

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DES ARMÉES

Arrêté du 15 mars 2021 portant approbation de l'instruction ministérielle n° 900 sur la protection du secret et des informations *diffusion restreinte* et sensibles

NOR : ARMM2108698A

La ministre des armées,

Vu le code de la défense, notamment ses articles R. 2311-2 à R. 2311-9-1 ;

Vu le code pénal, notamment son article 413-9 ;

Vu l'arrêté du 29 novembre 2011 portant création de traitements automatisés de données à caractère personnel relatifs à la gestion des habilitations au secret de la défense nationale ;

Vu l'arrêté du 21 mars 2012 modifié portant délégation des pouvoirs du ministre de la défense en matière de décisions d'habilitation à connaître des informations et supports couverts par le secret de la défense nationale ;

Vu l'arrêté du 13 novembre 2020 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale,

Arrête :

Art. 1^{er}. – L'instruction ministérielle n° 900 sur la protection du secret et des informations *diffusion restreinte* et sensibles annexée au présent arrêté est approuvée.

Art. 2. – Le présent arrêté entre en vigueur le 1^{er} juillet 2021.

Art. 3. – Le présent arrêté sera publié au *Journal officiel* de la République française sans son annexe n° 20.

Fait le 15 mars 2021.

FLORENCE PARLY

ANNEXE



**MINISTÈRE
DES ARMÉES**

*Liberté
Égalité
Fraternité*

INSTRUCTION MINISTÉRIELLE
N°900/ARM/CAB/NP du 15 mars 2021

RELATIVE À
LA PROTECTION DU SECRET ET DES
INFORMATIONS *DIFFUSION RESTREINTE* ET
SENSIBLES

Abroge et remplace l'instruction ministérielle
N°900/DEF/CAB/DR du 26 janvier 2012

TABLE DES MATIERES

TITRE 1 : PRINCIPES GENERAUX	1
TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE.....	5
INTRODUCTION : CHAINES FONCTIONNELLES DE LA PROTECTION DU SECRET	5
2.1 : FONCTIONNAIRE DE SECURITE DE DEFENSE ET FONCTIONNAIRE DE SECURITE DES SYSTEMES D'INFORMATION	8
2.2 : SERVICES ENQUETEURS DU MINISTERE DE LA DEFENSE	10
2.3 : AUTORITES D'HABILITATION DU MINISTERE DE LA DEFENSE	12
2.4 : RESPONSABILITES DU RESPONSABLE D'ORGANISME	14
2.5 : OFFICIER DE SECURITE	16
2.6 : OFFICIER DE SECURITE DES SYSTEMES D'INFORMATION DES ORGANISMES LIES PAR CONTRAT OU CONVENTION.....	21
2.7 : BUREAU DE PROTECTION DU SECRET.....	24
2.8 : FORMATION ET SENSIBILISATION	27
2.9 : INSPECTIONS, AUDITS ET CONTRÔLES DES ORGANISMES DETENANT DES INFORMATIONS ET SUPPORTS CLASSIFIES, DES INFORMATIONS <i>DIFFUSION RESTREINTE</i> OU SENSIBLES	30
TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES.....	33
INTRODUCTION : PROCESSUS D'HABILITATION DU PERSONNEL	33
3.1 : CATALOGUE DES EMPLOIS	34
3.2 : DEMANDE D'HABILITATION	36
3.3 : AVIS DE SECURITE	39
3.4 : MISE EN EVEIL ET MISE EN GARDE.....	42
3.5 : DECISION D'HABILITATION OU DE REFUS D'HABILITATION	44
3.6 : GESTION ET FIN DE L'HABILITATION	47
3.7 : CAS DES HABILITATIONS OTAN ET UE	51
3.8 : CONTROLE DES RESSORTISSANTS ETRANGERS EN CAS D'HABILITATION OU D'ACCES A DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES OU CONTENANT DES INFORMATIONS <i>DIFFUSION RESTREINTE</i> OU SENSIBLES	53
3.9 : ENQUETES ADMINISTRATIVES PREALABLES AUX ACCES AUX SITES ET EMPLOIS SENSIBLES	56
3.10 : OBLIGATION DE RESERVE, DISCRETION PROFESSIONNELLE ET SECRET PROFESSIONNEL POUR LES AGENTS DU MINISTERE DE LA DEFENSE	61
3.11 : PROTECTION DES DONNEES A CARACTERE PERSONNEL COMPORTANT LA MENTION DE LA QUALITE DE MILITAIRE (DCPM)	65
TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS.....	69
PRINCIPES GENERAUX DE LA PROTECTION DU SECRET DANS LES CONTRATS	69
4.1 : ACTEURS DES CONTRATS.....	72
4.2 : CHOIX DU TYPE DE CONTRAT	76
4.3 : MODALITES DE PASSATION D'UN CONTRAT SENSIBLE	79
4.4 : PRISE EN COMPTE DE LA PROTECTION DU SECRET DANS LA PROCEDURE D'ACHAT.....	81
4.5 : PROCEDURE D'ACHAT POUR LES CONTRATS AVEC ACCES OU DETENTION D'INFORMATIONS ET SUPPORTS CLASSIFIES : SELECTION DES CANDIDATS ADMIS A SOUMISSIIONNER ET CONTENU DES OFFRES	83
4.6 : PROCEDURE D'ACHAT POUR LES CONTRATS AVEC ACCES OU DETENTION D'INFORMATIONS ET SUPPORTS CLASSIFIES : CONSULTATION DES ISC DURANT LA PERIODE D'ELABORATION DES OFFRES	86
4.7 : PROCEDURE D'ACHAT POUR LES CONTRATS AVEC ACCES OU DETENTION D'INFORMATIONS ET SUPPORTS CLASSIFIES : EXAMEN DES OFFRES, CHOIX DE L'ATTRIBUTAIRE ET SIGNATURE	89

4.8 : PROCEDURE D'ACHAT POUR LES CONTRATS AVEC ACCES OU DETENTION D'INFORMATIONS ET SUPPORTS CLASSIFIES : PLAN CONTRACTUEL DE SECURITE	91
4.9 : CAS D'UNE PERSONNE MORALE ETRANGERE CANDIDATE A LA PASSATION D'UN CONTRAT AVEC ACCES OU DETENTION D'INFORMATIONS ET SUPPORTS CLASSIFIES	95
4.10 : HABILITATION INITIALE DE LA PERSONNE MORALE	97
4.11 : GESTION ET FIN DE L'HABILITATION DE LA PERSONNE MORALE	101
4.12 : GESTION DES SOUS-CONTRACTANTS DANS LES CONTRATS AVEC ACCES OU DETENTION D'INFORMATIONS ET SUPPORTS CLASSIFIES	103
4.13 : CONTRÔLES DES PERSONNES MORALES PAR LES AUTORITES CONTRACTANTES DE REFERENCE, LES AUTORITES D'HABILITATION ET L'AUTORITE DE SECURITE DELEGUEE.....	105

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS

CLASSIFIES 108

INTRODUCTION : NORMES DE PROTECTION PHYSIQUE ET LOGIQUE APPLICABLES AUX INFORMATIONS ET SUPPORTS CLASSIFIES.....	108
5.1 : ZONE RESERVEE.....	118
5.2 : ELEMENTS CLASSIFIÉS CONSERVÉS « HORS COFFRE »	122
5.3 : ACTIVITÉS NÉCESSITANT L'ACCÈS À DES INFORMATIONS ET SUPPORTS CLASSIFIES EN DEHORS DE LEUR LIEU ABRITANT	125
5.4 : MATERIEL D'IMPRESSION, DE REPRODUCTION ET DE DESTRUCTION DES INFORMATIONS ET SUPPORTS CLASSIFIES	128
5.5 : PROTECTION CONTRE LES COMPROMISSIONS VIA LES EQUIPEMENTS ELECTRONIQUES	130
5.6 : CONTROLES D'APTITUDES PHYSIQUE A LA DETENTION D'INFORMATIONS ET SUPPORTS CLASSIFIES.....	133
5.7 : ACCES DE PERSONNES NON QUALIFIEES AUX LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES	138
5.8 : ACCES DES MAGISTRATS AUX INFORMATIONS ET SUPPORTS CLASSIFIES	141

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT

PRIVE 144

REMARQUES GENERALES	144
6.1 : CARTOGRAPHIE DES SYSTEMES D'INFORMATION DES ENTITES CONTRACTANTES.....	145
6.2 : LE PROCESSUS D'HOMOLOGATION	147
6.3 : CONTRÔLE D'APTITUDE AU TRAITEMENT D'INFORMATIONS NUMERIQUES CLASSIFIEES	154
6.4 : LES AUDITS DE SECURITE.....	157
6.5 : SOUS-CONTRACTANCE A UN TIERS EN MATIERE INFORMATIQUE	159
6.6 : PRISE EN COMPTE DE LA SECURITE DANS LE CYCLE DE VIE DES SYSTEMES D'INFORMATION	162
6.7 : EQUIPEMENTS MOBILES ET SUPPORTS AMOVIBLES.....	166
6.8 : SUPERVISION DE SECURITE D'UN SYSTEME D'INFORMATION	169
6.9 : LES ACSSI.....	171
6.10 : SECURITE DU CABLAGE ET CIRCUITS APPROUVES	174

TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES TOUT AU LONG

DE LEUR CYCLE DE VIE 176

PRINCIPES ET DEFINITIONS	176
7.1 : ELABORATION D'INFORMATIONS ET SUPPORTS CLASSIFIES.....	179
7.2 : MENTION DE PROTECTION <i>DIFFUSION RESTREINTE</i>	184
7.3 : MENTION DE PROTECTION <i>SPECIAL FRANCE</i>	188
7.4 : MENTION DE PROTECTION <i>COMMUNICABLE A [SERVICES, ETATS, ORGANISATIONS INTERNATIONALES, INSTITUTIONS, ORGANES OU ORGANISMES DE L'UE]</i>	190
7.5 : MENTIONS DE CONFIDENTIALITE SPECIFIQUES	191

7.6 : CAS PARTICULIER DES INFORMATIONS ET SUPPORTS CLASSIFIES <i>TRES SECRET</i>	
« CLASSIFICATION SPECIALE »	197
7.7 : ENREGISTREMENT ET INVENTAIRE	198
7.8 : DIFFUSION ET TRANSPORT DES INFORMATIONS ET SUPPORTS CLASSIFIES.....	201
7.9 : IMPRESSION/REPRODUCTION DES INFORMATIONS CLASSIFIEES.....	208
7.10 : STOCKAGE DES INFORMATIONS ET SUPPORTS CLASSIFIES	210
7.11 : VERSEMENT DANS UN SERVICE D'ARCHIVES	212
7.12 : DECLASSIFICATION OU DECLASSEMENT D'UNE INFORMATION CLASSIFIEE	214
7.13 : DESTRUCTION DES INFORMATIONS ET SUPPORTS CLASSIFIES ET DES INFORMATIONS DIFFUSION RESTREINTE OU SENSIBLES	218
7.14 : EVACUATION ET DESTRUCTION D'URGENCE	220
TITRE 8 : GESTION ET REPRESSION DES ATTEINTES AU SECRET DE LA DEFENSE NATIONALE	222
GENERALITES	222
8.1 : TRAITEMENT DES COMPROMISSIONS	224
8.2 : COMPROMISSION AFFECTANT UN SYSTÈME D'INFORMATION.....	227
8.3 : COMPROMISSION D'INFORMATIONS CLASSIFIEES ETRANGERES	229
TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES.....	231
PRINCIPES DE LA PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES	231
9.1 : AUTORITE NATIONALE DE SECURITE ET AUTORITE DE SECURITE DELEGUEE.....	232
9.2 : CONDITIONS POUR ECHANGER DES INFORMATIONS ET SUPPORTS CLASSIFIES AVEC L'ETRANGER	234
9.3 : CAS SPECIFIQUE DES CONTRATS INTERNATIONAUX : PLAN CONTRACTUEL DE SECURITE INTERNATIONAL (PCSI).....	238
9.4 : ÉCHANGES D'INFORMATIONS ET SUPPORTS CLASSIFIES AVEC LES ORGANISATIONS INTERNATIONALES	240
9.5 : ECHANGES NUMERIQUES CLASSIFIES AVEC L'ETRANGER	246
9.6 : MISSIONS ET SEJOURS A L'ETRANGER	247
ANNEXES.....	251
ANNEXE 1 : MODELE DE FICHE CONFIDENTIELLE	252
ANNEXE 2 : LISTE DES EMPLOIS SENSIBLES	253
ANNEXE 3 : MODELE DE DOSSIER DE DEMANDE D'HABILITATION D'UNE PERSONNE MORALE	254
ANNEXE 4 : MODELE DE DECISION DE CREATION DE ZONE RESERVEE	260
ANNEXE 5 : LISTE DES PIECES CONSTITUTIVES DU DOSSIER D'APTITUDE D'UN ETABLISSEMENT POUR L'EXECUTION D'UN CONTRAT AVEC DETENTION D'INFORMATIONS ET SUPPORTS CLASSIFIES	261
ANNEXE 6 : MODELE D'AVIS TECHNIQUE D'APTITUDE / D'INAPTITUDE PHYSIQUE	262
ANNEXE 7 : MODELE D'AVIS D'APTITUDE SUITE A UNE COMMISSION DE MISE EN CONFORMITE.....	264
ANNEXE 8 : CONDITIONS D'EMPLOI DES NIVEAUX DE CLASSIFICATION <i>SECRET</i> ET <i>TRES SECRET</i>	266
ANNEXE 9 : MODELES DE TIMBRES DE CLASSIFICATION, DE PROTECTION, DE DECLASSEMENT ET DE DECLASSIFICATION DES INFORMATIONS ET SUPPORTS CLASSIFIES	275
ANNEXE 10 : MODELE D'ENGAGEMENT DE NON DIVULGATION DES INFORMATIONS ET SUPPORTS DIFFUSION RESTREINTE	277
ANNEXE 11 : MODELE DE FICHE DE POSITION	278
ANNEXE 12 : MODELE DE CAHIER D'ENREGISTREMENT DU COURRIER CLASSIFIE	279
ANNEXE 13 : MODELE D'UN ISC DE NIVEAU <i>TRES SECRET</i>	281
ANNEXE 14 : MODELE D'INVENTAIRE OCCASIONNEL	285
ANNEXE 15 : MODELE DE DEMANDE DE DESTRUCTION D'ISC <i>TRES SECRET</i>	287

ANNEXE 16 : MESURES CONSERVATOIRES ET CONDUITE A TENIR EN CAS DE
COMPROMISSION POSSIBLE AFFECTANT UN SYSTEME D'INFORMATION289

ANNEXE 17 : DOCUMENTS TRAITANT D'INFORMATIONS ET SUPPORTS CLASSIFIES A
L'INTERNATIONAL.....290

ANNEXE 18 : ORGANISATION DES RESEAUX OTAN ET UE.....296

ANNEXE 19 : MISE EN GARDE DES FRANÇAIS EN DEPLACEMENT OU EN MISSION A
L'ETRANGER299

ANNEXE 20300

TITRE 1 : PRINCIPES GENERAUX**1****Références :**

- Règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), notamment ses articles 2, 23, 24, 30 et 33
- Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 6, 31, 58, 115 et suivants
- Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment son article 85 et ses articles 140 et suivants
- Arrêté du 13 novembre 2020 portant approbation de l'instruction générale n°1300 sur la protection du secret de la défense nationale (IGI 1300/SGDSN/PSE/PSD sur la protection du secret de la défense nationale)
- II 2100/SGDN/SSD pour l'application en France du système de sécurité de l'OTAN
- IGI 2102/SGDSN/PSE/PSD sur la protection en France des informations classifiées de l'UE
- IGI 6600/SGDSN/PSE/PSN du 7 janvier 2014 relative à la sécurité des activités d'importance vitale
- Instruction ARM/SGA/DAJ/D2P/DPSP du 31 janvier 2020 relative à la mise en œuvre du règlement européen sur la protection des données personnelles au ministère de la défense

Points clés :

- La présente instruction décline la politique de protection du secret de la défense nationale en modalités d'application pour le périmètre du ministère de la défense (MINARM).
- Elle s'applique aux états-majors, directions et services ministériels, aux établissements publics sous tutelle exclusive du MINARM¹, au CEA/DAM et aux entités parties prenantes à la dissuasion ou contractantes avec le MINARM ou le CEA/DAM.
- Cette instruction intègre également des dispositions relatives à la protection des informations et supports qui, sans être classifiés ou protégés par la mention *Diffusion Restreinte*, sont considérés comme sensibles au MINARM.

1. La protection du secret de la défense 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.

¹ Elle s'applique également aux organismes sous tutelle partagée, sous réserve de l'accord du/des autres ministères de tutelle.

TITRE 1 : PRINCIPES GENERAUX**1**

La divulgation à un tiers non qualifié (personne physique ou morale) d'informations et supports classifiés (ISC) peut avoir des conséquences extrêmement préjudiciables, notamment dans les domaines militaire, scientifique et technique ou industriel. Les ISC constituent ainsi de potentielles cibles pour les services étrangers ou pour toute organisation ou individu souhaitant déstabiliser l'État. Indépendamment du caractère malveillant de certains actes, la négligence ou la méconnaissance de la réglementation par le personnel manipulant des ISC font également courir le risque d'une compromission du secret.

Ces menaces justifient la mise en place d'un cadre juridique précis régissant la protection du secret de la défense nationale, exposé dans l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale (IGI 1300), approuvée par arrêté du Premier ministre.

Les dispositions de l'IGI 1300 sont également applicables à la protection des ISC de l'OTAN et de l'UE. Elles sont complétées par l'instruction interministérielle 2100, pour l'OTAN, et l'instruction générale interministérielle 2102, pour l'UE.

2. Déclinaison par le ministère de la défense

La politique de protection du secret appliquée par le MINARM décline les orientations énoncées par le Premier ministre dans l'IGI 1300 et dans les réglementations de l'OTAN et de l'UE. La présente instruction ministérielle (IM 900) définit les modalités d'application des mesures arrêtées par le Premier ministre en les adaptant aux spécificités du ministère.

- Elle reprend les récentes évolutions de l'IGI 1300, notamment la nouvelle nomenclature de classification (*Secret*, *Très secret*), le renforcement de la sécurité des ISC pendant leur transport et les nouvelles règles techniques relative à la protection des informations classifiées dématérialisées et des systèmes d'information classifiés et rappelle les obligations en matière de protection du secret pour les organismes liés par contrat ou convention avec le MINARM ou avec le CEA/DAM ;
- Elle traduit également les dispositions nouvelles de l'IGI 1300 visant à favoriser la déclassification des informations et supports classifiés avant l'échéance des délais de communicabilité prévus à l'article L. 213-2 du code du patrimoine et encourage le réexamen du niveau de classification de l'ISC tout au long de son cycle de vie ;
- Elle tient compte des particularités du MINARM et apporte ainsi les précisions nécessaires relatives à la typologie des enquêtes administratives² pour le renseignement et la sûreté (contrôles primaires ou élémentaires, habilitations), aux missions et tâches de l'officier de sécurité (OS), de l'officier de sécurité des systèmes d'information (OSSSI) ou aux modalités des contrôles, audits et inspections.
- Elle précise également les règles relatives à la protection du secret applicables aux personnes morales de droit privé liées par contrat ou convention au MINARM ou au CEA/DAM, notamment les industries de défense.

En complément, l'IM 900 fixe également les consignes à respecter pour la protection des informations qui, sans être classifiées ou protégées par la mention de protection *Diffusion Restreinte*, peuvent néanmoins revêtir un caractère sensible. Au sens de cette

² Conformément à l'article L. 114-1 du code de la sécurité intérieure.

TITRE 1 : PRINCIPES GÉNÉRAUX**1**

instruction, une information ou un support sensible est une information ou un support non classifié ou non protégé par la mention de protection *Diffusion Restreinte* mais qui, s'il était révélé au public (*via* tout moyen de communication, vers le cercle professionnel ne disposant pas du besoin d'en connaître ou dans le cadre de l'environnement personnel) ou si un document était falsifié, pourrait nuire à l'image ou aux intérêts du MINARM, des organismes placés sous son autorité, sa tutelle ou liés par contrat ou convention, ou à leur personnel³. Ainsi, sont considérées comme sensibles :

- l'ensemble des informations protégées par des mentions spécifiques (*Confidentiel médical, Confidentiel industrie*, par exemple), énumérées dans les fiches 7.3 à 7.5 ;
- les données à caractère personnel comportant la qualité de la mention de militaire (DCPM), cf. fiche 3.10.
- et, plus largement, les informations stratégiques et organisationnelles, les informations techniques et technico-commerciales, les informations commerciales et les données économiques et financières.

Pour précision, la mention *Diffusion Restreinte* ou toute autre mention spécifique de protection n'est pas, à elle seule, de nature à restreindre le droit de communication des archives et documents administratifs tel qu'il est fixé par les dispositions respectives des codes du patrimoine et des relations entre le public et l'administration⁴. Ces mentions ont pour seul objet d'alerter le détenteur des informations ou supports concernés quant à la nécessaire discrétion dont il convient de faire preuve afin d'éviter d'en révéler l'existence ou de les communiquer à des personnes n'ayant pas le besoin d'en connaître.

Il appartient au chef d'organisme⁵ de définir les types d'informations qu'il considère comme sensibles.

Organisée sous forme de fiches techniques, la présente instruction facilite l'appropriation de la réglementation relative à la protection des ISC et des informations *Diffusion Restreinte* ou sensibles par les acteurs du ministère. Si la plupart de ces fiches ont une portée générale, certaines sont néanmoins adressées à des publics spécifiques (par exemple, les entités contractantes pour le titre 6 traitant de la sécurité des systèmes d'information -SSI⁶).

Les modalités particulières qui s'appliquent aux seules entités liées par contrat ou convention au MINARM ou au CEA/DAM sont signalées par un encadré dans le corps du texte.

³ La définition proposée ici se distingue de celles établie par la loi informatique et libertés et le règlement général de protection des données (RGPD). Ces textes définissent les informations sensibles comme des données relatives aux origines raciales ou ethniques des personnes, à leurs opinions politiques / philosophiques ou religieuses, à leur santé ou à leur orientation sexuelle ainsi que les données biométriques, génétiques et relatives à la vie sexuelle des personnes. Il est par principe interdit de faire figurer ces données dans un traitement, sauf exception.

⁴ A l'exception des identités des agents des services RENS protégés par la LOPPSI 2.

⁵ Au titre de la présente instruction, tout service de l'Etat (services centraux, services déconcentrés, services à compétence nationale, organismes extérieurs), personnes morales ayant accès, même à titre provisoire, à des informations et supports classifiés ou protégés par la mention de protection *Diffusion Restreinte* ou des informations sensibles.

⁶ Les entités du département ministériel sont astreintes, quant à elles, à l'instruction ministérielle (IM) n° 7326/ARM/CAB du 25 juin 2018, relative à la PSSI du MINARM.

TITRE 1 : PRINCIPES GENERAUX**1****3. Périmètre d'application de l'IM 900 et mise à jour**

La présente IM 900 est principalement destinée à l'usage des officiers de sécurité (OS ou OSSI), maillons essentiels de la chaîne de protection du secret. Elle permet, plus largement, une meilleure sensibilisation aux enjeux de la protection du secret.

Cette instruction est applicable :

- au sein du département ministériel (armées, directions et services) ;
- aux établissements publics sous tutelle exclusive du MINARM ainsi qu'au CEA/DAM⁷, à l'exception du titre 6, qui s'applique uniquement aux entités liées par contrat ou convention au MINARM ou au CEA/DAM ;
- aux organismes sous tutelle partagée, sous réserve d'un accord du/des autres ministères de tutelle ;
- aux entités liées par contrat ou convention au MINARM ou au CEA/DAM ;
- aux opérateurs d'importance vitale (OIV) relevant des directives nationales de sécurité pour les activités militaires de l'Etat et les industries de défense (DNS AME et ID).

Elle est applicable dans le respect de l'organisation du contrôle gouvernemental de la dissuasion (CG) défini par l'article R 1411-11 du code de la défense.

La mise à jour des différentes fiches de l'IM 900, en fonction des évolutions législatives ou réglementaires, voire pratiques, est effectuée par le moyen d'instructions modificatives signées par délégation du ministre par le HFCDS⁸.

⁷ Tout comme les entités du département ministériel, ces établissements sont astreints à l'instruction ministérielle (IM) n°7326/ARM/CAB du 25 juin 2018, relative à la PSSI du MINARM.

⁸ Après avis du SGDSN, le HFCDS fait ensuite mettre en ligne à disposition des utilisateurs la dernière version complète de l'instruction.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

INTRODUCTION : CHAINES FONCTIONNELLES DE LA PROTECTION DU SECRET

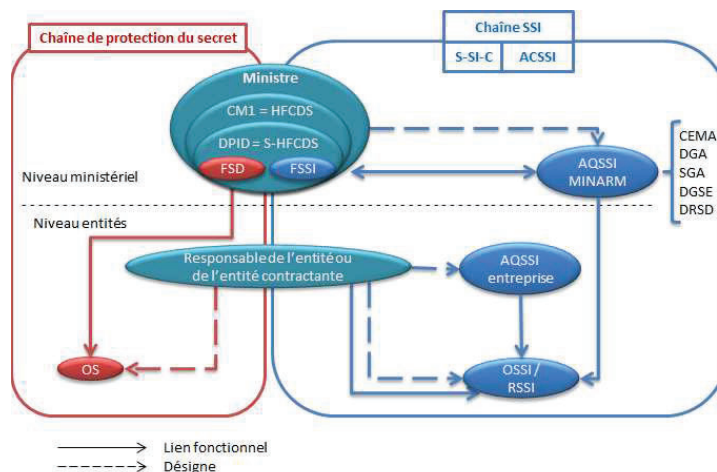
Références :

- IGI 1300 – 2.2
- IM n° 7326/ARM/CAB du 25 juin 2018 relative à la politique de sécurité des systèmes d'information du ministère des armées (PSSI-M).

Points clés :

- Le chef d'un organisme manipulant des ISC assume la responsabilité des mesures de sécurité relatives à la protection du secret de la défense nationale.
- Au MINARM, la protection du secret, assurée par le responsable d'organisme, s'appuie sur deux chaînes : la chaîne de protection du secret, dirigée par le fonctionnaire de sécurité et de défense (FSD) et la chaîne « sécurité des systèmes d'information », dirigée par le fonctionnaire de sécurité des systèmes d'information (FSSI). Cette dernière comprend la « sécurité des systèmes d'information classifiés » et celle des « articles contrôlés de la sécurité des systèmes d'informations ».
- Afin d'assurer une cohérence d'ensemble de la protection, les acteurs des deux chaînes doivent travailler en collaboration étroite.
- Il en est de même pour le titulaire d'un contrat, directeur de l'entité contractante et personne morale, qui endosse de surcroît une responsabilité contractuelle. Le plan contractuel de sécurité de ce contrat énumère les dispositions particulières relatives aux ISC.
- Chaque acteur de la protection du secret, quelle que soit la chaîne à laquelle il appartient, doit pouvoir être remplacé à tout moment afin d'assurer la permanence de la fonction.

Schéma général des chaînes de protection du secret



TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

1. Le niveau ministériel

Le **ministre** est responsable de la protection du secret de la défense nationale et en contrôle l'application. Il fixe, au travers de la présente instruction, les exigences à respecter pour les entités placées sous son autorité ou sa tutelle ainsi que pour les autres entités relevant de son champ de compétences.

Il est assisté du **haut fonctionnaire correspondant de défense et de sécurité** (HFCDS), **chef du cabinet militaire** (CM1), qui anime et coordonne la politique de défense et de sécurité.

Le HFCDS est assisté par la **direction de la protection des installations, moyens et activités de la défense** (DPID), dont le directeur est HFCDS adjoint, **qui agit en tant que service du HFCDS** (S-HFCDS). La DPID anime les chaînes fonctionnelles de la protection du secret. Elle dispose notamment d'un **fonctionnaire de sécurité de défense** (FSD) et d'un **fonctionnaire de sécurité des systèmes d'information** (FSSI) (cf. fiche 2.1).

2. La chaîne fonctionnelle de protection du secret

Elle s'assure de la protection des informations et supports classifiés ainsi que de celle des informations et supports *Diffusion Restreinte* ou sensibles. Elle est **animée par le FSD**. Elle a pour finalité d'assurer la sécurité relative aux personnes physiques et morales, de veiller à la gestion et à la protection physique des informations et supports classifiés, protégés par la mention de protection *Diffusion Restreinte* ou sensibles et au bon fonctionnement des entités qui les manipulent, d'assurer un suivi des lieux abritant⁹ des éléments couverts par le secret, de procéder aux contrôles et inspections nécessaires et de proposer toutes dispositions destinées à renforcer l'efficacité des mesures de protection mises en place.

Dans chaque organisme, l'**officier de sécurité** (cf. fiche 2.5), désigné par le **responsable d'organisme** (commandant de formation administrative / chef d'établissement – CFA/CE ou chef d'un organisme lié par contrat ou convention avec le MINARM), constitue un maillon de cette chaîne, qui contribue à la mise en application des consignes de sécurité.

Le respect du besoin d'en connaître étant un des fondements de la protection du secret, en conséquence, nul ne peut être simultanément officier de sécurité de deux entités distinctes.

Afin de relayer et compléter l'action de l'OS au plus près des divers secteurs d'activités du titulaire du contrat dans lesquels sont traités ou détenus des ISC, le chef d'organisme peut désigner des **correspondants de sécurité** (CS)¹⁰ dans ces secteurs d'activité sous le contrôle fonctionnel de l'OS. Ils reçoivent, pour cette mission, les orientations et consignes de l'OS.

3. La chaîne « sécurité des systèmes d'information » (SSI)

La chaîne « sécurité des systèmes d'information », **animée par le FSSI**, comprend la « sécurité des systèmes d'information » et les « articles contrôlés de la sécurité des systèmes d'informations » (ACSSI). Elle s'appuie sur les personnes exerçant la fonction

⁹ Un lieu abritant des éléments couverts par le secret de la défense nationale est un local dans lequel sont conservés des informations et supports classifiés, quel qu'en soit le niveau.

¹⁰ Il est alors conseillé à l'OS de se rapprocher du service enquêteur pour vérifier l'absence de restriction quant à la désignation.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

d'autorité qualifiée en sécurité des systèmes d'information (AQSSI), d'officier de sécurité des systèmes d'information (OSSI) et de responsable de la sécurité des systèmes d'information (RSSI) (cf. fiche 2.6).

Au sein des organismes liés par contrat ou convention avec le ministère, la chaîne SSI est conduite par le responsable de l'organisme. Elle s'appuie de la même façon sur des personnes exerçant la fonction d'AQSSI, d'OSSI ou de RSSI.

Pour le département ministériel, l'organisation de la chaîne SSI est décrite dans le politique de sécurité des systèmes d'information ministérielle (PSSI-M).

La chaîne **SSI** assure notamment l'élaboration, la diffusion et la promotion de la réglementation et des exigences particulières en matière de sécurité des systèmes d'information traitant d'informations classifiées et contrôle leur application. Elle veille au déploiement et à la gestion des articles contrôlés de la sécurité des systèmes d'information (ACSSI). Elle est notamment chargée de vérifier l'adéquation des moyens de communication sécurisés avec les besoins de son entité et contribue à la prescription des inspections et contrôles nécessaires.

L'autorité qualifiée en sécurité des systèmes d'information (AQSSI), désignée par le ministre ou le responsable d'entité contractante, est responsable de la SSI auprès d'un service ou d'une direction du ministère, ou d'une entité relevant du ministère. Elle travaille en collaboration avec le FSSI et est chargée d'organiser et d'animer, pour son périmètre de responsabilités¹¹, la chaîne SSI placée sous son autorité.

¹¹ Cf. Instruction ministérielle n°7326/ARM/CAB du 25 juin 2018 relative à la politique de sécurité des systèmes d'information du ministère des armées (PSSI-M).

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.1****FONCTIONNAIRE DE SECURITE DE DEFENSE ET FONCTIONNAIRE DE SECURITE DES SYSTEMES D'INFORMATION****Référence :**

IGI 1300 - 2.1.2.2.

Points clés :

- Le FSD et le FSSI sont respectivement les têtes des chaînes fonctionnelles ministérielles « protection du secret » et « sécurité des systèmes d'information ». Ils sont placés auprès du DPID, adjoint du HFCDS.
- Ils assurent notamment l'élaboration, la diffusion et la promotion de la réglementation et des exigences spécifiques à leur chaîne respective et en font contrôler leur application.
- Le FSD et le FSSI travaillent en relation étroite.

1. Le Fonctionnaire de sécurité de défense

Le fonctionnaire de sécurité de défense (FSD) est placé auprès du DPID, adjoint du HFCDS. Il est en charge de la conduite de la chaîne fonctionnelle de protection du secret. A ce titre, il définit les mesures de protection des informations et supports classifiés, protégés par la mention de protection *Diffusion Restreinte* ou sensibles et en fait contrôler l'application sur l'ensemble des entités relevant du champ de compétences du ministre de la défense. Il est aussi en charge de leur mise en œuvre sur le seul périmètre du département ministériel. Le FSD du ministère de la défense est le **chef du département politique de protection** de la **DPID**. Ses responsabilités font l'objet d'une note particulière.

Pour l'assister dans l'exécution de ses attributions, le FSD s'appuie sur les officiers de sécurité (cf. fiche 2.5) de niveau 1 ou centraux.

