoin d'accéder à des informations ou supports classifiés pour l'exécution de la convention inscrit au catalogue des emplois mentionné dans le plan contractuel de sécurité	Oui, même en l'absence de détention au sein de l'organisme	Si hébergement ou exploitation d'un système d'information classifié	Oui, au plus tard à l'occasion des contrôles organisés par le haut fonctionnaire de défense et de sécurité du ministre cocontractant	Oui, préalablement à la détention	Oui, préalablement au déploiement et à l'exploitation du système	Plan contractuel de sécurité
Contrat de la commande publique/ contrat de sous-traitance ou sous-contrat à un contrat de la commande publique / contrat de subvention	Oui, exigence préalable à la signature du contrat	Oui, exigence préalable à la signature du contrat	Tout personnel du cocontractant ayant besoin d'accéder à des informations ou supports classifiés pour l'exécution du contrat inscrit au catalogue des emplois mentionné dans le plan contractuel de sécurité			Oui, préalablement à l'exécution des prestations du contrat nécessitant la détention d'ISC par le cocontractant			Plan contractuel de sécurité

Annexe 17 – Clauses-types générales contractuelles de protection du secret de la défense nationale à insérer dans les conventions et les contrats

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

1. Clauses générales de protection du secret de la défense nationale

En application des dispositions législatives et réglementaires en matière de protection du secret de la défense nationale, le titulaire de la convention ou du contrat s'engage à assurer la protection des informations et supports classifiés qu'il aura à connaître et, le cas échéant détenir, en tenant compte des dispositions particulières stipulées dans le plan contractuel de sécurité.

Il reconnaît avoir pris connaissance des textes suivants portant sur ses obligations résultant de la connaissance et de la détention d'informations et supports classifiés :

- le code pénal, notamment ses articles 413-9 à 414-9 ;
- l'arrêté [xxxx] portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale ;
- [l'arrêté [xxxx] portant approbation de l'instruction ministérielle xxx]
- le cas échéant : [les directives techniques particulières [xxx]].
- Le cas échéant : [l'accord entre le Gouvernement de la République française et ...]

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 l'abrogation de la décision d'habilitation au secret de la défense nationale de la personne morale et, par voie de conséquence, la résiliation de la convention ou du contrat, sans préjudice des peines prévues par les dispositions des articles 413-9 à 413-12 du code pénal.

2. Stipulations additionnelles relatives aux conventions ou aux contrats nécessitant la détention d'informations et supports classifiés

Les lieux du titulaire de la convention ou du contrat voués à abriter des informations et supports classifiés, ainsi que les systèmes d'information utilisés pour traiter des informations et supports classifiés doivent présenter toutes les garanties pour assurer la protection du secret de la défense nationale et peuvent faire l'objet d'inspections, de contrôles ou d'audits de la part de l'autorité administrative.

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

À l'achèvement des prestations du contrat nécessitant l'accès à des informations et supports classifiés, le titulaire dispose d'un délai d'un mois pour en informer l'autorité contractante qui détermine, dans la fiche de clôture du plan contractuel de sécurité, la destination à donner aux informations et supports classifiés jusqu'alors détenus par le titulaire ainsi que les conditions de démantèlement du système d'information classifié. Le titulaire s'engage à respecter ces dispositions. En cas d'inexécution, le titulaire s'expose à des sanctions pénales et contractuelles.

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 et supports classifiés se rapportant au contrat et à faire apposer les scellés sur les meubles de sécurité et les locaux à l'intérieur desquels les documents et matériels réclamés par l'administration sont conservés en vue d'assurer leur protection.

Les informations et supports classifiés énumérés dans le plan contractuel de sécurité doivent être intégralement retournés à l'autorité contractante au terme du contrat.

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 d'inspections, de contrôles ou d'audits de la part de l'autorité administrative.

4. Stipulations relatives à la protection du secret dans le contrat de travail d'une personne habilitée

En application 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 et supports classifiés qu'il peut, sous réserve du besoin d'en connaître, être amené à connaître ou détenir, au titre de la décision d'habilitation délivrée par l'autorité administrative compétente.

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

5. Stipulations relatives à la protection du secret dans le contrat de travail d'une personne non habilitée

En application 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 et 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. Le titulaire est informé qu'il n'est pas autorisé à connaître d'informations et supports couverts par le secret de la défense nationale.

6. Stipulations relatives à la protection du secret en cas de disparition de la personne morale

En cas de cessation d'activité ou de dissolution, le titulaire du contrat [restitue/détruit/archive] les informations et supports classifiés qu'il détient au titre du contrat selon les modalités suivantes : [modalités à définir par l'autorité publique contractante].

Annexe 18 – Schéma présentant la procédure d’habilitation d’une personne morale française



Annexe 19 – Modèle de désignation d'un officier de sécurité

Je soussigné(e)¹⁵¹ :

désigne¹⁵² :

pour exercer la fonction d'officier de sécurité de¹⁵³ :

Adresse de la personne morale :

Le cas échéant, n° RCS ou SIRET :

chargé, sous ma responsabilité, de mettre en œuvre les dispositions législatives et réglementaires en matière de protection du secret de la défense nationale pour assurer la protection des informations et supports classifiés confiés dans le cadre d'une convention/d'un contrat. Je m'engage à lui donner les moyens nécessaires pour accomplir les missions qui lui sont confiées, qu'il exerce pour mon compte et sous ma responsabilité.

A
Le
Signature

¹⁵¹ Nom, prénom du représentant légal de la personne morale.

¹⁵² Nom, prénom de l'officier de sécurité.

¹⁵³ Raison ou dénomination sociale de la personne morale.

Annexe 20 – Modèle de dossier de demande d’habilitation d’une personne morale



À REMPLIR PAR LA PERSONNE MORALE	
Dénomination ou raison sociale :	Date et signature du représentant de la personne morale
N° RCS :	
Procédure d’habilitation engagée :	<input type="checkbox"/> ADMISSION <input type="checkbox"/> RENOUELEMENT <input type="checkbox"/> RÉVISION

À REMPLIR PAR L’AUTORITE CONTRACTANTE/LE MAITRE D’ŒUVRE/L’ACHETEUR/LE PRIMO-CONTRACTANT (DANS LE CAS D’UNE SOUS-TRAITANCE/D’UN SOUS-CONTRAT)	
Niveau d’habilitation demandé :	<input type="checkbox"/> CONFIDENTIEL (uniquement UE et OTAN) <input type="checkbox"/> SECRET <input type="checkbox"/> TRÈS SECRET <input type="checkbox"/> CLASSIFICATION SPECIALE
Nature des informations et supports classifiés	<input type="checkbox"/> France <input type="checkbox"/> UE <input type="checkbox"/> OTAN <input type="checkbox"/> Autres, préciser (ESA, OCCAr, etc.) :
Modalités d’accès et production d’informations et supports classifiés	
Objet du contrat:	
Motif du besoin d’en connaître :	
Accès à des informations et supports classifiés en phase précontractuelle	<input type="checkbox"/> OUI <input type="checkbox"/> NON
Accès sans détention d’informations et supports classifiés	<input type="checkbox"/> OUI <input type="checkbox"/> NON
Accès avec détention d’informations et supports classifiés dans les locaux de la personne morale	<input type="checkbox"/> OUI <input type="checkbox"/> NON
Le cas échéant, préciser le(s) lieu(x) :	
Utilisation d’un système d’information classifié :	<input type="checkbox"/> OUI <input type="checkbox"/> NON

Renseignements relatifs au contrat¹⁵⁴

1. Description de la prestation confiée à la personne morale :

2. Lieux d'exécution du contrat :

3. Date prévisionnelle de notification du contrat :

4. Date et durée d'exécution du contrat :

5. En cas de sous-traitance/sous-contrat, préciser :
dénomination ou raison sociale du contractant :

N° d'identification et date de notification :

N° d'identification et date d'approbation du plan contractuel de sécurité :

6. Conséquences (opérationnelles, calendaires, financières, techniques, etc.) si l'entreprise :
- n'est pas habilitée à la date prévisionnelle indiquée au point 5 :

- ne peut pas être habilitée :

Nom de l'autorité contractante/acheteur :

Nom, prénom et coordonnées de la personne en charge du dossier :

Date :

À REMPLIR PAR L'AUTORITE D'HABILITATION

Ministère :

N° de la demande d'habilitation :

Date :

¹⁵⁴ Ne concerne que les contrats prévoyant les prestations suivantes : travaux, fournitures, services.

PARTIE 1 - DESCRIPTION DE LA PERSONNE MORALE

Nom :
 Nom abrégé :
 Raison sociale :
 Enseigne commerciale :
 Nationalité(s) :
 Commune d'implantation :
 Code postal :
 Début d'activité (RCS)

Identification de la personne morale

Numéro RC :
 Numéro SIREN :
 Numéro NIC
 Numéro SIRET :

Adresse

N°, voie :
 Commune
 Code postal :
 Pays :
 Depuis le :

Données complémentaires

Forme juridique :
 Type/taille :

Domaine d'activité

Code Naf :

Effectifs

Nombre :
 Date

Gouvernance

Nom :
 Prénom (si personne physique) :
 Sexe (si personne physique) :
 Date de naissance (si personne physique) :
 Lieu de naissance (si personne physique) :
 Fonction :
 Date de prise de fonction :
 SIREN :

Nationalité(s) :

Tél. professionnel :

Tél. portable :

Fax :

Email professionnel :

Site internet :

Officier de sécurité (à remplir s'il est différent du représentant de la personne morale)

Nom - prénom :

Fonction :

Tél. bureau :

Tél. portable :

Fax :

¹⁵⁵ À renseigner également par les indépendants, les microentreprises.

Email :

Officier de sécurité des systèmes d'information

☐ Cocher si sans objet

Nom - prénom :

Fonction :

Tél. bureau :

Tél. portable :

Fax :

Email :

Officier de sécurité des systèmes d'information

☐ Cocher si sans objet

Nom :

Prénom :

Date de naissance :

Lieu de naissance :

Téléphone :

Habilitation déjà détenue par la personne morale

☐ Cocher si sans objet

La personne morale a-t-elle déjà été habilitée au secret de la défense nationale ?

☐ OUI ☐ NON

Si oui, préciser :

- l'autorité d'habilitation :
- la date de la décision d'habilitation :
- la date de fin de validité de l'avis de sécurité :
- le niveau d'habilitation :
- la nature de l'habilitation (France, UE, OTAN, autres) :

La personne morale dispose-t-elle d'un local apte à conserver des informations et supports classifiés ?

☐ OUI ☐ NON

Si oui, préciser :

- l'emplacement et le numéro du local :
- l'autorité ayant délivré l'avis technique d'aptitude physique :
- la date de délivrance de cet avis :
- le niveau de classification des supports pouvant être conservés dans le local :

La personne morale dispose-t-elle d'un système d'information homologué pour traiter des informations classifiées ?

☐ OUI ☐ NON

Si oui, préciser :

- l'autorité ayant délivré la décision d'homologation :
- la date de délivrance de la décision d'homologation :
- le niveau de classification des informations pouvant être traitées sur le système d'information :

Capital social (dans le cadre d'un contrat de la commande publique, d'un contrat de sous-traitance ou de sous-contrat à un contrat de la commande publique, d'un contrat de subvention).