2. Le Fonctionnaire de sécurité des systèmes d'information

Le fonctionnaire de sécurité des systèmes d'information (FSSI) est placé auprès du DPID, adjoint du HFCDS.

En tant que tête de chaîne SSI, le FSSI :

- porte la réglementation interministérielle à la connaissance des différents organismes ;
- élabore la réglementation propre au ministère des armées ;
- définit les mesures concernant la sécurité des systèmes d'information, notamment classifiés, en définissant pour chaque type de système d'information les mesures de protection précisées dans la politique de sécurité des systèmes d'information (PSSI) du MINARM ;
- s'assure du contrôle de l'application de la réglementation et l'efficacité des mesures prescrites ;
- veille à la bonne organisation de la chaîne SSI en matière de sensibilisation et de formation des personnels.

**TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN
ŒUVRE****2.1**

Au sein du MINARM, pour l'assister dans l'exécution de ses attributions, le FSSI s'appuie sur les officiers de sécurité des systèmes d'information (OSSI) (cf. fiche 2.6), organisés en chaîne. Il travaille en collaboration étroite avec l'AQSSI ou son représentant (RAQSSI).

Le FSD et le FSSI diffusent la réglementation vers les entités contractantes par l'intermédiaire de leur autorité contractante, notamment *via* la DGA.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.2****SERVICES ENQUÊTEURS DU MINISTÈRE DE LA DÉFENSE****Références :**

- Code de la défense – art. D. 3126-5 et suivants
- Code de la sécurité intérieure – Art. L. 114-1 et L. 114-2 et R. 114-1 à R. 114-6
- IGI 1300 – 2.5.2, 3.2, 3.3.1.3, 4.4.1.4 et 4.4.1.5, 5.3.3.1, 6.1.3

Points clés :

- La direction du renseignement et de la sécurité de la défense (DRSD) est le service de renseignement dont dispose le ministre pour assumer ses responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles.
- Désignée par le Premier ministre comme service enquêteur en matière de protection du secret de la défense nationale pour la sphère de défense, la DRSD mène les enquêtes administratives pour le renseignement et la sûreté (EARS) nécessaires pour détecter toute vulnérabilité dans ce domaine.
- Elle conseille et inspecte les armées, directions, services, les entreprises et les organismes sous tutelle du MINARM pour vérifier le respect des dispositions réglementaires, les mesures de protection physique des locaux et les règles d'accès aux lieux ainsi que les mesures de protection logique des systèmes d'information.
- Elle réalise des inspections.
- La direction générale de la sécurité extérieure (DGSE) agit également comme service enquêteur pour son propre périmètre. Elle vérifie, dans le cadre de contractualisations réalisées avec des personnes morales de droit privé, le respect des dispositions réglementaires, de protection physique des locaux et les règles d'accès aux lieux ainsi que les mesures de protection logique des systèmes d'information.

1. Missions de la DRSD dans le cadre de la protection du secret

- En sa qualité de **service enquêteur** :
 - elle réalise des enquêtes administratives pour le renseignement et la sûreté (R. 114-2 et R. 114-6 du CSI) qui visent à s'assurer de l'intégrité d'une personne (cf. fiche 3.9). Ces enquêtes sont réalisées :
 - o préalablement au recrutement des militaires ;
 - o préalablement à l'habilitation du personnel¹² et des personnes morales ayant accès à des informations et supports classifiés ;
 - o préalablement à la délivrance d'autorisations d'accès à des zones protégées ;
 - o en cours de carrière, en vue de s'assurer que le comportement d'une personne n'est pas devenu incompatible avec les fonctions ou les missions exercées (cf. notamment lutte contre la radicalisation¹³) ;

¹² Personnel militaire ou civil relevant du ministère des armées ou employé dans les organismes et entreprises travaillant à son profit et des personnes morales devant accéder à des ISC ; personnel militaire de la gendarmerie nationale.

¹³ Articles L. 114-1 et R. 114-6-1 du CSI.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.2

- o sur les personnes accédant à des traitements de données à caractère personnel comportant la mention de la qualité de militaire¹⁴.
- elle rend également des **avis techniques** sur l'aptitude des locaux et des systèmes d'information à abriter des ISC dans les organismes relevant du périmètre de compétences du MINARM.
- Elle **conseille** les armées, directions, services et les différents échelons du commandement ainsi que les entreprises en relation avec la défense (au sens de l'article D 3126-7 du code de la défense) détenant ou ayant accès à des ISC pour l'exercice de leurs responsabilités en matière de sécurité ;
- Elle **conduit et réalise des inspections** et des contrôles de l'application des instructions et directives relatives à la protection du secret au sein des armées, organismes, établissements, points d'importance vitale (dont les installations prioritaires de défense) placés sous l'autorité du ministre, des organismes et emprises qui en relèvent ainsi que dans les organismes sous convention ou titulaires de contrats intéressant la défense ou sous-traités à son profit et nécessitant la prise de précautions particulières¹⁵. Ses inspections font l'objet d'un compte rendu adressé au ministre ainsi qu'aux organismes ayant le besoin d'en connaître.

2. Organisation

En matière de protection du secret, la DRSD est organisée en trois niveaux distincts :

- le niveau local, qui est le contact privilégié de l'OS de niveau 3 (cf. fiche 2.5) ;
- le niveau zonal, qui assure une coordination des postes locaux avec une vision géographique plus vaste. C'est le contact privilégié des OS de niveau 2 et des OSSl. Enfin, il participe à la mission de contrôle avec, notamment, les visites post-inspections ;
- le niveau central, qui anime la fonction contre-ingérence, en milieu militaire comme dans l'industrie de défense, conduit et réalise les inspections.

3. Missions de la DGSE en tant que service enquêteur

Pour son propre périmètre, la DGSE conduit des enquêtes administratives préalables aux accès (emplois, emprises, habilitations).

Elle réalise des **inspections et des contrôles** de l'application des instructions et directives relatives à la protection du secret au sein des organismes sous convention ou titulaires de contrats intéressant la défense ou sous-traités à son profit et nécessitant la prise de précautions particulières.

¹⁴ Cf. dispositions de l'article L. 4123-9-1 du code de la défense (périmètre : secteur privé).

¹⁵ Hors INID.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.3****AUTORITES D'HABILITATION DU MINISTÈRE DE LA DÉFENSE****Références :**

- IGI 1300 – chapitres 3 et 4
- Arrêté du 21 mars 2012 modifié¹⁶ portant délégation des pouvoirs du ministre de la défense en matière de décisions d'habilitation à connaître des informations et supports couverts par le secret de la défense nationale

Points clés :

- L'autorité d'habilitation est l'autorité décisionnaire en la matière. Ce pouvoir du ministre est délégué, par voie réglementaire, à certaines autorités qui lui sont subordonnées.
- L'autorité d'habilitation pour toutes les entreprises travaillant au profit du MINARM et du CEA/DAM, à l'exception de celles de la DGSE pour son propre périmètre, est la DGA.
- Le SGDSN est l'autorité d'habilitation pour le niveau *Très Secret* faisant l'objet de classifications spéciales.

L'autorité d'habilitation est **l'autorité compétente pour émettre la décision ou le refus d'habilitation**¹⁷, en fonction notamment des conclusions transmises par le service enquêteur.

Le secrétaire général de la défense et de la sécurité nationale est l'autorité d'habilitation, par délégation du Premier ministre, pour les demandes d'habilitation au niveau *Très Secret* faisant l'objet d'une classification spéciale.

Par voie réglementaire, le ministre de la défense **délègue son pouvoir d'habilitation** à des autorités qui lui sont subordonnées, avec mention du périmètre des compétences associé, au profit du personnel placé sous leur autorité. Ces délégataires peuvent, si nécessaire, déléguer leur signature à certains subordonnés choisis. Reçoivent, notamment, délégation de pouvoir du ministre les autorités mentionnées ci-dessous.

1. Pour les niveaux *Secret* et *Très Secret* (hors classifications spéciales) :

En administration centrale du ministère et pour les autorités directement rattachées au ministre :

- | | |
|--|---|
| - haut fonctionnaire correspondant de défense et de sécurité du ministère des armées | - directeurs généraux |
| - chefs d'état-major | - directeurs et chefs de service d'administration centrale |
| - délégué général pour l'armement | - chef du contrôle général des armées et membres des corps d'inspection |
| - secrétaire général pour l'administration | directement rattachés au ministre |

¹⁶ Notamment par l'arrêté du 28 avril 2017 prenant en compte les transferts de responsabilités pour les habilitations liées au CEA/DAM.

¹⁷ Elles sont également compétentes pour se prononcer sur l'accès aux ISC TS COSMIC et TS UE.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.3

- délégué à la sûreté nucléaire et à la radioprotection pour les activités et installations intéressant la défense

Hors administration centrale : les commandants organiques et opérationnels des forces et commandants interarmées.

2. Pour le niveau **Secret** seulement :

- les commandants des formations administratives ou des organismes administrés comme tels ;
- les commandants des écoles de formation ;
- les directeurs n'appartenant pas à l'administration centrale du ministère des armées.

Le **délégué général pour l'armement** et le **directeur général de la sécurité extérieure**, **seulement pour leur périmètre de compétence**, ont délégation de pouvoir du ministre pour signer les **décisions d'habilitation des personnes morales** candidates ou titulaires d'un contrat nécessitant la détention ou l'accès à des ISC ainsi que des personnes physiques qui en dépendent.

Afin de remplir cette mission au nom du ministre, la DGA dispose d'une entité spécifique, le **service de la sécurité de défense et des systèmes d'information (SSDI)**. Ce service est aussi chargé de prononcer les décisions d'agrément des officiers de sécurité (OS, OSSI et leurs adjoints) proposés par les entités habilitées, après avis du service enquêteur (cf. fiche 2.2).

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.4****RESPONSABILITES DU RESPONSABLE D'ORGANISME****Références :**

- IGI 1300 – 2.2.1
- Pour les établissements du MINARM, ses établissements publics sous tutelle et les INID du CEA : IM 1544/DEF/CAB/DR du 17 janvier 2017, version du 10 août 2020, relative à la défense-sécurité des activités, moyens et installations relevant du ministère de la défense - 2.4
- Arrêté du 21 mars 2012 modifié portant délégation des pouvoirs du ministre de la défense en matière de décisions d'habilitation à connaître des informations et supports couverts par le secret de la défense nationale

Points clés :

- Le responsable d'organisme exerce la responsabilité plénière de la protection du secret dans son organisme (cf. glossaire IGI 1300).
- Le responsable d'organisme (commandant de formation administrative ou chef d'établissement - CFA/ CE - ou chef d'entreprise) est le responsable local de la sécurité de son personnel, de ses matériels et de ses installations : ce champ de responsabilités englobe la protection du secret (ISC, SI classifiés, lieux abritant des ISC, habilitations du personnel) et celle des informations et supports protégés par la mention *Diffusion Restreinte* et des informations sensibles.
- Il désigne un officier de sécurité (OS) et un officier de sécurité des systèmes d'information (OSSI) pour l'appuyer dans l'exercice de ses responsabilités.

Le responsable d'organisme est le responsable local¹⁸ de la sécurité de son personnel, de ses matériels et de ses installations. Dans ce cadre général, il approuve la politique de protection du secret rédigée par son officier de sécurité, assume la responsabilité des mesures de sécurité relatives à la protection du secret (documents papiers ou dématérialisés, réseaux, matériels classifiés, habilitation du personnel) et des installations (lieux abritant des ISC).

Il organise les deux chaînes fonctionnelles de protection du secret. A cet effet, il désigne un OS et un OSSI et, dans la mesure du possible, un adjoint ou suppléant pour chacun d'eux, au sein de son organisme (cf. fiche 2.5 et 2.6). A défaut d'OS et/ou d'OSSI, le responsable d'organisme se charge lui-même de l'accomplissement des tâches relatives à la protection du secret pour son entité.

¹⁸ Dans le cas où l'organisme occupe plusieurs sites, le responsable d'organisme porte la responsabilité de la protection de toutes ses emprises, même distantes.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.4

Missions	Tâches à réaliser
Garantir la protection du secret au sein de son entité	Contrôle de l'application de la politique de protection du secret (IGI 1300, présente instruction, PSSI-M, dispositions contractuelles applicables pour les personnes morales)
Organiser la chaîne de protection du secret	Désignation (nominative) de l'OS, l'OSSI et de leurs suppléants Création d'un bureau de protection du secret, obligatoire pour le <i>Très Secret</i> Validation de la note permanente d'organisation de la protection du secret au sein de son organisme, rédigée par son OS. Pour les organismes privés ou publics autres que les établissements publics de l'Etat : désignation d'une autorité qualifiée pour les SI
Veiller à la bonne gestion des habilitations et à la mise à jour annuelle, ou lors de réorganisation de service, du catalogue des emplois (ou équivalent)	Décision d'habilitation pour le niveau <i>SECRET</i> par délégation de pouvoir du MINARM (pour le département ministériel seulement, cf. fiche 2.3)
Assurer la formation du personnel et mettre à sa disposition les moyens nécessaires en matière de protection du secret	Veille à l'organisation de l'instruction de sécurité et de la sensibilisation du personnel placé sous ses ordres
Organiser le système général de sécurité en fonction du degré de sensibilité de ses installations, que celles-ci contiennent ou non des ISC et rédiger un plan de protection du site dont il a la responsabilité	Demandes de création de ZP ou création de ZR et définition des règles d'accès et de circulation, autorisation d'accéder à ses emprises

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.5****OFFICIER DE SECURITE****Références :**

- IGI 1300 - 2.2.2.1
- Pour les établissements du MINARM, ses établissements publics sous tutelle et les INID du CEA : IM 1544/DEF/CAB/DR du 17 janvier 2017, version du 10 août 2020, relative à la défense-sécurité des activités, moyens et installations relevant du ministère de la défense - 2.5

Points clés :

- L'officier de sécurité (OS) est un maillon essentiel de la chaîne de protection du secret, des informations et supports protégés par la mention de protection *Diffusion Restreinte* et des informations sensibles. Il rédige la politique de protection du secret de son organisme et veille à son application. Il forme le personnel de la chaîne de protection du secret qui lui est subordonné et sensibilise régulièrement l'ensemble du personnel habilité. Il dirige généralement le bureau de protection du secret (BPS). Il travaille en liaison étroite avec l'officier de sécurité des systèmes d'information (OSSI).
- L'OS est formé, a un niveau hiérarchique suffisant et dispose des moyens nécessaires pour accomplir ses missions. Sa prise de fonction est conditionnée par un niveau d'habilitation adéquat et par l'obtention d'un agrément.
- Au-delà du seul domaine de la protection du secret, le MINARM recommande que les OS de son périmètre soient aussi chargés de tout ou partie des autres domaines de la défense-sécurité, notamment de la protection physique des installations.

L'officier de sécurité (OS) est appelé à exercer des prérogatives plus larges dans le domaine de la défense-sécurité (champs de la protection des installations, du personnel et des biens – cf. IM 1544 pour les organismes étatiques). La présente fiche détaille exclusivement ses attributions en matière de protection du secret, de protection des informations et supports protégés par la mention *Diffusion Restreinte* et celle des informations sensibles.

1. Attributions en matière de protection du secret

L'OS met en œuvre et peut diriger les moyens de protection du secret (bureau de protection du secret - BPS, structure de sécurité) en coopération étroite avec l'officier de sécurité des systèmes d'information (OSSI). Il rédige à cet effet la politique de protection du secret de son organisme. Il assure la formation du personnel de la chaîne fonctionnelle de protection du secret et la sensibilisation du personnel traitant d'ISC de son entité.

Il dispose, si possible, d'un adjoint ou d'un suppléant, qui répond aux mêmes exigences de désignation que lui (cf. paragraphe 2 pour les entités MINARM et 3 pour les contractants).

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.5

Au sein des entités contractantes, l'OS est également chargé de la rédaction de la politique de protection du secret, validée ensuite par le responsable d'organisme.

L'OS est le contact privilégié, pour son organisme, de l'autorité d'habilitation, du FSD (pour les OS têtes de chaîne) et du service enquêteur.

Il rend compte à l'autorité d'habilitation et à sa hiérarchie et signale à la DRSD les vulnérabilités portées à sa connaissance apparaissant après une décision d'habilitation d'une personne morale ou physique.

En cas de compromissions avérées ou supposées, l'OS, avec l'OSSI le cas échéant, rend compte à sa chaîne hiérarchique, à la chaîne fonctionnelle de protection du secret et en informe la DRSD.

Les tâches de l'OS en matière de protection du secret sont regroupées en trois principaux domaines d'action : la protection du personnel, celle des informations et supports classifiés ou protégés par la mention de protection *Diffusion Restreinte* et des informations sensibles et enfin celle des lieux abritant des informations et supports classifiés.

Les OS des entités contractantes avec le ministère de la défense sont de surcroît chargés du suivi des exigences de sécurité figurant dans les contrats et des plans contractuels de sécurité.

Les attributions de l'officier de sécurité	
Protection du personnel	Protection des ISC et informations sensibles
<ul style="list-style-type: none"> Gestion des habilitations et enquêtes administratives (demandes via SOPHIA ou par la tenue à jour des registres d'habilitations) Tenue à jour du ou des catalogues des emplois (un par réseau¹⁹ et par niveau d'habilitation²⁰) Appréciation des avis de sécurité consécutifs aux enquêtes administratives et établissement des droits d'accès (visiteurs, prestataires,...) lorsque l'autorité dont il dépend est le CFA/CE de l'installation Suivi et contrôle des autorisations d'accès Suivi et contrôle des ressortissants étrangers Suivi des séjours à l'étranger (stage, mission, permissions) Au sein du MINARM, rapport des faits préjudiciables au moral et à la discipline ; surveillance du personnel potentiellement à risque Compte-rendu des compromissions avérées ou supposées Organisation de séances d'instruction ou de sensibilisation (séance annuelle de sensibilisation, mise à jour d'un registre d'instruction) 	<ul style="list-style-type: none"> Rédaction de la politique de protection du secret de son organisme Si désigné par le chef d'organisme pour cette mission, commandement du bureau de protection du secret (BPS) Surveillance, protection et contrôle des ISC et des informations sensibles Contrôle du personnel ayant accès aux ISC Participation, le cas échéant, au suivi de la sécurité des SI classifiés avec l'OSSI Contrôle de l'application des règles de protection, de manipulation et de destruction des ISC
	Protection des lieux abritant des ISC
	<ul style="list-style-type: none"> Suivi des arrêtés concernant les zones protégées ; tenue à jour des

¹⁹ Secret de la défense nationale, OTAN, UE

²⁰ Secret, Très Secret. Les catalogues des classifications spéciales font l'objet de consignes particulières qui ne sont pas développées dans cette IM.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.5

<ul style="list-style-type: none"> • Sensibilisation avant une mission ou un départ à l'étranger 	<ul style="list-style-type: none"> documents constitutifs des zones réservées (ZR) • Suivi des avis d'aptitude des lieux abritant des ISC • Suivi des dossiers de consignes, des autorisations d'accès, des visites
Suivi des contrats et plans contractuels de sécurité de son périmètre	
<ul style="list-style-type: none"> • S'assure de la tenue à jour de la liste des contrats avec détention ou accès à des ISC • Validation du plan contractuel de sécurité • Conseil en matière de prise en compte de la sécurité de défense dans les contrats auprès des acheteurs de son organisme • Contrôle de la protection du secret chez les contractants et éventuels sous-contractants 	

2. Désignation

L'OS est désigné nominativement par le chef de service employeur parmi son personnel, s'il satisfait aux conditions suivantes :

- il appartient de façon suffisamment stable à l'organisme²¹ ;
- il est habilité au niveau *Très Secret* (pour le MINARM) ;
- il reçoit l'agrément de la DRSD²² ;
- il a validé un stage initial de formation (à défaut, le valide dans l'année suivant sa nomination) ;
- il est de nationalité française si l'organisme est appelé à traiter des informations et supports classifiés portant la mention de protection *Spécial France* ;
- il dispose d'un accès direct au responsable d'organisme et d'un niveau hiérarchique suffisant pour le conseiller ;
- il dispose de tous les moyens nécessaires à l'accomplissement de sa mission ;
- ses coordonnées sont transmises au FSD *via* son OS tête de chaîne.

Pour les organismes désignés opérateurs d'importance vitale (OIV)²³, le délégué pour la défense et la sécurité (DDS), 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. De même, les délégués locaux à la défense et à la sécurité (DLDS) exercent la fonction d'OS 2 ou 3 ou d'OS d'établissement (OSE).

3. Formation

La formation de l'OS relève de la responsabilité du chef qui l'a désigné.

Avant sa prise de fonction (ou dans l'année de sa désignation), l'OS suit un stage de formation initiale qualifiant :

- pour les OS du département ministériel, il est organisé par les bureaux de protection principaux des armées et de l'EMA. Dans la mesure du possible, l'OS d'une autorité contractante de référence effectue un stage organisé par le centre d'instruction à la sécurité industrielle de l'armement de la DGA (CISIA).

²¹ La sous-traitance de cette fonction est interdite.

²² A l'exception des OS agréés par la DGSE.

²³ A l'exception du CEA/DAM.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

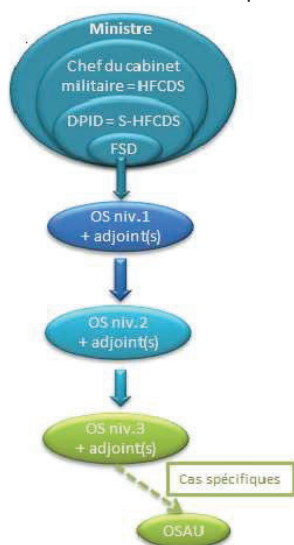
2.5

- pour les OS des entités contractantes, il est organisé par le CISIA.

Une actualisation régulière de la formation est recommandée.

4. L'OS du département ministériel

Pour chaque armée/direction/service (ADS) du MINARM, la chaîne fonctionnelle de protection du secret permet un maillage territorial et fonctionnel garantissant la



couverture de l'ensemble de son périmètre et appliquant le principe de subsidiarité :

- un **OS de niveau 1** (OS 1) est placé auprès de chaque ADS²⁴. Tête de chaîne et correspondant privilégié du FSD, il est le conseiller de sa hiérarchie, à laquelle il propose l'organisation de la chaîne de protection du secret adaptée aux spécificités de son armée, de sa direction ou de son service. Il est généralement chef du bureau principal de protection du secret de sa chaîne (BPPS – cf. fiche 2.7). Les OS 1 ne peuvent avoir d'autres fonctions que celles relevant du domaine de la défense-sécurité ;
- au niveau intermédiaire, il est créé autant de postes **d'OS de niveau 2** (OS 2) que nécessaire. Subordonné fonctionnellement à son OS 1, il conseille sa hiérarchie et son DDS régional s'il existe. L'OS 2 prolonge l'action de l'OS 1. Il est généralement chef d'un bureau secondaire de protection du secret (BSPS) ;
- chaque formation administrative ou établissement

dispose d'un **OS de niveau 3** (OS 3), conseiller du CFA/CE et le plus souvent, chef d'un bureau de protection du secret. Le CFA/CE peut désigner des correspondants de sécurité (CS) subordonnés à l'OS de niveau 3, **pour prolonger son action au sein de l'entité**. Pour ce dernier, une demande d'accord de principe est recommandée auprès du service enquêteur concerné. En cas d'éloignement important de la portion centrale ou de sensibilité particulière d'une installation, au lieu d'un CS, le CFA/CE désigne un officier de sécurité adjoint d'unité (OSAU). En sa qualité d'OS, l'OSAU satisfait aux exigences fixées *supra*.

Point particulier : Nul ne peut être simultanément officier de sécurité de deux entités relevant d'autorités fonctionnelles distinctes.

5. L'OS au sein d'un organisme lié par contrat ou convention avec le MINARM

L'OS est désigné nominativement (cf. IGI 1300 – annexe 19) par le chef de service employeur s'il satisfait aux conditions évoquées dans le paragraphe 2 de cette fiche ainsi qu'aux conditions spécifiques suivantes :

- il est habilité au même niveau que la personne morale dont il dépend ;

²⁴ A l'exception des directions et services subordonnés au CEMA.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.5

- il reçoit l'agrément de l'autorité d'habilitation sur un avis émis par le service enquêteur.

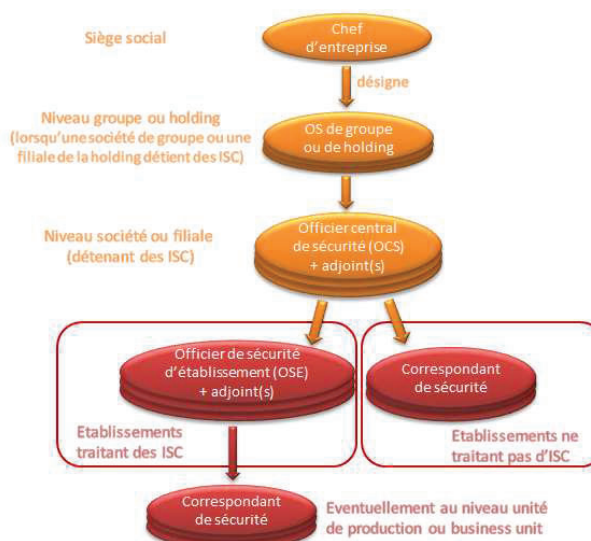
Si plusieurs établissements de l'entreprise ou organisme détiennent des ISC, un **officier de sécurité d'établissement (OSE)** est désigné dans chacun d'entre eux. L'OS du siège social est alors identifié comme **officier central de sécurité (OCS)** de l'entreprise ou de l'organisme.

Dans le cas des groupes de sociétés ou des sociétés holding, si au moins une société du groupe ou une filiale a accès au secret de la défense nationale, un officier de sécurité de groupe ou de holding peut être désigné pour assurer une cohérence entre la gouvernance et les enjeux de protection du secret.

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.

Processus d'agrément des OS lorsque la DGA est autorité d'habilitation :

Le service enquêteur transmet un avis d'agrément à la DGA, qui décide ou non d'agréer l'OS. Ce dernier ne peut exercer ses fonctions tant que la DGA ne délivre pas sa décision d'agrément. En cas de refus d'agrément, l'entité contractante propose une autre personne et recommence le processus.



TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.6****OFFICIER DE SECURITE DES SYSTEMES D'INFORMATION DES ORGANISMES LIES PAR CONTRAT OU CONVENTION****Référence :**

IGI 1300 – 2.2.3.2

Points clés :

- L'officier de sécurité des systèmes d'information (OSSI) assure :
 - l'organisation générale de la protection des ISC contenus ou circulant dans les systèmes d'information classifiés de l'organisme ;
 - la rédaction de la PSSI de son organisme ;
 - l'organisation de l'homologation²⁵ des systèmes d'information ;
 - la formation de ses utilisateurs ainsi que de la coordination de l'action SSI.
- Les OSSI centraux des personnes morales sont les correspondants locaux du FSSI.
- L'OSSI se coordonne avec l'OS.

Les dispositions suivantes s'appliquent uniquement aux entités liées par contrat ou convention au ministère. Pour les organismes relevant du ministère des Armées et pour les organismes publics sous la tutelle du ministère des Armées, les éléments figurent dans l'IM 7326 « politique SSI ministérielle ».

1. Principes généraux

Employé en SSI auprès d'une autorité pour l'aider à mettre en œuvre les processus opérationnels et supports qui lui incombent, l'OSSI conçoit et met en œuvre un système de management du système d'information (SMSI). Il coordonne les moyens liés à sa mission, vérifie la mise en œuvre de la politique SSI de protection des ISC, conseille son autorité et sensibilise (formation et information) les personnels concernés. Il coordonne son action avec celle de l'OS. Il est désigné dans les mêmes conditions que l'officier de sécurité, est formé (SSI, ACSSI) et dispose des moyens nécessaires pour accomplir ses missions.

L'OSSI est en relation régulière avec la DGA/SSDI et son point de contact au service enquêteur.

Dans le **cadre des organismes contractants**, le chef d'organisme désigne un officier central de sécurité des systèmes d'information (OCSSI). Par défaut, l'OSSI du siège social est **OCSSI** lorsque l'entreprise dispose d'autres établissements, eux-mêmes disposant alors d'**OSSI locaux (OSSI-L)**, placés auprès du chef d'entité d'un site local d'entreprise.

En fonction de la taille de l'organisme, du niveau de classification des informations traitées et de la nature des systèmes à protéger, l'OSSI peut disposer de **correspondants de sécurité des systèmes d'information (CSSI)**, désignés par le chef d'organisme. Il veille

²⁵ La démarche d'homologation de sécurité, préalable impératif à la mise en service du SI, permet d'identifier tous les risques, d'atteindre puis de maintenir un niveau de risques de sécurité acceptable pour le système d'information considéré, compte tenu du niveau de protection requis.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.6

à la mise en place de **responsables de sécurité des systèmes d'information** (RSSI) dans le cadre du développement et de l'exploitation d'un système d'information classifié.

Le RSSI est désigné 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, il 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 responsable de l'exploitation 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.

Les OSSI disposent, pour faire exécuter tout ou partie des tâches leur incombant en matière de SSI, de **bureaux SSI** (BSSI centraux ou locaux) lorsque la taille de l'organisme le permet.

2. Attributions

Les attributions de l'OSSI se répartissent en quatre champs de compétences :

Les attributions de l'officier de sécurité des systèmes d'information	
Politique de sécurité des SI	Suivi des supports d'informations classifiées numériques
<ul style="list-style-type: none"> - Valider les procédures d'exploitation de sécurité des systèmes d'information établies par le RSSI - S'assurer que les personnes, employées à titre permanent ou occasionnel, administratrices ou utilisatrices d'un traitement numérique des informations classifiées sont habilitées au niveau adéquat - Faire surveiller en permanence les activités des utilisateurs extérieurs appelés à effectuer des travaux temporaires sur le SI et les opérations de maintenance - S'assurer que les sociétés prestataires de service ont fait l'objet de contrats avec accès à des ISC ou de contrats sensibles - S'assurer de l'application, par le personnel d'exploitation et les utilisateurs, des règles de sécurité prescrites - Assurer la formation et la sensibilisation du personnel en matière de SSI - Vérifier périodiquement le bon fonctionnement des dispositifs de sécurité - Veiller au respect des procédures opérationnelles de sécurité propres au système de traitement utilisé - S'assurer de l'installation correcte des différents matériels utilisés 	<ul style="list-style-type: none"> - En liaison avec l'OS, établir des mesures de protection, des consignes particulières relatives au stockage, à la conservation, la prise en compte et la destruction des supports d'informations classifiées numériques et contrôler leur application
	Homologation des SI
	<ul style="list-style-type: none"> - Faire tenir à jour le dossier de sécurité des différents systèmes d'information - Préparer l'homologation, en lien avec la DZ RSD pour l'aptitude informatique des SI, y compris des SI de sûreté (CADIVS : contrôle d'accès, détection d'intrusion et vidéo-surveillance)
	Suivi des ACSSI
	<ul style="list-style-type: none"> - S'assurer de l'identification des ACSSI, de leur prise en compte par un détenteur et de leur enregistrement

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.6**

- | | |
|--|--|
| <ul style="list-style-type: none">- S'assurer de l'aptitude physique des locaux en liaison avec l'OS et le poste RSD compétent pour les SI classifiés- Rend compte de toute compromission et incident constatés (chaîne hiérarchique, chaîne SSI, OS, DRSD, autorité contractante, autorité d'habilitation) | |
|--|--|

En matière de protection des SI, l'OSSI intervient à tous les stades d'étude, de réalisation, d'utilisation, d'évolution, de démantèlement d'un SI et de destruction des supports. Pour ce qui concerne les supports d'informations classifiées numériques (clés USB, disques durs, etc....), l'OSSI se coordonne avec l'OS.

L'ensemble des attributions de l'OSSI fait l'objet d'un ou de documents écrits établissant clairement la nature de la délégation de responsabilité et des pouvoirs sur les moyens associés entre le chef d'entreprise ou d'organisme et l'OSSI. Par ailleurs, l'OSSI peut être amené à intervenir dans l'élaboration et la validation des contrats et plans contractuels de sécurité sur la dimension SSI, en coopération avec l'OS.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.7****BUREAU DE PROTECTION DU SECRET****Référence :**

IGI 1300 – 7.2.1.1, 7.2.1.2, 7.2.2.1 et 7.2.2.2

Point clé :

La création d'un bureau de protection du secret (BPS) est obligatoire lorsque l'entité détient des ISC de niveau *Très Secret* ; elle est recommandée pour le *Secret*.

Le bureau de protection du secret (BPS) est la dénomination de la structure constituée dans l'organisme pour s'occuper de la gestion du secret. Par extension, le terme désigne aussi les locaux qui permettent cette mission. Le BPS est placé sous la responsabilité de l'OS.

L'existence d'un bureau de protection du secret (BPS) est obligatoire pour organiser l'élaboration, le marquage, l'enregistrement, le stockage, l'acheminement, le suivi et la destruction des informations et supports classifiés (ISC) de niveau *Très Secret*, hors classifications spéciales²⁶. A cette fin, le BPS dispose d'une zone réservée (ZR), où les tâches afférentes à la gestion du *Très Secret* sont réalisées.

La création de ce bureau est recommandée pour la gestion des ISC de niveau *Secret*. Dans ce cas, la ZR n'est pas nécessaire. Le BPS, par ses missions, est différent d'un bureau courrier.

Le BPS assure également la gestion des ISC étrangers, à l'exception des ISC UE ou OTAN, gérés par des bureaux de protection du secret distincts (bureaux d'ordre).

1. Missions

Le BPS :

- trace les ISC émis/reçus par son entité, notamment au travers d'un suivi rigoureux des bordereaux ABB' (cf. fiche 7.8) et des documents dématérialisés ;
- contrôle la position des ISC de niveau *Très Secret* via une fiche de suivi, établie pour chaque support et émargée par chaque personne qualifiée y ayant accès, qu'il conserve et rattache au support dès que les nécessités du service permettent de le réintégrer ;
- s'assure de l'établissement d'un inventaire annuel des informations et supports classifiés de niveaux *Secret* et *Très Secret* détenus par son entité ;
- assure la gestion des dossiers d'habilitation du personnel de son périmètre ;
- participe à l'animation des séances d'instruction et de sensibilisation ;
- coordonne l'action du personnel des BPS qui lui sont subordonnés ;
- participe à la mise à jour du catalogue des emplois de niveau TS et/ou S ;

²⁶ Les ISC de niveau TS faisant l'objet d'une classification spéciale répondent à des mesures de protection spécifiques.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.7

- peut organiser le contrôle d'une ZR en dehors des heures d'utilisation (fermeture, fonctionnement des systèmes de détection, vidage des corbeilles à papier, absence d'ISC hors meubles).

Placées sous la direction de l'officier de sécurité (OS), les activités du BPS sont organisées de telle sorte que les informations traitées, les documents, matériels ou électroniques, reçus, émis et conservés, ne soient accessibles qu'aux personnes qualifiées.

Le personnel qui y est affecté (secrétaire(s) de sécurité) appartient en propre à l'entité et est habilité au niveau approprié.

Le personnel du BPS met annuellement à jour son registre d'état de signature afin qu'il puisse être identifié formellement.

Aucun organisme ne peut élaborer, traiter, stocker, 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.

2. Moyens

Pour faciliter le suivi des ISC, le BPS détient pour chaque document les informations suivantes, qui peuvent être mises en place par voie informatique :

Identification du support d'information

- | | |
|--|---|
| - numéro d'enregistrement arrivée ou départ (timbre) | - titre ou objet |
| - autorité émettrice | - pagination |
| - auteur de l'ISC | - niveau de classification |
| - date de création | - mode et date prévue de déclassification |
| - domaine | - nombre d'exemplaires gérés par le BPS |
| | - numéro de l'exemplaire |

Traçabilité des événements concernant les exemplaires du support d'information

- | | |
|---------------------------|---|
| - arrivée | - numéro de référence de l'événement |
| - départ | - date de l'événement |
| - impression/reproduction | - référence individuelle des exemplaires |
| - archivage | - nom et fonction du détenteur de chaque exemplaire |
| - destruction | - intervention technique |
| - déclassification | |

Modification éventuelle des données précédentes

Recherche sur les supports d'information

- détenteurs successifs d'un exemplaire
- date de création
- service émetteur

Inventaire des informations et supports classifiés

Fourniture d'états relatifs aux actions effectuées sur les supports d'information

- | | |
|---|--------------------------------|
| - historique | - procès-verbal de destruction |
| - fiche d'enregistrement | - avis de déclassification |
| - fiche de suivi | - archivage |
| - bordereau d'envoi (suivi strict des ABB') | - impression/reproduction |

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.7

3. Organisation au MINARM

Au sein du MINARM, suivant son positionnement hiérarchique dans la chaîne de protection du secret, un BPS peut être :

- un bureau principal de protection du secret (BPPS)²⁷ ;
- un bureau secondaire de protection du secret (BSPS), subordonné à un BPPS ;
- un bureau de protection du secret (BPS), subordonné à un BSPS ou directement au BPPS.

Il est dirigé par un officier de sécurité qui, selon son périmètre de responsabilité, est de niveau 1, 2 ou 3.

Lorsqu'un officier de sécurité adjoint d'unité (OSAU) est désigné, le CFA/CE peut le renforcer d'un ou plusieurs secrétaires de sécurité fonctionnellement rattachés au BPS.

²⁷ Les BPPS du MINARM sont : BPPS EMA, BPPS EMAT, BPPS EMAA, BPPS EMM, BPPS DGSE, BPPS DRSD, BPPS DGA, BPPS CAB/MINARM. Un BPPS SGA est en cours de création.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.8****FORMATION ET SENSIBILISATION****Référence :**

IGI 1300 – 3.6

Points clés :

- L'OS et l'OSSI sont chargés de la formation des spécialistes de leur chaîne comme de la sensibilisation de l'ensemble du personnel.
- La formation initiale est dispensée à l'occasion de stages qualifiants. Elle est entretenue au sein de la chaîne de défense-sécurité.
- La sensibilisation initiale faite à la personne habilitée lors de la délivrance d'une décision d'habilitation donne lieu à la signature d'un engagement de responsabilité. Elle est renouvelée tout au long de l'emploi.

1. Formation du personnel armant les structures de sécurité

Dans le cadre de sa **formation initiale**, l'OS suit une formation qualifiante :

- les OS du département ministériel suivent un stage organisé par les bureaux de protection principaux des armées et de l'EMA²⁸. Dans la mesure du possible, l'OS d'une autorité publique contractante de référence effectue un stage organisé par le centre d'instruction à la sécurité industrielle de l'armement de la DGA (CISIA) ;
- les OS des organismes liés par contrat ou convention effectuent un stage organisé par le CISIA.

Le cas des OSSI, également soumis à cette obligation de formation qualifiante, est traité par ailleurs (cf. fiche 2.6 pour les OSSI des entités contractantes et PSSI-M pour les OSSI du département ministériel).

Au sein du MINARM, en complément de cette formation initiale obligatoire, les personnes ayant des responsabilités particulièrement sensibles au regard de la protection du secret²⁹ bénéficient d'une **formation continue** dispensée par la chaîne de défense-sécurité de l'ADS à laquelle elles appartiennent.

Le centre d'instruction à la sécurité industrielle de l'armement (CISIA) de la DGA organise la formation initiale des OS et OSSI pour les entreprises en relation avec la défense ainsi que des stages de remise à niveau.

Les OS et OSSI d'entreprises peuvent bénéficier en complément d'une formation continue organisée par la DRSD au niveau régional.

2. Sensibilisation initiale du personnel habilité

L'ensemble du personnel habilité est sensibilisé aux enjeux, aux risques et à ses responsabilités en matière de protection du secret de la défense nationale. La

²⁸ L'EMA, en liaison avec la DPID, développe et adapte le programme de formation annuellement.

²⁹ 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.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.8

sensibilisation initiale s'appuie sur les textes réglementaires en vigueur et est officialisée par la signature d'un **engagement de responsabilité** (voir fiche 3.5).

Cette sensibilisation est organisée par l'OS et l'OSSI qui précisent à cette occasion les obligations de confidentialité, comme de ne pas se prévaloir de sa décision d'habilitation en dehors de l'exercice de ses fonctions ou de l'accomplissement de sa mission, et à chacun les risques propres à son activité (secrétariats, rédacteurs, détenteurs, acheteurs...).

Les **responsables de sécurité** (OS, OSSI,...) reçoivent quant à eux de leur poste de rattachement RSD compétent une information générique en matière de protection du secret adaptée à leur situation (responsabilités futures, outils, contacts).

3. Sensibilisation des autres personnels

Une sensibilisation régulière est la clé de voûte de la prévention en matière de protection, notamment celle du secret de la défense nationale. Elle permet de convaincre de la nécessaire adhésion à la politique de sécurité. Elle est menée par l'OS et l'OSSI, appuyés par le personnel des BPS.

La sensibilisation courante s'adresse à un public déterminé en fonction de son emploi et de sa proximité au regard du secret de la défense nationale ou des informations considérées comme sensibles. Le message consiste à rappeler :

- les risques d'investigations ou d'approches par des individus ou des organisations étrangers ;
- les dispositions législatives et réglementaires en vigueur (code pénal, code de la défense, présente instruction, autre 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 au système d'information ;
- les mesures à prendre en cas de compromission, ainsi qu'en cas d'incident affectant la sécurité d'un système d'information.

Son efficacité repose sur la présentation de cas concrets étayés et commentés. Elle peut prendre la forme d'une conférence, d'un face-à-face, d'un document, voire d'un e-learning.

La sensibilisation à la sécurité des systèmes d'information s'adresse à tout public. Elle s'appuie sur des cas concrets d'attaque ou de failles relevées et indique les conséquences de ces dernières. Elle vise à améliorer l'hygiène informatique de tous.

La sensibilisation SSI donne les mesures et les pratiques à adopter pour diminuer le risque. Elle aborde différents sujets actuels de la SSI en adéquation avec les vecteurs de menaces du moment (supports numérique, « *malwares* », réseaux sociaux, « *Smartphone* », « *cloud* »,...). Elle peut intervenir en complément d'une autre sensibilisation.

La sensibilisation aux risques de compromission s'adresse au personnel manipulant des ISC. Elle consiste en un rappel des obligations réglementaires, des procédures à respecter à tous les stades de vie des ISC et du risque pénal et contractuel encouru, des mesures à

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.8**

prendre en cas de compromission, ainsi qu'en cas d'incident affectant la sécurité d'un système d'information. Elle développe notamment les situations de compromission potentielles au cours de périodes de vulnérabilité particulières (déménagements, restructurations,...).

La sensibilisation préalable à un déplacement à l'étranger : l'officier de sécurité effectue une sensibilisation générique périodique auprès de l'ensemble des personnes habilitées ou ayant accès à des informations sensibles ou protégées par la mention de protection *Diffusion Restreinte* concernant les voyages à l'étranger pour des raisons professionnelles ou personnelles.

Lorsqu'une personne habilitée est amenée à se rendre pour des raisons professionnelles hors du territoire national³⁰, dans un pays jugé par l'organisme comme présentant des risques particuliers pour son activité, elle avertit son officier de sécurité afin qu'il la sensibilise de manière spécifique. En cas de déplacements fréquents, la sensibilisation n'est pas systématique avant chaque déplacement si le niveau de menace et les mesures de sécurité n'ont pas évolué.

La sensibilisation à la sécurité économique s'adresse au personnel de l'entreprise et, plus particulièrement, à tous ceux qui sont en relation avec des acteurs extérieurs à la société. Elle met en exergue les menaces pouvant obérer la capacité de production de l'entreprise et l'incidence économique résultante. Elle s'attache à développer les risques induits par les comportements humains à risques, dans l'emploi de nouvelles technologies, ou dans l'application des règles établies. Elle met en exergue les risques d'atteinte à l'image et à la notoriété.

³⁰ De surcroît, le militaire demande l'autorisation à sa chaîne hiérarchique en initiant une demande de séjour à l'étranger (cf. fiche 9.6).

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.9****INSPECTIONS, AUDITS ET CONTRÔLES DES ORGANISMES
DETENANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS, DES
INFORMATIONS *DIFFUSION RESTREINTE* OU SENSIBLES****Références :**

- IGI 1300 – 2.3.3
- Pour les établissements du MINARM, ses établissements publics sous tutelle et les INID du CEA : IM n° 1544/DEF/CAB/DR du 17 janvier 2017, version du 10 août 2020, relative à la défense-sécurité des activités, moyens et installations relevant du ministère de la défense

Points clés :

- Des contrôles internes et externes permettent de vérifier la bonne application des mesures de protection du secret par chaque entité :
 - quel que soit l'organisme, le contrôle interne, effectué ou piloté par l'OS, constitue le cadre d'action privilégié pour évaluer le niveau de protection des informations classifiées, *Diffusion Restreinte* ou sensibles.
 - pour les organismes ministériels les plus sensibles, des inspections sont conduites selon les exigences de l'IM 1544.
 - les entités liées par contrat ou convention sont soumises au contrôle externe du représentant du pouvoir adjudicateur (RPA) (entité contractante de référence), de l'autorité d'habilitation, de l'autorité de sécurité déléguée (cf. fiche 9.1) et du service enquêteur concerné.
- Pour le MINARM, la protection des informations, qu'elles soient classifiées, *Diffusion Restreinte* ou sensibles, s'inscrit dans un processus de contrôle plus large englobant tous les domaines de la défense-sécurité (protection du secret de la défense nationale, sécurité des activités d'importance vitale, protection du potentiel scientifique et technique de la nation).
- Le SGDSN procède aux inspections relatives aux classifications spéciales.

Les inspections, audits et contrôles ont pour objet la vérification de :

- la capacité des organismes à réagir efficacement aux risques et aux menaces identifiés ;
- la conformité des entités aux dispositifs de protection et à la réglementation définie dans les documents de référence.

Inspection : mission d'évaluation conduite pour le compte d'une autorité, et consistant pour les services enquêteurs à s'assurer que les objectifs fixés par la présente instruction et ses déclinaisons ministérielles soient compris et appliqués. Elle donne lieu à la rédaction et diffusion d'un rapport.

Audit : mission d'expertise dont le périmètre est défini par l'autorité demanderesse, interne ou externe de l'organisme. Cette action recouvre des opérations d'investigation, de vérification, de contrôle et d'évaluation répondant à des exigences normatives et réglementaires. Cette mission se traduit par un diagnostic de l'organisation et

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.9

l'identification de vulnérabilités, faiblesses et/ou de non conformités afin d'apporter les recommandations permettant de définir et de mener toutes actions correctives nécessaires et des actions de progrès. Elle donne lieu à la rédaction et diffusion d'un rapport.

Contrôle : vérification administrative, consistant à vérifier un écart par rapport à une norme, une référence, à la conformité avec la présente instruction et imposer les corrections nécessaires. Elle donne lieu à la rédaction et diffusion d'un rapport.

1. Contrôle interne au sein des chaînes de protection du secret

Les contrôles internes, conduits directement par les entités, constituent l'action de contrôle essentielle en matière de protection du secret pour l'ensemble des sites.

Cette action est à la charge de la chaîne de protection du secret au sein des ADS et des entités contractantes ou liées par convention. Sous la responsabilité du chef d'entité (cf. fiche 2.4), les contrôles sont **proposés et menés ou pilotés par les OS et OSSI**, chacun dans leur domaine respectif.

L'OS de niveau 1 (ou l'OCS, OS de groupe ou de holding, pour les entreprises contractantes) est responsable du contrôle de la chaîne de protection du secret dont il est l'autorité fonctionnelle³¹. Ces contrôles sont réalisés avec une périodicité maximale de trois ans.

2. Contrôle externe

Les organismes relevant du département ministériel et les entités contractantes ou liées par convention au MINARM sont soumises aux inspections du service enquêteur.

Les inspections sont soit planifiées, soit conduites de manière inopinées à la diligence du ministre ou du directeur du service enquêteur. Pour les sites désignés « point d'importance vitale », les modalités d'inspections sont décrites dans l'IM1544.

Les rapports d'inspection utilisent des critères communs d'appréciation du niveau de sécurité afin de permettre la tenue à jour de tableaux de bord ministériels.

Après la transmission du rapport d'inspection, l'entité inspectée dispose de 6 mois pour rendre compte des mesures correctives engagées sur son site

Des audits peuvent être demandés par la chaîne hiérarchique dans les domaines relevant de sa compétence.

Pour les entités contractantes ou liées par convention relevant de son périmètre³², la DGA planifie, en coordination avec la DRSD, et conduit des audits de sécurité de défense et des systèmes d'informations au titre de son rôle d'autorité d'habilitation, d'autorité de sécurité déléguée et d'autorité contractante de référence. Les rapports établissent les niveaux de sécurité sur la base des critères fournis par l'IM 1544. L'entité auditée

³¹ Pour effectuer ses contrôles *in situ*, il lui est recommandé de s'appuyer sur une grille d'évaluation des vulnérabilités constatées dont le modèle est à adapter en fonction des spécificités du site.

³² Toutes les entreprises contractant avec le MINARM hors DGSE. La DGSE planifie et conduit seule ou en coordination avec la DRSD des audits de sécurité de défense et des systèmes d'informations au titre de son rôle d'autorité d'habilitation et d'autorité contractante de référence.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.9**

dispose d'un délai de 6 mois pour remettre un plan d'actions qui sera suivi régulièrement. A la suite de l'alerte de tiers, d'un incident de sécurité, ou sur demande d'une autorité, la DGA peut réaliser, le cas échéant de manière inopinée, des contrôles.

Les contrôles, inspections ou audits sont détaillés dans la fiche 4.13 relative aux contrôles des personnes morales par les autorités contractantes de référence, l'autorité d'habilitation, l'autorité de sécurité déléguée ou le service enquêteur.

3. Cas particuliers : Contrôle gouvernemental de la dissuasion et TS « classification spéciale »

La protection du secret dans le cadre du contrôle gouvernemental de la dissuasion (CG) fait l'objet de mesures de contrôle ou d'inspections supplémentaires détaillées dans des instructions spécifiques.

Des contrôles et des inspections sont organisés périodiquement par le SGDSN pour vérifier l'application, par les organismes émettant, recevant, traitant ou conservant des ISC de niveau TS « classification spéciale », des instructions et des directives relatives à la protection du secret. Le SGDSN propose toutes mesures propres à améliorer les conditions générales de sécurité. Les rapports de synthèse incluant les mesures préconisées pour rectifier les déficiences constatées et leur planification sont adressés aux autorités responsables des entités contrôlées et au ministre de la défense. En cas d'anomalies constatées, le SGDSN peut saisir le procureur, par l'intermédiaire du ministre.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES

INTRODUCTION : PROCESSUS D'HABILITATION DU PERSONNEL

Référence :

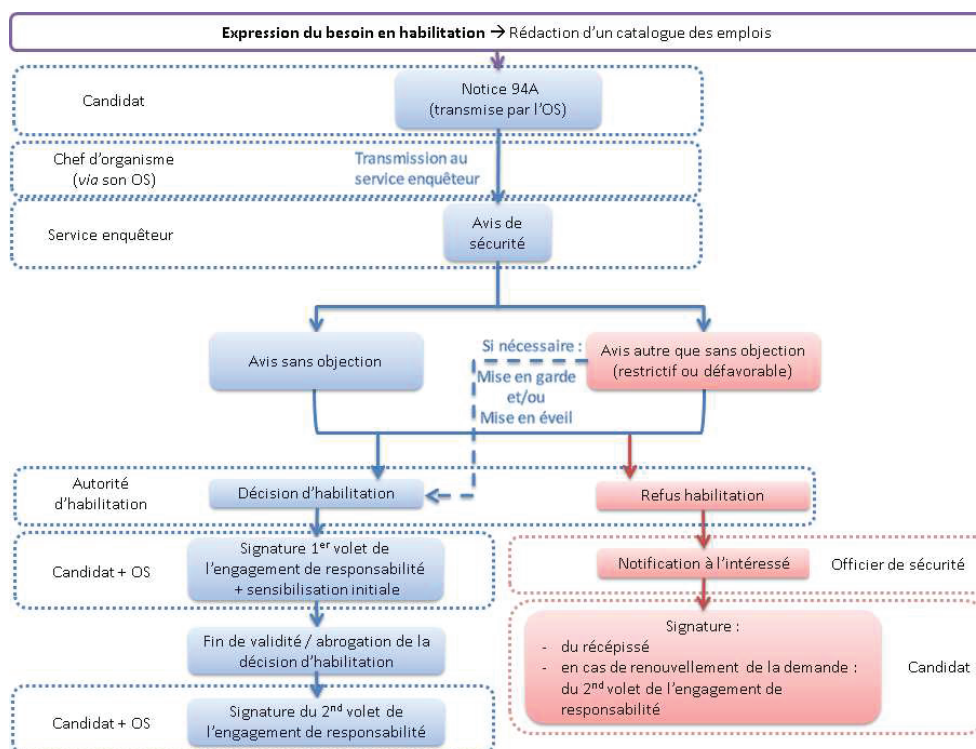
IGI 1300 – chapitre 3

Point clé :

L'accès aux ISC est subordonné à l'habilitation du personnel concerné et à son besoin d'en connaître.

En application du code de la défense³³, « Nul n'est qualifié pour connaître des informations ou supports classifiés s'il n'a fait au préalable l'objet d'une décision d'habilitation et s'il n'a besoin, selon l'appréciation de l'autorité d'emploi sous laquelle il est placé, au regard notamment du catalogue d'emplois justifiant une habilitation établie par cette autorité, de les connaître pour l'exercice de sa fonction ou l'accomplissement de sa mission ».

Le processus d'habilitation au MINARM suit un cheminement rigoureux décrit dans le schéma ci-dessous et précisé dans les fiches 3.1 à 3.6.



³³ Article R. 2311-7 du code de la défense.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.1**CATALOGUE DES EMPLOIS****Référence :**

IGI 1300 – 3.1.2

Points clés :

- Le catalogue des emplois établit pour chaque niveau de classification la liste des postes pour lesquels le besoin d'en connaître est avéré et une procédure d'habilitation doit être engagée.
- L'appréciation du besoin d'en connaître doit être rigoureuse et mesurée au plus juste.
- Les personnes morales de droit privé exécutant un contrat soumis au respect de la protection du secret doivent être habilitées et détenir également un catalogue des emplois.

1. Généralités

L'appréciation du « besoin d'en connaître » est fondée sur le principe selon lequel une personne ne peut avoir accès à des informations et supports classifiés que dans la mesure où son poste l'exige (pour l'exercice de sa fonction ou l'accomplissement de sa mission).

Cette appréciation doit être rigoureuse et mesurée. Il convient ainsi d'éviter la solution de facilité consistant, faute de vouloir discriminer ceux qui ont véritablement besoin de connaître des informations classifiées, à demander des habilitations pour tout le personnel d'un état-major, d'un service, d'une entreprise, d'une unité ou d'une formation, d'une promotion d'élèves ou d'un stage. Le besoin d'en connaître est attesté par la demande d'habilitation, adjointe à la notice individuelle de sécurité (94A), incluse dans le dossier d'habilitation (cf. IGI 1300 - annexes 5 et 7) où figure, en particulier, le numéro d'inscription au catalogue des emplois.

2. Procédure

L'autorité d'emploi, qu'il s'agisse d'un organisme du MINARM ou d'un organisme lié par contrat ou convention avec ce dernier, établit pour chaque nature et niveau d'habilitation un catalogue des emplois³⁴ qui précise, via l'octroi d'un numéro de poste, les fonctions et missions impliquant nécessairement l'accès à des informations et supports classifiés (ISC) de niveau *Secret* et *Très Secret* (hors classifications spéciales) ainsi que les nom et prénom des personnes physiques les occupant. Une copie du catalogue des emplois est adressée à l'autorité d'habilitation. Au sein du département ministériel, ce catalogue est, en outre, validé par l'autorité d'habilitation.

Les demandes d'habilitation sont établies en référence au catalogue des emplois. Lorsqu'une demande d'habilitation lui parvient, l'officier de sécurité (OS) vérifie l'inscription de la fonction concernée dans le catalogue des emplois correspondant. Il

³⁴ Peuvent coexister au sein d'un organisme des catalogues *Secret* OTAN (SO) et *Secret* UE (SUE) par exemple.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.1

examine, à titre exceptionnel, le bien-fondé de la demande lorsque l'emploi ne figure pas au catalogue et le modifie en conséquence.

Les catalogues doivent être mis à jour au moins une fois par an³⁵ et à l'occasion de chaque réorganisation de service. Il peut faire l'objet d'un contrôle par l'autorité d'habilitation ou par le HFCDS afin de vérifier notamment si les titulaires des fonctions répertoriées ont effectivement eu accès à des informations et supports classifiés pour le niveau concerné.

Tout agent occupant ou envisageant d'exercer une fonction ou d'accomplir une mission requérant un accès à des informations et supports classifiés est tenu de se soumettre à une procédure d'habilitation. Tout refus entraîne de facto l'impossibilité pour l'intéressé d'occuper cet emploi.

³⁵ Pour les organismes MINARM, la période estivale est à privilégier.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.2**DEMANDE D'HABILITATION****Référence :**

IGI 1300 – 3.3

Points clés :

- La demande d'habilitation est engagée lorsque la fonction est inscrite au catalogue des emplois ou lorsqu'un besoin d'accéder à des informations et supports classifiés pour des opérations est avéré.
- Exceptionnellement, la demande d'habilitation peut suivre des procédures dérogatoires à la procédure de droit commun (procédure d'urgence et procédure simplifiée). Le recours à celles-ci est dûment justifié.
- Le recours aux procédures dérogatoires est prohibé pour l'habilitation des agents des services de renseignement.

1. Lancement de la procédure

Le chef d'organisme employeur *via* son officier de sécurité s'assure en premier lieu que la demande d'habilitation est justifiée par le besoin d'accéder à des informations et supports classifiés pour exercer une fonction ou accomplir une mission inscrite au catalogue des emplois.

L'officier de sécurité informe ensuite le candidat des obligations induites par l'habilitation ainsi que des dispositions relatives à sa responsabilité pénale en cas de compromission. Il lui précise la procédure d'habilitation choisie.

2. Procédure de droit commun

L'OS transmet au candidat une notice individuelle de sécurité 94A. Ce dernier la complète sous forme informatique³⁶. Un exemplaire est signé par le candidat. Cette pièce officielle, dont la complétude et la cohérence sont vérifiées par l'OS avant d'initier la demande d'habilitation, est conservée par l'employeur. Ce dernier doit être en mesure de la produire en cas de réclamation. Elle est détruite un an après la fin de validité de l'avis de sécurité émis par le service enquêteur.

Le dossier d'habilitation se compose des documents énumérés ci-dessous :

- d'un dossier d'habilitation³⁷ organisé en deux parties :
 - o une demande d'habilitation signée par le chef d'organisme ou l'officier de sécurité attestant le besoin de connaître des informations et supports classifiés à un niveau donné ;
 - o la notice individuelle de sécurité (94A) renseignée intégralement par le candidat.
- une photographie récente (moins de trois mois, format identique à celui demandé pour la carte nationale d'identité) numérisée.

³⁶ Formulaire à télécharger sur le site Intradef de la DRSD ou sur le site Internet www.ixarm.com pour les entités contractantes.

³⁷ *Idem*

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.2

Le chef d'organisme employeur transmet le dossier d'habilitation au niveau S ou TS à l'autorité d'habilitation, qui le poste sur SOPHIA³⁸ :

Les demandes d'habilitation au niveau TS faisant l'objet d'une classification spéciale, sont transmises selon une procédure spécifique et instruites par le SGDSN, autorité d'habilitation.

La procédure d'habilitation de niveau *Secret* ou *Très Secret* n'est engagée qu'au seul profit de la personne effectivement nommée dans l'emploi. L'anticipation peut néanmoins être une mesure de bonne gestion permettant à l'agent de prendre connaissance des ISC dès sa prise de fonction.

3. Procédures dérogatoires à la procédure de droit commun³⁹

Ces procédures sont prohibées pour l'habilitation des agents des services spécialisés de renseignement.

a. Procédure d'urgence

Certaines fonctions, affectations ou situations qui impliquent une prise de connaissance immédiate d'ISC ne peuvent se satisfaire des délais de la procédure normale.

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.

Cette procédure ne remplace ni n'interrompt la procédure normale. Elle doit être légitime, motivée par écrit sur le formulaire de demande, rester exceptionnelle et en aucun cas pallier un manque de planification des organismes demandeurs. Le service enquêteur peut refuser de traiter une telle demande si elle constate un détournement de cette procédure. Ce détournement est caractérisé notamment par une motivation stéréotypée ou lacunaire.

Pour les dossiers d'habilitation au niveau *Très Secret* « *classification spéciale* », seul le SGDSN au regard des éléments transmis par l'autorité compétente, peut engager une telle procédure⁴⁰.

b. Procédure simplifiée

La procédure simplifiée n'est pas applicable au personnel des entités privées exécutant des contrats conclus au profit du MINARM.

³⁸ Les procédures d'utilisation du SI SOPHIA sont disponibles sur le site Intradef de la DRSD ou sur le site Internet www.ixarm.com

³⁹ Les habilitations du personnel de la DGSE et des entités contractantes qui lui sont rattachées répondent à une procédure qui lui est propre.

⁴⁰ La procédure d'urgence au sein de la DGSE diffère également de celle énoncée dans cette instruction.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.2

Le personnel militaire et le personnel civil du ministère des armées⁴¹ peuvent être exceptionnellement habilités au niveau *Secret* uniquement par l'autorité d'habilitation dont ils relèvent sans intervention du service enquêteur.

L'usage de cette procédure dérogatoire doit demeurer exceptionnel. Il est impératif de ne l'employer qu'en cas de nécessité avérée et pour des habilitations d'une durée **inférieure ou égale à trois mois** (stages, vacations, formations, emploi provisoire).

Cette procédure peut être appliquée à condition que le candidat :

- ait fait l'objet d'une enquête administrative en application des articles L. 114-1 et L. 114-2 du code de la sécurité intérieure (cf. fiche 3.9) au moment du recrutement, de la nomination ou de l'affectation ;
- ait rempli la notice individuelle de sécurité (94A) ;
- ait signé le premier volet de l'engagement de responsabilité.

La décision d'habilitation est notifiée à l'intéressé dans les conditions ordinaires. Le service enquêteur doit en être informé.

A tout moment, le chef d'organisme employeur comme l'autorité d'habilitation peuvent demander qu'une enquête administrative soit effectuée par le service enquêteur, selon la procédure d'habilitation ordinaire.

⁴¹ 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 décret n° 2012-32 du 9 janvier 2012 relatif aux emplois de chef de service et de sous-directeur des administrations de l'État.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.3**AVIS DE SECURITE****Référence :**

IGI 1300 – 3.3.1.3

Points clés :

- L'enquête administrative pour le renseignement et la sûreté préalable à une habilitation est menée par le service enquêteur. Elle s'achève par l'émission d'un avis de sécurité.
- L'autorité d'habilitation n'est pas liée à la conclusion de l'avis de sécurité émis. Elle prend sa décision après avoir apprécié les différents éléments recueillis pendant l'instruction du dossier.

1. Généralités

L'avis de sécurité est une évaluation des vulnérabilités éventuellement détectées lors de l'enquête administrative. Il permet à l'autorité d'habilitation d'apprécier l'opportunité de l'habilitation du candidat, au regard des éléments communiqués et des garanties qu'il présente pour le niveau d'habilitation requis.

L'enquête administrative pour le renseignement et la sûreté préalable à une habilitation est du ressort :

- de la DRSD :
 - o pour les personnels civils et militaires relevant du MINARM⁴²,
 - o pour les entreprises contractantes avec le MINARM et leur personnel effectuant les travaux prévus par ces contrats ;
 - o les personnels militaires de la gendarmerie,
- de la DGSE :
 - o pour les personnels civils ou militaires qui y sont affectés ;
 - o pour les entreprises contractantes avec la DGSE et leur personnel effectuant les travaux prévus par ces contrats.

La durée maximale de l'enquête de sécurité est en principe de 3 mois pour un dossier d'habilitation au niveau *Secret* et de 6 mois au niveau *Très secret*, à compter de sa réception par le service enquêteur. Passé ce délai, la demande peut être relancée après contact préalable avec le service enquêteur.

Les conclusions de l'avis de sécurité de la DRSD sont de trois types :

- **sans objection**, lorsque 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**, lorsque 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

⁴² 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.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.3

l'officier de sécurité, et le cas échéant, une sensibilisation particulière du candidat, permettraient de maîtriser. Dans ce cas, le service enquêteur peut recommander une procédure de mise en garde de l'employeur, de mise en éveil de l'intéressé, ou qu'il soit recouru à ces deux procédures (cf. fiche 3.4) ;

- **avis défavorable**, lorsque 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. Néanmoins, dans le cas où l'autorité d'habilitation ne suit pas l'avis du service enquêteur et décide d'habiliter le candidat, le service enquêteur peut recommander une procédure de mise en garde de l'employeur, de mise en éveil de l'intéressé, ou qu'il soit recouru à ces deux procédures (cf. fiche 3.4).

Les avis de sécurité autres que sans objection sont classifiés.

2. Validité de l'avis de sécurité

Sauf précision contraire du service enquêteur, l'avis de sécurité est valable jusqu'au niveau pour lequel il a été requis et, le cas échéant, pour le niveau inférieur. Dans ce cas, la durée de validité ne dépasse pas celle de l'avis initial.

La durée de validité de l'avis de sécurité est fonction 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 ne constitue en soi ni une autorisation, ni un refus, et ne lie pas l'autorité d'habilitation, qui prend sa décision après avoir apprécié les différents éléments recueillis pendant l'instruction du dossier (nature de l'avis de sécurité, sensibilité du poste tenu par l'intéressé et tout autre élément permettant à l'autorité d'habilitation d'apprécier le degré de confiance à accorder).

3. Transmission des avis de sécurité⁴³

Selon le cas, le service enquêteur fait parvenir à l'autorité d'habilitation :

- l'avis de sécurité sans objection *via* SOPHIA (à l'exception du TS « classification spéciale ») ;
- deux exemplaires de l'avis de sécurité « restrictif » ou « défavorable » (cf. IGI 1300 - annexe 15) *via* un agent du service enquêteur, accompagnés d'une fiche confidentielle (cf. [annexe 1](#)), exposant les motifs justifiant l'avis. Un exemplaire est conservé, l'autre est renvoyé complété au service enquêteur.