Pour les entreprises non cotées, fournir l'actionnariat détaillé

Capital :

Date :

1^{er} niveau d'actionnariat

Nom(s) (et prénom(s) pour les personnes physiques) du ou des actionnaires	Nationalité(s)	Date et lieu de naissance des personnes physiques	N° RCS pour les personnes morales (Kbis à fournir)	% détenu	Droit de vote (%)

2^e niveau d'actionnariat

Nom(s) (et prénom(s) pour les personnes physiques) du ou des actionnaires	Nationalité(s)	Date et lieu de naissance des personnes physiques	N° RCS pour les personnes morales (Kbis à fournir)	% détenu	Droit de vote (%)

3 ^e niveau d'actionnariat					
Nom(s) (et prénom(s) pour les personnes physiques) du ou des actionnaires	Nationalité(s)	Date et lieu de naissance des personnes physiques	N° RCS pour les personnes morales (Kbis à fournir)	% détenu	Droit de vote (%)
Tête de groupe et bénéficiaires effectifs					
Nom(s) (et prénom(s) pour les personnes physiques) du ou des actionnaires	Nationalité(s)	Date et lieu de naissance des personnes physiques	N° RCS pour les personnes morales (Kbis à fournir)	% détenu	Droit de vote (%)

PARTIE 2 – GESTION DES RISQUES

Assurances

Biens immobiliers :

Responsabilité civile :

Risques perte exploitation :

La fonction de « risk manager » ou équivalent existe-t-elle ?

☐ OUI

Nom :

Prénom :

Date de naissance :

Lieu de naissance :

Téléphone :

☐ NON, comment la personne morale gère-t-elle ses risques ?

La fonction de « compliance officer » est-elle prise en compte ?

☐ Cocher si sans objet

Nom :

Prénom :

Date de naissance :

Lieu de naissance :

Téléphone :

La fonction de « control expert manager » est-elle prise en compte ?

☐ Cocher si sans objet

Nom :

Prénom :

Date de naissance :

Lieu de naissance :

Téléphone :

Normes

Qualité :

Environnement :

Autres :

Recours à un cabinets d'avocats/audits/conseils accompagnant, y compris intervenant ou ayant intervenu dans les locaux de la personne morale ces cinq dernières années

☐ Cocher si sans objet

Nom du(es) cabinet(s)/société(s):

Date(s)/période(s) :

Nationalité(s)

N° RCS :

Informations complémentaires :

PARTIE 3 – ENVIRONNEMENT INTERNATIONAL

Implantations à l'étranger : filiales, établissements, etc. ☐ Cocher si sans objet

Pays	Nom(s)de la (des) filiale(s), établissement(s), etc.	N° d'identification	Adresse(s)

Liens commerciaux avec des pays étrangers (contrats d'exportation) ☐ Cocher si sans objet

Pays	Nom(s)de la (des) société(s)	N° d'identification	Produits/services

La personne morale a-t-elle des fournisseurs clé étrangers ? ☐ Cocher si sans objet

Pays	Nom(s)de la (des) société(s)	N° d'identification	Produits/services (s)

La personne morale a-t-elle des échanges avec des entreprises ou organismes étrangers ☐ Cocher si sans objet

Pays	Nom(s)de la (des) société(s)	N° d'identification	Raison(s)

PARTIE 4 – INFORMATIONS RELATIVES A LA PERSONNE MORALE (dans le cadre d'un contrat de la commande publique, d'un contrat de sous-traitance ou de sous-contrat à un contrat de la commande publique, d'un contrat de subvention)

La personne morale détient-elle l'exclusivité du savoir-faire pour les travaux classifiés ?

☐ Oui, décrire le savoir-faire :

☐ Non. Si une autre entreprise détient ce savoir-faire, expliquer la raison pour laquelle elle n'a pas été retenue ou pas consultée ?

PARTIE 5 – RENSEIGNEMENTS DE SECURITE

Répondre aux questions suivantes

- Votre société fait-elle l'objet d'enquêtes, de poursuites ou de mises en accusation de la part d'une juridiction financière ? ☐ OUI ☐ NON
- Des pressions ont-elles été exercées sur votre société, ou sur ☐ OUI ☐ NON

des employés de votre société, à la survenue sur un territoire étranger ?

3. Votre société a-t-elle été l'objet d'approches de la part d'un service de renseignement ou de sécurité étranger ? ☐ OUI ☐ NON

En cas de réponse(s) positive(s), décrire les circonstances :

-
4. Votre société a-t-elle fait l'objet ou fait-elle l'objet de velléités de rachat par une personne morale ou une personne physique étrangère ? ☐ OUI ☐ NON

5. Prévoit-elle ou est-elle en négociation de rachat/cession/fusion/absorption avec une société étrangère ? ☐ OUI ☐ NON

En cas de réponse(s) positive(s), décrire les circonstances :

-
6. Souhaitez-vous évoquer un point particulier avec le service chargé de l'instruction du dossier ? ☐ OUI ☐ NON

Liste des pièces requises pour le dossier d'habilitation « personne morale »

■ **Par la personne morale, en complément de la notice de sécurité :**

- ☐ Demande d'habilitation de la personne morale
- ☐ Demande d'habilitation de chaque dirigeant de droit de la personne morale
- ☐ Demande d'habilitation de l'officier de sécurité de la personne morale pressenti, candidate à l'habilitation, et lettre de désignation
- ☐ Kbis complet récent
- ☐ Kbis complet récent des personnes morales détenant la majorité du capital social
- ☐ Extrait en cours de validité du registre du commerce et des sociétés (modèle L bis) ou copie du bail de location
- ☐ Statuts à jour
- ☐ Composition du conseil d'administration et des organes de gouvernance (conseil de surveillance, directoire, etc.)
- ☐ Liste des autres conseils d'administration au sein desquels les représentants de la personne morale siègeraient
- ☐ Organigramme positionnant la société dans le groupe
- ☐ Organigramme fonctionnel de la personne morale (y compris les membres n'ayant pas le pouvoir d'engager la société) pour le siège social
- ☐ Organigramme fonctionnel et nominatif de l'établissement
- ☐ Pacte d'actionnaires (SA, SAS, etc.) ou pacte d'associés (SARL, SCI, etc.)
- ☐ Document relatif au(x) bénéficiaire(s) effectif(s) d'une société
- ☐ Plaquette de présentation de l'entreprise
- ☐ Liste des dettes principales par origine (prêts des établissements bancaires, etc.)
- ☐ Dernier bilan
- ☐ Liste des sous-traitants ou sous-contractants intervenant dans l'établissement, en identifiant les prestataires de services au titre d'un contrat sensible

Si la personne morale a déjà été habilitée :

- ☐ Attestation d'habilitation de l'autorité d'habilitation ou attestation d'avis de sécurité en cas de changement d'autorité d'habilitation
- ☐ Attestation de non-changement (fait et droit) de la personne morale depuis la dernière habilitation

Si le présent contrat/convention prévoit la détention d'informations et supports classifiés :

- ☐ Copie de l'avis technique d'aptitude physique du service enquêteur
- ☐ Attestation de conformité physique
- ☐ Identification et description de la protection, actuelle et envisagée, du local dans lequel est envisagé la conservation des informations et supports classifiés
- ☐ Plan de masse de l'établissement
- ☐ Organisation et moyens de protection et de gardiennage de l'établissement
- ☐ En cas d'avis technique avec réserve ou défavorable, lettre du dirigeant de la personne morale par laquelle celui-ci s'engage à mettre en place, avant le début de l'exécution des prestations du contrat nécessitant l'accès à des informations et des supports classifiés, les dispositions nécessaires à la protection des informations et supports classifiés qui lui seront confiés

Si le présent contrat/convention prévoit l'utilisation d'un système d'information classifié :

- ☐ Copie de la décision d'homologation
- ☐ Dossier de sécurité du système d'information

■ **À transmettre par l'autorité contractante ou l'acheteur :**

- ☐ Plan contractuel de sécurité ou projet

Annexe 21 – Modèle d’attestation d’avis de sécurité d’une personne morale

Ministère :

Organisme :

Date et numéro d’enregistrement :

ATTESTATION D’AVIS DE SECURITE D’UNE PERSONNE MORALE **Attestation of a positive facility clearance procedure**

Délivré par (ministère, organisme) :

Issued by (ministry, entity)

Date et lieu de délivrance :

Date and place of issue

Il est certifié, par le présent document, que la personne morale

It is hereby certified that the company

Dénomination ou raison sociale :

Full company name

fait l’objet d’un avis de sécurité (sans objection, restrictif ou défavorable)¹⁵⁶ délivré par :

hold a security notice delivered by

valable jusqu’au :

expiring on DD/MM/AAAA

pour l’accès aux informations et supports classifiés au niveau¹⁵⁷ :

for access up to and including the level

Nom, qualité, signature de l’autorité d’habilitation
et cachet de l’organisme

¹⁵⁶ Rayer la mention inutile.

¹⁵⁷ Niveau de classification maximum (maximum level of classification).

Annexe 22 – Modèle d’attestation d’habilitation d’une personne morale

Ministère :

Organisme :

Date et numéro d’enregistrement :

ATTESTATION HABILITATION D’UNE PERSONNE MORALE **Attestation of facility security clearance decision**

Délivré par (ministère, organisme) :

Issued by (ministry, entity)

Date et lieu de délivrance :

Date and place

Il est certifié par le présent document que la personne morale

It is hereby certified that the company

Dénomination ou raison sociale :

Full facility name

fait l’objet d’une décision d’habilitation délivrée par :

hold a facility security clearance decision delivered by

valable jusqu’au :

expiring on DD/MM/AAAA

pour l’accès aux informations et supports classifiés au niveau¹⁵⁸ :

for access up to and including the level

Nom, qualité, signature de l’autorité compétente
et cachet de l’organisme

¹⁵⁸ Niveau de classification maximum.
(maximum level of classification)

Annexe 23 – Modèle de décision d’habilitation d’une personne morale

Ministère :

Organisme :

Date et numéro d’enregistrement :

DECISION D’HABILITATION D’UNE PERSONNE MORALE

Le¹⁵⁹ :

décide que

Dénomination ou raison sociale :

Adresse :

N° RCS ou SIRET :

est habilitée jusqu’au¹⁶⁰ :

pour accéder à des informations et supports classifiés au(x) niveau(x) :

☐ TRÈS SECRET

☐ TRÈS SECRET UE/
EU TOP SECRET

☐ COSMIC TRÈS SECRET /
COSMIC TOP SECRET

☐ SECRET

☐ SECRET UE/
EU SECRET

☐ NATO SECRET/
NATO SECRET

☐ CONFIDENTIEL UE/
EU CONFIDENTIAL

☐ NATO CONFIDENTIEL/
NATO CONFIDENTIAL

dans le domaine suivant¹⁶¹ :

A

Le

Signature et cachet de l’autorité d’habilitation

¹⁵⁹ Autorité d’habilitation ou autorité ayant reçu délégation à cet effet.

¹⁶⁰ Date d’expiration de la décision.

¹⁶¹ Préciser le domaine en cas de limitation du champ de l’habilitation.

Annexe 24 – Modèle de décision de refus d’habilitation ou d’abrogation d’une décision d’habilitation d’une personne morale

Ministère :

Organisme :

Date et numéro d’enregistrement :

DECISION DE REFUS D’HABILITATION OU D’ABROGATION D’UNE DECISION D’HABILITATION D’UNE PERSONNE MORALE

☐ Refus d’habilitation

☐ Abrogation de la décision d’habilitation¹⁶² :

concernant

Dénomination ou raison sociale :

Adresse :

N° RCS ou SIRET :

La présente décision sera notifiée au représentant légal de la personne morale conformément à l’instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

À

Le

Nom, qualité, signature de l’autorité compétente¹⁶³
et cachet de l’organisme

¹⁶² Référence et date de la décision d’habilitation.