La fiche confidentielle est composée de deux parties distinctes, permettant de séparer les éléments non classifiés, qui peuvent être communiqués au candidat, de ceux le cas échéant classifiés, qui ne peuvent être portés qu'à la connaissance de l'autorité d'habilitation ou de son OS.

Ne pouvant être reproduite, la fiche confidentielle est retournée après communication et sans délai au service enquêteur. L'autorité d'habilitation peut, en tant que de besoin,

⁴³ La transmission des avis de sécurité de la DGSE répond à une procédure spécifique différente de celle-ci.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.3

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.

L'autorité d'habilitation informe le service enquêteur de la décision prise (refus ou admission à l'habilitation) ainsi que des suites données aux recommandations (réalisation des procédures de mise en garde et de mise en éveil par exemple).

La validité de la décision d'habilitation ne peut excéder celle de l'avis de sécurité initial.

4. Durée de conservation

L'exemplaire de l'avis de sécurité signé et retourné au service enquêteur est conservé par celui-ci sous forme numérique sans limitation de durée. L'exemplaire⁴⁴ conservé par l'autorité d'habilitation doit être détruit un an après l'expiration de la validité de l'avis de sécurité.

⁴⁴ Seuls les avis autres que sans objection sont transmis en version papier.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.4**MISE EN EVEIL ET MISE EN GARDE****Référence :**

IGI 1300 –3.4.1.2

Points clés :

- 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 qui sont la mise en éveil de l'intéressé et la mise en garde de l'employeur.
 - La mise en éveil est une sensibilisation de l'intéressé sur les éléments communicables de vulnérabilité révélés par l'enquête.
 - La mise en garde concerne exclusivement l'OS et son employeur. En aucun cas, la personne habilitée n'est informée de la procédure de mise en garde.

1. Généralités

L'enquête administrative effectuée par le service enquêteur se traduit par l'émission d'un avis de sécurité destiné à l'autorité d'habilitation. En cas d'avis autre que sans objection, l'autorité d'habilitation peut décider de n'accorder l'habilitation qu'après la mise en œuvre de l'une ou l'autre des mesures de sécurité suivantes :

- la mise en éveil de l'intéressé⁴⁵ ;
- la mise en garde de l'autorité compétente ou de l'OS de l'organisme dont relève le candidat à l'habilitation.

Les procédures de mise en garde et de mise en éveil peuvent être cumulées.

2. Procédure de mise en éveil de l'intéressé

La mise en éveil consiste à sensibiliser le candidat à l'habilitation sur les éléments communicables de vulnérabilité révélés par l'enquête⁴⁶.

En coordination avec l'autorité d'habilitation, l'OS effectue la mise en éveil avec l'appui du service enquêteur le cas échéant. Il étudie avec ce service les mesures de sécurité complémentaires à mettre en œuvre au regard de la situation.

A l'issue de l'entretien de mise en éveil, une attestation (cf. IGI 1300 - annexe 10) est signée par le représentant de l'autorité d'habilitation⁴⁷, par l'OS concerné et par l'intéressé puis est conservée par l'autorité d'habilitation. La décision d'habilitation n'est rendue qu'à l'issue de la procédure. L'OS informe le service enquêteur de la notification de la mise en éveil.

⁴⁵ Le service enquêteur peut d'initiative procéder à la mise en éveil.

⁴⁶ Il peut s'agir par exemple de ses attaches avec l'étranger ou de diverses particularités de son environnement. Il revient au service enquêteur d'apprécier, pour chaque cas, ce qui peut constituer une vulnérabilité.

⁴⁷ Qui peut être l'OS.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.4

3. Procédure de mise en garde de l'autorité compétente

La mise en garde consiste, pour l'autorité d'habilitation, après avoir été informée par le service enquêteur et avec son concours le cas échéant, à avertir l'employeur ou son OS des éléments de vulnérabilité révélés par l'enquête, en dehors de la présence du candidat à l'habilitation. L'autorité d'habilitation demande alors à l'employeur de mettre en œuvre des mesures de sécurité ou de prendre des précautions particulières à l'égard de l'intéressé, si nécessaire avec le conseil du service enquêteur.

A l'issue de l'entretien de mise en garde, une attestation (cf. IGI 1300 - annexe 9) est signée par 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.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.5**DECISION D'HABILITATION OU DE REFUS D'HABILITATION****Références :**

- IGI 1300 – 3.4
- Arrêté du 21 mars 2012 modifié portant délégation des pouvoirs du ministre de la défense en matière de décisions d'habilitation à connaître des informations et supports couverts par le secret de la défense nationale

Points clés :

- La décision d'habilitation est prise par l'autorité d'habilitation compétente.
- Elle s'appuie notamment sur l'avis de sécurité émis par le service enquêteur⁴⁸.
- La notification de la décision d'habilitation à l'intéressé s'accompagne de la signature par ce dernier d'un engagement de responsabilité (1^{er} volet).
- Un refus d'habilitation n'a pas à être motivé auprès de l'intéressé.

1. Prise de décision

A l'issue de l'enquête administrative pour le renseignement et la sûreté, le service enquêteur émet un avis de sécurité (cf. fiche 3.3) à destination de l'autorité d'habilitation, sur lequel celle-ci s'appuie notamment pour prendre sa décision⁴⁹. Les conclusions de l'avis de sécurité ne lient pas l'autorité d'habilitation.

a. Avis de sécurité sans objection

En présence d'un avis de sécurité sans objection, l'autorité d'habilitation peut établir une décision d'habilitation (cf. IGI 1300 - annexe 8), qu'elle adresse via son officier de sécurité au chef d'organisme employeur.

b. Avis de sécurité autre que sans objection (AQSO)

En présence d'un avis de sécurité restrictif ou défavorable, l'autorité d'habilitation peut décider ou non de prononcer l'admission.

Premier cas : l'autorité d'habilitation prononce l'admission.

- Elle peut demander une mise en éveil de l'intéressé et / ou effectuer une mise en garde de l'employeur (cf. fiche 3.4) et étudie avec l'employeur et le service enquêteur, le cas échéant, les mesures de sécurité adéquates ;
- Elle réceptionne l'attestation de bon déroulement de cette ou ces procédures (IGI 1300 - annexes 9 et 10) ;
- Elle donne son accord aux mesures de sécurité envisagées localement ;
- Elle établit une décision d'habilitation et l'adresse au chef d'organisme employeur.

⁴⁸ A l'exception de la procédure simplifiée qui ne concerne que le personnel du MINARM (cf. fiche 3.3 paragraphe 2.b).

⁴⁹ Il convient d'informer le demandeur sur la disposition selon laquelle le silence gardé par l'administration pendant deux mois vaut décision implicite de rejet de la demande (décret 2014-1266). La durée maximale de l'enquête dépassant ce délai, cette disposition n'empêche pas une décision d'habilitation favorable si aucune objection n'est formulée.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.5

Second cas : l'autorité d'habilitation prononce un refus d'habilitation.

L'autorité d'habilitation établit une décision de refus (cf. IGI 1300 - annexe 12) et l'adresse au chef d'organisme employeur.

La décision de refus est notifiée et remise à l'intéressé (cf. IGI 1300 - annexe 13). Elle n'a pas à être motivée en application du b) du 2° de l'article L. 311-5 du code des relations entre le public et l'administration.

Lors de cet entretien, l'intéressé est informé des voies de recours administratifs et contentieux, ainsi que des délais qui lui sont ouverts pour contester cette décision. A cette fin, l'officier de sécurité lui remet un récépissé de notification de décision de refus d'habilitation⁵⁰ (cf. IGI 1300 - annexe 13) dont un exemplaire, daté et signé par l'intéressé, est conservé par l'autorité d'habilitation. Une copie de la décision ainsi que du récépissé de notification est adressée au service enquêteur.

Si l'autorité d'habilitation décide ultérieurement d'accorder l'habilitation, après l'avoir refusée dans un premier temps, elle doit en informer le service enquêteur.

Les raisons ayant motivé l'avis ne peuvent être communiquées que dans les conditions fixées dans la fiche 3.3.

c. Décision d'habilitation temporaire

La décision d'habilitation temporaire ne s'applique pas à la personne morale de droit privé, ni aux personnes physiques travaillant pour le compte de cette dernière dans le cadre d'un contrat prévoyant l'exécution de travaux classifiés.

L'autorité d'habilitation peut accorder une décision d'habilitation temporaire autorisant un agent habilité au niveau *Secret* à prendre connaissance ponctuellement d'ISC de niveau *Très Secret* hors classifications spéciales, pour une durée de trois mois non renouvelable dans sa fonction. Elle en informe le service enquêteur. Cette période ne peut être fractionnée.

2. Durée de la décision

La durée de validité de la décision ne peut en aucun cas excéder la durée de validité de l'avis de sécurité initial. Elle peut en revanche être plus courte :

- sur décision de l'autorité d'habilitation au regard des vulnérabilités qui auront été portées à sa connaissance (avis AQSO) ou compte tenu de la mission ;
- en cas de procédure d'urgence (cf. fiche 3.2).

Chaque décision est émise pour un poste, une mission ou une fonction. Elle cesse d'être valide dès que la personne cesse l'activité pour laquelle elle a été émise.

3. Exploitation de la décision

La décision prise par l'autorité d'habilitation est transmise au chef d'organisme employeur via l'OS. Dès réception, ce dernier notifie au candidat à l'habilitation la décision individuelle prise à son endroit, qu'elle soit favorable ou non.

⁵⁰ Article L. 211-2 du code des relations entre le public et l'administration.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.5

- Lors de la notification de la décision d'habilitation, il fait signer le premier volet⁵¹ de l'engagement de responsabilité (cf. IGI 1300 - annexe 11). Cette notification doit être assortie d'une sensibilisation aux obligations particulières imposées par l'accès à des ISC (cf. fiche 2.8).
- Lors de la notification du refus d'habilitation, il fait signer le récépissé de notification de refus d'habilitation sur lequel sont portées les mentions relatives au recours (cf. IGI 1300 - annexe 13) dont un exemplaire, daté et signé par l'intéressé, est conservé par l'autorité d'habilitation (cf. 1.b. second cas). Dans le cas d'une procédure de renouvellement, il fait également signer le second volet de l'engagement de responsabilité (cf. IGI 1300 - annexe 11).

La personne physique titulaire d'une décision d'habilitation ne peut faire publiquement état de cette décision ou s'en prévaloir en dehors de l'exercice de ses fonctions ou de l'accomplissement de sa mission.

⁵¹ Le second volet de cet engagement est signé lors de la cessation de fonction ou du retrait de l'habilitation.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.6**GESTION ET FIN DE L'HABILITATION****Référence :**

IGI 1300 – 3.5.2 à 3.5.8

Points clés :

- La validité d'une décision ne peut excéder la validité de l'avis de sécurité émis pour un niveau donné d'habilitation (hors disposition spécifique du renouvellement).
- Une décision d'habilitation peut être abrogée à tout moment par l'autorité d'habilitation.
- Lorsqu'une personne cesse d'être habilitée, elle est tenue de ne pas divulguer les informations classifiées dont elle aurait eu connaissance pendant l'exercice de ses fonctions ou l'accomplissement de sa mission.

En complément du catalogue des emplois, le chef d'organisme employeur, *via* son OS, fait tenir, pour chaque niveau de classification, un répertoire des dossiers d'habilitation en cours d'instruction et de suivi des habilitations en cours de validité. Ce dernier facilite la gestion des habilitations et permet de retrouver, de manière très rapide, les différentes informations nécessaires sur les personnes habilitées (date d'émission de la demande, niveau et nature d'habilitation, fonction ou mission du candidat, durée de validité, etc.).

Dans les entités ministérielles, l'OS archive la décision d'habilitation ou de refus d'habilitation.

En cas de nécessité, quel que soit l'organisme, un certificat de sécurité (cf. IGI 1300 - annexe 14) peut être délivré par l'autorité d'habilitation ou par l'OS de l'organisme de l'intéressé pour une mission ou pour une période déterminées.

1. Durée de validité des décisions d'habilitation

L'habilitation arrive à échéance au terme fixé dans la décision et, en tout état de cause, à la cessation des fonctions au titre desquelles elle a été accordée, quand bien même la date de fin de validité inscrite sur la décision n'est pas échue.

Elle peut être émise pour une durée inférieure à la durée initiale de validité de l'avis de sécurité mais ne peut l'excéder (cf. fiche 3.5).

2. Conservation des décisions

Les décisions d'habilitation sont conservées par l'officier de sécurité pendant leur durée de validité et un an au-delà, à l'exception de celles rendues au niveau *Très Secret* « classification spéciale », dont les modalités de gestion sont définies selon des directives spécifiques. Elles ne sont en aucun cas remises aux intéressés, ni reproduites.

Les données relatives à l'identité des personnes habilitées et aux éléments techniques de gestion des dossiers d'habilitation (formulaire 94A par exemple) sont conservées pour une durée d'un an après la fin de validité de l'avis de sécurité émis par le service enquêteur.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.6

3. Certificat de sécurité

Chaque fois qu'il est nécessaire, pour l'accomplissement d'une mission en métropole ou à l'extérieur, de présenter un document attestant une habilitation au niveau requis, un certificat de sécurité (cf. IGI 1300 - annexe 14) est délivré à l'intéressé par l'autorité d'habilitation ou l'OS de l'organisme auquel il appartient au vu de la décision d'habilitation effectivement détenue.

La durée de validité de ce document, limitée à un an au maximum, doit être précisée et, en tout état de cause, ne peut dépasser celle de l'habilitation correspondante.

Avant la fin de validité du certificat et au terme de la mission, l'intéressé procède ou fait procéder à sa destruction.

4. Renouvellement des habilitations

Le renouvellement de l'habilitation, pour les mêmes fonctions, est demandé dans le délai d'un an minimum à trois mois au plus tard avant la date d'expiration de la validité de l'habilitation initiale. Si cette disposition est respectée, la décision d'habilitation initiale est tacitement prorogée pendant les douze mois qui suivent son expiration.

La procédure est mise en œuvre dans les mêmes conditions que la demande initiale.

5. Changement de situation de l'habilité et révision de l'habilitation

- a. La personne habilitée a l'obligation d'informer le chef d'organisme employeur, *via* son OS, de tout changement affectant sa vie personnelle. Elle l'informe de tout contact suivi, dépassant le strict cadre professionnel, avec un ou des ressortissants étrangers.

L'OS lui fait alors remplir une notice individuelle de sécurité (94A) et la transmet à l'autorité d'habilitation, qui la transmet ensuite au service enquêteur.

Ce changement de situation peut entraîner une révision du dossier d'habilitation et l'émission d'un nouvel avis de sécurité.

- b. Si une vulnérabilité nouvelle est portée à la connaissance de l'autorité d'emploi, celle-ci peut décider de lancer une procédure de révision de la décision d'habilitation.
- c. Si une vulnérabilité nouvelle est portée à la connaissance du service enquêteur, celui-ci peut décider de lancer une procédure de révision de l'avis de sécurité.

6. Cessation de fonction

L'habilitation, liée à l'occupation d'un poste ou à l'exercice d'une fonction déterminée, expire lorsque son titulaire cesse ses fonctions. En quittant l'emploi précisé dans la décision d'habilitation, le titulaire signe le second volet de l'engagement de responsabilité.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.6

7. Portabilité de l'avis de sécurité en cas de changement de fonction

Lorsqu'une personne habilitée change d'affectation, son habilitation pour le poste initial prend fin⁵². Une autre décision d'habilitation, demandée par le nouvel employeur, est prise, si la nouvelle affectation l'exige, sur la base de l'avis de sécurité en cours. La notice individuelle de sécurité doit être à nouveau renseignée et transmise au service enquêteur.

En cas de changement d'autorité d'habilitation, l'officier de sécurité de l'entité quittée renvoie la décision d'habilitation et l'engagement de responsabilité à l'autorité d'habilitation. Afin d'informer la nouvelle autorité d'habilitation qu'un avis de sécurité est en cours de validité, l'autorité d'habilitation de l'entité quittée lui transmet une **attestation d'avis de sécurité**⁵³ (cf. IGI 1300 - annexe 15) mentionnant la fin de validité de l'avis de sécurité. Si l'avis est restrictif ou défavorable, la nouvelle autorité d'habilitation doit, pour prendre sa décision, demander au service enquêteur à connaître les motifs qui l'ont justifié.

8. Abrogation de la décision d'habilitation

L'habilitation peut être abrogée à tout moment ou à l'occasion d'une demande de renouvellement ou de révision, si l'intéressé ne remplit plus les conditions nécessaires à sa délivrance. Cela peut être le cas lorsque des éléments de vulnérabilités apparaissent, signalés notamment par le service enquêteur, l'autorité compétente ou l'officier de sécurité concerné, à la suite d'un changement de situation ou de comportement révélant un risque pour la défense nationale.

La décision portant abrogation de la décision d'habilitation (cf. IGI 1300 - annexe 12) est notifiée et remise à l'intéressé dans les mêmes formes que le refus d'habilitation. L'intéressé est informé des voies de recours administratif et contentieux, ainsi que des délais qui lui sont ouverts pour contester la décision (cf. IGI 1300 - annexe 13). L'OS s'assure que le service enquêteur est informé de cette décision.

En cas d'abrogation de sa décision d'habilitation, le titulaire signe le second volet de l'engagement de responsabilité. Il ne peut alors plus accéder à des ISC au risque de caractériser une compromission.

Pour le personnel habilité d'une entité contractante, le changement d'employeur (personne morale) entraîne l'abrogation de l'habilitation.

9. Achèvement ou modification des droits associés aux fonctions

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 accompagné de la décision. Il est conservé un an après la fin de validité de l'habilitation.

⁵² A l'exception d'une décision d'habilitation couvrant expressément plusieurs postes, conformément à l'article R. 2311-8 du code de la défense.

⁵³ Seulement lorsque la mutation dans le système SOPHIA n'est pas possible.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.6

Il peut s'avérer nécessaire d'informer les interlocuteurs habituels ayant le besoin d'en connaître des changements intervenus chez le personnel ou au sein de l'organisme.

Le bureau RH de l'entité doit indiquer à l'autorité hiérarchique comme à l'officier de sécurité les informations relatives 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'OS s'assure du retrait immédiat des différents droits d'accès. Il en informe l'OSSI concerné qui s'assure du retrait des droits et moyens d'accès aux systèmes d'informations classifiés. Un inventaire des informations et supports classifiés, dont l'intéressé a été le détenteur, est établi dans les conditions énumérées au titre 5 de la présente instruction.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.7**CAS DES HABILITATIONS OTAN ET UE****Références :**

- IGI 1300 – 3.4.4
- II 2100/SGDSN/SSD pour l'application en France du système de sécurité de l'OTAN
- IGI 2102/SGDSN/PSE/PSD sur la protection en France des informations classifiées de l'UE

Points clés :

- La procédure d'habilitation pour l'accès aux ISC OTAN et UE répond aux mêmes principes que la procédure nationale.
- Ces habilitations sont établies à partir d'un avis de sécurité pour un niveau d'habilitation national par l'autorité d'habilitation dont dépend le demandeur.
- L'habilitation nationale permet l'obtention d'une habilitation multinationale par référence, si nécessaire, tandis que la situation inverse n'est pas possible.

1. Dispositions générales

Il appartient aux autorités d'habilitation (cf. fiche 2.3) d'établir les décisions d'habilitation à connaître des ISC de l'Organisation du traité de l'Atlantique Nord (OTAN) et de l'Union européenne (UE). Le service enquêteur n'émet des avis de sécurité que pour un niveau d'habilitation national.

Nul ne peut connaître des ISC de l'OTAN et des informations classifiées de l'UE (ICUE) ou de toute autre organisation internationale régie par un règlement de sécurité approuvé par la France en raison de sa qualité ou de son emploi s'il ne satisfait pas aux deux conditions suivantes :

- avoir besoin d'en connaître pour l'accomplissement de sa mission ;
- y avoir été préalablement autorisé (habilitation).

La procédure d'habilitation consiste à acquérir la garantie générale qu'une personne peut, sans risque pour la collectivité comme pour elle-même, connaître des ISC. Les décisions d'habilitation à accéder à des ISC de l'OTAN ou de l'UE sont distinctes de celles concernant la protection du secret de la défense nationale. Néanmoins les décisions d'habilitation à accéder à des ISC français peuvent, en soi, à défaut d'une habilitation spécifique et sous réserve du besoin d'en connaître, donner accès aux ISC de l'OTAN ou ICUE de niveau correspondant et des niveaux inférieurs. La situation inverse n'est pas possible.

Il faut tenir compte des délais variables que peut exiger la procédure d'habilitation :

- pour l'affectation du personnel ;
- pour les prévisions de désignation du personnel à envoyer en mission, en stage, ou en liaison, auprès d'organismes nationaux ou internationaux.

La procédure d'habilitation pour l'accès aux informations classifiées de l'OTAN ou de l'UE concerne le personnel qui ne possède pas l'habilitation requise au regard de la nature (UE, OTAN) et/ou du niveau de classification des ISC OTAN ou ICUE auxquels il doit accéder ou qui doit engager un renouvellement de cette habilitation.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.7

L'habilitation est délivrée selon les procédures nationales (cf. fiches 3.1 à 3.6). Elle se concrétise par la délivrance d'une décision d'habilitation (cf. IGI 1300 - annexe 8), au vu de laquelle peut être délivré un certificat de sécurité (cf. IGI 1300 - annexe 14) précisant le niveau et la nature des ISC auxquels la personne habilitée peut avoir accès et la date de fin de validité de cette habilitation.

Le titulaire d'une habilitation signe l'engagement de responsabilité dans les mêmes conditions que pour l'habilitation nationale (réception et cessation d'habilitation).

2. Règles d'habilitation pour l'OTAN

Les dossiers d'habilitation, instruits par le service enquêteur, sont acheminés par les bureaux d'ordre COSMIC⁵⁴.

La décision d'accès au COSMIC TOP SECRET /Très Secret COSMIC (TSC) ou au NATO SECRET / Secret OTAN (SO) est délivrée dans les conditions prévues pour les informations nationales de niveau équivalent.

3. Règles d'habilitation pour l'UE

Les dossiers d'habilitation, instruits par le service enquêteur, sont acheminés par les bureaux d'ordre UE.

Toute personne ayant besoin de connaître des informations *Très Secret UE/EU TOP SECRET (TS-UE/EU-TS)*, *Secret UE/EU SECRET (S-UE/EU-S)* et *Confidentiel UE/EU CONFIDENTIAL (C-UE/EU-C)* fait l'objet d'une procédure d'habilitation permettant l'accès à ces informations. Elle doit avoir connaissance des règles de sécurité et des conséquences de toute négligence.

La décision d'habilitation aux niveaux TS-UE/UE-TS ou S-UE/UE-S est délivrée dans les conditions prévues pour les informations nationales de niveau équivalent.

La décision d'habilitation au niveau C-UE/EU-C est rendue par les autorités d'habilitation du niveau Secret.

4. Habilitations par référence

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 Etats membres de l'OTAN et des dispositions mises en place dans le cadre de l'UE.

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

Attention : l'habilitation au secret de la défense nationale par référence à une habilitation OTAN ou UE n'est pas autorisée. Une demande d'habilitation nationale est nécessaire.

⁵⁴ Control of secret material in an international command.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.8**CONTROLE DES RESSORTISSANTS ETRANGERS EN CAS
D'HABILITATION OU D'ACCES A DES LIEUX ABRITANT DES
INFORMATIONS ET SUPPORTS CLASSIFIES OU CONTENANT DES
INFORMATIONS *DIFFUSION RESTREINTE* OU SENSIBLES****Référence :**

IGI 1300 – 3.2.5

Points clés :

- Sauf cas exceptionnel, les ressortissants étrangers peuvent être habilités au niveau *Secret* ou *Très Secret* à la condition qu'il existe un accord entre la France et l'État dont l'intéressé est ressortissant.
- Même habilités, les ressortissants étrangers ne peuvent avoir accès ni au « *Spécial France* », ni au *Très Secret* classification spéciale.
- L'accès à des informations *Diffusion Restreinte* ou sensibles peut être autorisé aux ressortissants étrangers.

1. Habilitations des ressortissants étrangers

Les ressortissants étrangers⁵⁵, occupant une fonction nécessitant l'accès à des informations et 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 général de sécurité ou un accord spécifique couvrant le sujet des habilitations entre la France et l'État dont l'intéressé est ressortissant et qu'il soit déjà détenteur d'une décision nationale au niveau requis. Si un tel accord est en vigueur, deux situations peuvent se présenter :

- le **ressortissant étranger, dans le cadre d'une coopération étatique**, est muté, détaché ou en mission dans une entité française : l'attestation d'habilitation ou le certificat de sécurité délivré(e) par son autorité d'habilitation d'origine peut suffire, en fonction du tableau d'équivalence et des dispositions de l'accord de sécurité, à lui délivrer une décision d'habilitation lui autorisant l'accès aux informations et supports classifiés. Selon les dispositions de l'accord de sécurité, l'autorité d'habilitation française peut ainsi prendre une décision d'habilitation au regard de l'attestation de sécurité produite par l'autorité d'habilitation d'origine et, si nécessaire, émettre un certificat de sécurité ou faire mener selon les cas des compléments d'investigation avant de prendre une décision d'habilitation ;
- lorsque le **ressortissant étranger est recruté par une entité française**, 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 :

⁵⁵ 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 l'origine de sa double nationalité, est considéré en France comme jouissant de la seule nationalité française.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.8

- 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 ;
- l'autorité d'habilitation, à savoir le ministre, son délégué⁵⁶ ou l'autorité de sécurité déléguée (ASD)⁵⁷, saisit le service enquêteur compétent selon les procédures habituelles ;
- parallèlement, l'autorité d'habilitation saisit le secrétaire général de la défense et de la sécurité nationale (SGDSN), en sa qualité d'autorité nationale de sécurité⁵⁸ (ANS). Cette saisine est transmise *via* le haut fonctionnaire correspondant de défense et de sécurité quand l'autorité d'habilitation est distincte de celui-ci ;
- le SGDSN assure la liaison avec l'autorité nationale de sécurité étrangère soit pour obtenir l'assurance que le ressortissant étranger fait l'objet d'une habilitation et, en cas d'absence d'habilitation, de lui demander d'habiliter ce ressortissant étranger, soit pour obtenir l'assurance qu'il n'existe aucune information défavorable sur l'intéressé de nature à constituer une vulnérabilité pour le secret de la défense nationale. Les éléments ainsi obtenus ne sont pas liants pour la délivrance de la décision d'habilitation ;
- le SGDSN transmet les éléments reçus de son homologue étranger au HFCDs, 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 déléguée⁵⁹, et sous réserve des dispositions précisées dans la délégation du SGDSN, cette dernière saisit directement son homologue étranger pour les mêmes demandes que celles effectuées par le SGDSN et mentionnées ci-avant. 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.

Un ressortissant étranger habilité ne peut, en aucun cas, avoir accès à des informations et supports classifiés marqués *Spécial France*, ni à des informations et supports classifiés relevant du niveau *Très Secret « classification spéciale »*. Son habilitation peut exclure également les informations relatives à des parties de programme ou domaines d'activité jugés sensibles au regard du pays dont le candidat à l'habilitation est ressortissant.

Afin de déterminer les conditions d'accès des ressortissants étrangers à des informations classifiées du domaine international, en particulier de ceux de l'Organisation du traité de l'Atlantique nord (OTAN) et de l'UE, il convient de se référer aux instructions ministérielles applicables.

Si l'habilitation concerne l'accès à des ISC sur un programme en coopération pour un ressortissant d'un pays tiers à cette coopération, une consultation des autres pays

⁵⁶ Articles R. 2311-8-1 et R. 2311-8-2 du code de la défense.

⁵⁷ Cf. fiche 9.1.

⁵⁸ *Idem*

⁵⁹ Pour le ministère des armées, la DGA/SSDI est l'ASD compétente pour l'industrie de défense ; à ce titre elle assure le rôle d'intermédiaire exclusif entre la France et les ASD compétentes étrangères (cf. fiche 9.1).

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.8

participants est lancée conformément aux accords de sécurité en vigueur, complétés par les stipulations précisées dans le cadre juridique de la coopération (l'ISP ou les réglementations de l'OTAN, l'UE, le European defence industry restructuring / framework agreement - EDIR/FA, l'Organisme conjoint en matière de coopération - OCCAR).

Lorsqu'il n'existe aucun accord de sécurité entre la France et l'État dont l'intéressé est ressortissant, aucune habilitation ne peut, par principe, être délivrée par une autorité française d'habilitation. Toutefois, à titre exceptionnel, si le besoin d'en connaître est avéré et dûment motivé, l'autorité requérante saisit le secrétaire général de la défense et de la sécurité nationale en sa qualité d'ANS qui apprécie l'opportunité de l'habilitation et définit, le cas échéant, la procédure à suivre afin que l'autorité d'habilitation puisse prendre sa décision.

2. Accès des ressortissants étrangers aux lieux contenant des informations *Diffusion Restreinte* ou sensibles

Dans les cas où l'habilitation n'est pas nécessaire, les demandes d'accueil de ressortissants étrangers dans un organisme du périmètre du MINARM pouvant donner lieu à l'accès à des informations *Diffusion Restreinte* ou sensibles doivent être adressées par l'OS de l'entité visitée au service enquêteur dans la mesure du possible au minimum deux mois avant le début du séjour. A défaut, l'OS de l'organisme visité communique au service enquêteur dans les meilleurs délais les informations relatives aux visiteurs étrangers.

Ces modalités ne préjugent en rien de celles qui sont effectuées au titre de la protection du potentiel scientifique et technique de la nation (PPSTN) en cas d'accès à une zone à régime restrictif⁶⁰.

Les modalités pratiques des séjours diffèrent suivant leur nature, la durée et le site visité.

⁶⁰ Décret n° 2011-1425 du 02/11/2011 et arrêté du 03/07/2012 relatifs à la protection du potentiel scientifique et technique de la nation et pour le ministère de la défense, instruction ministérielle n° 298 du 5 mars 2014 relative à la mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation par le ministère de la défense.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.9**ENQUETES ADMINISTRATIVES PREALABLES AUX ACCES AUX
SITES ET EMPLOIS SENSIBLES****Références :**

- Code de la défense (notamment L.1332-2-1, R. 2361-1 et R.2362-1)
- Code de la sécurité intérieure (notamment L.114-1 et R. 114-1 et suivants)
- Code pénal (R. 413-1 et suivants)
- IGI 1300 – 3.3.1.3, 3.5.3, 5.3.2.3 et annexe 6
- Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation
- Décret n° 2018-141 du 27 février 2018
- Décret n° 2018-135 du 27 février 2018
- Pour les établissements du MINARM, ses établissements publics sous tutelle et les INID du CEA : IM 1544/DEF/CAB/DR du 17 janvier 2017, version du 10 août 2020, relative à la défense-sécurité des activités, moyens et installations relevant du ministère de la défense
- Instruction ministérielle n° 298 du 5 mars 2014 relative à la mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation par le ministère de la défense

Points clés :

- Le MINARM distingue trois types d'enquêtes administratives pour le renseignement et la sûreté (EARS) selon le niveau d'accès requis : le contrôle primaire (CP), le contrôle élémentaire (CE) et l'enquête d'habilitation.
- Une personne pour laquelle une enquête administrative pour le renseignement et la sûreté est à mener doit en être avertie préalablement.

Le dispositif de contrôle de confiance du personnel accédant aux zones et emplois sensibles a initialement été organisé pour protéger les points d'importance vitale et préserver le secret de la défense nationale ainsi que le potentiel scientifique et technique de la nation (cf. documents de références). Les garanties qu'il offre permettent de réduire les risques de compromission du secret, qu'elle soit volontaire (espionnage) ou accidentelle (négligences).

Depuis les attentats de 2015, le contrôle des personnes physiques, basé sur des enquêtes administratives pour le renseignement et la sûreté (EARS) préalables, est également utilisé pour se prémunir contre les actes de malveillance, la criminalité et les actes violents (jusqu'à l'action de type terroriste) envers les agents (militaires comme civils), les installations (au-delà des seuls points d'importance vitale) et les moyens, dont les systèmes d'information ou les données, du ministère des Armées.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.9

1. Cadre réglementaire

Le cadre dessiné par les codes de référence permet aux entités du ministère et aux entreprises contractantes de demander des enquêtes administratives pour le renseignement et la sûreté (EARS)⁶¹ pour :

- autoriser l'accès aux zones sensibles, et notamment aux « zones militaires ou placées sous le contrôle de l'autorité militaire » ou aux zones protégées (ZP) ;
- prendre des décisions relatives à l'accès à certains emplois ou recrutements (pour le MINARM exclusivement).

L'accès aux fichiers utiles aux enquêtes administratives, prévu par les codes cités en référence, est limité aux services enquêteurs⁶².

Au sein du MINARM, la nouvelle rédaction du code de la sécurité intérieure⁶³ permet au commandement de vérifier, en cas de suspicion, que le comportement d'un agent autorisé à tenir un poste à l'issue d'une enquête administrative est toujours compatible avec ce poste. Lorsque la nouvelle enquête administrative diligentée par le commandement fait apparaître que le comportement de l'agent est effectivement devenu incompatible avec l'exercice de ses fonctions, l'administration procède, après une procédure contradictoire, à son affectation ou sa mutation dans l'intérêt du service dans un emploi comportant l'exercice d'autres fonctions. En cas d'impossibilité de mettre en œuvre une telle mesure ou lorsque le comportement de l'agent est incompatible avec d'autres fonctions, l'autorité administrative procède à la radiation des cadres de l'agent civil ou du militaire.

2. Les enquêtes administratives pour le renseignement et la sûreté

a. Principes généraux

- L'individu soumis à une enquête administrative doit en avoir été averti au préalable.
- Le ministère de la défense distingue trois types d'enquêtes administratives pour le renseignement et la sûreté (EARS) : le contrôle primaire (CP), le contrôle élémentaire (CE) et l'enquête d'habilitation, qui se différencient selon :
 - o le besoin qu'elles couvrent : accès à des ISC, recrutement comme militaire, accès à une zone particulière, accès à un emploi sensible.
 - o la ou les menaces principales auxquelles elles répondent : espionnage ou malveillance/criminalité/terrorisme.
 - o leurs objets : l'individu seul, son cercle proche, son cercle relationnel plus éloigné.
 - o le rythme de leur renouvellement.
- Le résultat d'une enquête administrative, valable à un instant donné en fonction des informations consultables offre une garantie relative. Le dispositif d'enquête administrative décrit dans la présente fiche ne se substitue pas à la connaissance de

⁶¹ Pour les installations nucléaires intéressant la dissuasion ne relevant pas du ministre de la défense au sens de l'article R*. 1411-9 du code de la défense, le COSSEN procède aux enquêtes administratives relatives aux personnes physiques accédant aux installations et communique les avis aux organismes demandeurs.

⁶² Les gendarmeries spécialisées peuvent effectuer certaines missions en concertation avec la DRSD.

⁶³ Article L.114-1 du CSI, modifié par la loi n°2017-1510 du 30 octobre 2017, renforçant la sécurité intérieure et la lutte contre le terrorisme.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.9

l'environnement humain par l'encadrement, qui demeure une donnée essentielle de l'évaluation de la confiance.

b. Le contrôle primaire

Le contrôle primaire⁶⁴ (CP) est défini, par la présente instruction, comme une enquête administrative simple, qui donne lieu au ministère des Armées à l'émission d'un avis de sécurité écrit (*sans objection ; vulnérabilité réduite ; vulnérabilité étendue*)⁶⁵ d'une durée de validité de trois ans au *maximum*, facilitant la prise de décision de l'employeur, de l'autorité contractante, du commandant de formation administrative / chef d'établissement (CFA/CE) ou de l'officier de sécurité (OS).

Il est requis pour tous les accès en zone (sauf ZRR), à savoir :

- une zone protégée (ZP⁶⁶) ;
- un point d'importance vitale (PIV) ;
- une zone nucléaire d'accès réglementé (ZNAR) ;
- une zone réservée (ZR) ;
- un terrain militaire (TM) clos (le CP, facultatif dans ce cas, doit être motivé par écrit par l'employeur).

Dans le cas d'un accès à une emprise incluse dans un site rassemblant plusieurs emprises, l'OS du site formule une demande de CP. En cas d'avis autres que sans objection, il en informe l'OS de l'emprise accueillante et statue avec lui sur les suites à donner et les mesures à prendre.

Cette enquête administrative pour le renseignement et la sûreté peut également être sollicitée par l'autorité contractante à l'encontre des personnes morales exécutant un contrat sensible.

Le CP s'applique au personnel du ministère (militaires et agents civils) ainsi qu'au personnel non ressortissant du MINARM mais agissant pour son compte, notamment dans le cadre de marchés de prestations (contrats sensibles), susceptibles de pénétrer dans une de ces zones.

Il est à la charge de la DRSD, qui est responsable de l'enquête administrative pour le renseignement et la sûreté. En concertation avec la DRSD et selon le processus défini par elle, les gendarmeries spécialisées peuvent participer à l'enquête administrative pour le renseignement et la sûreté.

Les visiteurs, obligatoirement accompagnés et dont les déplacements sont encadrés, ne sont pas astreints aux CP.

c. Le contrôle élémentaire

Le contrôle élémentaire (CE) est défini par la présente instruction comme une enquête administrative sollicitée par l'employeur, l'organisme de recrutement, le commandant

⁶⁴ Demande de type CPR sur Sophia.

⁶⁵ Le formulaire de CP du système SOPHIA comporte seulement deux cases : sans objection (SO) ou autre que sans objection (AQSO) : les 3 niveaux sont mentionnés en commentaire.

⁶⁶ Demande de type CAZ sur Sophia.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.9

de formation administrative / chef d'établissement (CFA/CE) ou l'officier de sécurité (OS), destinée à s'assurer du degré de confiance qu'il est possible d'accorder pour :

- être recruté comme militaire⁶⁷,
- accéder à une zone à régime restrictif (ZRR)⁶⁸,
- exercer dans une zone sensible⁶⁹ un emploi dans une des fonctions décrites en [annexe 2](#)⁷⁰.

Les conclusions techniques résultant de l'enquête administrative effectuée exclusivement par le service enquêteur se traduisent par des avis de sécurité écrits (*sans objection/ restrictif/ défavorable*) adressés à l'autorité d'habilitation ou au chef d'établissement, ou à l'OS d'une entreprise habilitée.

La durée de validité de cet avis n'excède pas trois ans à l'exception des accès à une zone à régime restrictif, dont la durée de validité maximum est de 5 ans.

d. L'enquête d'habilitation

Menée exclusivement par le service enquêteur, elle est conforme aux prescriptions des documents de références.

L'avis de sécurité rédigé par le service enquêteur après cette EARS permet à l'autorité d'habilitation de délivrer (ou non) une habilitation à connaître des informations couvertes par le secret de la défense nationale.

La durée maximum de cet avis est fonction du niveau de l'habilitation demandée. Elle ne peut excéder :

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

3. Modalités de mise en œuvre des enquêtes

- L'avis de sécurité pour les habilitations ayant une durée de validité longue, il est conseillé aux autorités d'habilitation ayant prescrit ces enquêtes de faire procéder à un ou plusieurs CP intermédiaires, à un rythme adapté à leurs vulnérabilités et à la sensibilité des fonctions occupées, qu'elles définissent après accord de la DRSD ou de l'unité de gendarmerie spécialisée dont elles disposent.
- La mise en commun du résultat des décisions d'accès au profit des autorités décisionnaires (dans la limite du besoin d'en connaître) est à rechercher pour une plus grande efficacité⁷¹.
- La bonne exécution des directives de la présente fiche et de leur déclinaison par les ADS, comme par les OIV civils relevant du MINARM, est vérifiée à l'occasion des visites de contrôle interne ou d'inspection (contrôle externe). Pour les établissements du

⁶⁷ Demande de type CER sur Sophia.

⁶⁸ Demande de type AZR sur Sophia.

⁶⁹ PIV, ZP, ZNAR, ZR, TM.

⁷⁰ Demande sur Sophia de type CES (ou CNV pour le cas particulier des convoyeurs d'ISC).

⁷¹ A titre illustratif, l'officier de sécurité d'un régiment de l'armée de Terre peut avoir intérêt à savoir que l'artisan auquel est confiée une prestation s'est vu refuser l'accès de la base aérienne située sur la même garnison.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES 3.9

MINARM, ses établissements publics sous tutelle et les INID du CEA, ces dernières sont prévues par l'instruction ministérielle 1544 de référence⁷².

Intensité de l'EARS				Volume de personnel concerné
	ENQUETE D'HABILITATION	CONTRÔLE ELEMENTAIRE	CONTRÔLE PRIMAIRE	
	<ul style="list-style-type: none"> ✓ HABILITATION TS CLASSIFICATION SPECIALE ✓ HABILITATION TS ✓ HABILITATION S 			
		<ul style="list-style-type: none"> ✓ EMPLOIS SENSIBLES ✓ ACCES ZRR ✓ RECRUTEMENT 		
			<ul style="list-style-type: none"> ✓ ACCES PIV ✓ ACCES ZP ✓ ACCES ZR ✓ ACCES ZNAR ✓ ACCES TM (CLOS) 	

⁷² En particulier dans les paragraphes 7.1.1 et 7.1.2.

**TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
PHYSIQUES** **3.10****OBLIGATION DE RESERVE, DISCRETION PROFESSIONNELLE ET
SECRET PROFESSIONNEL POUR LES AGENTS DU MINISTERE DE LA
DEFENSE****Références :**

- Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires – Art. 26
- Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique – Art. 6 à 16
- Code de la défense (livre premier portant statut général des militaires) – Art. L. 4121-2 et L. 4122-4
- Code pénal – Art. 226-13 et 226-14 (atteinte au secret professionnel) et art. 413-9 à 413-12 (atteinte au secret de la défense nationale)
- Code de procédure pénale – Art. 40 (lanceurs d’alerte)
- Décret n° 2015-386 du 3 avril 2015 fixant le statut des fonctionnaires de la direction générale de la sécurité extérieure

Points clés :

- Faire état, directement ou indirectement, de sa qualité de personnel du ministère des Armées (MINARM) engage l’image de l’institution. Il convient donc de respecter le devoir de réserve et les règles de discrétion et de secret professionnel.
- Toute information diffusée alors qu’elle n’est pas destinée au public peut présenter des risques pour la sécurité du personnel, la sécurité des opérations et peut porter atteinte à l’image du ministère.

Au-delà du respect du secret de la défense nationale, les agents du MINARM, militaires comme civils, sont soumis à une obligation de réserve, au devoir de discrétion et au respect du secret professionnel. Ainsi, la communication d’informations d’origine professionnelle s’inscrit dans un cadre juridique visant à protéger ces informations afin notamment de ne pas compromettre les opérations en cours ou à venir et, plus largement, à ne pas porter atteinte à l’image de l’institution par dénigrement ou par brouillage de la communication officielle.

1. Champ d’application

Les dispositions s’appliquent quel que soit le mode d’expression choisi.

Sont concernés les militaires, d’active ou de réserve, et les agents civils du MINARM, ouvriers, fonctionnaires ou contractuels.

2. Obligations**a. Obligation de réserve**

Le personnel du ministère doit faire preuve de réserve et de mesure dans l’expression écrite et orale de ses opinions personnelles. Il s’interdit, afin de préserver le bon

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES **3.10**

fonctionnement du service, tout propos de nature à porter préjudice à la considération et à la confiance dont l'Administration et ses autorités doivent bénéficier.

Elle s'applique pendant et en dehors des heures de service. Il en est de même pour les agents suspendus de leurs fonctions ou en disponibilité.

b. Discretion professionnelle

La discretion professionnelle est requise au sein du MINARM afin d'éviter la divulgation d'informations relatives à l'activité ou au fonctionnement de l'administration ou au déroulement des opérations militaires. Ce devoir de discretion concerne les documents, informations ou faits qui n'ont pas vocation à être communiqués au public.

Cette obligation s'applique à l'extérieur de l'environnement professionnel, mais également à l'égard des personnels qui n'ont pas le besoin d'en connaître. Elle peut être levée par décision de l'autorité hiérarchique.

c. Secret professionnel

Les agents disposant d'un accès à des informations personnelles (santé, comportement, situation familiale, etc.) ne doivent pas les divulguer, à moins de recueillir l'assentiment exprès de la personne concernée.

Le secret professionnel peut être levé sur ordre de l'autorité compétente⁷³, notamment en vue de la préservation de la santé publique ou de l'ordre public, ou du bon déroulement des procédures de justice (voir notamment les situations évoquées à l'article 226-14 du code pénal).

Tout manquement aux obligations de réserve et de discretion peut donner lieu à des sanctions disciplinaires. La violation du secret professionnel est punie d'un an d'emprisonnement et de 15 000€ d'amende.

3. Cas particulier des lanceurs d'alerte et de l'article 40 du code de procédure pénale

Le lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi :

- un crime (vol aggravé, viol, faux en écriture publique...) ou un délit (corruption, prise illégale d'intérêts, trafic d'influence, usage illégal de fonds publics, harcèlement moral ou sexuel, discrimination...);
- la violation grave et manifeste d'un engagement international, d'une loi ou d'un règlement;
- toute menace ou préjudice grave pour l'intérêt général.

Il doit avoir eu personnellement connaissance des faits constitutifs de l'alerte.

Le lanceur d'alerte bénéficie de garanties accordées par la loi. La confidentialité de son identité doit être respectée et il ne peut être sanctionné ou faire l'objet d'une mesure discriminatoire pour avoir signalé une alerte. Cette dernière protection ne vaut cependant, pour les militaires, qu'à la condition que le signalement de l'alerte ait d'abord

⁷³ Au regard de l'article 226-14 du code pénal, le détenteur d'un secret professionnel a parfois l'obligation de le révéler d'initiative.

**TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
PHYSIQUES****3.10**

été porté à la connaissance du supérieur hiérarchique, direct ou indirect, de l'employeur ou d'un référent désigné par celui-ci (cf. code de la défense - art. L. 4122-4).

Les faits couverts par le secret de la défense nationale sont exclus du régime de l'alerte tel que défini par la loi relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique. Tout signalement abusif peut entraîner des conséquences sur le plan pénal ou disciplinaire.

Indépendamment du régime du lanceur d'alerte, tout agent civil ou militaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu, en vertu de l'article 40 du code de procédure pénale, d'en donner avis sans délai au procureur de la République. Il s'agit d'une obligation, mais qui vise les seuls faits dont l'intéressé a eu connaissance dans l'exercice de ses fonctions, si ces faits lui paraissent suffisamment établis et s'il estime qu'ils portent une atteinte suffisamment caractérisée aux dispositions dont il a pour mission d'assurer l'application.

4. Sensibilisation aux bonnes pratiques sur les réseaux sociaux⁷⁴

L'usage désormais courant des réseaux sociaux accroît les risques de communication, volontaire ou non, d'informations professionnelles et personnelles sensibles. Le respect des dispositions énoncées précédemment impose des pratiques de bon sens sur les réseaux sociaux, qui peuvent être rappelées au personnel par l'OS de l'entité :

- séparer sa vie professionnelle de sa vie personnelle ;
- sécuriser au maximum ses comptes et profils (utilisation de pseudonymes, d'avatars, etc.)⁷⁵ ;
- maîtriser l'utilisation des réseaux sociaux et le contenu de ses publications (configuration en mode privé, accès aux contacts autorisés) ;
- porter une attention particulière aux visages, bandes patronymiques et arrière-plans de ses photos/vidéos (l'appartenance au ministère ne doit pas être identifiable) ;
- sur les profils professionnels (Linkedin, Viadeo) :
 - o les contenus ne doivent pas être trop détaillés (affectation, spécialité, etc.) ;
 - o préférer l'appellation « agent de la fonction publique » ;
 - o ne pas diffuser d'informations privées (adresse, téléphone, etc.) ;
- respecter le cadre particulier des opérations :
 - o ne pas évoquer ses missions ;
 - o ne pas utiliser de géolocalisation ;
 - o ne pas diffuser de photos ou vidéos informant sur les missions ou la situation de la zone de stationnement ;
- ne pas identifier les autres agents ;
- ne pas utiliser les applications de flux direct (Facebook Live et Periscope) dans son environnement professionnel (utilisation interdite dans les enceintes militaires).

Il est également important de sensibiliser son entourage. L'agent et son entourage doivent avoir ces principes en mémoire :

⁷⁴ Un guide du bon usage des réseaux sociaux est disponible en téléchargement à cette adresse : www.defense.gouv.fr/guide-medias-sociaux/telecharger.pdf

⁷⁵ Pour en savoir plus, des guides sont disponibles sur le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) : www.ssi.gouv.fr

**TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
PHYSIQUES** **3.10**

- rien ne disparaît ;
- les données publiées n'appartiennent plus à l'auteur ;
- toute publication est une porte d'entrée pour obtenir des informations nécessaires à une surveillance, une localisation, des menaces, etc. Il faut donc expliquer à son entourage ce qu'il peut et ne peut pas faire ;
- encourager l'entourage à respecter la discrétion de l'agent (ne pas identifier/tagguer l'agent, ne pas faire état de sa fonction, ...).

**TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
PHYSIQUES****3.11****PROTECTION DES DONNEES A CARACTERE PERSONNEL
COMPORTANT LA MENTION DE LA QUALITE DE MILITAIRE
(DCPM)****Références :**

- Code de la défense – art. L. 4123-9-1, R. 4123-45 et suivants (personnel militaire)
- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données (II de l'article 18) ;
- II n° 901/SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'informations sensibles

Points clés :

- Une attention particulière est portée aux données à caractère personnel des militaires (DCPM) permettant d'associer facilement ce militaire à une opération extérieure ou à une activité sensible dans laquelle il serait impliqué ou d'associer facilement les données professionnelles avec des données privées.
- Le caractère sensible des activités de certaines entités contractantes avec le MINARM justifie une protection des données à caractère personnel (DCP).
- Ces données doivent être protégées contre les menaces informatiques (attaque d'un système d'information depuis internet) et physiques (vol de matériels ou supports contenant ces données).

1. Définition

La donnée personnelle revêt une sensibilité particulière dès lors qu'elle associe trois éléments en même temps :

- l'identité de la personne ;
- une donnée à caractère professionnel révélant directement sa profession ;
- une information relevant de la sphère privée (adresse personnelle, composition de la famille, etc.).

A ce titre, sa divulgation pourrait nuire aux intérêts de l'Etat, permettre d'exercer des menaces ciblées sur les opérations et activités du MINARM, de ses entités sous tutelle ou cocontractantes, mais également sur la personne concernée ainsi que sur son cercle familial.

Les systèmes d'information traitant de données à caractère personnel des agents du MINARM se regroupent en quatre catégories :

- les SI internes au ministère ;
- les SI d'organismes sous tutelle ;
- les SI dépendants de prestataires extérieurs ;
- les SI d'organismes externes sans lien contractuel ni institutionnel avec le ministère (entreprises, associations,...).

A cette liste s'ajoutent les SI internes aux entités contractantes avec le ministère, qui traitent les DCP de leur personnel.

**TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
PHYSIQUES****3.11****2. Mesures de sécurité**

Des dispositifs de protection de ces DCP permettent de renforcer l'anonymat des personnels travaillant au sein du ministère des armées.

En raison de la nature sensible des postes que peut occuper le personnel des entités contractantes (ex. industriels d'armement), des dispositifs de protection doivent également être appliqués.

a. Rôle des armées, directions et services (ADS)

Les ADS sont chargés de mener les actions de sécurité vis-à-vis des trois premières catégories de SI énoncées au 1. Chaque entité a pour tâche de recenser et catégoriser ses détenteurs de données et de prendre contact avec les entités extérieures susceptibles de traiter ces DCP.

Au sein du ministère, les mesures de protection doivent être adaptées au niveau de la menace. Elles se traduisent par une homologation permanente de ces SI et, en cas de risque identifié, par des mesures immédiates de renforcement de la sécurité laissées à l'appréciation du responsable de traitement en lien avec l'AQSSI. De manière générale, les fichiers réalisés pour le compte de l'Etat sont soumis aux exigences de la PSSI.

Le MINARM s'assure également de la sensibilisation de ses personnels et des organismes sous tutelle aux menaces et que des mesures appropriées soient mises en place. Il en est de même pour les prestataires extérieurs, qui sont de surcroît soumis à des obligations contractuelles adaptées au traitement de ces DCP.

Concernant les SI d'organismes externes sans lien contractuel ni institutionnel avec le ministère, les ADS sont invités à contribuer à la sensibilisation des entités identifiées et à signaler à la DGNUM les entités dont les faiblesses constatées en matière de sécurité des DCP pourraient nécessiter un dialogue particulier.

b. Rôle de la DRSD

Le responsable d'un traitement de données ne peut traiter les données dans lesquelles figure la mention de la qualité de militaire des personnes concernées que si cette mention est strictement nécessaire à l'une des finalités du traitement.

A l'exclusion des traitements mis en œuvre pour le compte de l'Etat, des collectivités territoriales et de leurs groupements ainsi que des associations à but non lucratif, les responsables des traitements informent le ministre des armées (en l'occurrence la DRSD) de la mise en œuvre de traitements comportant des DCPM à l'adresse suivante : drsd-dcpm.contact.fct@intradef.gouv.fr. La DRSD peut réaliser une enquête administrative sur les personnes accédant aux DCPM aux seules fins d'identifier si elles constituent une menace pour la sécurité des militaires concernés.

c. Rôle du chef d'organisme contractant

Le chef d'organisme applique, via son AQSSI, le même type de mesures qu'énoncées précédemment pour assurer la protection des DCP de son personnel, à savoir :

- recensement et catégorisation de ses détenteurs de données ;
- homologation permanente de ses SI ;

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES PHYSIQUES**3.11**

- gestion des fichiers soumis à la PSSI de l'entité ;
- sensibilisation de son personnel aux menaces.

d. Rôle du responsable de traitement

Le responsable de traitement⁷⁶ est une personne physique ou morale, une autorité publique, un service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Les responsables de traitement sont soumis à quatre principes de sécurité :

1. Ne collecter ou conserver que les données pertinentes : le responsable de traitement s'assure que seules sont collectées et conservées, les données pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.
2. Maîtriser les exports de données : les transferts de données vers un tiers (sous-traitant par exemple) sont réduits au strict minimum et/ou filtrés (suppression d'une partie des informations) afin de ne pas divulguer de DCP. Les obligations afférentes en matière de sécurité des données doivent être mentionnées dans les conventions ou contrats (nature des traitements, durée de conservation, transferts ultérieurs, etc.).
Les exports de données peuvent aussi concerner la mise en ligne, par exemple au travers d'un site web ou l'utilisation de technologies de type informatique en nuage (cloud computing). Un niveau de protection technique adéquat des données doit être assuré.
3. Mettre en place des mécanismes de contrôle d'accès et d'imputation : les SI manipulant des DCP doivent permettre de contrôler et d'imputer l'accès aux données pour ne l'accorder qu'aux personnes autorisées et dûment identifiées.
4. Gérer les incidents relatifs aux DCPM : le responsable de traitement informe sans délai en cas de tentative d'attaque ou d'incident pouvant avoir mené à une divulgation de DCP la chaîne de lutte informatique défensive (LID), la DRSD et le délégué à la protection des données⁷⁷ (daj.delegue.fct@intradef.gouv.fr).

3. Protection juridique du personnel du ministère de la défense en matière de protection des données personnelles et de respect de l'anonymat

Plus largement, la protection juridique du personnel du MINARM (civils et militaires) en matière de protection des données (traitées par le ministère ou par d'autres organismes) et d'anonymat est définie dans le tableau ci-après.

⁷⁶ Les responsables de traitement du ministère des armées ont été désignés par arrêté du 13 juin 2018 fixant la liste des responsables de traitement au sein des états-majors, directions et services et des organismes qui leur sont rattachés.

⁷⁷ Toute violation de sécurité doit donner lieu à une information du délégué à la protection des données (DPD) en application des articles 33 et 34 du RGPD et des procédures RGPD mises en place au sein du MINARM dans un délai de 72h (cf. instruction ARM/SGA/DAJ/D2P/DPSP du 31 janvier 2020 relative à la mise en œuvre du règlement européen sur la protection des données personnelles au ministère de la défense).

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
PHYSIQUES

3.11

	Dispositions	Tout ministère		Services spécialisés		Entités contractantes	
		Personnel civil (PC)	Personnel militaire (PM)	Services de renseignement (PM / PC)	Forces spéciales (PM)	Personnel civil (PC)	Personnel militaire (PM)
Protection des données	Règlement européen sur la protection des données (RGPD) et loi 78-17 du 06/01/1978 modifiée dite "loi informatique et liberté" -> fichiers de droit commun	X	X	X	X	X	X
		X	X	X	X	X	X
		X	X	X	X	X	X
	Loi 78-17 du 06/01/1978 modifiée dite "loi informatique et liberté", article 31 -> fichiers de souveraineté	NC	NC	NC	NC	NC	NC
		selon les dispositions de l'acte réglementaire portant création du traitement de données concerné				NC	NC
Protection de l'anonymat	Article L. 4123-9-1 du code de la défense (introduit par l'article 117 de la loi n° 2016-731 du 03/06/2016) Articles R. 4123-45 et s. du code de la défense Loi n° 2018-493 du 20 juin 2018 relative à la protection des données (II de l'article 18)	NC	NC	NC	NC	NC	X
	Article 226-17-1 du code pénal	NC	NC	NC	NC	NC	X
	Article 226-16 du code pénal	X	X	X	X	X	X
	Loi du 29/07/1981 sur la presse Arrêté du 7 avril 2011 relatif à l'anonymat	X	X	X	X	X	X
	Article 861-1 du code de la sécurité intérieure - services spécialisés de renseignement (L.811-2 CSJ) - autres services autorisés à recourir aux techniques de renseignement (L.811-4 CSJ)	X	X	X	X	NC	NC
	Article 413-13 du code pénal	X	X	X	X	X	X
	Article 413-14 du code pénal Arrêté du 20 octobre 2016 fixant la liste des unités spéciales concernées	NC	X	X	X	X	X

TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

PRINCIPES GENERAUX DE LA PROTECTION DU SECRET DANS LES CONTRATS

Référence :

IGI 1300 – 4

Points clés :

- La réglementation relative à la protection du secret encadre les contrats avec accès ou détention d'ISC ainsi que les contrats sensibles. Il est néanmoins possible d'introduire des mesures de protection dans n'importe quel type de contrat.
- Le besoin de protection des ISC est exprimé par le prescripteur technique.
- La mise en œuvre des mesures de protection comprises dans le contrat incombe à la personne morale.
- Seuls les contrats avec accès ou détention d'ISC nécessitent l'habilitation de la personne morale (PM).
- L'habilitation au niveau Secret d'un administrateur de SI de niveau maximal *Diffusion Restreinte* n'est pas conditionnée par l'habilitation de la PM à laquelle il appartient.
- L'habilitation de la PM doit être obtenue avant la signature du contrat.
- A l'exception de son responsable légal et en dehors des phases précontractuelles, l'habilitation de la PM est le préalable indispensable à l'habilitation du personnel de la société, sauf lorsque celle-ci possède la qualité d'opérateur d'importance vitale.

Les principes évoqués dans la présente fiche s'appliquent à tout contrat de la commande publique, de sous-traitance aux contrats de la commande publique ou contrats de subvention, quel que soit son régime juridique ou sa dénomination, pour l'exécution duquel doivent être prises des mesures de protection du secret de la défense nationale.

La sensibilité des informations dans les contrats passés entre le ministère des armées et les personnes morales ainsi que leurs sous-contractants peut exiger la prise en compte rigoureuse des besoins de protection dans les contrats dès l'engagement de la consultation ou dès l'envoi à la publication de l'avis d'appel à la concurrence. Le rôle du prescripteur technique est à ce titre essentiel : il doit préciser le besoin de protection du secret dès le début de la procédure précontractuelle.

La mise en œuvre de ces mesures incombe aux responsables légaux des personnes morales. Les personnes morales titulaires des contrats se doivent en effet de mettre en œuvre les prescriptions réglementaires et contractuelles pour assurer la sécurité des informations et supports classifiés (ISC). Cette responsabilité vaut également vis-à-vis des sous-contractants de tout rang.

1. Expression du besoin de protection

Au regard de la protection des informations existent plusieurs types de contrats :

- les contrats qui nécessitent l'habilitation préalable de l'entreprise :

TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

- contrats avec accès à des ISC ;
- contrats avec détention d'ISC.
- les contrats sensibles.

Au-delà de ces types de contrats encadrés par la réglementation relative à la protection du secret de la défense nationale et décrits dans la présente instruction, des mesures ponctuelles de protection des informations sensibles ou des mesures de défense-sécurité peuvent être intégrées dans n'importe quel type de contrat⁷⁸.

Pour toute procédure de passation devant aboutir à un contrat avec accès ou détention d'ISC (cf. fiche 4.5 et suivantes) ou à un contrat sensible (cf. fiche 4.3), le prescripteur technique, avec le concours de son officier de sécurité, doit préciser lors de la demande d'achat, le besoin de protection concernant la préparation et l'exécution du contrat.

L'expression de ce besoin fait l'objet d'une fiche de besoin de protection du secret, rédigée sous la responsabilité du prescripteur technique avec le concours de l'officier de sécurité de l'autorité contractante, qui doit impérativement être jointe à la demande d'achat.

2. Habilitation de la personne morale

L'habilitation d'une personne morale correspond au besoin de l'administration d'apprécier les garanties présentées avant d'attribuer un marché avec accès ou détention d'ISC.

La décision d'habilitation permet :

- à une autorité contractante d'attribuer des marchés comportant l'accès ou la détention d'ISC à une personne morale ;
- à cette personne morale d'exécuter de tels contrats.

La détention d'ISC impose aux personnes morales de disposer, en plus de l'habilitation, des aptitudes physiques des locaux et des systèmes d'information homologués (selon les cas spécifiques).

Les personnes morales doivent être habilitées, au plus tard à la date de signature du contrat⁷⁹, pour l'exécution de travaux classifiés dans le cadre d'un contrat conclu avec l'autorité publique, directement ou de manière indirecte, dans le cadre des sous-traitances ou, pour les marchés publics de défense ou de sécurité, dans le cadre des sous-contrats.

L'habilitation de la PM et de son responsable légal sont un préalable indispensable à l'habilitation du personnel de la société. A l'exception toutefois :

- des phases précontractuelles nécessitant l'accès ou la détention des ISC pour l'établissement du contrat, pour lesquelles une ou des personnes physiques spécifiquement désignées doivent obtenir l'habilitation ;
- de celle de l'administrateur d'un système d'information de niveau *Diffusion restreinte*.

En cas de non-respect de la procédure d'habilitation lors de la procédure de passation du contrat (absence de fourniture de son dossier de demande d'habilitation dans les

⁷⁸ Pour les entités du MINARM, ces mesures sont détaillées dans le titre 5 de l'IM 1544

⁷⁹ Articles R. 2343-4 et R. 2343-5 du code de la commande publique

TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

délais fixés par l'autorité contractante, par exemple), la candidature est déclarée irrecevable. Le candidat ne peut donc plus prétendre à l'attribution du contrat.

Les décisions d'habilitation délivrées à l'occasion de la passation d'un contrat nécessitant l'accès à des ISC ou leur détention comportent une date limite de validité fixée par l'autorité d'habilitation⁸⁰ ainsi que, s'il y a lieu, un domaine particulier.

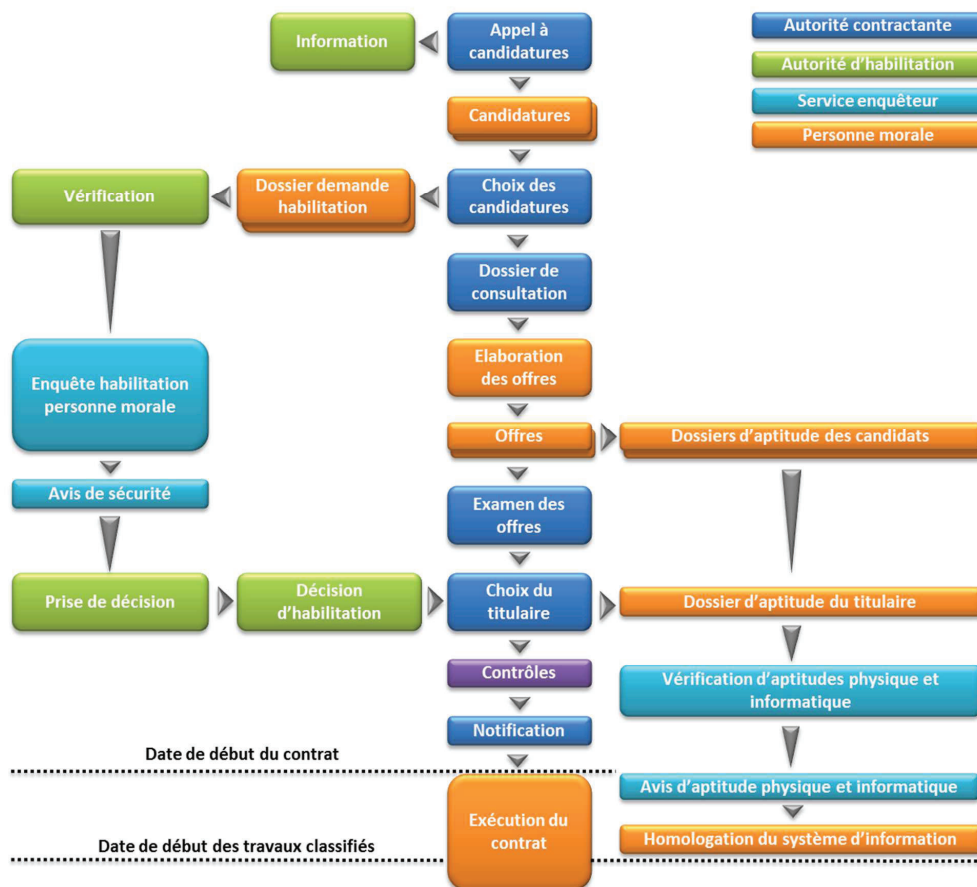
L'habilitation d'une personne morale s'accompagne pour celle-ci de la mise en place d'une structure de sécurité adaptée aux travaux classifiés qu'elle doit exécuter.

3. Simultanéité des procédures

Le schéma suivant présente de façon synthétique la synchronisation classique des processus d'achat, d'habilitation et d'aptitude. L'habilitation est parfois exigée dès la phase précontractuelle.

Les détails de chacune des étapes figurent dans les fiches 4.4 à 4.11.