¹⁶³ Autorité de décision ayant reçu délégation à cet effet.

Annexe 25 – Modèle de récépissé de notification d’une décision de refus d’habilitation ou d’abrogation d’une décision d’habilitation d’une personne morale

Ministère :

Organisme :

Date et numéro d’enregistrement :

**RECEPISSE DE NOTIFICATION D’UNE DECISION DE REFUS D’HABILITATION OU D’ABROGATION D’UNE
DECISION D’HABILITATION D’UNE PERSONNE MORALE**

Je soussigné(e)¹⁶⁴ :

reconnais que l’autorité suivante¹⁶⁵ :

m’a notifié et remis ce jour la décision¹⁶⁶ :

prise par¹⁶⁷ :

portant refus de délivrance ou d’abrogation de l’autorisation d’accéder aux informations et supports classifiés au(x) niveau(x) :

- | | | |
|--------------------------------------|--|--|
| <input type="checkbox"/> TRÈS SECRET | <input type="checkbox"/> TRÈS SECRET UE/
EU TOP SECRET | <input type="checkbox"/> COSMIC TRÈS SECRET /
COSMIC TOP SECRET |
| <input type="checkbox"/> SECRET | <input type="checkbox"/> SECRET UE/
EU SECRET | <input type="checkbox"/> NATO SECRET/
NATO SECRET |
| | <input type="checkbox"/> CONFIDENTIEL UE/
EU CONFIDENTIAL | <input type="checkbox"/> NATO CONFIDENTIEL/
NATO CONFIDENTIAL |

Je prends connaissance des voies et délais de recours relatifs à cette décision, indiqués ci-après :

Il est rappelé qu’aux termes de l’article L. 411-2 du code des relations entre le public et l’administration « Toute décision administrative peut faire l’objet, dans le délai imparti pour l’introduction d’un recours contentieux, d’un recours gracieux ou hiérarchique qui interrompt le cours de ce délai. / Lorsque dans le délai initial du recours contentieux ouvert à l’encontre de la décision, sont exercés contre cette décision un recours gracieux et un recours hiérarchique, le délai du recours contentieux, prorogé par l’exercice de ces recours administratifs, ne recommence à courir à l’égard de la décision initiale que lorsqu’ils ont été l’un et l’autre rejetés ».

A
Le
Signature

¹⁶⁴ Nom, prénom du responsable de la personne morale.

¹⁶⁵ Dénomination de l’autorité d’habilitation ou de l’autorité administrative compétente.

¹⁶⁶ Référence et date de la décision.

¹⁶⁷ Autorité d’habilitation ou autorité ayant reçu délégation à cet effet.

Annexe 26 – Modèle d’attestation de conformité physique

Organisme :

Date et numéro d’enregistrement :

ATTESTATION DE CONFORMITE PHYSIQUE

Je soussigné(e)¹⁶⁸ :

atteste que les lieux où seront reçus, manipulés, élaborés, conservés et émis des informations et supports classifiés au sein de mon organisme¹⁶⁹

pour les établissements ci-dessous mentionnés :

au titre de la convention/du contrat :

bénéficient des conditions de protection prévues par la réglementation en vigueur.

La vérification de ces lieux a été effectuée le :

par le service enquêteur¹⁷⁰ :

et a donné lieu à un avis technique d’aptitude physique¹⁷¹ :

A
Le
Signature

¹⁶⁸ Nom, prénom, qualité du responsable de la personne morale.

¹⁶⁹ Dénomination ou raison sociale.

¹⁷⁰ Préciser le service ayant émis l’avis technique d’aptitude physique.

¹⁷¹ Date et référence de l’avis technique d’aptitude physique.

Annexe 27 – Modèle de certificat de mise aux normes de sécurité physique

Organisme :

Date et numéro d'enregistrement :

CERTIFICAT DE MISE AUX NORMES DE SECURITE PHYSIQUE

Je soussigné(e) ¹⁷² :

certifie que les locaux où seront reçus, manipulés, élaborés, conservés et émis des informations et supports classifiés au sein de mon organisme ¹⁷³

pour les établissements ci-dessous mentionnés :

au titre de la convention/du contrat :

à la suite de la vérification de ces locaux effectuée le :

par le service enquêteur ¹⁷⁴ :

ayant donné lieu à l'avis technique ¹⁷⁵ :

ont fait l'objet de travaux de mise en conformité et bénéficient des conditions de protection prévues par la réglementation en vigueur.

A
Le
Signature

¹⁷² Nom, prénom, qualité du responsable de la personne morale.

¹⁷³ Dénomination ou raison sociale.

¹⁷⁴ Préciser le service ayant émis l'avis technique d'aptitude physique.

¹⁷⁵ Date et référence de l'avis technique.

Annexe 28 – Prescriptions relatives aux plans contractuels de sécurité, aux plans de sécurité d’opérateurs et aux plans particuliers de protection

Ces plans comportent notamment les éléments suivants :

- l’engagement pris par le contractant ou l’opérateur d’importance vitale de s’assurer que les personnes qui ont besoin d’accéder à des informations et supports classifiés dans l’exercice de leurs fonctions ou l’accomplissement d’une mission ont fait l’objet d’une décision d’habilitation au niveau requis ;
- l’engagement pris par le contractant ou l’opérateur d’importance vitale de s’assurer que toutes les personnes qui ont accès à des informations et supports classifiés sont informées de leur responsabilité en matière de protection desdits informations et supports 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 et supports classifiés couverts par la convention, le contrat ou l’activité d’importance vitale ;
- l’identification des personnes parties à la chaîne de sécurité et chargées de coordonner la protection des informations et supports classifiés couverts par la convention, le contrat ou l’activité d’importance vitale, en particulier, l’officier de sécurité, l’officier de sécurité des systèmes d’information et le cas échéant, toute autre personne exerçant une fonction en lien avec la protection du secret ;
- les locaux dans lesquels la convention ou le contrat doit être exécuté et les informations et supports classifiés abrités et conservés ; la liste de ces locaux peut évoluer ;
- les systèmes d’information utilisés pour l’exécution de la convention ou du contrat ou l’activité d’importance vitale, dont la liste peut évoluer ;
- la liste des informations et supports classifiés et pouvant être générés, leurs niveaux respectifs de classification (guide de classification) et les modalités de déclassification ou déclassement ainsi que les conditions de protection dont chaque information ou support doit faire l’objet, conformément aux dispositions de l’instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale et aux textes réglementaires qui la déclinent, ainsi que leurs modalités d’archivage et de destruction ;
- les mesures particulières de sécurité qui doivent être prises pour l’exécution de ce contrat en vue de garantir la protection des informations et supports classifiés ;
- les modes de diffusion, y compris par voie dématérialisée, des informations et supports classifiés ;
- la liste des sous-contractants et sous-traitants identifiés lors de la rédaction du plan contractuel de sécurité et devant être mise à jour ;
- les modalités de diffusion des informations et supports classifiés aux sous-contractants et sous-traitants ;
- les modalités de gestion prévisionnelle des informations et supports classifiés et des systèmes d’information classifiés à la fin de la convention ou du contrat ou de la caducité du plan de sécurité opérateur ou du plan particulier de protection ;
- les modalités de destruction, d’archivage ou de restitution des informations et supports classifiés détenus par le contractant et, le cas échéant, ses sous-contractants et sous-traitants participant à l’exécution du contrat, en cas de cessation d’activité ou de dissolution du contractant ou, le cas échéant, de l’un de ses sous-contractants et sous-traitants participant à l’exécution du contrat.

Un exemplaire du plan contractuel de sécurité est transmis au service enquêteur chargé du suivi de la personne morale par l’autorité contractante ou l’acheteur.

Pour les titulaires d’une convention ou d’un contrat, ces éléments sont complémentaires des clauses-types générales (cf. Annexe 17).

Annexe 29 – Types de mesures de protection physique

L'ensemble des mesures de protection se compose de quatre éléments combinés ou dissociés en fonction du niveau de classification :

- un ou plusieurs dispositifs de dissuasion (indications) ;
- un ou plusieurs dispositifs de détection et d'alarme ;
- un ou plusieurs dispositifs de freinage (les obstacles) ;
- des moyens d'intervention articulés sur des procédures et des consignes préétablies.

Ainsi, selon une logique de défense en profondeur, 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 de risques et :

- être multifonctions, c'est-à-dire 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 et supports classifiés détenus, la protection physique comprend nécessairement un système d'information de sûreté dont la composante « contrôle d'accès » est décrite en Annexe 31.

Annexe 30 – Protection physique des informations et supports classifiés : méthode et recommandations

1. Méthode et effet final recherché en matière de protection physique des informations et supports classifiés

Dans un contexte où les malveillants disposent de capacités élevées, l'identification des moyens à mettre en œuvre pour garantir la protection physique des informations et supports classifiés, déclinée dans la politique de protection du secret, s'appuie sur une analyse de risques réalisée par l'organisme abritant ou, le cas échéant, par le service enquêteur.

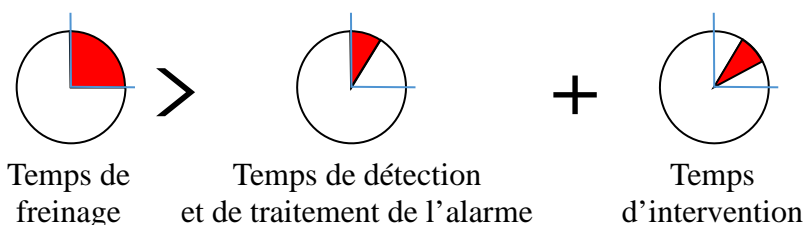
Conformément au principe de défense en profondeur qui doit guider l'analyse de risques, la protection des informations et supports classifiés s'obtient par une combinaison globale de moyens techniques, humains et organisationnels ainsi que, pour les systèmes d'information (SI), logiques.

Les moyens physiques mis en œuvre visent à détecter et freiner l'intrusion afin de permettre l'intervention. Ils doivent, en outre, permettre d'assurer la traçabilité en cas d'effraction. Ils s'inscrivent dans la profondeur en étagant différentes couches de protection, appelées également barrières (périphériques¹⁷⁶, périmétriques¹⁷⁷ et intérieures), qui s'appuient essentiellement sur :

- l'emprise (ou le site) et/ou le bâtiment ;
- le local (ou un groupe de locaux regroupés en zone) ;
- le meuble ;
- le système d'information (au niveau du poste utilisateur) contenant les informations et supports classifiés.

Le choix du dispositif global de protection par le responsable d'organisme, sur les conseils de l'officier de sécurité, doit permettre d'atteindre l'équation de sûreté, définie comme suit (T pour « temps ») :

$$\mathbf{T \text{ freinage} > T \text{ de détection et de traitement de l'alarme} + T \text{ intervention}}$$



Le temps de freinage équivaut au temps mis par l'intrus pour franchir les différentes barrières de protection placées entre la détection et les actifs ou la zone à protéger.

Le temps de détection et de traitement de l'alarme correspond au délai existant entre l'alarme par le premier moyen de détection d'intrusion et sa prise en compte effective par l'élément chargé d'exécuter l'intervention dans les meilleurs délais. Il inclut les délais de levée de doute et de transmission.