Synchronisation des processus d'achat, d'habilitation et d'aptitude



⁸⁰ Cette durée d'habilitation ne peut excéder 5 ans pour le Très Secret et 7 ans pour le Secret.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.1****ACTEURS DES CONTRATS****Référence :**

IGI 1300 – 4.1 à 4.2, 4.4.1.2, 4.4.2.2

Points clés :

- L'autorité d'habilitation délivre les habilitations de la personne morale et des personnes physiques qui lui sont rattachées.
- L'autorité contractante désigne le pouvoir adjudicateur, lequel détermine le type de contrat et ses conséquences sur la procédure contractuelle.
- En cas d'accès ou de détention d'ISC, la PM candidate doit se soumettre, si elle n'est pas déjà habilitée, si son habilitation porte sur un autre domaine que celui du contrat ou si les éléments constitutifs ont changé, à une procédure d'habilitation pour que sa candidature soit retenue.
- Le service enquêteur effectue les enquêtes d'habilitation des PM et de leur personnel et émet des avis techniques d'aptitude physique (ATAP) ou informatique (ATAI) en vue respectivement de l'aptitude des lieux abritant des ISC et de l'homologation des systèmes d'information.

1. L'autorité d'habilitation

L'autorité d'habilitation est l'organisme chargé de délivrer les agréments des OS (cf. fiche 2.3) ainsi que les décisions d'habilitation (ou de refus) des personnes morales (PM) et de leur personnel, sur la base de l'avis de sécurité émis par le service enquêteur.

- Pour le *Très Secret classification spéciale*, l'autorité d'habilitation est le SGDSN.
- Pour les habilitations de niveau *Secret* ou *Très Secret* ainsi qu'aux niveaux équivalents de l'OTAN et de l'UE, l'autorité d'habilitation pour le MINARM est le DGA⁸¹.

2. L'autorité contractante

Elle désigne toute personne publique ou privée qui fait appel à un fournisseur ou à un prestataire pour l'exécution d'un contrat ou d'un marché. Lorsque le marché est régi par les dispositions du code de la commande publique, l'expression « autorité contractante » désigne le pouvoir adjudicateur. Lorsqu'un marché est régi par les dispositions du code de la commande publique et entraîne des contrats de sous-traitance ou des sous-contrats, le pouvoir adjudicateur à l'origine de celui-ci est appelé « autorité contractante de référence ».

En cas de nécessité d'habilitation pour l'accès ou la détention d'ISC, c'est à l'autorité contractante qu'incombe :

- l'information de l'autorité d'habilitation du lancement de la procédure d'achat ;
- le choix du type de contrat (avec accès ou détention d'ISC) approprié à la protection du secret de la défense nationale ;
- l'information des PM candidates sur les modalités à observer pour se procurer les formulaires de constitution du dossier d'habilitation ;

⁸¹ A l'exception de la DGSE, qui dispose de sa propre autorité d'habilitation.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.1**

- le visa des documents relatifs à la définition et à la justification du besoin d'en connaître et sa transmission à l'autorité d'habilitation ;
- la détermination, en concertation avec l'autorité d'habilitation, de la date limite de remise du dossier de demande d'habilitation de la PM ;
- la détermination, en concertation avec l'autorité d'habilitation, de la date limite de remise des dossiers d'aptitude physique des locaux et des systèmes d'information ;
- l'autorisation ou le refus de recourir à la sous-traitance de travaux classifiés ;
- la transmission des dossiers de demande d'habilitation à l'autorité d'habilitation ;
- la transmission des projets de plans contractuels de sécurité aux candidats ;
- la transmission au titulaire du plan contractuel de sécurité dans le cadre du marché ;
- la mise en cohérence du plan contractuel de sécurité avec les évolutions éventuelles des autres documents constitutifs du marché.

Elle doit notamment s'assurer, si nécessaire auprès de l'autorité d'habilitation, que :

- le projet de plan contractuel de sécurité a été établi afin de le joindre au dossier de consultation⁸² ;
- les candidats ont fourni l'attestation d'habilitation appropriée ou déposé un dossier de demande d'habilitation ;
- pour les contrats nécessitant l'accès ou la détention d'ISC en phase précontractuelle, que les candidats admis à soumissionner aient fait l'objet d'une décision d'habilitation ou engagé le processus d'habilitation nécessaire avant la mise à disposition des documents de la consultation nécessaire à l'élaboration de leur offre ;
- que l'attributaire pressenti ait fait l'objet d'une décision d'habilitation, au plus tard le jour de la signature du contrat.

En fonction du type de contrat à passer (contrat avec accès ou détention d'ISC, contrat sensible), l'autorité contractante détermine les conséquences sur la procédure d'acquisition (avis d'appel à candidatures, modalités particulières de consultation, plan contractuel de sécurité, demandes d'habilitation de candidats, etc.).

Pour l'assister dans ces missions, l'autorité contractante recourt à un binôme prescripteur technique/acheteur et à son officier de sécurité.

a. Binôme prescripteur technique/acheteur

Il doit vérifier, dès l'expression du besoin, s'il existe des informations sensibles, *Diffusion Restreinte* ou classifiées à protéger :

- dans la phase précontractuelle (en particulier si le dossier de consultation comporte des éléments classifiés) ;
- dans la phase contractuelle.

Il est responsable de :

- l'identification des informations à protéger ;
- l'élaboration de la fiche de besoin de protection du secret ;
- l'élaboration des plans contractuels de sécurité liés aux contrats avec détention ou avec accès à des ISC dont il demande la passation ;
- l'élaboration de la fiche de suivi de passation du contrat ;

⁸² A l'exception des contrats cadres, pour lesquels une ébauche de plan contractuel ou un plan contractuel cadre (type PCS père-fils) est suffisante.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.1**

- la gestion de l'arborescence (sous-traitance) des travaux classifiés réalisés au titre du contrat.

b. Officier de sécurité de l'autorité contractante

En matière de protection des ISC dans les contrats, l'OS conseille le binôme prescripteur technique/acheteur et l'autorité contractante :

- sur le choix du contrat (avec détention ou avec accès aux ISC) ;
- pour l'élaboration du plan contractuel de sécurité et la gestion de l'arborescence des travaux classifiés réalisés au titre du contrat ;
- sur chaque intention d'achat conduisant à la communication d'ISC ;
- pour l'expression des besoins d'habilitation des PM candidates à la passation de contrats avec accès à des ISC ou détention d'ISC..

En outre, il contrôle ou fait contrôler l'application des plans contractuels de sécurité aux contrats avec accès ou détention d'ISC passés par l'autorité contractante.

En matière de protection des informations sensibles, l'OS conseille le binôme prescripteur technique/acheteur sur les mesures de protection à mettre en œuvre dans le futur contrat.

3. La personne morale**a. Cas général des personnes morales régies par le droit privé⁸³**

La PM peut être selon les différentes phases des procédures d'achat :

- tout d'abord candidat ;
- puis soumissionnaire ;
- attributaire ;
- et enfin titulaire ou contractant.

Si le candidat n'est pas déjà habilité ou si les éléments constitutifs de la PM ont évolué depuis la décision d'habilitation, il doit se soumettre à la procédure d'habilitation pour que sa candidature à un contrat avec accès ou détention d'ISC soit retenue ou que son offre soit examinée. Il constitue son dossier de demande d'habilitation (cf. [annexe 3](#)) en se reportant aux exigences décrites dans les documents de consultation.

Dans le cas de la passation d'un contrat avec détention d'ISC, le soumissionnaire⁸⁴ doit aussi remettre un dossier d'aptitude en vue d'apprécier sa capacité à détenir et protéger des ISC.

Toutes les PM habilitées doivent disposer d'un officier de sécurité (OS). En fonction de leur organisation, elles peuvent disposer d'officiers de sécurité d'établissement (OSE), encadrés par un officier central de sécurité (OCS). Les rôles et missions de l'OS sont précisés dans la fiche 2.5.

⁸³ Cette catégorie inclut les établissements publics à caractère industriel et commercial (EPIC) qui, dans le cadre d'un contrat prévoyant l'exécution de travaux classifiés, sont habilités.

⁸⁴ Ce dossier n'est pas exigé au stade de la candidature.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.1****b. Cas particulier des établissements publics administratifs**

Les établissements publics administratifs peuvent accéder à des informations et supports classifiés sans habilitation de la personne morale sous réserve de disposer d'un besoin d'en connaître reconnu par le ministre. Ils restent assujettis aux dispositions de la présente instruction s'agissant notamment des dossiers d'aptitude et des habilitations de leur personnel.

Une habilitation PM peut néanmoins être exigée dans le cadre d'une candidature à un appel d'offres ou un appel à projet international nécessitant l'accès à des informations et supports classifiés.

c. Cas particulier de l'auto-entrepreneur ou de la société par actions simplifiée unipersonnelle (SASU)

Dans le cadre des habilitations, le MINARM considère l'auto-entrepreneur et la SASU comme des entreprises et leur applique donc la procédure d'habilitation des personnes morales décrite dans ce chapitre (avec aptitude physique ou informatique en cas de détention d'ISC).

d. Cas des sous-traitant et des sous-contractants

Dans le cadre d'un contrat, une partie des prestations peuvent être sous-traitées. Le sous-traitant doit alors être déclaré et, si nécessaire, habilité.

Dans le cadre de sous-contrats, par exemple d'achats de fournitures, le sous-contractant doit également être identifié et, si nécessaire, habilité.

La PM avec laquelle l'autorité contractante a conclu un contrat est qualifiée de primo contractante et est responsable des déclarations et habilitations de tout sous-traitant et sous contractant.

4. Le service enquêteur

La DRSD, service enquêteur du MINARM, est chargée d'effectuer les enquêtes d'habilitation des PM et de leur personnel devant accéder ou détenir des ISC, de l'aptitude physique et des systèmes d'information des PM, mais aussi des visites, contrôles et inspections. À ce titre, elle émet des avis de sécurité au profit de l'autorité d'habilitation et des avis techniques d'aptitude physique ou informatique au profit des autorités contractantes et des PM détenant des ISC.

La DGSE est, pour ses propres besoins, service enquêteur et son directeur est autorisé d'habilitation.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.2****CHOIX DU TYPE DE CONTRAT****Référence :**

IGI 1300 – 4.4, 5.3.2

Points clés :

- Les contrats avec accès ou détention d'ISC comportent des clauses de protection du secret et un plan contractuel de sécurité.
- Dans le cadre d'un contrat avec accès à des ISC, l'autorité contractante est responsable de la protection de ces derniers.
- Dans le cadre d'un contrat avec détention d'ISC, la PM est responsable de la protection des ISC qu'elle détient.
- La passation d'un contrat sensible ne nécessite ni l'habilitation de l'entreprise, ni celle de son personnel. Le personnel fait cependant systématiquement l'objet d'une enquête administrative. La PM peut également faire l'objet d'une enquête sur demande de l'autorité contractante.
- Il est également possible d'introduire des dispositions de protection dans n'importe quel type de contrat.

1. Contrat avec accès à des ISC

Il s'agit de tout contrat, quel que soit le régime juridique qui lui est applicable ou sa dénomination, dans lequel une personne morale, publique ou privée, est amenée, à l'occasion de la passation du contrat ou de son exécution, à avoir accès à des ISC sans les détenir.

L'exécution de ce contrat nécessite l'habilitation de la personne morale et de son personnel ayant à connaître des ISC au titre du contrat. Les personnes physiques employées par la personne morale accèdent aux ISC sous la responsabilité de leur détenteur. L'autorité contractante reste responsable de la protection des ISC nécessaires à l'exécution du contrat ou produits à l'occasion de son exécution. Les aptitudes physiques des locaux ou l'homologation des systèmes d'informations sont sans objet pour ce type de contrat, le candidat ou le titulaire ne détenant pas d'ISC à ce titre.

Les établissements de la personne morale ayant du personnel habilité participant à l'exécution du contrat doivent être identifiés auprès de l'autorité d'habilitation et du service enquêteur

Tout contrat avec accès à des ISC comporte :

- **des clauses de protection du secret** (cf. IGI 1300 – annexe 17) qui précisent les conditions de protection des ISC et d'exécution des travaux classifiés du contrat ;
- **un plan contractuel de sécurité** spécifique au contrat auquel il est associé dont les modalités d'élaboration et d'approbation sont précisées dans la fiche 4.8.

2. Contrat avec détention d'ISC

Il s'agit de tout contrat, quel que soit son régime juridique ou sa dénomination, dans lequel une personne morale, publique ou privée, est amenée à l'occasion de la passation du contrat ou de son exécution à détenir des ISC dans ses propres locaux.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.2**

Dans ce type de contrat, des ISC sont transférés à un ou plusieurs établissements relevant d'une personne morale qui a l'obligation de mettre en œuvre, dans ses installations, les mesures de protection réglementaires. Elle est alors responsable de la protection des ISC qu'elle détient. Les personnes physiques employées par la personne morale détenant des ISC au titre du contrat sont responsables de leur protection.

La notification d'un contrat avec détention d'ISC nécessite de remplir toutes les conditions énoncées au §1 et de détenir :

- l'aptitude physique des locaux où sont exécutées les prestations classifiées du contrat ou où sont détenues des ISC ;
- l'homologation des systèmes d'information⁸⁵ sur lesquels ces informations sont stockées.

3. Contrat sensible

Il s'agit de tout contrat, quel que soit son régime juridique ou sa dénomination, à l'exception des contrats de travail, dont l'exécution s'exerce dans des locaux abritant des éléments couverts par le secret de la défense nationale, dans lequel un cocontractant de l'administration, public ou privé, prend des mesures de précaution, y compris dans les contrats de travail de ses employés, tendant à assurer que les conditions d'exécution de la prestation ne mettent pas en cause la sûreté ou les intérêts essentiels de l'État.

Les contrats sensibles s'appliquent notamment aux prestations suivantes :

- les prestations d'entreprises de prévention et de sécurité (gardiennage, intervention, levée de doute, contrôle d'accès, détection d'intrusion, vidéosurveillance, télésurveillance,...) au sein d'un service ou dans un local abritant des éléments couverts par le secret de défense nationale ;
- les prestations réalisées sur les éléments et réseaux de sûreté, pouvant remettre en cause l'équation de protection (installation et maintenance de systèmes de contrôle d'accès, de détection d'intrusion, de vidéosurveillance,...) ;
- les prestations réalisées dans les emprises où sont stockés des éléments couverts par le secret de défense nationale (l'entretien, la maintenance et les travaux d'infrastructure par exemple), qui ne nécessitent pas l'accès à des ISC.

La passation d'un contrat sensible ne nécessite ni l'habilitation de l'entreprise, ni celle de son personnel mais justifie plusieurs enquêtes administratives sollicitées par l'officier de sécurité de l'autorité contractante auprès du service enquêteur compétent :

- à la diligence de l'autorité contractante, celle de la PM ;
- systématiquement celles relatives au personnel du titulaire exécutant ce contrat.

Tout contrat sensible comporte une clause type de protection du secret précisant les mesures de sécurité particulières devant être prises pour l'exécution du contrat (limite des lieux, horaires d'intervention...)⁸⁶.

⁸⁵ Ou une autorisation provisoire d'emploi délivrée dans les conditions définies dans la fiche 6.2. Cette disposition s'applique à l'ensemble du titre 4.

⁸⁶ Annexe 33 de l'IGI 1300.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.2**

Lorsqu'un contrat sensible s'exécute dans une zone réservée en l'absence du personnel occupant habituellement la zone, le prestataire doit être accompagné ou surveillé par l'autorité responsable de la ZR.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.3****MODALITES DE PASSATION D'UN CONTRAT SENSIBLE****Référence :**

IGI 1300 – 5.3.2.1 et annexe 33

Points clés :

- Les personnes morales soumissionnaires en vue de la passation d'un contrat sensible peuvent faire l'objet d'une enquête administrative (contrôle primaire) préalablement à la passation du contrat
- Dans tous les cas, il est procédé aux enquêtes administratives à l'endroit des personnes physiques.
- Aucune de ces enquêtes ne conduit à l'habilitation.

1. Lancement de la procédure d'achat

Pour toute procédure de passation d'un contrat sensible, le prescripteur technique estime les mesures de protection devant être adossées au projet de contrat.

Si la sensibilité des prestations à réaliser au titre du contrat le nécessite, et après concertation entre l'officier de sécurité de l'autorité contractante et le service enquêteur, une enquête administrative de la personne morale peut être réalisée (cf. fiche 3.9). Dans tous les cas, les personnes physiques sont soumises à une enquête administrative.

L'acheteur, lors du lancement de la consultation, informe les candidats potentiels de la procédure d'enquête de la personne morale (le cas échéant) et des personnes physiques (dans tous les cas) devant participer aux prestations du contrat.

2. Traitement des enquêtes administratives de la personne morale des candidats admis à soumissionner

En cas de choix par l'autorité contractante d'une enquête administrative sur la personne morale, dès qu'elle a fixé la liste des candidats admis à soumissionner, les soumissionnaires adressent à l'autorité contractante les extraits du registre du commerce et des sociétés (Kbis) et leurs fiches de renseignement (fiches de renseignement des sociétés et fiches de contrôle élémentaire des dirigeants ayant pouvoir d'engager la société).

Les soumissionnaires n'ayant pas remis les documents prévus à la date fixée sont réputés avoir renoncé à l'exécution des prestations du contrat sensible.

Pour chacun des soumissionnaires, après analyse de la complétude des pièces par l'OS de l'autorité contractante, celui-ci transmet les éléments nécessaires à l'enquête administrative au service enquêteur en précisant la date souhaitée pour disposer des avis avant le choix de l'attributaire.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.3****3. Choix de l'attributaire du contrat**

Le résultat de l'enquête administrative menée, le cas échéant, sur chaque personne morale soumissionnaire ayant remis une offre acceptable est pris en compte pour le choix de l'attributaire.

Avant la date de choix de l'attributaire du contrat, l'autorité contractante s'assure auprès de son OS que tous les avis d'enquête nécessaires sont disponibles à cette date. Si certains de ces avis risquent de ne pas être donnés à temps, l'acheteur et l'OS examinent la possibilité d'adaptation des délais des procédures d'achat et de contrôle. En dernier ressort, en cas d'urgence justifiée, l'OS, après consultation du service enquêteur, prend la décision appropriée.

Après la prise de connaissance de l'avis du service enquêteur, l'autorité contractante procède au choix de l'attributaire du contrat.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.4****PRISE EN COMPTE DE LA PROTECTION DU SECRET DANS LA
PROCEDURE D'ACHAT****Références :**

- Code de la commande publique - Art. R. 2343-4 et R. 2343-5
- IGI 1300 – 4.4.1

Points clés :

- L'acheteur, en lien avec le prescripteur technique et l'OS concerné, établit une fiche de suivi de passation du contrat en se basant sur l'analyse du degré de protection à accorder lors de la passation et de l'exécution du contrat figurant sur la fiche de besoin de protection du secret.
- Les contrats avec accès ou détention d'ISC ne peuvent être signés qu'après réception de l'attestation d'habilitation de la personne morale ou physique retenue.

1. Expression du besoin de protection du secret

La prise en compte des besoins de protection du secret dans la phase précontractuelle et l'exécution du contrat doit être appréhendée différemment selon la procédure d'acquisition envisagée.

Pour toute procédure de passation devant aboutir à un contrat avec accès ou détention d'ISC ou un contrat sensible, le prescripteur technique doit préciser avec le concours de son OS, lors de la demande d'achat, le besoin de protection du secret concernant la phase précontractuelle et l'exécution du contrat. Si nécessaire, ce dernier consulte l'autorité d'habilitation.

L'expression de ce besoin fait l'objet d'une fiche de besoin de protection du secret⁸⁷. Cette fiche doit impérativement être jointe à la demande d'achat.

Les renseignements relatifs au type de contrat et à la procédure d'acquisition retenus par l'acheteur, en lien avec le prescripteur technique et l'OS concerné, sont portés sur la fiche de suivi de passation du contrat qui sera transmise à l'autorité d'habilitation.

Si les informations font l'objet de la mention « Spécial France », le service prescripteur consulte l'OS ou l'autorité d'habilitation pour déterminer les dispositions les plus appropriées.

2. Habilitations et/ou aptitudes et homologations nécessaires

L'autorité contractante ne peut signer aucun contrat nécessitant l'accès ou la détention à des ISC avant la réception de l'attestation d'habilitation de la personne morale ou physique attributaire. Lorsque le contrat nécessite :

- la détention d'informations et supports classifiés, cette dernière ne peut débiter avant l'obtention de l'attestation d'aptitude physique au niveau requis⁸⁸ ;

⁸⁷ Un modèle de fiche de besoin de protection du secret est disponible sur IXARM.

⁸⁸ Le candidat s'engage à déposer un dossier d'aptitude puis le soumissionnaire dépose un dossier d'aptitude. Le marché peut être attribué puis notifié.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.4**

- l'usage d'un système d'information amené à contenir de l'information classifiée, l'exécution des travaux classifiés liés au SI ne peut débiter avant la date d'homologation de ce système (cf. fiche 6.2).

Pour un contrat avec détention d'ISC, au stade de sa candidature, la personne morale transmet, parallèlement au dossier d'habilitation, un engagement à déposer, au titre de son offre, un dossier d'aptitude.

Au stade de la remise de son offre, le soumissionnaire dépose un dossier d'aptitude (allégé ou complet, cf. fiche 4.5. §3) pour chacun de ses locaux et/ou SI destiné à traiter des ISC.

Si le titulaire du marché avec détention d'ISC fait l'objet d'un avis d'inaptitude, l'autorité contractante peut prendre les sanctions adéquates, allant jusqu'à la résiliation du marché à ses torts.

Pour un marché de défense ou de sécurité, lorsqu'un candidat n'est pas habilité au moment de sa candidature à la passation d'un contrat avec accès ou détention d'ISC, l'autorité contractante peut accorder un délai supplémentaire à ce candidat pour obtenir cette habilitation⁸⁹. Pour les marchés autres que ceux de défense ou de sécurité, le fait pour un candidat de ne pas être habilité au moment de sa candidature à la passation d'un contrat avec accès à des ISC ou détention d'ISC ne constitue pas une raison suffisante pour justifier *a priori* son exclusion de la procédure de passation de ce contrat.

Dans tous les cas, s'il y a refus de se soumettre à la procédure d'habilitation lors de la procédure de passation du contrat (absence de fourniture de son dossier de demande d'habilitation dans les délais fixés par l'autorité contractante par exemple), le candidat est exclu de la procédure de passation de ce contrat.

⁸⁹ Articles R2343-4 et R2343-5 du code de la commande publique.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.5****PROCEDURE D'ACHAT POUR LES CONTRATS AVEC ACCES OU
DETENTION D'INFORMATIONS ET SUPPORTS CLASSIFIES :
SELECTION DES CANDIDATS ADMIS A SOUMISSIONNER ET
CONTENU DES OFFRES****Référence :**

IGI 1300 – 4.4.1.3, 4.4.1.5

Points clés :

- Après examen de la validité des habilitations des candidats ou des demandes en cours par l'autorité d'habilitation, l'autorité contractante établit la liste des candidats admis à soumissionner.
- Un dossier de consultation, établi par l'acheteur, est adressé aux candidats admis à soumissionner. Il inclut le projet de plan contractuel de sécurité.
- Un dossier d'aptitude des locaux ou des SI est établi par l'entreprise pour les contrats avec détention ISC.

1. Lancement de la procédure d'achat

Pour toute procédure de passation d'un contrat avec accès ou détention d'ISC, l'acheteur établit, en liaison avec le prescripteur technique et l'OS de l'autorité contractante, la fiche de suivi de passation du contrat⁹⁰. Cette fiche est transmise à l'autorité d'habilitation.

L'acheteur fournit à l'autorité d'habilitation les dates prévisionnelles de choix de l'attributaire et de notification du contrat (ou éventuellement de mise à disposition des ISC si cette date est notablement différente de celle de la notification du contrat).

En cas de procédure avec publicité, l'acheteur établit l'avis d'appel public à la concurrence (AAPC), qui précise les modalités et conditions de participation à la consultation, notamment :

- pour les candidats non habilités, les informations relatives à la constitution et au dépôt d'un dossier de demande d'habilitation ;
- pour les candidats déjà habilités, la production d'attestations d'habilitation accompagnées d'une attestation de non changement de la personne morale depuis la dernière décision d'habilitation ou un justificatif prouvant que les démarches de mise à jour de l'habilitation ont été entreprises auprès de DGA/SSDI ou d'une autre autorité d'habilitation (cf. fiche 4.11) ;
- le niveau et la nature des travaux classifiés à réaliser ainsi que le niveau et la nature de l'habilitation de la personne morale candidate ;
- en cas de contrat avec détention d'ISC, le niveau et la nature des aptitudes à détenir et un engagement à fournir un dossier d'aptitude ;
- les destinataires des pièces constitutives du dossier de candidature

⁹⁰ Le modèle de fiche de suivi de passation du contrat est disponible sur le site www.ixarm.com.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.5**

Pour une procédure sans publicité, l'acheteur établit une lettre d'invitation à participer à une consultation en y faisant apparaître les mêmes éléments que cités *supra* dans le cadre d'un AAPC et en fonction de la fiche de suivi de passation du contrat.

Dans le dossier de consultation établi en vue de la passation d'un contrat avec détention d'ISC, l'acheteur fait connaître à chaque candidat admis à soumissionner qu'il doit adresser en même temps que son offre, un dossier d'aptitude pour chaque établissement dans lequel il envisage de réaliser des travaux classifiés au titre du contrat et procéder à l'homologation des SI susceptibles d'héberger des ISC

Si le dossier de consultation comporte des éléments classifiés, l'acheteur fait prendre les dispositions décrites dans la fiche 4.6.

Si le contrat en cause est un marché de défense ou de sécurité, conformément aux articles R. 2343-4 et R. 2343-5 du code de la commande publique, l'autorité contractante peut exiger que les candidats soient habilités dès le dépôt des candidatures. Elle peut cependant accorder aux candidats qui ne sont pas habilités au moment du dépôt de leur candidature un délai supplémentaire pour obtenir cette habilitation. Elle indique ce délai dans l'avis d'appel à la concurrence.

2. Choix des candidatures

L'autorité contractante adresse à l'autorité d'habilitation, *via* son OS, la liste des candidats, accompagnée des éléments relatifs à leur habilitation ou des documents nécessaires au dépôt d'une demande d'habilitation. Après examen des éléments transmis, et selon le contexte, l'autorité d'habilitation :

- certifie à l'autorité contractante que les candidats disposent effectivement des habilitations requises ;
- informe l'autorité contractante de la complétude des informations transmises permettant de lancer un dossier de demande d'habilitation ;
- ou informe l'autorité contractante que les dossiers déposés sont incomplets et que des éléments complémentaires sont nécessaires pour admettre le candidat à soumissionner.

L'autorité contractante établit la liste des candidats admis à soumissionner, en tenant compte des éléments fournis par l'autorité d'habilitation après examen des attestations d'habilitation ou de la complétude des demandes d'habilitation.

Lorsque les dossiers sont complets, l'autorité d'habilitation engage la procédure d'habilitation des candidats admis à soumissionner en transmettant au service enquêteur les dossiers de demande d'habilitation des candidats concernés en vue de l'établissement d'un avis de sécurité.

3. Dossier de consultation

L'acheteur adresse le dossier de consultation aux candidats retenus. Si le dossier de consultation ne comporte aucun ISC, il est transmis à tous les candidats admis à soumissionner, qu'ils soient habilités ou non. Si le dossier de consultation comporte des éléments classifiés, les dispositions de la fiche 4.6 doivent être appliquées.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.5**

Le contrat devant comporter un plan contractuel de sécurité, le projet de plan contractuel de sécurité est élaboré sous le contrôle du prescripteur technique, avec le concours de l'OS. Ce projet est joint au dossier de consultation.

Dans le cas d'un contrat avec accès à des ISC, l'acheteur informe chaque candidat admis à soumissionner qu'il doit adresser à l'autorité contractante, en même temps que son offre, un dossier d'identification pour chacun de ses établissements dont le personnel doit participer aux travaux classifiés au titre du contrat.

Dans le cas d'un contrat avec détention d'ISC, l'acheteur indique les documents nécessaires à la constitution du dossier d'aptitude. Ces documents doivent être fournis avec l'offre dans les délais fixés dans le règlement de la consultation. Ils peuvent prendre deux formes :

- un dossier d'aptitude complet si la personne morale envisage de réaliser les travaux classifiés dans un local n'ayant pas au préalable fait l'objet d'avis d'aptitude « sans objection » et sur un système d'information non homologué, ou si le local et le système d'information ont fait l'objet de modifications rendant caducs les avis d'aptitude et les homologations précédemment émis ;
- un dossier d'aptitude allégé comprenant les copies des avis d'aptitude déjà obtenus, accompagnés des attestations de conformité et des homologations des SI déjà émises, si la personne morale envisage de faire les travaux classifiés du contrat dans des locaux ayant précédemment fait l'objet d'avis techniques d'aptitude physique et sur des systèmes d'information homologués⁹¹.

4. Contenu des offres au regard de la protection du secret

Le candidat doit remettre à l'autorité contractante dans son offre :

- dans le cas d'un contrat avec accès à des ISC, un dossier d'identification pour chaque établissement dont le personnel intervient dans les travaux classifiés du contrat ;
- dans le cas d'un contrat avec détention d'ISC, en plus du dossier précité pour les contrats avec accès, un dossier d'aptitude⁹² pour chaque établissement dans lequel sont envisagés les travaux classifiés du contrat ainsi que la liste des SI destinés à héberger des ISC et pour lesquels une décision d'homologation devra être émise.

⁹¹ La personne morale doit accompagner ce dossier d'un engagement de non changement des conditions ayant conduit à l'obtention des avis techniques d'aptitude physique et des homologations.

⁹² Si la personne morale dispose déjà de locaux aptes et des SI homologués et si les travaux classifiés du futur contrat doivent y être réalisés, alors son OS établit les certificats de conformité des locaux tels que décrits dans l'annexe 26 de l'IGI 1300 et produit les décisions d'homologation correspondantes.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.6****PROCEDURE D'ACHAT POUR LES CONTRATS AVEC ACCES OU
DETENTION D'INFORMATIONS ET SUPPORTS CLASSIFIES :
CONSULTATION DES ISC DURANT LA PERIODE D'ELABORATION
DES OFFRES****Référence :**

IGI 1300 – 4.4.1.3

Points clés :

- Les personnes morales candidates admises à soumissionner non habilitées ne peuvent se voir confier des ISC contenus dans le dossier de consultation des entreprises (DCE).
- Cependant, lorsque leur connaissance est nécessaire pour établir une offre et à condition que la procédure d'habilitation de la personne morale soit engagée, l'accès aux ISC du DCE peut être autorisé à un nombre limité de personnes habilitées.
- Lorsque les exigences d'aptitude physique des locaux ou l'absence d'homologation des SI des candidats ne permettent pas l'étude des ISC du DCE sur place, celle-ci est effectuée dans les locaux de l'autorité contractante.

1. Principes généraux

Lorsque le dossier de consultation comporte des ISC dont les candidats admis à soumissionner doivent avoir connaissance pour établir leurs offres, les dispositions décrites ci-après doivent être prises.

Il convient tout d'abord de séparer les éléments classifiés de ceux qui ne le sont pas.

Il est formellement interdit de confier des ISC à un candidat admis à soumissionner non habilité.

Il est formellement interdit de confier des ISC à un candidat admis à soumissionner habilité dont les locaux n'ont pas l'aptitude physique requise ou qui ne dispose pas d'un système d'information homologué.

Il est toutefois possible de donner accès à des ISC au personnel d'une personne morale non encore habilitée, soumissionnaire à un contrat avec accès ou détention d'ISC dont la connaissance leur est nécessaire pour établir leur offre, sous réserve que :

- la procédure d'habilitation de la personne morale soit engagée auprès du service enquêteur;
- le personnel concerné soit habilité.

Une procédure d'habilitation d'urgence (cf. fiche 3.2. §3.a.) peut être engagée par l'autorité d'habilitation pour un nombre de personnes physiques strictement limité à ce seul besoin. Les ISC, ne pouvant être transmis à la personne morale candidate non habilitée, sont consultés dans les locaux de l'autorité contractante par des personnels habilités. Un soin particulier doit être pris pour éviter que la présence dans les locaux de l'autorité contractante du personnel d'une personne morale candidate ne conduise à

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.6**

une inégalité de traitement entre les candidats. La mise en œuvre de cette disposition incombe au prescripteur technique avec le concours de son OS.

La transmission d'ISC (cf. fiche 7.8) à un candidat admis à soumissionner et habilité doit suivre la procédure réglementaire.

2. Obligations de l'autorité passant un contrat dans lequel tout ou partie des documents de consultation sont classifiés

L'acheteur tient compte, pour la fixation des délais de remise des offres, du délai d'obtention de l'habilitation des personnes physiques devant accéder aux ISC du dossier de consultation des entreprises (DCE) et, le cas échéant, du délai du contrôle d'aptitude des locaux et de l'homologation des systèmes d'information si ceux-ci doivent héberger des ISC.