Le temps d'intervention est le temps mis par l'élément chargé de l'intervention (interne ou externe¹⁷⁸ à l'emprise du lieu abritant) pour se trouver au cœur de la zone d'action. Il tient compte de la distance à parcourir pour se rendre sur place, du temps moyen constaté pour la parcourir et de la disponibilité moyenne de l'élément d'intervention. En cas de doute, le temps majorant est retenu.

¹⁷⁶ Partie extérieure de l'emprise (ou site) à protéger, souvent matérialisée par la limite de propriété.

¹⁷⁷ Zone située entre la partie extérieure de la propriété et les locaux à protéger, souvent matérialisée par l'enveloppe du bâtiment

¹⁷⁸ L'élément d'intervention peut être externe et s'entend au sens des forces de sécurité intérieure, d'une société de gardiennage, etc.

Des moyens de freinage sont déployés en nombre et en nature suffisants pour que la somme des délais de freinage, depuis la première barrière dotée d'une détection (l'extérieur de l'emprise (ou site) ou du bâtiment) jusqu'aux informations et supports classifiés, soit supérieure au temps cumulé nécessaire à l'intervention.

2. Recommandations pour atteindre l'équation de sûreté

Les tableaux qui suivent formulent des recommandations sur les combinaisons possibles de moyens techniques, humains et organisationnels¹⁷⁹ permettant d'atteindre l'équation de sûreté, en réponse aux scénarios de menaces mis en évidence par l'analyse de risques.

Ces recommandations constituent un ensemble cohérent et homogène permettant de répondre à l'équation de sûreté. En cas d'impossibilité, des solutions équivalentes doivent être mises en œuvre pour atteindre cet objectif global.

Le niveau de protection des informations et supports classifiés repose sur la mise en place de trois barrières, réparties en classes de résistance (de la moins résistante à la plus résistante).

a. Classes du bâtiment (ou site) et/ou de l'emprise ou du site

CLASSE	DESCRIPTION
4	<p>Emprise (ou site) dont le périmètre est délimité physiquement, disposant d'une protection mécanique (clôture dont le franchissement n'est pas possible sans facilitateur¹⁸⁰) et dont tous les points d'accès sont contrôlés¹⁸¹ et assortis d'un dispositif de verrouillage mécanique ou électromécanique¹⁸².</p> <p style="text-align: center;">Ou</p> <p>Bâtiment dont les ouvrants accessibles¹⁸³ sont, dans la mesure du possible rendus discrets¹⁸⁴ et systématiquement dotés d'une protection mécanique (barreaux par exemple) et dont tous les points d'accès sont contrôlés¹⁸⁵ et assortis d'un dispositif de verrouillage mécanique ou électromagnétique¹⁸⁶.</p> <p><i>Nota</i> : Bien que la présence de moyens de détection d'intrusion ne soit pas imposée à ce niveau, l'existence d'un tel dispositif permet d'augmenter significativement le niveau de sûreté et peut donc être pris en compte dans l'équation de sûreté.</p>
3	<p>Enceinte¹⁸⁷ de classe 4 :</p> <ul style="list-style-type: none"> + contrôle d'accès conforme à l'Annexe 31, par identification¹⁸⁸ en périmétrie pour les flux piétons et véhicules, + personnel de surveillance¹⁸⁹ présent en permanence, effectuant des rondes dans l'enceinte et ses sous-ensembles,

¹⁷⁹ Les moyens organisationnels incluent les dispositifs juridiques.

¹⁸⁰ Pierre servant de marchepieds, perche, canne, escalade, etc.

¹⁸¹ Au moyen d'une solution ou d'un dispositif de contrôle d'accès adapté.

¹⁸² Ce dispositif assure un verrouillage permanent en cas de coupure de courant.

¹⁸³ Etant entendu que l'accessibilité s'apprécie au regard d'un seuil minimal de 40 cm × 11 cm.

¹⁸⁴ Moyen permanent interdisant les vues de l'extérieur (par exemple : film opacifiant).

¹⁸⁵ Au moyen d'une solution ou d'un dispositif de contrôle d'accès adapté.

¹⁸⁶ Ce dispositif assure un verrouillage permanent en cas de coupure du courant.

¹⁸⁷ Emprise (ou site) et/ou bâtiment.

¹⁸⁸ L'identification s'appuie sur un des facteurs suivants :

- ce que l'on sait (un code) ;
- ce que l'on a (un badge, une clé) ;
- ce que l'on est (comparaison biométrique ; cela inclut également ce que l'on sait faire).

¹⁸⁹ Par exemple, agent privé de sécurité, gardien-veilleur, garde.

	<ul style="list-style-type: none"> + élément d'intervention extérieur mobilisable sur alarme du personnel de surveillance. <p style="text-align: center;">ou</p> <p>Enceinte¹⁹⁰ de classe 4 :</p> <ul style="list-style-type: none"> + contrôle d'accès conforme à l'Annexe 31, par identification en périmétrie pour les flux piétons et véhicules ; + moyen de détection d'ouverture sur les ouvrants accessibles et les points d'accès reliés à une centrale d'intrusion + système de vidéosurveillance/détection sur les zones sensibles pour la levée de doute. <p>Ces dispositifs techniques de détection-alarme sont reliés à un élément d'intervention extérieur.</p>
2	<p>Les exigences de sécurité à remplir pour une emprise de classe 2 peuvent être atteintes par une combinaison de moyens humains et techniques, s'ajoutant aux éléments de la classe 4 et s'articulant de la façon suivante :</p> <p>Enceinte de classe 4 :</p> <ul style="list-style-type: none"> + contrôle d'accès conforme à l'Annexe 31, par identification en périmétrie pour les flux piétons et véhicules ; + personnel de surveillance présent en permanence effectuant des rondes dans l'enceinte et ses sous-ensembles ; + ensemble de télé-sécurité (télésurveillance + intervention) ; + dispositifs techniques de détection-alarme dont ; <ul style="list-style-type: none"> - un moyen de détection volumétrique sur les lieux de passage permettant d'accéder aux lieux abritant des informations et supports classifiés ; - traçabilité des entrées et sorties au niveau du bâtiment (ou d'un groupement de bâtiments) hébergeant les lieux abritant des informations et supports classifiés.
1	<p>Enceinte de classe 2 :</p> <ul style="list-style-type: none"> + présence à l'extérieur du local d'un système de vidéosurveillance des accès ; + moyen de détection d'intrusion placé sur tous les points d'accès des lieux abritant des informations et supports classifiés ; + présence permanente sur site d'un élément humain d'intervention.

b. Classes du local

Si l'emprise ne présente pas de dispositif de détection-alarme, un dispositif de ce type doit être installé au niveau du local.

Les parois (plafonds, sols et murs) des locaux ainsi que les ouvrants (portes, fenêtres, etc.)¹⁹¹, leurs serrures et leurs sûretés doivent présenter une résistance mécanique suffisante et homogène pour retarder l'intrusion et permettre la mise en œuvre des moyens d'intervention.

¹⁹⁰ Emprise (ou site) et/ou bâtiment.

¹⁹¹ Les dispositifs électromécaniques ou électromagnétiques de fermeture des ouvrants ne peuvent pas à eux seuls garantir l'intégrité des accès aux bâtiments ou aux emprises. Ils doivent obligatoirement être complétés par des systèmes mécaniques de verrouillage mis en service en dehors des périodes d'occupation des bâtiments.

Toutes les serrures des portes des locaux sont équipées d'un dispositif de verrouillage mécanique, électromagnétique ou motorisé comme dispositif principal¹⁹².

Les fabricants de serrure de sûreté à clef justifient que leurs produits possèdent :

- une technologie qui s'oppose aux techniques d'ouverture à l'aide d'outils manuels ;
- une conception qui complique l'usage de moyens d'ouverture fine (outils spécifiques dit « de crochetage »).

La fourniture et la reproduction de la clef ne doivent être possibles qu'après l'authentification d'une personne désignée auprès du fournisseur. La présence d'une carte dite de propriété ne peut pas, à elle seule, suffire comme moyen de protection contre la copie.

CLASSE	DESCRIPTION
d	Local avec bloc-porte à serrure mono-point et baies fermées (fenêtres, évacuateur de fumées, bloc d'un climatiseur, etc.).
c	<p>Local avec :</p> <ul style="list-style-type: none"> - bloc-porte (métallique ou en bois plein ou matériau équivalent) à serrure mécanique multipoints ; - sûreté à clef présentant un temps de résistance suffisant¹⁹³ ; - contrôle d'accès par identification ; - fenêtres protégées lorsqu'elles sont accessibles (depuis le sol, toit, corniche, descente d'eau pluviale, promontoire, etc.). <p>À l'intérieur des lieux abritant des informations et supports classifiés :</p> <ul style="list-style-type: none"> - moyen de détection volumétrique double technologie relié à une centrale d'intrusion ; ou - moyen de détection d'intrusion sur les ouvrants et serrure mécanique de fermeture sur les points d'accès (bloc-portes, baies, etc.).
b	<p>Local avec :</p> <ul style="list-style-type: none"> - bloc-porte renforcé équipé d'un système anti-dégondage, à serrure mécanique multipoints avec détecteur ; - sûreté à clef présentant un temps de résistance suffisant¹⁹⁴ ; - fenêtres protégées lorsqu'elles sont accessibles (depuis le sol, toit, corniche, descente d'eau pluviale, promontoire, etc.) ; - contrôle d'accès par authentification avec traçabilité des entrées et sorties. <p>À l'intérieur des lieux abritant les informations et supports classifiés :</p> <ul style="list-style-type: none"> - moyen de détection intrusion sur les ouvrants et serrure mécanique de fermeture sur les points d'accès (bloc-portes, baies, etc.) ; - moyen de détection volumétrique double technologie relié à une centrale d'intrusion ; - système permettant la levée de doute en dehors des heures de service (vidéosurveillance par ex.).

¹⁹² Le cas échéant, tout dispositif électronique est complété par un dispositif de verrouillage mécanique, électromagnétique ou motorisé. Les clés de secours sont conservées selon les dispositions du 7.2.3.

¹⁹³ En référence à la norme NF-EN 1627 ou équivalente, la classe de résistance CR3 (= 5 minutes) peut servir de référence. L'outillage est précisé.

¹⁹⁴ En référence à la norme NF-EN 1627 ou équivalente, la classe de résistance CR5 (= 15 minutes) peut servir de référence. L'outillage est précisé.

a	Chambre forte ¹⁹⁵ dont le bloc-porte est au minimum équipé des systèmes de sécurité des armoires fortes de classe B.
---	---

c. *Classes du meuble*

Les meubles de sécurité destinés à la conservation des informations et supports classifiés ne peuvent pas être ouverts frauduleusement sans effraction : toute tentative d'ouverture illégitime laisse des traces visibles détectables par l'utilisateur. Ils sont dotés par défaut de serrure à combinaison mécanique conforme à la norme EN1300 niveau B (ou équivalente) minimum.

Les meubles prévus pour protéger des équipements électroniques en fonctionnement sont naturellement pourvus d'ouïes de ventilation. En raison de l'accès visuel sur le contenu offert par leur présence, ces meubles ne doivent pas contenir de supports à lecture directe.

CLASSE	DESCRIPTION
C	Armoire forte à structure métallique d'au moins 2 millimètres d'épaisseur, munie d'une serrure mécanique à combinaison silencieuse et à manœuvre discrète. Les battants possèdent 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.
B	<p>Armoire forte de structure identique à la classe C :</p> <ul style="list-style-type: none"> + renforcement de la structure de la zone située entre la face avant de la porte et les organes essentiels dont la présence peut être vérifiée visuellement par démontage du foncet de porte (face intérieure de la porte) ; + dispositif délateur, à déclenchement mécanique et thermique, bloquant définitivement les mécanismes d'ouverture en cas de tentative d'ouverture illégitime ; + plombage du foncet de porte (face intérieure de la porte) permettant de détecter aisément un démontage ; + système à clef interdisant l'accès au dispositif de changement de la combinaison pour les modèles mécaniques ; + 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'un meuble à porte unique ; + dispositif qui interdit aux pênes de la porte principale, une fois sortis, de se rétracter à moins que la combinaison soit à nouveau composée ; + 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, conforme à la norme EN1300 niveau B au minimum, disposant d'un dispositif de composition discret et assurant la traçabilité des combinaisons, peut être autorisé s'il est justifié. <p>Le meuble équipé d'une combinaison électronique comporte une serrure mécanique à clef facilement permutable en supplément. Cette clef est prisonnière de la serrure tant que le pêne de la combinaison et les pênes du meuble ne sont pas sortis portes fermées ;</p> <ul style="list-style-type: none"> + système de tringlerie métallique en acier assurant sur la porte principale une répartition géographique de plusieurs pênes horizontaux et verticaux. Si une

¹⁹⁵ Le local répond aux exigences de la norme NF-EN 1143-1 ou équivalente.

	<p>poignée actionne ce système, elle possède un point de rupture pour éviter un effort trop conséquent sur la tringlerie.</p> <p>Les portes sont dépourvues de toute plaque de propreté et de tout enjoliveur.</p>
A	<p>Coffre-fort blindé sur toutes ses faces, d'un poids minimum à vide de 500 kg 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.</p> <p>Ce meuble comporte tous les systèmes de sécurité de la classe B</p> <ul style="list-style-type: none"> + une ou plusieurs serrures pouvant s'adapter à un nouveau jeu de clefs (serrures mécaniques dites à clef facilement permutable) ; + au moins une serrure dont la clef reste prisonnière du mécanisme tant que le pêne de la combinaison et les pénes du meuble ne sont pas sortis porte fermée. <p>La marque et le numéro de série du meuble sont estampillés de façon apparente et inaltérable, à l'extérieur de celui-ci, sur le corps et sur toutes les portes du meuble ; le numéro de série et l'année de fabrication de chaque serrure figurent sur celles-ci.</p>

d. Classes des postes utilisateurs classifiés

Il est possible de déroger aux mesures de protection logiques prévues ci-dessous en mettant en œuvre des mesures de protection compensatoires, sous réserve de leur validation formelle par l'autorité d'homologation pour le niveau *Secret* ou, pour le niveau *Très Secret*, par l'autorité qualifiée en sécurité des systèmes d'information.

DESCRIPTION	CLASSE γ DE BASE	CLASSE β RENFORCE	CLASSE α FORT
Intégrité physique des éléments constitutifs du SI	<p>Scellés génériques de contrôle d'ouverture de l'équipement avec traçabilité des équipements ayant reçu des scellés</p> <p>Contrôle ponctuel de l'intégrité des scellés par l'utilisateur.</p>	<p>Protection de la classe γ</p> <p>+ Contrôle annuel de l'intégrité des scellés.</p>	<p>Dispositif de détection d'ouverture de l'équipement ou scellés numérotés de contrôle d'ouverture de l'équipement avec traçabilité des équipements ayant reçu ces scellés</p> <p>Contrôle semestriel de l'intégrité des scellés.</p>

Confidentialité des données lorsque le terminal ¹⁹⁶ n'est pas en fonctionnement	Chiffrement des données utilisateur par un logiciel agréé pour la protection des informations portant la mention <i>Diffusion Restreinte</i> ou Stockage à distance des données sur l'infrastructure d'hébergement du SI ou Mémoire de masse extractible ou équipement mobile stockable dans un meuble de classe adaptée à la classification des données en clair	Chiffrement intégral du disque par un logiciel agréé pour la protection des informations portant la mention <i>Diffusion Restreinte</i> ou Stockage à distance des données sur l'infrastructure d'hébergement du SI ou Mémoire de masse extractible ou équipement mobile stockable dans un meuble de classe adaptée à la classification des données en clair	Protection de la classe β
Sécurité du contrôle d'accès de l'utilisateur	Mot de passe avec politique de sécurité des mots de passe conforme à la politique de sécurité de l'organisme	Dispositif d'authentification forte, par exemple basée sur une infrastructure de gestion de clefs (IGC) conforme au RGS** ¹⁹⁷ - homologuée par l'organisme	Dispositif d'authentification forte, par exemple basée sur une IGC qualifiée au moins RGS**.
Accès aux dispositifs d'import - export du poste utilisateur	Réservé aux utilisateurs authentifiés sur le terminal + supports amovibles préalablement « enrôlés » sur le système et autorisés pour cet utilisateur	Protection de la classe γ	Réservé aux utilisateurs assurant une fonction d'enregistrement des documents classifiés ou de gestion des échanges
Contrôle des équipements connectés au réseau	Désactivation des services non utilisés (conformité)	Protection de la classe γ + Authentification des équipements au réseau	Protection de la classe β
Cloisonnement et	Cloisonnement par	Cloisonnement entre les	Cloisonnement par le

¹⁹⁶ Le terminal s'entend comme le poste utilisateur fixe, nomade ou mobile, qui permet l'accès et le traitement des informations classifiées lorsqu'il est en fonctionnement.

¹⁹⁷ Le référentiel général de sécurité (RGS) publié par l'ANSSI est le cadre réglementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens. Son niveau est déterminé par le nombre d'étoiles (une, deux ou trois étoiles).

filtrage	fonction homogène au sein du SI (cloisonnement des réseaux locaux-LANs-par population)	utilisateurs d'une même population, exemple P-VLAN.	chiffre pour chaque poste utilisateur (tunnel dédié vers les services)
Capacité à restreindre la visualisation des IC par un tiers.	Disposition des terminaux par rapport aux ouvertures du local (portes, fenêtres, vasistas, hublots, etc.) et protection des vis-à-vis	Protection de la classe γ	Protection de la classe β

3. Tableaux de combinaison des classes

L'objectif final est d'égaliser ou de surpasser le temps de freinage tel que défini au point 1 pour obtenir un niveau de sécurité minimal pour les informations et supports classifiés.

La détermination de ce niveau est réalisée en deux temps :

- la classification des barrières (emprise (ou site) ou bâtiment, local, meuble ou moyen logique) à travers les moyens de détection d'intrusion ou de freinage qui leur sont associées ;
- la vérification de la validité de la combinaison des classes des barrières en fonction du niveau de classification des informations et supports classifiés.

Dans le cas où le niveau minimal de sécurité ne peut être atteint, il faut faire évoluer la classe d'une ou des barrières pour atteindre ce niveau.

a. Protection des informations et supports classifiés

La protection des informations et supports classifiés est assurée par trois barrières physiques successives au niveau de l'emprise (ou site) ou du bâtiment, du local et du meuble.

Les tableaux 1 et 2 définissent, pour chaque niveau de classification, la classe minimale du meuble en fonction des classes de protection du bâtiment et du local.

Tableau 1 : niveau *Secret*

CLASSE DU BATIMENT	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

Si des informations et supports classifiés au niveau *Secret*, hors systèmes d'information classifiés, ne peuvent être conservés dans un meuble de sécurité en raison de leur dimension, ils sont alors conservés dans un local renforcé correspondant aux caractéristiques suivantes :

- l'emprise (ou site) ou le bâtiment est au minimum de classe 3. Un contrôle permanent de la zone est organisé en s'appuyant sur un dispositif de détection-alarme relié à un élément d'intervention extérieur ;

- le local est au minimum de classe c avec un dispositif de détection-alarme indépendant de ceux de l'emprise/bâtiment¹⁹⁸.

S'agissant des systèmes d'informations classifiés au niveau *Secret*, les mesures de sécurité sont conformes à celles définies au tableau 3.

Tableau 2 : niveau *Très Secret*

CLASSE DU BATIMENT	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

Si des informations et supports classifiés au niveau *Très Secret*, hors systèmes d'information classifiés, ne peuvent être conservés dans un meuble de sécurité en raison de leur dimension, ils sont alors conservés dans un local renforcé correspondant aux caractéristiques suivantes :

- l'emprise (ou site) ou le bâtiment est au minimum de classe 2. Un contrôle permanent de la zone est organisé en s'appuyant sur un dispositif de détection-alarme relié à un élément d'intervention extérieur ;
- le local est au minimum de classe b avec un dispositif de détection-alarme indépendant de ceux de l'emprise/bâtiment⁹.

S'agissant des systèmes d'informations classifiés au niveau *Très Secret*, les mesures de sécurité sont conformes à celles définies au tableau 4.

b. Protection des systèmes d'information classifiés

La protection des systèmes d'information classifiés est assurée par la combinaison de deux barrières physiques et d'une barrière logique.

Les tableaux 3 et 4 définissent, pour chaque niveau de classification, la classe minimale de la protection logique en fonction des classes de protection physique de l'emprise (ou site) ou du bâtiment et du local. La lettre grecque désigne la classe du système d'information classifié.

Tableau 3 : niveau *Secret*

CLASSE DU BATIMENT	CLASSE DU LOCAL			
	a	b	c	d
1	γ	γ	β	β
2	γ	γ	β	β
3	γ	γ	β	α
4	γ	γ	α	interdit

¹⁹⁸ Les détecteurs sont généralement raccordés à une centrale locale placée dans le local ou la zone, sans qu'aucun élément (câblage par exemple) ne sorte de la zone à protéger. C'est la liaison entre les centrales locale et générale qui peut sortir de la zone, sous réserve qu'elle soit chiffrée. C'est en cela que le système est indépendant. Il ne s'agit donc pas obligatoirement de déployer deux systèmes d'information de détection d'intrusion.

Tableau 4 : niveau *Très Secret*

CLASSE DU BATIMENT	CLASSE DU LOCAL			
	a	b	c	d
1	β	β	interdit	interdit
2	β	β	interdit	interdit
3	β	β	interdit	interdit
4	interdit	interdit	interdit	interdit

Dans l'hypothèse où les barrières physiques sont assurées par le local et un meuble adapté¹⁹⁹, sans considération du niveau de protection du bâtiment, le tableau 5 définit, pour le seul niveau de classification *Secret*, la classe minimale de protection logique.

Tableau 5 : niveau *Secret*

CLASSE DU MEUBLE	CLASSE DU LOCAL			
	a	b	c	d
A	γ	γ	β	α
B	γ	γ	β	α
C	γ	β	α	α

¹⁹⁹ Par exemple, baie technique blindée ou armoire forte dédiée aux serveurs.

Annexe 31 – Contrôle d'accès

Le contrôle d'accès s'intègre dans un dispositif global de sécurité fondé sur son association avec les protections décrites à l'Annexe 29. Composant d'un système de management de la sûreté, il est déployé en cohérence avec les systèmes de détection d'intrusion et de vidéosurveillance. Il comprend les moyens suivants :

- identification pour recueillir les droits d'accès de l'individu et les transmettre à un moyen de traitement ;
- traitement qui valide, selon les droits accordés, les informations fournies par le moyen de contrôle afin de lever l'obstacle et de libérer le passage. Il recouvre trois méthodes : l'action d'une personne, celle d'un système automatisé ou la combinaison des deux ;
- freinage pour faire obstacle à l'intrusion et gagner le temps nécessaire à l'intervention ;
- les mesures organisationnelles et humaines qui permettent sa mise en œuvre et la conduite à tenir en cas d'incident.