Lorsque le dossier de consultation comporte des ISC dont les candidats admis à soumissionner doivent avoir connaissance pour établir leurs offres, l'OS de l'autorité contractante doit :

- vérifier l'habilitation des personnes morales : niveau/nature, durée d'habilitation⁹³ ;
- lancer la procédure d'habilitation pour les personnes morales ne disposant pas des habilitations requises par la consultation ;
- vérifier, lorsqu'il y a détention d'ISC, les aptitudes physiques des locaux des personnes morales ;
- vérifier, lorsqu'il y a détention d'ISC, l'homologation des systèmes d'information de la personne morale destinés à héberger des ISC ;
- s'assurer que seul le personnel habilité des personnes morales accède aux ISC ;
- s'assurer de la destruction ou de la restitution des ISC des candidats dont l'offre n'est pas retenue.

3. Obligations de la personne morale répondant à un contrat dans lequel tout ou partie des documents de consultation sont classifiés

Lorsque le dossier de consultation comporte des ISC dont la personne morale doit avoir connaissance pour établir l'offre, le candidat admis à soumissionner s'engage à :

- apporter la preuve de son habilitation au bon niveau/nature, soit au travers d'un certificat de sécurité fourni par l'autorité ayant délivré l'habilitation, soit à l'issue de la procédure d'habilitation initiée auprès de l'autorité d'habilitation ;
- apporter la preuve, lorsqu'il y a détention d'ISC, des aptitudes physiques de l'établissement concerné ;
- apporter la preuve, lorsqu'il y a détention d'ISC, de l'homologation des systèmes d'information destinés à héberger des ISC ;
- s'assurer que seul du personnel habilité de la personne morale accède aux ISC ;
- détruire ou restituer les ISC à leur émetteur dès la notification du rejet de l'offre de la personne morale, selon des modalités définies par l'autorité contractante.

Ces dispositions sont explicitement intégrées au DCE.

⁹³ Si l'habilitation arrive à son terme, s'assurer de la prorogation de l'habilitation (12 mois maximum) auprès de l'autorité d'habilitation.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.6**

Si la personne morale ne dispose pas de locaux aptes, ni de SI homologués, son OS peut demander que la consultation des ISC se fasse dans les locaux de l'autorité contractante. Si cela n'est pas possible, la communication de ces documents se révélant indispensable, un contrôle de l'aptitude des locaux et l'homologation des SI est effectué au préalable. Dans ce cas, il est nécessaire de prendre contact avec l'autorité d'habilitation et la DRSD afin de réaliser ces opérations le plus tôt possible⁹⁴.

⁹⁴ Cette démarche est à accomplir en respectant les prescriptions de l'article R. 2351-1 du CCP, « l'acheteur fixe les délais de réception des offres en tenant compte de la complexité du marché et du temps nécessaire aux opérateurs économiques pour préparer leur offre ». L'égalité de traitement des candidats est respectée.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.7****PROCEDURE D'ACHAT POUR LES CONTRATS AVEC ACCES OU
DETENTION D'INFORMATIONS ET SUPPORTS CLASSIFIES :
EXAMEN DES OFFRES, CHOIX DE L' ATTRIBUTAIRE ET SIGNATURE****Référence :**

IGI 1300 – 4.4.2.1

Points clés :

- En fonction des éléments fournis par l'autorité d'habilitation, l'autorité contractante sélectionne les offres conformes.
- Le début des travaux classifiés dans le cadre de contrats avec détention d'ISC est soumis à l'avis technique d'aptitude physique du service enquêteur et à l'homologation des systèmes d'information.
- Lorsque des carences de protection physique ou informatique sont constatées à la suite des avis d'aptitude émis par le service enquêteur, la PM dispose d'un délai fixé par l'autorité contractante pour se mettre en conformité avant le début des travaux classifiés.

1. Examen des offres et décision d'habilitation

Pendant les périodes d'élaboration et d'examen des offres, le service enquêteur instruit les dossiers de demande d'habilitation des personnes morales candidates admises à soumissionner⁹⁵ sollicités par l'autorité d'habilitation. Sur la base des avis de sécurité qui sont émis, l'autorité d'habilitation établit la décision d'habilitation ou de refus de la personne morale⁹⁶ et avertit l'autorité contractante.

2. Choix de l'attributaire du contrat et signature

L'autorité contractante s'assure auprès de l'autorité d'habilitation, avant la signature du contrat, que toutes les décisions d'habilitation nécessaires sont disponibles. Si certaines de ces décisions risquent de ne pas être prises à temps, l'acheteur et l'autorité d'habilitation examinent la possibilité d'adaptation des délais des procédures d'achat et d'habilitation. En dernier ressort, en cas d'urgence dûment justifiée, l'autorité d'habilitation, après consultation du service enquêteur, prend la décision appropriée sans le résultat définitif de l'enquête, à condition que la personne morale ait déjà fait l'objet d'une habilitation et qu'aucun changement dans la direction, les statuts ou l'actionnariat ne soit survenu depuis la précédente habilitation. Cette consultation à caractère urgent ne peut-être qu'informelle, l'avis de sécurité formel n'étant rendu qu'à l'issue d'une enquête de sécurité complète. L'habilitation émise est provisoire et ne peut excéder 6 mois.

Si l'attributaire pressenti fait l'objet d'un refus d'habilitation, le contrat peut alors être attribué au soumissionnaire suivant dans l'ordre de classement des offres reçues sous réserve qu'il soit habilité.

⁹⁵ Il convient de porter une attention au délai nécessaire à l'enquête d'habilitation. En effet, l'émission d'un avis de sécurité par le service enquêteur peut prendre plusieurs mois.

⁹⁶ L'habilitation peut être soumise à conditions : émise pour une activité, un contrat spécifique ou une durée.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.7****3. Vérification d'aptitude du titulaire à exécuter des travaux classifiés**

Tout titulaire d'un contrat avec détention d'ISC met en œuvre les dispositions réglementaires et les clauses contractuelles de protection des ISC liées à ce contrat.

Dès le choix du titulaire, l'autorité contractante informe l'autorité d'habilitation qui transmet le dossier d'aptitude du candidat retenu au service enquêteur. Ce service émet des avis d'aptitude physique et informatique⁹⁷ (cf. fiches 5.6 et 6.3) dès que les procédures et les moyens de protection requis pour la conservation et le traitement des ISC sont en place. Les avis d'aptitude sont adressés au titulaire avec copie à l'autorité d'habilitation.

Les prestations classifiées attendues peuvent débuter dès lors que le service enquêteur a adressé des avis « sans objection » au titulaire du contrat et que, lorsque nécessaire, l'homologation des SI concernés a été prononcée

Il incombe à l'officier de sécurité de l'autorité contractante de référence de vérifier le respect des procédures générales de protection du secret mises en œuvre par la personne morale (cf. fiche 4.13). Lorsque ce n'est pas le cas, la personne morale peut voir sa décision d'habilitation abrogée.

⁹⁷ L'aptitude informatique est un des éléments contribuant à la constitution des dossiers d'homologation des systèmes d'information.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.8****PROCEDURE D'ACHAT POUR LES CONTRATS AVEC ACCES OU
DETENTION D'INFORMATIONS ET SUPPORTS CLASSIFIES : PLAN
CONTRACTUEL DE SECURITE****Référence :**

IGI 1300 – 4.4.2.3.a et annexe 28

Points clés :

- Le plan contractuel de sécurité (PCS) accompagne le contrat et décrit les mesures de protection requises pour l'exécution du contrat.
- L'autorité contractante de référence contrôle l'ensemble des activités de protection des ISC, qu'il s'agisse de celles effectuées par le primo-contractant ou par ses sous-contractants.
- Chaque sous-contractant doit établir un PCS avec l'autorité contractante. Cette dernière tient à jour l'arborescence des travaux classifiés pour faciliter le contrôle de la protection des ISC.
- La fin d'exécution des travaux classifiés fait l'objet d'une fiche de clôture du PCS (FICPS)

1. Principes

Le plan contractuel de sécurité⁹⁸ (PCS) est un document contractuel qui détermine les mesures de protection nécessaires et suffisantes à appliquer dans le cadre du contrat auquel il est rattaché. Il est négocié dans la limite des exigences de la réglementation. Il est éventuellement classifié.

La signature du PCS peut intervenir avant la signature du contrat afin d'inscrire l'engagement de la PM en matière de protection du secret.

Il porte sur les prescriptions mentionnées en annexe 28 de l'IGI 1300 et a pour objectif d'énumérer les instructions de sécurité relatives au contrat et d'identifier les ISC ainsi que leur niveau de classification et les lieux d'exécution des différentes phases des travaux classifiés.

Il permet au service enquêteur d'exercer ses missions de conseil et de contrôle dans le cadre des contrats et des sous-contrats qui en découlent.

Il engage :

- l'autorité contractante de référence, responsable de la définition du niveau de protection des ISC et du contrôle de l'établissement du PCS dans le cas d'un contrat passé par l'administration ;
- le titulaire (contractant), responsable de l'application des mesures de protection :
 - o au sein de ses établissements ;
 - o par ses sous-contractants, vis-à-vis desquels il est responsable de la définition du secret des travaux sous-traités et de l'établissement du PCS de sous-contractance ;

⁹⁸ Le plan contractuel de sécurité est la nouvelle appellation de l'annexe de sécurité. Un modèle est disponible sur IXARM accompagné d'un guide d'aide à son élaboration.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.8**

- le sous-contractant, responsable de l'application des mesures de protection dans ses établissements. Il assume lui-même les responsabilités d'un contractant s'il sous-traite une partie de ses travaux classifiés.

Le PCS, dont le plan-type est mis à disposition par la DGA, comprend notamment :

- la liste des participants et des lieux d'exécution en appendice ;
- un cahier des prescriptions de protection du secret (CPPS) ;
- une page des signatures (selon le rang : autorité contractante et son OS, titulaire et son OS, sous-contractant, fournisseurs, etc.) ;
- la fiche de clôture de plan contractuel de sécurité (FICPCS).

Un PCS peut également être établi dans le cadre :

- de travaux dont l'exécution est confiée par l'autorité contractante à un organisme appartenant au ministère des armées ;
- d'études, développements et fabrications sur fonds privés utilisant les acquis des contrats cités au présent titre ou susceptibles de générer des informations classifiées ou non classifiées. Il n'existe pas de contrat *stricto sensu* dans ce cas. Les obligations des personnes morales découlent des seules dispositions législatives relatives à la protection du secret.
- de conventions.

2. Élaboration du plan contractuel de sécurité

Le PCS est établi dès la phase préparatoire du lancement de la consultation, dès que le caractère secret des prestations du contrat nécessitant l'accès ou la détention d'ISC est confirmé et afin de permettre :

- d'une part, la protection de ces informations le plus tôt possible ;
- d'autre part, l'appréciation par les candidats des exigences de sécurité liées à l'exécution du contrat envisagé, le coût des mesures de protection et le calendrier de leur réalisation, afin de déterminer les dispositions utiles de protection à mettre en place dès le début des travaux classifiés.

Un PCS reste applicable tant qu'il n'est pas remplacé par un autre PCS ou qu'il ne fait pas l'objet d'une fiche de clôture de plan contractuel de sécurité (FICPCS).

3. Identification, approbation et diffusion

Outre les références au contrat auquel il se rapporte, le PCS est identifié selon les quatre éléments suivants⁹⁹ :

- le code de l'opération protégée (OP) constitué d'une lettre et de 5 chiffres. La lettre, spécifique à une autorité contractante, est attribuée par le service enquêteur ;
- le numéro du PCS composé de 5 chiffres indiquant notamment le niveau de sous-traitance. Celui-ci est identifiable grâce au 3^{ème} chiffre : 0 pour les primo-contractants, 1 pour une sous-traitance de 1^{er} niveau, 2 pour une sous-traitance de 2^{ème} niveau, etc. ;
- l'indice de modification (A pour une première version, puis B, C, D, etc.) en fonction des changements effectués sur la première page ou dans le corps du CPPS du PC ;
- la date de l'indice qui doit être actualisée à chaque changement d'indice.

⁹⁹ A l'exception du CEA/DAM, qui applique sa propre nomenclature.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.8**

Chaque autorité contractante (autorité contractante de référence ou entité primo-contractante) est responsable de l'identification des plans contractuels de sécurité établis par elle-même, et des plans contractuels de sécurité de sous-contractants qui en découlent.

Les PCS sont contresignés par le titulaire du contrat et le contractant¹⁰⁰. Ils sont approuvés par l'officier de sécurité de l'autorité contractante de référence après visa du prescripteur technique.

L'autorité contractante diffuse le PCS aux acteurs identifiés par celui-ci ainsi qu'au service enquêteur.

4. Gestion des plans contractuels de sécurité et conservation

La gestion des PCS comprend :

- la gestion des contrats auxquels sont associés les plans contractuels de sécurité ;
- le suivi des modifications des plans contractuels de sécurité ;
- la prise en compte des FICPCS.

Au titre du PCS, chaque autorité contractante :

- établit et tient à jour la liste des contrats en cours, notifiés par elle, ainsi que ceux passés en sous-contractant ;
- s'assure que chacun de ses contrats comporte un PCS signé avant la notification du contrat ;
- adresse semestriellement au service enquêteur et à l'autorité d'habilitation un état récapitulatif des contrats qu'elle notifie (modèle de fiche signalétique disponible sur le site www.ixarm.com). Cet état peut être transmis par voie électronique sécurisée.

L'historique des contrats¹⁰¹ est conservé pendant dix ans par l'autorité contractante et trois ans par le service enquêteur.

5. Arborescence des travaux classifiés

La complexité de certains programmes et la diversité des spécialités nécessitent la participation de nombreuses personnes morales qui interviennent à différents niveaux des études et des réalisations.

L'autorité contractante de référence, avec l'appui de son OS, a la charge du contrôle de l'ensemble des activités visant la protection des ISC, quel que soit le rang du sous-contractant. Elle doit en particulier s'assurer que chaque titulaire de contrat nécessitant l'accès ou la détention d'ISC autorisé à sous-traiter des travaux classifiés a établi un PCS spécifique à ces travaux classifiés sous-traités et doit approuver explicitement ce PCS.

Pour que l'autorité contractante de référence, l'autorité d'habilitation et le service enquêteur soient en mesure de contrôler la protection des ISC quel que soit le rang du

¹⁰⁰ Il s'agit de l'autorité contractante de référence dans le cas d'un PCS père. Les PCS fils conclus dans le cadre de sous-traitance ou d'un sous-contrat sont contresignés par la personne morale à l'origine de cette sous-traitance ou de ce sous-contrat.

¹⁰¹ Par historique, il faut entendre l'ensemble des éléments de chaque contrat permettant de suivre les travaux classifiés s'y reportant. Les délais précisés ci-dessus courent pour chaque contrat à compter de la date de signature par l'autorité contractante de la FICPCS correspondante.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.8**

sous-contractant, une arborescence des travaux classifiés doit être tenue à jour en permanence par l'autorité contractante de référence.

Cette arborescence met en évidence, aux divers rangs de sous-contractants, les liens contractuels entre chaque titulaire et ses sous-contractants.

Le titulaire d'un contrat nécessitant l'accès ou la détention d'ISC ne peut communiquer à ses sous-contractants que les ISC décrits dans le PCS de sous-contractant approuvé par l'OS de l'autorité contractante de référence.

6. Modification et clôture du plan contractuel de sécurité

Un PCS peut être modifié au cours de l'exécution du contrat, à l'initiative de l'autorité contractante ou sur proposition du titulaire, dès que son contenu, en particulier la définition des informations à protéger, nécessite une révision ou lorsque des anomalies apparaissent pendant l'exécution des travaux classifiés. Le PCS modifié doit être transmis aux destinataires figurant sur le plan initial.

La fin d'exécution des travaux classifiés couverts par un PCS est matérialisée par une fiche de clôture du plan contractuel de sécurité (FICPCS).

La FICPCS permet d'enregistrer la fin d'exécution des travaux classifiés couverts par le PCS, et de préciser la destination des ISC détenus par le titulaire pour les contrats avec détention. Si le titulaire demande à conserver des ISC, il joint l'inventaire des ISC qu'il a besoin de conserver, en motivant sa demande. Cette demande doit être approuvée par l'autorité contractante de référence. Il précise la durée de conservation de ces ISC. Si nécessaire, cet inventaire peut être complété d'un inventaire des supports d'informations protégées et/ou de diffusion restreinte que le titulaire a besoin de conserver. Lorsqu'une personne morale conserve des ISC après la clôture d'un PCS, elle doit faire l'objet d'une décision d'habilitation valide et d'un suivi par un service enquêteur, quand bien même cette personne morale ne serait titulaire d'aucun autre contrat générant des éléments couverts par le secret de la défense nationale.

La FICPCS est établie par le titulaire du contrat et adressée à l'autorité contractante de référence dans un délai maximum d'un mois à compter de la fin des travaux classifiés. Le contrat peut comporter une clause liant le paiement pour solde à la fourniture de la FICPCS et/ou des pénalités en cas de retard.

Dans le cas d'un contrat de sous-traitance, la FICPCS doit recevoir l'accord du primo-contractant (émetteur du PCS à clore), avant d'être transmise à l'autorité contractante de référence pour décision.

L'OS de l'autorité contractante de référence :

- retourne au titulaire la FICPCS datée et signée en mentionnant son accord ou son refus quant à la conservation des ISC par le titulaire en spécifiant une durée. En cas de refus, il précise si les ISC figurant dans l'inventaire précité doivent lui être retournés ou être détruits par le titulaire ;
- communique simultanément la FICPCS au service enquêteur.

Le PCS d'un contrat ayant généré un ou plusieurs sous-contrats ne peut être clôturé qu'après la clôture des plans contractuels de sécurité relatifs aux sous-contrats.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.9****CAS D'UNE PERSONNE MORALE ETRANGERE CANDIDATE A LA
PASSATION D' UN CONTRAT AVEC ACCES OU DETENTION
D'INFORMATIONS ET SUPPORTS CLASSIFIES****Référence :**

IGI 1300 – 4.4.1.4.f

Points clés :

- Une personne morale étrangère peut candidater à un contrat avec accès ou détention d'ISC sous plusieurs conditions précises qui sont vérifiées par l'autorité contractante, en liaison avec l'autorité d'habilitation.
- Les contrats impliquant la détention d'ISC portant la mention *Spécial France* ne sont pas ouverts aux candidatures de personnes morales de droit étranger.

La candidature d'une personne morale étrangère à la passation d'un contrat avec accès ou détention d'ISC nécessite que soient remplies les conditions préalables suivantes :

- il doit exister entre la France et le pays de cette personne morale un accord de sécurité définissant les principes de protection des ISC et les équivalences entre les niveaux d'habilitation français et ceux de ce pays (cf. fiche 9.2). Cet accord de sécurité doit couvrir le domaine concerné par le projet de contrat ;
- la communication d'ISC (cf. fiche 7.8) à une personne morale étrangère est subordonnée à l'autorisation écrite préalable de l'organisme à l'origine de ces ISC. Il appartient au prescripteur technique d'obtenir cette autorisation ;
- la personne morale étrangère et son personnel amené à avoir accès aux ISC doivent disposer des habilitations appropriées. La vérification de ces habilitations, auprès de l'autorité compétente de l'Etat dont la personne morale relève, est faite par l'autorité nationale de sécurité (Cf. fiche 9.1) sur demande de l'OS de l'autorité contractante. Si la personne morale étrangère et son personnel ne sont pas habilités au niveau approprié, une demande d'habilitation peut être formulée auprès de l'autorité étrangère compétente, *via* l'autorité nationale de sécurité ou, le cas échéant, l'autorité de sécurité déléguée compétente, si l'accord de sécurité entre le pays de cette personne morale et la France le prévoit.

Si une personne morale étrangère présente sa candidature, l'autorité contractante en informe l'autorité d'habilitation qui engage immédiatement les actions nécessaires, telles que la vérification de l'habilitation de la personne morale ou le déclenchement de la procédure d'habilitation, auprès de l'autorité de sécurité compétente dont relève la personne morale *via* l'autorité nationale de sécurité ou, le cas échéant, l'autorité de sécurité déléguée compétente.

La lettre d'invitation à participer à une consultation de tout projet de contrat nécessitant l'accès ou la détention à des informations portant la mention « Spécial France » ne s'adresse qu'à des personnes morales de droit français.

L'autorité nationale de sécurité ou, le cas échéant, l'autorité de sécurité déléguée compétente, peut demander à l'autorité compétente de l'Etat dont le candidat relève, de vérifier la conformité des locaux et installations ainsi que l'homologation des SI

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES
DANS LE CADRE DES CONTRATS****4.9**

susceptibles d'être utilisés, les procédures industrielles et administratives qui seront suivies, les modalités de gestion de l'information ou la situation du personnel susceptible d'être employé pour l'exécution du marché.

TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

4.10

HABILITATION INITIALE DE LA PERSONNE MORALE

Références :

- Code des relations entre le public et l'administration – Art. L. 211-2
- IGI 1300 – 4.4.1.4

Points clés :

- Sauf exception¹⁰², la procédure d'habilitation des personnes physiques employées par la personne morale (PM) est conditionnée par l'habilitation préalable de la PM.
- La durée de validité d'un avis de sécurité pour une habilitation PM est de cinq ans pour le niveau *Très Secret* et de sept ans pour le niveau *Secret*.

La personne morale (PM) doit disposer d'une habilitation en cours de validité et être titulaire du contrat ou être en phase pré contractuelle pour être autorisée à engager la procédure d'habilitation de ses employés (cf. fiche 3.2), sous réserve de justifier pour chacune de ces personnes du besoin d'en connaître.

La procédure d'habilitation initiale obéit à la chronologie suivante :

- détermination du besoin d'habilitation (accès ou détention, niveau et nature) ;
- constitution du dossier d'habilitation de la personne morale ;
- enquête du service enquêteur qui émet un avis de sécurité adressé à l'autorité d'habilitation (AH) ;
- décision prise par l'AH donnant lieu à l'habilitation ou non de la personne morale.



1. Détermination du besoin d'habilitation

La demande d'habilitation d'une PM est motivée par la nécessité pour son personnel de détenir ou d'avoir accès à des ISC. L'exactitude et la précision des renseignements fournis dans la demande d'habilitation de la personne morale doivent faire l'objet d'un soin tout particulier.

Toute demande sans besoin d'en connaître avéré est à proscrire.

2. Constitution du dossier d'habilitation

Le dossier d'habilitation est constitué de la demande d'habilitation de la personne morale telle que précisée dans l'annexe 20 de l'IGI 1300. Il comporte une partie

¹⁰² Il existe des habilitations « personne physique » (ex : administrateur) sans qu'il soit nécessaire que la personne morale soit habilitée préalablement.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.10**

renseignée par le candidat à habilitier et l'autre par l'autorité contractante et est accompagné de pièces jointes dont la liste est fournie par la DGA ou toute autre autorité d'habilitation, basée sur la liste des pièces de l'annexe 20 de l'IGI 1300¹⁰³. Ce dossier comprend également la demande d'habilitation du responsable de la personne morale concernée.

Le dossier d'habilitation est remis directement par le candidat à l'autorité contractante qui le retransmet à l'autorité d'habilitation. S'il est incomplet, l'autorité d'habilitation en informe l'autorité contractante qui peut informer le candidat de la liste des pièces manquantes ou non conformes et de la date limite de fourniture de ces pièces.

Les éléments suivants sont précisés lors de la transmission des dossiers :

- l'objet du contrat ;
- le calendrier de la phase précontractuelle.

3. Avis de sécurité

Dès lors que le dossier de demande d'habilitation est complet, l'autorité d'habilitation le transmet au service enquêteur qui l'instruit et fait connaître à l'autorité d'habilitation ses conclusions sous forme de deux avis de sécurité, l'un concernant la personne morale, l'autre son responsable

Les avis de sécurité tiennent compte du niveau de classification et de la nature (national/OTAN/UE) pour lesquels la procédure d'habilitation est initialisée.

Ils sont transmis uniquement à l'autorité d'habilitation.

S'agissant de la personne morale, les conclusions de l'avis de sécurité sont de trois types :

- « avis sans objection », lorsque l'instruction n'a révélé aucun élément de vulnérabilité de nature à constituer un risque pour la sécurité des informations ou supports classifiés ;
- « avis restrictif », lorsque la PM présente certaines vulnérabilités constituant des risques directs ou indirects pour la sécurité des informations ou supports classifiés auxquels elle aurait accès, mais que des mesures de sécurité spécifiques prises par l'officier de sécurité permettraient de maîtriser ;
- « avis défavorable », lorsque des informations font apparaître que la PM présente des vulnérabilités faisant peser sur le secret des risques tels qu'aucune mesure de sécurité ne semble suffisante à les neutraliser.

S'agissant de l'habilitation du responsable légal, se référer à la fiche 3.3 de la présente instruction.

Les avis de sécurité sont émis pour un niveau donné d'habilitation. L'avis « sans objection » est valable pour le niveau précisé ainsi que le(s) niveau(x) inférieur(s).

Les avis restrictifs ou défavorables sont classifiés. Ils sont assortis d'une fiche confidentielle indiquant les motifs de l'avis. Cette fiche peut être classifiée en fonction des motifs de vulnérabilité identifiés lors de l'enquête. Ces motifs ne peuvent être portés qu'à la connaissance de la seule autorité d'habilitation. Ne pouvant être reproduite, la fiche confidentielle est retournée après communication et sans délai au service enquêteur. L'autorité d'habilitation peut, en tant que de besoin, demander à nouveau

¹⁰³ Un guide d'aide à la rédaction de cette demande est disponible sur le site www.ixarm.com.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.10**

communication des éléments qu'elle contient, en particulier, lorsqu'elle est chargée de mettre en garde l'autorité contractante, en cas d'évolution de la situation de la personne morale, à l'occasion de l'instruction d'une nouvelle demande d'habilitation la 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 d'un avis de sécurité est fixée au maximum à :

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

Un avis de sécurité peut être révisé à tout moment.

4. Décision d'habilitation**a. Procédure normale**

L'autorité d'habilitation prend sa décision après avoir pris connaissance des avis de sécurité. La décision n'est pas nécessairement conforme à cet avis. Conformément à l'article 4.4.1.1.a de l'IGI 1300, la décision d'habilitation du responsable légal de la personne morale est concomitante de la décision d'habilitation de cette même personne morale. Ces deux décisions doivent être prises au même niveau. L'autorité d'habilitation notifie sa décision à la personne morale, à l'adresse du siège social, et en informe l'autorité contractante et le service enquêteur. La décision prise par l'autorité d'habilitation vaut pour l'ensemble des autorités contractantes du MINARM et celles agissant au profit du CEA/DAM, y compris les marchés duaux.

Lorsque l'autorité d'habilitation considère que la personne morale et/ou son responsable légal présentent des risques tels que la sécurité des ISC ne peut être garantie, elle refuse l'habilitation. Le contrat envisagé ne peut donc être attribué à la PM en question.

La décision de refus d'habilitation est dispensée de motivation¹⁰⁴.

b. Procédure d'urgence

Lorsque l'avis de sécurité n'est pas émis à la date demandée, l'autorité d'habilitation peut prendre une décision d'habilitation provisoire au vu des éléments en sa possession (procédure d'urgence). Elle est d'une durée maximale de six mois. Une nouvelle décision est prise à la réception de l'avis de sécurité.

5. Domaine de validité de la décision d'habilitation

La décision d'habilitation précise le domaine de validité pour lequel elle est accordée.

Le domaine de validité concerne :

- le niveau maximum de classification des ISC qui peuvent être détenus par la PM habilitée ou communiqués au personnel habilité de cette dernière ;
- les éventuelles restrictions décidées par l'autorité d'habilitation, par exemple une habilitation valable pour un programme, pour un type de contrat, pour un ou plusieurs contrats explicitement mentionnés, etc. Ces restrictions sont dispensées de motivation.

¹⁰⁴ Article L. 211-2 du code des relations entre le public et l'administration.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.10****6. Identification des établissements**

Lorsque le titulaire du contrat fait effectuer des travaux classifiés par des personnes relevant de plusieurs établissements, tous doivent faire l'objet d'une identification.

Cette identification doit s'effectuer lors de la transmission du dossier d'identification d'un établissement par l'autorité d'habilitation au service enquêteur.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.11****GESTION ET FIN DE L'HABILITATION DE LA PERSONNE MORALE****Référence :**

IGI 1300 – 4.4.3.1

Points clés :

- La durée de validité d'une décision d'habilitation de la personne morale ne peut excéder la durée de validité des avis de sécurité.
- Une attestation d'habilitation peut être fournie par l'autorité d'habilitation lorsque la PM, qui dispose d'une habilitation en cours de validité, postule à un nouveau contrat avec accès ou détention d'ISC.

1. Durée de validité d'une décision d'habilitation

La décision d'habilitation comporte une date de fin de validité qui peut être antérieure à celle qui figure sur l'avis de sécurité. Elle ne peut excéder la durée de validité de l'avis de sécurité.

La décision demeure valable pour toute autre consultation d'une autorité contractante relevant du ministère, à l'occasion d'un autre contrat, dans les limites de date et de domaine de validité de cette habilitation et sauf changement dans la situation de fait ou de droit de la personne morale considérée.

La durée de validité d'une décision d'habilitation est au maximum de :

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

2. Attestation d'habilitation

Le titulaire d'un contrat détenteur d'une décision d'habilitation en cours de validité peut faire valoir cette qualité auprès d'une autorité d'habilitation, d'une autorité contractante ou d'un OS en produisant une attestation sollicitée auprès de l'autorité ayant prononcé l'habilitation.

Aucune communication d'informations à des tiers, à caractère commercial, publicitaire, technique ou scientifique, par des titulaires de contrats avec accès ou détention d'ISC ne doit contenir de mention se référant à ces contrats, sauf autorisation expresse de l'autorité contractante. Une telle clause doit obligatoirement figurer dans le contrat.

3. Renouvellement d'habilitation

Sous réserve que le titulaire du contrat ait toujours besoin d'être habilité, en particulier si la décision d'habilitation arrive à expiration en cours de contrat, le renouvellement de son habilitation doit être demandé, par son responsable légal ou son OS, dans l'année ou six mois au plus tard avant la date d'expiration de la décision d'habilitation en vigueur. Si cette disposition est respectée, la décision d'habilitation initiale reste valable pendant les 12 mois qui suivent son expiration.

La procédure est à engager directement auprès de l'autorité d'habilitation, qui s'assure auprès de l'autorité contractante du besoin de renouvellement.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.11**

Les pièces constitutives du dossier de renouvellement d'habilitation à fournir par le titulaire du contrat sont identiques à celles du dossier initial (cf. fiche 4.10).

Le dossier de renouvellement d'habilitation est transmis par l'autorité d'habilitation au service enquêteur¹⁰⁵, qui émet un nouvel avis de sécurité.

4. Réexamen d'habilitation

L'habilitation d'une personne morale peut faire l'objet d'un réexamen, à l'initiative du service enquêteur, de l'autorité d'habilitation ou de la PM concernée. C'est le cas en particulier lorsque :

- les caractéristiques de la PM ont subi des modifications (l'autorité d'habilitation apprécie si la modification intervenue au sein de la PM est de nature à remettre en cause sa décision d'habilitation et demande alors un nouvel avis) en particulier, les fusions, acquisitions, rachat ou cession d'activité de la PM sont de nature à remettre immédiatement en question la validité de l'habilitation.
- le titulaire du contrat ne respecte pas ses obligations réglementaires et contractuelles relatives à la protection du secret.

Lorsque le domaine de validité de la décision d'habilitation n'est pas approprié à un nouveau besoin, une nouvelle demande doit être effectuée. Dans son rôle de conseil de la direction de la PM, il est nécessaire que l'OS de celle-ci anticipe ces opérations et prenne l'avis du service enquêteur et de l'autorité d'habilitation. Cet avis peut porter sur l'éventuel maintien des habilitations ou sur les modalités de transfert des plans contractuels de sécurité liées aux contrats et permettra ainsi une mise en œuvre efficace du volet sécurité dans l'évolution de la PM.

Tout changement doit être porté sans délai à la connaissance de l'autorité d'habilitation et de l'autorité contractante de référence par l'OS ou le responsable de la PM. Sur la base des éléments recueillis et éventuellement d'un nouvel avis de sécurité, l'autorité d'habilitation peut prononcer une nouvelle décision d'habilitation.

5. Abrogation de l'habilitation de la personne morale

L'abrogation de l'habilitation de la PM titulaire d'un contrat peut intervenir si elle ne remplit plus les conditions nécessaires à sa délivrance. Cette abrogation est effectuée par décision de l'autorité d'habilitation, après avis du service enquêteur. Les autorités contractantes concernées sont informées par l'autorité d'habilitation.

L'abrogation de la décision d'habilitation n'entraîne pas nécessairement la résiliation du contrat, les conséquences d'une telle décision devant être examinées au cas par cas.

¹⁰⁵ Via SOPHIA pour la DRSD.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.12****GESTION DES SOUS-CONTRACTANTS¹⁰⁶ DANS LES CONTRATS
AVEC ACCES OU DETENTION D'INFORMATIONS ET SUPPORTS
CLASSIFIES****Références :**

- Code de la commande publique – Art. L. 2393-1 à L. 2393-9, L. 2393-10 à L. 2393-14, L. 2393-15, R. 2393-2 à R. 2393-23, R. 2393-24 à R. 2393-40, R. 2393-41 à R. 2393-44
- IGI 1300 – 4.4.2.2.c

Points clés :

- Le plan contractuel de sécurité (PCS) établi entre l'autorité contractante de référence et le primo-contractant intègre obligatoirement les informations nécessaires au suivi des prestations classifiées au sein des sous-contractants.
- C'est l'entité primo-contractante qui formule la demande d'habilitation pour ses PM parties à un sous-contrat auprès de l'autorité contractante de référence.
- Le contrat entre le primo-contractant et le sous-contractant doit comprendre un PCS spécifique à la nature des prestations classifiées de l'entité concernée.