Le contrôle d'accès consiste à vérifier si une personne demandant à accéder à un lieu est autorisée à pénétrer dans une enceinte ou un bâtiment. Il 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 :

- son utilité : accès à une emprise, un bâtiment, une zone, un local ;
- objet du contrôle : militaires, civils, scientifiques, personnel d'entretien, techniciens, personnel de maintenance ;
- menace dont il faut se protéger : menace interne, vandalisme ou renseignement.

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

- d'identifier, localiser, 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 existant 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, etc.) ;
- d'identifier les menaces potentielles (intrusion involontaire ou de curieux, pénétration délibérée de personnes initiées et/ou équipées, complicité interne, etc.) ;
- de prendre en compte les contraintes architecturales et réglementaires (incendie, protection du secret de la défense nationale, etc.).

Exemples de moyens pour contrôler les accès : portillons, portes à unicité de passage, barrières, sas, interphones, vidéophones, serrures à clefs, claviers à code, lecteurs de badge, lecteurs biométriques, lecteur de plaque d'immatriculation, etc.

Annexe 32 – Mesures applicables aux zones réservées

Dès lors que des informations et supports classifiés au niveau *Très Secret* 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.

Dans le cas des moyens mobiles (aéronefs, navires, etc.) conservant des informations et supports classifiés au niveau *Très Secret*, lorsque les conditions de création d'une zone protégée ne sont pas réunies, une zone réservée peut exceptionnellement y être créée et faire l'objet de modalités spécifiques de sécurité définies dans l'instruction ministérielle qui complètent ou se substituent aux dispositions suivantes.

Le traitement ou la conservation d'informations et supports classifiés dans ces locaux ne peut intervenir, sauf en cas d'impossibilité majeure, qu'après avis technique d'aptitude physique du service enquêteur quant à l'aptitude de ces locaux à accueillir des informations de niveau *Très Secret*.

Lorsque des services ou des organismes sont amenés à traiter de telles informations, pour des raisons opérationnelles et de manière temporaire, une zone réservée temporaire soumise aux mesures de sécurité détaillées plus haut peut être créée, y compris lorsque les conditions de création d'une zone protégée ne sont pas réunies.

Les lieux abritant des informations et supports classifiés au niveau *Très Secret*, faisant l'objet d'une classification spéciale, répondent aux normes complémentaires suivantes :

- un local pourvu d'ouvertures en nombre restreint à la protection renforcée ;
- ce local contient un meuble de sécurité approuvé ;
- un contrôle permanent du lieu est organisé, s'appuyant au minimum sur un des systèmes de protection décrits en Annexe 31.

1. 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 personnes qui y sont employées. Avant toute absence, ils vérifient la mise en sûreté des supports classifiés ainsi que la fermeture des meubles de sécurité et des bureaux.

En dehors des heures ouvrables, les autorités responsables s'organisent pour contrôler :

- le fonctionnement des systèmes de détection ;
- la fermeture des bureaux, des meubles de sécurité, 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'une enquête administrative conformément à l'article L. 114-1 du code de la sécurité intérieure et qui disposent de consignes écrites précisant leur mission. Ils ne sont pas autorisés à pénétrer dans ces zones réservées en l'absence du personnel de ces dernières, sauf nécessité de service (levée de doute, réglementation particulière, urgence avérée).

2. Contrôle des personnes et des visiteurs dans des lieux abritant des informations et supports classifiés Très Secret

Les personnes en service ayant accès, en raison de leurs fonctions au lieu abritant des éléments classifiés du niveau *Très Secret*, disposent d'un badge apparent.

Les visiteurs :

- font l'objet d'une autorisation individuelle de l'autorité responsable ;
- sont accompagnés pendant toute la durée de leur visite par une personne habilitée autorisée.

Le personnel d'entretien :

- a satisfait à une enquête administrative conformément à l'article L. 114-1 du code de sécurité intérieure ;
- appartient à une société ayant au préalable satisfait à une enquête administrative conformément à l'article L. 114-1 du code de la sécurité intérieure ;
- porte un badge apparent avec photographie ;
- intervient en présence d'une personne habilitée autorisée.

Annexe 33 – Clauses-types contractuelles 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 et de la sécurité nationale, le titulaire s'engage à prendre toutes les mesures utiles pour assurer lors de l'exécution du contrat la protection des informations et 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 et de la sécurité nationale.
3. Le titulaire reconnaît avoir fait signer une déclaration individuelle à l'ensemble du personnel appelé, sous sa responsabilité à un titre quelconque, à intervenir pour son compte pour exécuter les prestations. Par ce document, le personnel atteste :
 - avoir pris connaissance des articles 413-9 à 413-12 du code pénal ;
 - qu'il n'a pas, sous peine de poursuites pénales, à connaître ou détenir des informations couvertes par le secret de la défense et de la sécurité 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. Il ne peut être dérogé aux prescriptions ci-dessus, y compris en cas de 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.

Annexe 34 – Modèle de fiche navette

Ministère :

Organisme :

Date et numéro d'enregistrement :

FICHE NAVETTE

AVIS SUR UNE PERSONNE MORALE DANS LE CADRE D'UN CONTRAT SENSIBLE

Dénomination ou raison sociale de l'entreprise :

N° RCS du siège social ou SIRET de l'entreprise :

Adresse du siège social :

Identification de l'autorité contractante/acheteur bénéficiaire de la prestation :

Justification du recours au contrat sensible :

Dates prévisionnelles de début et de fin de travaux :

Lieu(x) d'exécution des prestations du contrat sensible :

Date d'expiration de la présente enquête administrative (s'il y a lieu) :

Avis du service enquêteur :

- ☐ Sans réserve
- ☐ Avec réserve

.....

.....

.....

A
Le
Autorité contractante/acheteur
Nom, prénom, qualité, signature

A
Le
Service enquêteur
Signature

Annexe 35 – Guide des mesures de sécurité applicables au cours d’une réunion impliquant des informations et supports classifiés

1. Avant la réunion

- l’organisateur détermine le niveau de classification de la réunion ;
- l’autorité destinataire de l’invitation adresse en temps utile à l’organisateur les noms et fonctions des personnes chargées de les représenter ainsi que leur niveau d’habilitation au moyen d’un certificat de sécurité ;
- l’organisateur établit la liste des participants, quel que soit leur qualité (auditeurs, conférenciers, assistants, techniciens chargés des projections ou essais, etc.). Cette liste est transmise à l’officier de sécurité ;
- l’officier de sécurité vérifie que l’habilitation des participants est valide et correspond au niveau des informations et supports qui vont être traités ;
- 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 et prend toutes les précautions utiles pour s’assurer qu’aucun appareil électronique ne soit susceptible de capter, réémettre ou enregistrer des sons, images ou informations sauf autorisation de sa part.

2. Au début de la réunion

- l’organisateur s’assure, conformément à la liste des participants, de l’identité et du niveau d’habilitation de ceux qui sont présents au vu de leur certificat de sécurité ;
- il leur indique le niveau maximal de classification des informations qui seront abordées au cours de la réunion et les règles de sécurité correspondantes ;
- assisté de l’officier de sécurité, l’organisateur 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 ou un ordinateur portable ou tout objet connecté. Dans certains établissements affectés aux besoins de la défense nationale, 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).

3. Pendant la réunion

- 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 ;
- l’organisateur peut interdire toute prise de note par les auditeurs. Il veille, en application des principes stricts de cloisonnement de l’information classifiée, en particulier au niveau *Très Secret*, y compris pour les classifications spéciales de ce niveau, à ce que la communication demeure limitée à l’objet de la réunion ;
- pendant les pauses, les participants sont autorisés à quitter la salle si la sécurité des supports classifiés qui y sont laissés est assurée. Les informations classifiées ne doivent pas être discutées en dehors de la salle de réunion ;
- 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.

4. À l’issue de la réunion

- les documents classifiés sont récupérés, rangés ou détruits sous la responsabilité de l’organisateur et de l’officier de sécurité dès lors qu’ils cessent d’être utiles ;
- l’organisateur rédige un document succinct, éventuellement classifié, dans lequel il est fait mention de la liste des participants, des domaines d’informations classifiées exposés ainsi que des mesures

prises pour en assurer la protection. Ce document peut être diffusé aux personnes qualifiées puis est géré dans les conditions fixées par la présente instruction ;

- 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 ;
- l'organisateur fait procéder à la récupération et à la mise en sécurité des supports classifiés éventuellement mis à la disposition des auditeurs (documents, graphiques, plans, films, bandes d'enregistrement, etc.) ainsi qu'à la destruction des supports provisoires et préparatoires ;
- les participants assument la pleine responsabilité de la protection de leurs documents de travail et de leurs notes, qui sont à classer au niveau correspondant à celui des informations recueillies. Ces documents sont détruits par leurs soins dès qu'ils ont cessé d'être utiles.

Annexe 36 – Exemple de document classifié

SECRET

SPÉCIAL FRANCE

À lieu, le date
N° enregistrement lors de l'émission

Déclassifié le [date]

Objet : [NP] Intitulé

[NP] Paragraphe d'introduction contenant des éléments non classifiés et non protégés.

1. Chapitre contenant des informations classifiées jusqu'au niveau *Secret* et protégées par la mention *Spécial France*

[NP] Paragraphe contenant des éléments non protégés.

Paragraphe contenant des éléments classifiés au niveau *Secret* et protégés par la mention *Spécial France*

2. Chapitre contenant des informations classifiées jusqu'au niveau *Secret* et protégées par la mention *Spécial France*

[DR] Paragraphe contenant des éléments protégés par la mention *Diffusion Restreinte*

Paragraphe contenant des éléments classifiés au niveau *Secret* et protégés par la mention *Spécial France*

SECRET

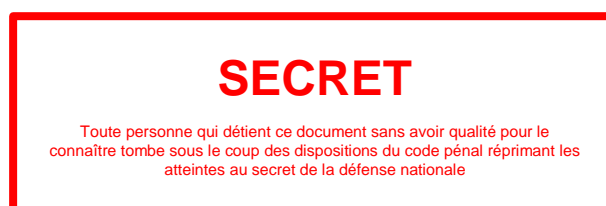
Annexe 37 – Modèles de timbres de classification et de protection

Les timbres sont apposés avec une encre indélébile de couleur rouge, sauf le timbre *Spécial France* qui est de couleur bleue.

1. Couverture et page de garde pour les documents reliés

Le timbre est apposé au milieu du bas de la couverture, selon les règles de marquage suivantes :

- Niveau de classification : centré, police Arial, gras, taille 18. Texte : taille 6 ;
- Epaisseur du cadre : 3 points.



La mention complémentaire de protection *Spécial France* est apposée sous le timbre de classification et respectent les règles de marquage prévues au point 2.

2. Pages du document

Le timbre est apposé au milieu du haut et du bas de la page (à l'exception du marquage *Spécial France* qui est apposé uniquement en haut de la page), selon les règles de marquage suivantes :

- Niveau de classification / *Spécial France* : centré, police Arial, gras, taille 18 ;
- Epaisseur du cadre : 2,5 points.



Annexe 38 – Modèles de timbres de déclassement et de déclassification

- Pour réévaluer le niveau de classification :

Classification à réévaluer le
[date]

- Pour abaisser le niveau de classification :

Le déclassement du niveau *Très Secret*
au niveau *Secret*
intervient le
par décision n°
du

- Pour rehausser le niveau de classification :

Le reclassement du niveau *Secret*
au niveau *Très Secret*
intervient le
par décision n°
du

- Pour déclassifier une information ou un support

À déclassifier
sur ordre de l'autorité émettrice

Déclassifié le [date]

DÉCLASSIFIÉ

Le [date]
par décision n°
du

Annexe 39 – Modèle de demande de reproduction d'un support classifié *Très Secret*

Ministère :

Organisme :

Date et numéro d'enregistrement :

DEMANDE DE REPRODUCTION D'UN SUPPORT CLASSIFIE *TRES SECRET*

Renseignements²⁰⁰ concernant le support classifié *Très Secret* dont la reproduction est demandée

- Numéro d'enregistrement :
- Date d'enregistrement :
- Numéro de l'exemplaire à partir duquel la reproduction sera effectuée :

Organisme demandeur :

Motif de la demande :

Copies demandées

- Nombre :
- Numérotation :
- Diffusion :

A

Le

Nom, qualité, signature de l'autorité responsable de la demande et cachet
de l'organisme

²⁰⁰ L'objet du support ne doit en aucun cas être mentionné.

Annexe 40 – Modèle d'autorisation de reproduction d'un support classifié Très Secret

Ministère :

Organisme :

Date et numéro d'enregistrement :

AUTORISATION DE REPRODUCTION D'UN SUPPORT CLASSIFIÉ *TRES SECRET*

Support classifié *Très Secret* dont la reproduction est autorisée

- Numéro d'enregistrement :
- Date d'enregistrement :
- Numéro de l'exemplaire à partir duquel la reproduction sera effectuée :

Organisme demandeur :

Référence de la demande :

Reproduction autorisée

- Nombre :
- Numérotation :
- Diffusion :

A

Le

Nom, qualité, signature de l'autorité responsable de la demande et cachet
de l'organisme

Destinataires :

.....
.....
.....

Annexe 41 – Modèle de bordereau de transmission de supports classifiés

Ministère :

Organisme :

Date et numéro d'enregistrement :

BORDEREAU DE TRANSMISSION DE SUPPORTS CLASSIFIES

A – B – B'

Références <i>(ne pas mentionner l'objet)</i>	Date de création	Niveau de classification/ Autres mentions	Numéro d'exemplaire	Numéro de copie	Noms des destinataires

Nom, qualité, signature de l'expéditeur
et cachet de l'organisme

Reçu le :

Par :

Organisme destinataire :

A : à conserver par le destinataire.

B : à renvoyer sans délai à l'expéditeur après émargement.

B' : à conserver en archives par l'expéditeur jusqu'à réception du feuillet B qui lui sera substitué.

Ministère :
Organisme :
Date et numéro d'enregistrement :

BORDEREAU DE TRANSMISSION DE SUPPORTS CLASSIFIES

A – B – B'

Références <i>(ne pas mentionner l'objet)</i>	Date de création	Niveau de classification/ Autres mentions	Numéro d'exemplaire	Numéro de copie	Noms des destinataires

Nom, qualité, signature de l'expéditeur
et cachet de l'organisme

Reçu le :
Par :
Organisme destinataire :

A : à conserver par le destinataire.
B : à renvoyer sans délai à l'expéditeur après émargement.
B' : à conserver en archives par l'expéditeur jusqu'à réception du feuillet B qui lui sera substitué.

Ministère :
Organisme :
Date et numéro d'enregistrement :

BORDEREAU DE TRANSMISSION DE SUPPORTS CLASSIFIES

A – B – B'

Références <i>(ne pas mentionner l'objet)</i>	Date de création	Niveau de classification/ Autres mentions	Numéro d'exemplaire	Numéro de copie	Noms des destinataires

Nom, qualité, signature de l'expéditeur
et cachet de l'organisme

Reçu le :
Par :
Organisme destinataire :

Annexe 42 – Modèle de décision de sécurité convoyeur

Ministère :

Organisme :

Date et numéro d'enregistrement :

DECISION DE SECURITE CONVOYEUR

Le²⁰¹ :

décide que

Madame/Monsieur²⁰² :

Date et lieu de naissance :

Grade ou titre :

Fonctions ou missions :

Peut effectuer le convoyage de supports classifiés jusques et y compris²⁰³ :

Cette décision est valable pour la mission suivante :

A

Le

Nom, qualité, signature de l'autorité compétente²⁰⁴ et
cachet de l'organisme

²⁰¹ Autorité d'habilitation ou autorité ayant reçu délégation à cet effet.

²⁰² Nom et prénom.

²⁰³ Préciser le niveau de classification et le domaine (France, UE ou OTAN).

²⁰⁴ Autorité d'habilitation ou autorité ayant reçu délégation à cet effet.

Annexe 43 – Modèle de certificat de courrier

Ministère :
Organisme :
Date et numéro d'enregistrement :

CERTIFICAT DE COURRIER

pour le convoyage international par porteur autorisé de supports et/ou matériels classifiés

Courier certificate

for international carriage of classified material and/or equipment

Nom du programme/projet :
Name of programme/project

Il est certifié que le porteur

This is to certify that the bearer

Madame/Monsieur (nom, prénom et titre) :
Ms/Mr (family name, first name and title)

Employé(e) par (organisme) :
Employed by (entity)

Né(e) le (jour/mois/année) :
Born on (day/month/year)

Pays :
Country

Nationalité :
Nationality

Titulaire du passeport ou de la carte d'identité n°
Holder of passport/identity card n°

Délivré(e) par (autorité) :
Issued by (issuing authority)

Le (jour/mois/année) :
On (day/month/year)

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

Départ le :
Departure on

Retour prévu le :
Planned return on

De (pays) :
From (country)

À (pays) :
To (country)

Via (pays traversés):
Through (countries)

Officier de sécurité de l'organisme

Entity security officer

Date, cachet et signature/*Date, stamp and signature*

Autorité nationale de sécurité ou autorité de sécurité déléguée

National Security Authority or Designed Security Authority
Date, cachet et signature/*Date, stamp and signature*

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

Annexe au certificat de courrier n°

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 content of this consignment is classified in the interests of national security of the countries mentioned 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 not be inspected other than by properly authorized persons or those with 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 porteur / *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 bearer;*
- 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 reclosed and marked by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened in order to show evidence of the opening;*
- 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 ensure the successful and secure delivery of the consignment.*

INSTRUCTIONS À L'ATTENTION DU PORTEUR AUTORISÉ

Annexe au certificat de courrier n°

Annexe à l'ordre de mission n°

Vous avez été désigné pour convoier un support classifié. Un certificat de courrier vous a été délivré. Avant le début du voyage, vous êtes informé des règles de sécurité relatives au convoiement de supports classifiés et de vos obligations en matière de sécurité durant ledit voyage (comportement à adopter, itinéraire, horaire, etc.). Il vous est également demandé de signer une déclaration attestant que vous avez lu et compris les obligations relatives à la sécurité.

Votre attention est appelée sur les généralités suivantes :

- 1) Vous êtes responsable du convoiement décrit dans le certificat de courrier.
- 2) Tout au long du voyage, l'envoi classifié doit rester en votre possession ou sous votre surveillance directe.
- 3) L'envoi ne doit pas être ouvert en cours de route, sauf dans les circonstances exposées au paragraphe 10 ci-dessous.
- 4) Vous ne devez 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 organismes publics ou privés, ayant les habilitations et aptitudes appropriées, peuvent être utilisés. Dans ce domaine, vous êtes renseigné par l'officier de sécurité de votre 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 devez prendre les mesures que vous jugez nécessaires à la protection de l'envoi, mais en aucun cas vous ne devez 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 passez en transit (cf. 12)). Si ces précisions ne vous ont pas été fournies, demandez-les à l'officier de sécurité de votre organisme.
- 8) Il appartient, à vous-même et à l'officier de sécurité de votre 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 point 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 traversez la frontière ; de ce fait, au cas où des agents demanderaient à connaître le contenu de l'envoi, vous leur montrez votre certificat de courrier et la présente note et vous insistez pour les présenter au chef du service de douane, de police et/ou d'immigration en personne. Cette démarche devrait 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 devez 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 demandez de refermer l'emballage ou de vous aider à le refermer immédiatement après achèvement de l'inspection.

Vous demandez 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 devez le faire savoir à l'officier de sécurité de l'organisme destinataire et à l'officier de sécurité de l'organisme

expéditrice, qui en informeront les autorités de sécurité compétentes de leur gouvernement respectif (autorité nationale de sécurité/autorité de sécurité déléguée).

- 11) À votre retour, vous devez produire un récépissé de l'envoi, signé par l'officier de sécurité de l'organisme ayant reçu l'envoi ou par une autorité de sécurité compétente du gouvernement destinataire.
- 12) Au cours de votre itinéraire, vous contactez les autorités désignées ci-après pour leur demander assistance :

DÉCLARATION DU PORTEUR AUTORISÉ

Annexe au certificat de courrier n°

Je, soussigné(e)²⁰⁵ :

employé(e) par²⁰⁶ :

déclare que

l'officier de sécurité de :

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

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

À mon arrivée, je remettrai au dépositaire désigné, contre signature du récépissé, les supports/matériels classifiés destinés à l'organisme réceptonnaire.

À
Le

Officier de sécurité
(nom, prénom et signature)

Porteur
(nom, prénom et signature)

²⁰⁵ Nom, prénom, fonction.

²⁰⁶ Dénomination de l'organisme.

DESCRIPTIF DU TRANSPORT

Annexe au certificat de courrier n°

Transport effectué par (nom et prénom) :

Transported by (family name and given name)

Départ le :

Departure on (date)

Retour prévu le :

Planned return (date)

De (pays) :

From (country)

À (pays) :

To (country)

Via (pays traversés) :

Through (countries)

Arrêts autorisés (pays) :

Authorized stops (countries)

Références du bordereau d'envoi ou du récépissé

References of shipping docket or receipt

Coordonnées des autorités susceptibles d'être contactées en cas de besoin :

Officials you may contact to request assistance

Officier de sécurité

(Nom, prénom et signature)

Compte rendu à remplir et signer à la fin du voyage

Je déclare sur l'honneur que durant le voyage correspondant au présent descriptif, il ne s'est produit à ma connaissance aucun événement ou acte, de mon fait ou du fait d'autrui, de nature à compromettre la sécurité de l'envoi, à l'exception des éléments signalés ci-dessous, le cas échéant :

.....

.....

.....

.....

À
Le

Officier de sécurité
(nom, prénom et signature)

Porteur
(nom, prénom et signature)

LISTE INVENTAIRE

Annexe au certificat de courrier n°

- | | | |
|---|--|---|
| <input type="checkbox"/> Documents, niveau(x) : | <input type="checkbox"/> <i>Secret</i> | <input type="checkbox"/> <i>Très Secret</i> |
| <input type="checkbox"/> Equipements, niveau(x) : | <input type="checkbox"/> <i>Secret</i> | <input type="checkbox"/> <i>Très Secret</i> |
| <input type="checkbox"/> Composants, niveau(x) : | <input type="checkbox"/> <i>Secret</i> | <input type="checkbox"/> <i>Très Secret</i> |

L'inventaire, inscrit au verso, a été approuvé par²⁰⁷ :

Dans le cadre du projet/contrat :

Référence de l'autorisation²⁰⁸ :

Toute inspection a été avalisée par²⁰⁹ :

Dans le cadre du projet/contrat :

Référence de l'autorisation²¹⁰ :

À
Le

Officier de sécurité
(nom, prénom et signature)

Porteur
(nom, prénom et signature)

RÉCÉPISSÉ²¹¹

Date et heure de remise au destinataire :

Cachet, timbre ou sceau officiel de l'organisme
destinataire

Nom et fonction du signataire

²⁰⁷ Nom, prénom, fonction, organisme, adresse de l'organisme.

²⁰⁸ Accordée par le directeur de programme au niveau *Très Secret*.

²⁰⁹ Nom, prénom, fonction, organisme, adresse de l'organisme.

²¹⁰ Accordée par le directeur de programme au niveau *Très Secret*.

²¹¹ Rayer si mention inutile. Nombre d'exemplaires :

- Procédure liste inventaire sans récépissé ;
- Procédure liste inventaire avec récépissé ;
- Archivage définitif : 1exemplaire officiel de sécurité expéditeur (dernier exemplaire en retour).

Annexe au certificat de courrier n°

PARTIE RESERVEE EN CAS D'INSPECTION DU OU DES COLIS

des douanes	
de la police	
des services de l'immigration	

Annexe 44 – Modèle de certificat de courrier multi-voyages

Ministère :
Organisme :
Date et numéro d'enregistrement :

CERTIFICAT DE COURRIER MULTI-VOYAGES
pour le convoi international par porteur autorisé de supports et/ou matériels classifiés
Multi-journey courier certificate
for international carriage of classified material and/or equipment

Nom du programme/projet :
Name of programme/project

Il est certifié que le porteur
This is to certify that the bearer

Madame/Monsieur (nom, prénom et titre) :
Ms/Mr (family name, first name and title)

Employé(e) par (organisme) :
Employed by (entity)

Né(e) le (jour/mois/année) :
Born on (day/month/year)

Pays :
Country

Nationalité :
Nationality

Titulaire du passeport ou de la carte d'identité n°
Holder of passport/identity card n°

Délivré(e) par (autorité) :
Issued by (issuing authority)

Le (jour/mois/année) :
On (day/month/year)

Est autorisé(e) à transporter des supports et/ou matériels classifiés (indiquer le n° des paquets, poids et dimensions de chaque colis) entre les pays suivants / Is authorized to carry classified material and/or equipment (number, weight and dimensions of each package) between the following countries:

Le porteur est autorisé à utiliser le présent certificat autant que de besoin, pour des transports de supports et/ou matériels classifiés entre les pays ci-dessus / The bearer is authorized to use this certificate as many times as necessary, for the transport of classified material and/or equipment between the countries mentioned above

jusqu'à (date de validité) :
until (validity date)

Officier de sécurité de l'organisme <i>Entity security officer</i> Date, cachet et signature/Date, stamp and signature	Autorité nationale de sécurité ou autorité de sécurité déléguée <i>National Security Authority or Designed Security Authority</i> Date, cachet et signature/Date, stamp and signature
---	--

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

Annexe au certificat de courrier multi-voyages n°

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 content of this consignment is classified in the interests of national security of the countries mentioned 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 not be inspected other than by properly authorized persons or those with 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 porteur / *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 bearer ;*
- 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 reclosed and marked by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened in order to show evidence of the opening ;*
- 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 ensure the successful and secure delivery of the consignment.*

INSTRUCTIONS À L'ATTENTION DU PORTEUR AUTORISÉ

Annexe au certificat de courrier multi-voyages n°
Annexe à l'ordre de mission n°

Vous avez été désigné pour convoier un support classifié. Un certificat de courrier vous a été délivré. Avant le début du voyage, vous êtes informé des règles de sécurité relatives au convoiement de supports classifiés et de vos obligations en matière de sécurité durant ledit voyage (comportement à adopter, itinéraire, horaire, etc.). Il vous est également demandé de signer une déclaration attestant que vous avez lu et compris les obligations relatives à la sécurité.

Votre attention est appelée sur les généralités suivantes :

- 1) Vous êtes responsable du convoiement décrit dans le certificat de courrier.
- 2) Tout au long du voyage, l'envoi classifié doit rester en votre possession ou sous votre surveillance directe.
- 3) L'envoi ne doit pas être ouvert en cours de route, sauf dans les circonstances exposées au paragraphe 10 ci-dessous.
- 4) Vous ne devez 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 organismes publics ou privés, ayant les habilitations et aptitudes appropriées, peuvent être utilisés. Dans ce domaine, vous êtes renseigné par l'officier de sécurité de votre 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 devez prendre les mesures que vous jugez nécessaires à la protection de l'envoi, mais en aucun cas vous ne devez 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 passez en transit (cf. 12)). Si ces précisions ne vous ont pas été fournies, demandez-les à l'officier de sécurité de votre organisme.
- 8) Il appartient, à vous-même et à l'officier de sécurité de votre 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 point 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 traversez la frontière ; de ce fait, au cas où des agents demanderaient à connaître le contenu de l'envoi, vous leur montrez votre certificat de courrier et la présente note et vous insistez pour les présenter au chef du service de douane, de police et/ou d'immigration en personne. Cette démarche devrait 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.
- 11) Vous devez 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 demandez de refermer l'emballage ou de vous aider à le refermer immédiatement après achèvement de l'inspection.
- 12) Vous demandez 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.
- 13) S'il vous a été demandé d'ouvrir l'envoi dans les circonstances exposées ci-dessus, vous devez le faire savoir à l'officier de sécurité de l'organisme destinataire et à l'officier de sécurité de

l'organisme expéditrice, qui en informeront les autorités de sécurité compétentes de leur gouvernement respectif (autorité nationale de sécurité/autorité de sécurité déléguée).

- 14) À votre retour, vous devez produire un récépissé de l'envoi, signé par l'officier de sécurité de l'organisme ayant reçu l'envoi ou par une autorité de sécurité compétente du gouvernement destinataire.
- 15) Au cours de votre itinéraire, vous contactez les autorités désignées ci-après pour leur demander assistance :

DÉCLARATION DU PORTEUR AUTORISÉ

Annexe au certificat de courrier multi-voyages n°

Je, soussigné(e)²¹² :

employé(e) par²¹³ :

déclare que

l'officier de sécurité de :

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

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

À mon arrivée, je remettrai au dépositaire désigné, contre signature du récépissé, les supports/matériels classifiés destinés à l'organisme réceptonnaire.

À

Le

Officier de sécurité
(nom, prénom et signature)

Porteur
(nom, prénom et signature)

²¹² Nom, prénom, fonction.

²¹³ Dénomination de l'organisme.

DESCRIPTIF DU TRANSPORT

Annexe au certificat de courrier multi-voyages n°

Transport effectué par (nom et prénom) :

Transported by (family name and given name)

Départ le :

Departure on (date)

Retour prévu le :

Planned return (date)

De (pays) :

From (country)

À (pays) :

To (country)

Via (pays traversés) :

Through (countries)

Arrêts autorisés (pays) :

Authorized stops (countries)

Références du bordereau d'envoi ou du récépissé

References of shipping docket or receipt

Coordonnées des autorités susceptibles d'être contactées en cas de besoin :

Officials you may contact to request assistance

Officier de sécurité

(Nom, prénom, signature)

Compte rendu à remplir et signer à la fin du voyage

Je déclare sur l'honneur que durant le voyage correspondant au présent descriptif, il ne s'est produit à ma connaissance aucun événement ou acte, de mon fait ou du fait d'autrui, de nature à compromettre la sécurité de l'envoi, à l'exception des éléments signalés ci-dessous, le cas échéant

:

.....

.....

.....

.....

À

Le

Officier de sécurité
(nom, prénom et signature)

Porteur
(nom, prénom et signature)

LISTE INVENTAIRE

Annexe au certificat de courrier multi-voyages n°

- | | | |
|---|--|---|
| <input type="checkbox"/> Documents, niveau(x) : | <input type="checkbox"/> <i>Secret</i> | <input type="checkbox"/> <i>Très Secret</i> |
| <input type="checkbox"/> Equipements, niveau(x) : | <input type="checkbox"/> <i>Secret</i> | <input type="checkbox"/> <i>Très Secret</i> |
| <input type="checkbox"/> Composants, niveau(x) : | <input type="checkbox"/> <i>Secret</i> | <input type="checkbox"/> <i>Très Secret</i> |

L'inventaire, inscrit au verso, a été approuvé par²¹⁴ :

Dans le cadre du projet/contrat :

Référence de l'autorisation²¹⁵ :

Toute inspection a été avalisée par²¹⁶ :

Dans le cadre du projet/contrat :

Référence de l'autorisation²¹⁷ :

À
Le

Officier de sécurité
(nom, prénom et signature)

Porteur
(nom, prénom et signature)

RÉCÉPISSÉ²¹⁸

Date et heure de remise au destinataire :

Cachet, timbre ou sceau officiel de l'organisme
destinataire

Nom et fonction du signataire

²¹⁴ Nom, prénom, fonction, organisme, adresse de l'organisme.

²¹⁵ Accordée par le directeur de programme au niveau *Très Secret*.

²¹⁶ Nom, prénom, fonction, organisme, adresse de l'organisme.

²¹⁷ Accordée par le directeur de programme au niveau *Très Secret*.

²¹⁸ Rayer si mention inutile. Nombre d'exemplaires :

- Procédure liste inventaire sans récépissé ;
- Procédure liste inventaire avec récépissé ;
- Archivage définitif : 1 exemplaire officiel de sécurité expéditeur (dernier exemplaire en retour).

INVENTAIRE

Annexe au certificat de courrier multi-voyages n°

Numéro d'ordre	Description précise des documents, équipements et/ou composants classifiés	Nombre d'exemplaires ou quantités	Nombre de pages par document y compris annexes	Nombre total de pages	Nombre de paquets
	Total :	Total :		Total :	

PARTIE RESERVEE EN CAS D'INSPECTION DU OU DES COLIS

Visa et sceau du chef :

des douanes	
de la police	
des services de l'immigration	

Annexe 45 – Modèle de procès-verbal de destruction de supports classifiés *Secret* ou *Très Secret*

Ministère :

Organisme :

Date et numéro d'enregistrement :

PROCES-VERBAL DE DESTRUCTION DE SUPPORTS CLASSIFIES SECRET OU TRES SECRET

Date et lieu de la destruction :

Référence de l'ordre de destruction :

Nom, grade, fonction du détenteur responsable :

Référence du support ²¹⁹	Date	Catégorie (éventuellement)	Numéro d'exemplaire	Numéro de copie

Nom, fonction et signature du témoin (Uniquement
pour la destruction d'un support *Très Secret*)

Nom, fonction, signature du détenteur responsable et
cachet de l'organisme

Copie à²²⁰

²¹⁹ Les références doivent être portées sur le procès-verbal de telle manière qu'il soit impossible de les modifier ou de les compléter ultérieurement, ajoutant par exemple, entre deux mentions, les références d'un autre document ou support.

²²⁰ Autorité ayant donné l'ordre de destruction.

Annexe 46 – Modèle d’inventaire des supports classifiés

Cote : [À renseigner par le service d’archives].

INVENTAIRE DES SUPPORTS CLASSIFIES CONTENUS DANS LA PRESENTE ENVELOPPE

Numéro d’ordre [à reporter sur le support inventorié]	Nom du service ayant procédé à la classification ou de l’auteur du support classifié	Numéro d’enregistrement	Date d’émission	Titre ou objet du document	Niveau de classification	Date d’échéance de la classification
1						
2						
3						
4						
5						