Lorsqu'une personne morale titulaire d'un contrat avec accès ou détention d'ISC conclut un sous-contrat amenant notamment à sous-traiter une partie des prestations classifiées dont elle a la charge, elle prend l'appellation « d'autorité contractante » vis-à-vis de son sous-contractant.

Tout contrat nécessitant l'accès ou la détention d'ISC donnant lieu à au moins un sous-contrat nécessitant lui-même un accès à des ISC doit intégrer dans son plan contractuel de sécurité la liste des sous-contractants concernés, les travaux réalisés et leurs dates prévisionnelles de début et de fin d'exécution ainsi que les ISC dont la connaissance est nécessaire à leur réalisation.

1. Habilitation du sous-contractant

Il incombe à l'OS du sous-contractant ou du primo-contractant de transmettre le dossier de demande d'habilitation auprès de l'autorité contractante de référence si le sous-contractant pressenti n'est pas habilité pour le domaine concerné ou au niveau requis pour les travaux concernés. L'autorité contractante de référence transmet ensuite ce dossier à l'autorité d'habilitation. La demande d'habilitation du sous-contractant est instruite selon la même procédure que celle relative à l'habilitation de la personne morale du primo-contractant.

L'habilitation du sous-contractant s'accompagne chez lui de la mise en place d'une structure de sécurité adaptée aux travaux classifiés qu'il doit exécuter.

¹⁰⁶ Les sous-contractants (CCP, art L. 2393-1 à L. 2393-9, R. 2393-2 à R. 2393-23) peuvent être des sous-traitants (CCP, art. L. 2393-1, L. 2393-10 à L. 2393-14, R. 2393-24 à R. 2393-40) ou des opérateurs ayant la qualité de fournisseurs ou de prestataires de services qui ne sont pas réalisés spécialement pour répondre aux besoins de l'acheteur (CCP, art. L. 2393-1 et L. 2393-15, R. 2393-41 à R. 2393-44).

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.12****2. Aptitude des locaux et homologation des systèmes d'information du sous-contractant**

La vérification des aptitudes et le début d'exécution des travaux classifiés au titre d'un sous-contrat avec détention d'ISC suivent les prescriptions des fiches 5.6 et 6.3. Le service enquêteur délivre ses avis d'aptitude à l'entreprise titulaire du sous-contrat et informe l'autorité contractante, l'autorité contractante de référence et l'autorité d'habilitation. Les SI du sous-contractant sont homologués au niveau requis pour l'exécution du contrat avant de pouvoir héberger des informations.

3. Le plan contractuel de sécurité associé au sous-contrat

Le sous-contrat comporte obligatoirement un plan contractuel de sécurité (PCS) dont l'établissement et la validation suivent les prescriptions de la fiche 4.8. Le sous-contrat comporte les clauses de protection du secret.

La simple copie de la totalité du PCS du primo-contractant dans le projet du PCS du sous-contrat est proscrite car elle alourdit inutilement le PCS lié au sous-contrat et peut conduire à des compromissions (besoin d'en connaître). Seules les rubriques concernant la participation effective du futur titulaire du sous-contrat doivent être retenues et développées selon les modalités d'exécution des travaux qui lui sont confiés.

Le PCS d'un contrat ayant généré un ou plusieurs sous-contrats ne peut être clôturé qu'après clôture de tous les PCS des sous-contrats (cf. fiche 4.8).

4. Information en cours d'exécution

Si, en cours d'exécution, l'autorité contractante est informée de l'existence d'un sous-traitant ou d'un sous-contractant non déclaré, elle doit mettre en demeure le primo-contractant de régulariser la situation. Une fois la déclaration effectuée, les demandes d'habilitation sont transmises à l'autorité contractante soit par le primo-contractant soit directement par le sous-traitant ou sous-contractant.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.13****CONTRÔLES DES PERSONNES MORALES PAR LES AUTORITES
CONTRACTANTES DE REFERENCE, LES AUTORITES
D'HABILITATION ET L'AUTORITE DE SECURITE DELEGUEE****Références :**

- Code de la défense – Art. R. 2311-9-3
- IGI 1300 – 2.3.3
- II n° 901/SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'informations sensibles
- II n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)
- II n° 920/SGDSN/DCSSI du 12/01/2005 relative aux systèmes traitant des informations classifiées de défense de niveau Confidentiel Défense

Points clés :

- Les personnes morales habilitées sont soumises au contrôle externe de l'autorité contractante de référence, de l'autorité d'habilitation, de l'autorité de sécurité déléguée et du service enquêteur.
- Ces contrôles permettent au MINARM de vérifier la bonne application des plans contractuels de sécurité et des mesures de protection du secret par les personnes morales sous contrat avec lui.

Les contrôles¹⁰⁷ menés par les autorités contractantes de référence et d'habilitation, du service enquêteur, voire de l'autorité de sécurité déléguée dans le cadre de contrats internationaux, ont pour objet la vérification de la conformité des dispositifs de protection mise en place en application :

- de la réglementation relative à la protection du secret (dont la présente IM) et aux ACSSI
- des dispositions du plan contractuel de sécurité.

Mesurant l'écart entre la réglementation en vigueur et son application par la personne morale, ils permettent de disposer d'un état des lieux global du niveau de protection, actualisé et objectivé, destiné à évaluer la capacité d'un titulaire ou d'un sous-contractant à répondre aux exigences du contrat dans les domaines de la conservation des informations sensibles ou *Diffusion Restreinte*, des ACSSI et du secret.

1. Périmètre

Les contrôles sont effectués dans les établissements des personnes morales titulaires de contrats avec détention d'ISC, d'ACSSI ou d'informations sensibles ou *Diffusion Restreinte*, comme des sous-traitants ou des sous-contractants, participant ou ayant participé à des travaux avec détention.

Ces contrôles ont pour but de s'assurer de la mise en place de mesures de protection conformes à la réglementation et d'en vérifier l'application, lorsque des ISC, ACSSI,

¹⁰⁷ La notion de contrôle recouvre les contrôles, inspections ou audits précisés dans la fiche 2.9.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.13**

informations sensibles ou *Diffusion Restreinte* sont détenus dans les établissements du contractant.

Ils portent sur les moyens humains, matériels, technologiques, organisationnels et d'infrastructures déployés par la personne morale pour assurer la protection, l'intégrité, la manipulation, la conservation et la traçabilité des ISC, des ACSSI et des informations *Diffusion Restreinte* ou sensibles, objet du contrat.

2. Périodicité

Les contrôles sont réalisés, dans la mesure du possible, en début de contrat avant la mise à disposition des informations sensibles ou *Diffusion Restreinte*, des ACSSI et des ISC dans les locaux du contractant et sur les SI devant abriter des informations *Diffusion Restreinte*, sensibles ou des ISC, à l'issue de manquement ou d'incident de sécurité impliquant le contractant, en cours d'exécution à l'initiative des autorités contractantes de référence, d'habilitation et de sécurité déléguée et à la clôture du contrat.

Toute personne morale liée au ministère des armées par un contrat avec détention ou accès à des ISC peut ainsi faire l'objet d'une inspection du service enquêteur ou d'un audit par l'autorité d'habilitation, l'autorité de sécurité déléguée ou l'autorité contractante (cf. fiche 2.9).

Le délai raisonnable entre deux inspections est fixé à cinq ans lorsqu'il y a détention d'ISC.

Le ministre et le directeur du service enquêteur ainsi que les autorités d'habilitation, contractantes de référence et de sécurité déléguée peuvent déclencher une inspection ou un audit de manière inopinée. L'autorité contractante peut solliciter une inspection auprès du service enquêteur.

3. Compte rendu et suite donnée au contrôle et aux inspections

A l'issue du contrôle, d'un audit ou d'une inspection, les autorités contractantes de référence et d'habilitation ou le service enquêteur rédigent un compte rendu de l'état des lieux objectif du niveau de protection de la personne morale et des éventuelles vulnérabilités constatées.

Lorsqu'elles révèlent des insuffisances, les conclusions des contrôles donnent lieu à des actions correctives. Dans ce cas un contrôle ultérieur permet d'en vérifier l'efficacité.

Après la transmission du compte rendu, la personne morale contrôlée dispose de six mois pour rendre compte à l'autorité contractante de référence, à l'autorité d'habilitation et au service enquêteur des mesures correctives apportées ou engagées sur son site.

Le refus de procéder à tout ou partie de ces actions correctives peut entraîner :

- sans préjudice des sanctions pénales et civiles, les conséquences dues au non-respect des dispositions acceptées contractuellement lors de l'engagement initial, comme la résiliation du contrat avec dédommagement de l'autorité contractante ;
- la révision temporaire ou définitive des aptitudes physique et informatique de l'établissement pour non-respect des prescriptions de sécurité et pour l'inobservation de la réglementation relative à la protection du secret de la défense nationale. Cette disposition peut entraîner la remise en cause du contrat et l'application de pénalités ;

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.13**

- l'abrogation des décisions d'habilitation de la personne morale et des personnes physiques.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES

INTRODUCTION : NORMES DE PROTECTION PHYSIQUE ET LOGIQUE APPLICABLES AUX INFORMATIONS ET SUPPORTS CLASSIFIES

Références :

- IGI 1300 – 5.2 et annexes 30 et 31
- Pour les établissements du MINARM, ses établissements publics sous tutelle et les INID du CEA : IM n° 1544/DEF/CAB/DR du 17 janvier 2017, version du 10 août 2020, relative à la défense-sécurité des activités, moyens et installations relevant du ministère de la défense - titres 5 et 6

Points clés :

- Les mesures de protection appliquées aux lieux abritant des ISC ont pour objet d'éviter toute perte, dégradation ou compromission. Elles comprennent des moyens organisationnels, humains, techniques et logiques dissociés ou combinés en fonction du niveau de classification et des menaces identifiées.
- La protection physique des ISC implique également de sécuriser l'accès à des locaux techniques qui peuvent être distants (énergie, moyens de communication par exemple) et assure une protection contre les menaces extérieures et environnementales (dispositifs contre les incendies, les dégâts des eaux, les risques liés à l'alimentation électrique et tout autre risque environnemental identifié).
- Lorsque les circonstances imposent la détention d'ISC mais ne permettent pas la mise en place des moyens habituels de protection, des mesures compensatoires sont prises afin de conserver le même niveau de protection. Ces mesures de substitution doivent procéder d'une analyse précise des risques, effectuée par l'autorité responsable du site concerné (ou l'AQSSI pour les mesures logiques), et suivre l'avis du service enquêteur compétent¹⁰⁸.
- Les normes de protection édictées ci-dessous concernent les lieux abritant des ISC, qu'il s'agisse de lieux de stockage ou des salles de réunion dédiées.

1. Principes généraux à appliquer en matière de protection

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 techniques doivent répondre au besoin de dissuader, détecter et freiner l'intrusion de façon à permettre l'intervention. Ils doivent, en outre, permettre de reconstituer tous les éléments, les actions et le cheminement de l'intrus dans l'espace et dans le temps en cas d'effraction. Ils s'inscrivent dans la profondeur en étagant différentes couches de protection, appelées aussi barrières (périphériques, périmétriques et intérieures), qui s'appuient essentiellement sur :

- l'emprise et/ou le bâtiment ;

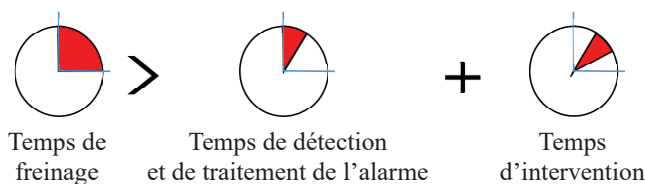
¹⁰⁸ DRSD pour le cas général, DGSE pour ses besoins propres.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES

- 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 être conforme aux exigences fixées par l'équation de protection, définie comme suit (T pour « temps ») :

T freinage > T de détection et de traitement de l'alarme + T 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. Il est matérialisé par la présence de moyens de freinage en nombre et en nature suffisants.

Le temps de détection et de traitement de l'alarme correspond au délai existant entre l'alarme émise par le premier moyen de détection d'intrusion et le déclenchement effectif de l'intervention par le poste chargé de traiter l'alarme. À titre d'exemple :

- dans le cas d'une alarme fondée sur une détection électronique, T de détection et de traitement de l'alarme = 0 + validation de l'information (levée de doute effectuée) + délais de transmission et prise en compte effective par le poste pouvant exécuter l'intervention immédiatement, 24h/24 et 7j/7 ;
- dans le cas de rondes en l'absence d'alarme ou de surveillance à distance, T de détection et de traitement de l'alarme = intervalle entre les rondes + validation de l'information (levée de doute effectuée) + délais de transmission et prise en compte effective par le poste pouvant exécuter l'intervention immédiatement, 24h/24 et 7j/7.

Le temps de détection comprend le temps mis par le moyen de détection pour transmettre l'alerte vers l'élément d'intervention (téléphonie automatique ou manuelle, radio portative, sirène, etc.). La nécessité de lever le doute de l'intrusion pour réaliser une intervention efficace (nature, volume, localisation et attitude des intrus) vient augmenter la valeur de ce paramètre.

Le temps d'intervention est le temps mis par l'élément chargé de l'intervention (interne ou externe) ou les forces de sécurité intérieures (FSI) pour se trouver au cœur de la zone d'action. Dans le cas d'un élément d'intervention externe ou d'une FSI, le temps d'intervention tient compte de la distance, du temps moyen constaté et de la disponibilité moyenne de l'élément. En cas de doute, le temps majorant est retenu.

2. Détermination des classes

Chaque barrière est répartie en 3 ou 4 classes (de la moins fiable à la plus sécurisée). Chacune de ces classes correspond aux moyens techniques, humains et organisationnels mis en œuvre pour assurer un niveau de protection au moins égal à celui décrit ci-après.

TITRE 5 : SECURITE DES LIEUX ABITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES

Les normes sont disponibles sur le site du SGDSN et actualisées. Elles permettent d'avoir une référence technique pour atteindre les niveaux minimums de protection exigés.

a. Classes du bâtiment et/ou de l'emprise ou du site

Classe	Description
4	<p>Emprise (ou site) dont le périmètre est délimité physiquement :</p> <ul style="list-style-type: none"> o dotée d'un contrôle d'accès conforme à l'annexe 31 de l'IGI 1300, d'une protection mécanique (clôture dont le franchissement n'est pas possible sans facilitateur¹⁰⁹) et dont tous les points d'accès sont équipés d'une serrure mécanique fonctionnelle. <p style="text-align: center;"><u>ou</u></p> <ul style="list-style-type: none"> o dotée d'un contrôle d'accès conforme à l'annexe 31 de l'IGI 1300, dont les ouvrants proches d'un point d'accès sont, dans la mesure du possible, rendus discrets (film opacifiant¹¹⁰) et systématiquement dotés d'une protection mécanique (limiteur d'ouverture, barreaux, etc.) et dont les points d'accès sont équipés d'une serrure mécanique fonctionnelle.
3	<p>Enceinte de classe 4 :</p> <ul style="list-style-type: none"> + contrôle d'accès par identification en périmétrie pour les flux piétons et véhicules ; + personnel de surveillance¹¹¹ présent en permanence, effectuant des rondes dans l'enceinte et ses sous-ensembles ; + élément d'intervention extérieur¹¹² mobilisable sur alarme du personnel de surveillance. <p style="text-align: center;"><u>ou</u></p> <p>Enceinte de classe 4 :</p> <ul style="list-style-type: none"> + contrôle d'accès par identification en périmétrie pour les flux piétons et véhicules ; + moyen de détection d'ouverture sur les ouvrants accessibles¹¹³ et les points d'accès relié à une centrale d'intrusion ; + système de vidéosurveillance/détection sur les locaux abritant permettant une levée de doute ; <p>Ces dispositifs techniques de détection-alarme sont reliés à un élément d'intervention extérieur.</p>
2	<p>Enceinte de classe 3 :</p> <ul style="list-style-type: none"> + personnel de surveillance présent en permanence, effectuant des rondes dans l'enceinte et ses sous-ensembles ; + ensemble de télé-sécurité (télésurveillance + intervention¹¹⁴) ; + dispositifs techniques de détection-alarme ; + moyen de détection volumétrique sur les lieux de passage permettant d'accéder aux locaux abritant des informations et supports classifiés (ISC) ;

¹⁰⁹ Pierre servant de marchepieds, perche, canne, escalade, etc.

¹¹⁰ Le film opacifiant protège uniquement contre les vues extérieures.

¹¹¹ Par exemple, agent de protection et de sécurité, gardien-veilleur, garde.

¹¹² Forces de sécurité intérieure ou agent privé de sécurité.

¹¹³ Depuis le sol, toit, corniche, descente d'eau pluviale, promontoire, etc. Un accès est un trou dans une paroi permettant le passage (estimé à 40cm*11cm).

¹¹⁴ Le moyen d'intervention retenu (capacité, volume) est cohérent avec l'analyse de risques et respecte les temps d'intervention établis avec l'équation de protection.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES

	+ traçabilité des entrées et sorties au niveau du bâtiment hébergeant les lieux abritant des ISC.
1	Enceinte de classe 2 : + dispositifs de détection-alarme placés sur tous les points d'accès de l'ensemble des locaux ; + système de vidéosurveillance sur les accès aux lieux abritant les ISC ; + moyen de détection d'intrusion placé au point d'accès de tous lieux abritant les ISC ; + 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, celui-ci doit être installé au niveau du local.

Les parois (les 6 faces du local : sols, murs et plafonds) des locaux, ainsi que les ouvrants (portes, fenêtres, etc.)¹¹⁵, leurs serrures et leurs sùretés doivent présenter une résistance mécanique suffisante et homogène pour retarder l'intrusion et permettre la mise en œuvre des moyens d'intervention.

Toutes les serrures des portes des locaux sont équipées de sùretés à clés mécaniques, comme dispositif principal ou comme moyen de secours de dispositifs électroniques.

Les fabricants de sùreté à clef justifient que leurs produits possèdent :

- une technologie qui s'oppose aux techniques d'ouvertures à l'aide d'outils manuels ;
- une conception qui complique l'usage de moyens d'ouvertures fines (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, blocs de climatiseur, etc.).
c	Local avec : <ul style="list-style-type: none"> o bloc-porte (métallique ou en bois plein ou matériau équivalent) à serrure mécanique multipoints ; o sùreté à clé présentant un temps de résistance d'au moins 5 minutes ; o contrôle d'accès par identification ; o fenêtres protégées lorsqu'elles sont accessibles (depuis le sol, toit, corniche, descente d'eau pluviale, promontoire, etc.). Dans le local abritant les ISC :

¹¹⁵ Les dispositifs électromécaniques ou électromagnétiques de fermeture des ouvrants ne peuvent pas toujours à eux seuls garantir l'intégrité des accès aux bâtiments ou aux emprises. Il est obligatoire de s'assurer de la mise en service, en dehors des périodes d'occupation des bâtiments, d'un verrouillage mécanique (quel que soit son type de commande – manuelle, électrique, etc.) du système de fermeture. La permanence de ce verrouillage doit, de plus, être assurée en cas de coupure d'alimentation électrique.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES

	<ul style="list-style-type: none"> o moyen de détection volumétrique double technologie relié à une centrale d'intrusion, ou o 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"> o bloc-porte renforcé équipé d'un système anti-dégondage, à serrure mécanique multipoints avec détecteur. o sûreté à clé doit présenter un temps de résistance d'au moins 15 minutes ; o contrôle d'accès par authentification avec traçabilité des entrées et sorties; o fenêtres protégées lorsqu'elles sont accessibles (depuis le sol, toit, corniche, descente d'eau pluviale, promontoire, etc.). <p>Dans le local abritant les ISC :</p> <ul style="list-style-type: none"> o moyen de détection d'intrusion sur les ouvrants et serrure mécanique de fermeture sur les points d'accès (bloc-portes, baies, etc.) ; o moyen de détection volumétrique double technologie relié à une centrale d'intrusion o un système permettant la levée de doute en dehors des heures de service (vidéosurveillance, par ex.).
a	Chambre forte 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/ou 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 serrures à combinaison mécanique conformes à la norme EN1300 niveau B 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 pènes, inaccessibles de l'extérieur, ne doivent pas pouvoir être démontés.
B	<p>Armoire forte de structure identique à celle de 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 ;

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES

	<ul style="list-style-type: none"> + 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 pènes 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 interdise aux pènes 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 pènes 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 pènes horizontaux et verticaux. Si une poignée actionne ce système, elle possède un point de rupture pour éviter un effort trop conséquent sur la tringlerie. <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 pènes 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 de la sécurité des systèmes d'information.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES

Description	Classe γ de base	Classe β renforcé	Classe α fort
Intégrité physique des éléments constitutifs du SI	Scellés génériques de contrôle d'ouverture de l'équipement avec traçabilité des équipements ayant reçu des scellés Contrôle ponctuel de l'intégrité des scellés par l'utilisateur.	Protection de la classe γ + Contrôle annuel de l'intégrité des scellés.	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 Contrôle semestriel de l'intégrité des scellés.
Confidentialité des données lorsque le terminal ¹¹⁶ 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 ^{**117} - homologuée par l'organisme	Dispositif d'authentification forte, par exemple basée sur une IGC qualifiée au moins RGS ^{**} .

¹¹⁶ 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

¹¹⁷ 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).

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES

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 filtrage	Cloisonnement par fonction homogène au sein du SI (cloisonnement des réseaux locaux-LANs-par population)	Cloisonnement entre les utilisateurs d'une même population, exemple P-VLAN.	Cloisonnement par le 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 énoncé dans les principes généraux pour obtenir un niveau de sécurité minimal pour les ISC.

La détermination de ce niveau est réalisée en deux temps :

- La classification des barrières (emprise, bâtiment, local, meuble ou moyen logique) à travers les moyens de détection d'intrusion ou de freinage qui leurs sont associés.
- La vérification de la validité de la combinaison des classes des barrières en fonction du niveau de classification de l'ISC.

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.

La protection des informations et supports classifiés est assurée par un minimum de trois barrières physiques successives au niveau de l'emprise ou du bâtiment, du local et du meuble.

La protection des systèmes d'information classifiés est assurée au choix par la combinaison de :

- trois barrières physiques successives au niveau de l'emprise ou du bâtiment, du local et du meuble de façon identique à la protection des informations et supports classifiés) ;

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES

- deux barrières physiques et d'une barrière logique.

Les tableaux suivants définissent, pour chaque niveau de classification, la classe minimale du meuble et celle de la protection logique en fonction des classes de protection physique du bâtiment et du local.

La lettre en majuscule désigne la classe du meuble dans lequel on entrepose l'ISC, la lettre grecque la classe du SI classifié.

Classe minimale du meuble et du SI pour le niveau Secret

Classe du bâtiment	Classe du local			
	a	b	c	d
1	C / γ	C / γ	C / β	C / β
2	C / γ	C / γ	C / β	C / β
3	C / γ	C / γ	C / β	B / α
4	C / γ	C / γ	B / α	interdit

Si des informations et supports ou systèmes d'information classifiés au niveau Secret ne peuvent être conservés dans un meuble de sécurité en raison de leur dimension, ils seront alors stockés dans un local renforcé correspondant aux caractéristiques suivantes :

- l'emprise 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/bâtiment¹¹⁸.

Dans l'hypothèse où les barrières physiques sont assurées par le local et un meuble adapté¹¹⁹, sans considération du niveau de protection du bâtiment, le tableau suivant définit, pour le seul niveau de classification Secret, la classe minimale de protection logique :

Cas particulier : classe minimale du SI pour le 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

¹¹⁸ Les détecteurs sont généralement raccordés à une centrale locale placées 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 centrale locale et générale qui peut sortir de la zone, pour peu qu'elle soit chiffrée. C'est en cela que le système est indépendant. Il ne s'agit donc pas obligatoirement de déployer deux SI de détection d'intrusion.

¹¹⁹ Par exemple, baie technique blindée ou armoire forte dédiée aux serveurs.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES**Classe minimale du meuble et de SI pour le niveau *Très Secret***

Classe du bâtiment	Classe du local			
	a	b	c	d
1	C / β	C / β	interdit	interdit
2	C / β	C / β	interdit	interdit
3	C / β	C / β	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 seront alors stockés dans un local renforcé correspondant aux caractéristiques suivantes :

- l'emprise 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/bâtiment.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES**5.1****ZONE RESERVEE****Références :**

- Code pénal – art. 413-7, 413-8 et art. R. 413-1 à R. 413-5 (zone protégée)
- IGI 1300 – 5.3.1.2, annexe 32
- II n° 2100/SGDN/SSD du 1^{er} décembre 1975 pour l'application en France du système de sécurité de l'Organisation du Traité de l'Atlantique Nord (OTAN).¹²⁰
- Instruction interministérielle n° 300/SGDSN/ANSSI du 23 juin 2014 sur la protection contre les signaux parasites compromettants.
- Pour les établissements du MINARM, ses établissements publics sous tutelle et les INID du CEA : IM 1544/DEF/CAB/DR du 17 janvier 2017, version du 10 août 2020, relative à la défense-sécurité des activités, moyens et installations relevant du ministère de la défense - titre 4, chapitre 4.2.4
- Note n° 3273/ARM/CAB/CM1-C.HFD/DR du 13 juin 2019 relative à l'utilisation de la carte d'identité multi-services (CIMS) pour le contrôle d'accès

Points clés :

- Une zone réservée (ZR) est obligatoire pour la protection physique des ISC de niveau *Très Secret*, y compris ceux faisant l'objet d'une classification spéciale. Ne conférant pas de protection juridique, elle doit être incluse dans une zone protégée (ZP).
- La ZR est dite de classe I si le fait de pénétrer dans la zone équivaut à avoir un accès direct aux ISC. Sinon elle est dite de classe II.

1. Principes

Une zone réservée (ZR) est obligatoire pour la protection physique des ISC de niveau *Très Secret* quelle que soit la nature (national, OTAN, UE), y compris ceux faisant l'objet d'une classification spéciale. Elle a pour but d'interdire l'accès aux systèmes d'information, toute pénétration par vues et par écoutes directes ou indirectes et tout accès à ces ISC par des personnes n'étant pas habilitées et n'ayant pas le besoin d'en connaître. La ZR n'apportant pas de protection juridique spécifique, elle doit donc être incluse¹²¹ dans une zone protégée (ZP) telle que définie par les textes en référence.

Le traitement ou la conservation d'ISC de niveau *Très Secret* en dehors d'une ZR n'est autorisé que dans les situations spécifiques (protection du secret en opération ou en déploiement opérationnel à l'étranger).

Dans les pays appartenant à l'OTAN, une zone réservée est dite de classe I si le fait de pénétrer dans la zone équivaut à avoir un accès direct aux ISC. Sinon elle est dite de classe II.

¹²⁰ Cette instruction induit pour les ZR (bureau COSMIC) un ATAP et une attestation de garanties matérielles de sécurité, différente de la décision de création de ZR.

¹²¹ Les impossibilités techniques empêchant la création d'une zone protégée doivent être justifiées (ISC détenues sur un mobile (bateau, avion, véhicule roulant...), à l'étranger)

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES

5.1

2. Dispositions administratives de création d'une ZR

Il appartient au chef d'organisme qui élabore, traite, reçoit ou détient des ISC de niveau *Très Secret*, y compris ceux faisant l'objet d'une classification spéciale, de créer une ZR (directeur de l'entreprise, commandant de formation administrative, chef d'établissement...).

Le traitement ou la conservation d'ISC dans ces locaux ne peut intervenir qu'après avis technique d'aptitude physique (ATAP) et, le cas échéant, d'un avis technique d'aptitude informatique (ATAI) conformes (cf. fiche 6.3). Ces avis sont rendus après dépôt auprès du service enquêteur d'un dossier de demande d'aptitude pour chaque lieu et/ou système d'exécution ou de détention de travaux classifiés, suivi d'une évaluation initiale d'aptitude (cf. fiche 5.6).

La décision de création, signée par le chef d'organisme, doit comprendre la localisation de la ZR ainsi que les références de la ZP dans laquelle se situe la ZR (cf. modèle en [annexe 4](#)).

3. Mesures de protection

a. Mesures de protection physique

Les mesures de protection de la ZR doivent respecter le principe de l'équation de protection (cf. Introduction du titre 5). A ce titre, le local érigé en ZR doit :

- être pourvu d'ouvertures en nombre restreint¹²² et à la protection renforcée ;
- contenir un meuble de sécurité de type approuvé ;
- être placé sous détection d'intrusion¹²³ dès que les locaux ne sont pas occupés ;
- disposer d'un système de détection-alarme qui soit autonome ou indépendant de toute autre système ;
- disposer d'ouvrants, y compris l'issue de secours, équipés d'un dispositif de détection d'intrusion ;

Si des systèmes d'information de niveau *Très Secret* sont utilisés dans la zone réservée, la ZR doit faire l'objet de l'application de mesures relatives aux circuits approuvés (cf. PSSI-M et fiche 6.10) et aux signaux parasites compromettants (SPC), précisée dans l'instruction interministérielle en référence.

Les ZR de classe I doivent en outre, dans la mesure des possibilités techniques, disposer d'un dispositif de masquage des ISC (ex : rideaux, diffusion d'une fumée opacifiante sur détection d'intrusion).

b. Mesures organisationnelles

Un contrôle permanent de la ZR doit être organisé en s'appuyant sur un dispositif de surveillance (humaine ou technique) complété par un dispositif de détection d'intrusion et de remontée d'alarme¹²⁴ relié à un poste central de protection (PCP) en mesure de

¹²² Fenêtres protégées, portes renforcées équipées de serrures de haute sécurité et issue de secours équipée d'un dispositif de détection d'intrusion

¹²³ Un système de détection volumétrique est recommandé.

¹²⁴ La mise sous alarme des locaux de la ZR doit être indépendante des autres systèmes de détections/surveillance. Lorsque les occupants sont absents le local doit systématiquement être sous surveillance.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES

5.1

déclencher une intervention. En cas de besoin de discrétion, la présence de panneaux indiquant la ZR n'est pas obligatoire.

Des rondes de sécurité aux abords sont régulièrement effectuées par des gardiens ayant fait l'objet d'une enquête administrative et disposant 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 (cf. fiche 5.7).

Pendant les heures d'utilisation, le contrôle de la ZR incombe au personnel qui y est employé. Avant de quitter les lieux, celui-ci vérifie la mise en sûreté des ISC, la fermeture des meubles de sécurité et de tous les ouvrants puis effectue les mises sous alarme.

En dehors des heures d'utilisation, des contrôles sont organisés par l'autorité responsable ou par son bureau de protection du secret, pour vérifier :

- la fermeture des locaux et le fonctionnement des systèmes de détection ;
- le vidage des corbeilles à papier et l'absence de brouillon ou document préparatoire aux informations classifiées ;
- l'absence d'ISC hors des meubles de sécurité¹²⁵ ;
- pour les ZR de classe I, le masquage des ISC.

4. Contrôle d'accès

Le dispositif (organisationnel, technique et/ou humain) de contrôle d'accès à une zone réservée doit assurer la conservation des données relatives aux accès et garantir l'authentification¹²⁶ de tous les accédants autorisés¹²⁷, de par leur fonction, par le responsable de la zone.

Le système de contrôle d'accès automatisé s'organise en deux phases :

- la phase d'identification : ce que l'on a (par exemple, un badge¹²⁸) ;
- la phase d'authentification : ce que l'on sait (un code) ou ce que l'on est (comparaison biométrique,...).

Pour chaque ZR, une liste nominative exhaustive, avec photographie, des personnes habilitées à pénétrer est maintenue à jour par le responsable de la ZR, via son OS. Pour toute nouvelle autorisation d'accès ou retrait, la liste actualisée est visée et paraphée par le responsable de la zone.

Le personnel de soutien ne peut pénétrer dans une ZR que s'il a satisfait à une enquête administrative pour le renseignement et la sûreté (cf. fiche 3.9) et, dans le cas de prestataires privés, il appartient à une société ayant au préalable satisfait à une enquête administrative. Le personnel de soutien dispose d'un laissez-passer (CIMS ou badge) permettant son identification et attestant de la décision d'accès. Il n'intervient qu'en

¹²⁵ A l'exception des ISC dont le volume et les dimensions ne permettent pas son rangement dans un meuble de sécurité.

¹²⁶ La perception d'une clé d'accès en ZR auprès de l'officier de permanence après signature d'un registre et un code unique pour désactiver l'alarme du local constituant pour exemple un système d'authentification valable.

¹²⁷ A l'exception du personnel permanent de la ZR.

¹²⁸ Les systèmes de type smartphone/ordiphone ne sont pas retenus actuellement comme supports d'identification ou d'authentification possibles.

**TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIES****5.1**

présence de personnels habilités de la zone réservée et lorsque les ISC ne lui sont plus accessibles.

Toutes les personnes n'ayant pas accès, de par leur fonction, à la ZR sont considérées comme des visiteurs. Pour pénétrer dans une ZR, les visiteurs doivent être identifiés et enregistrés¹²⁹ au préalable, faire l'objet d'une décision d'accès délivrée par l'autorité responsable de la ZR et être munis d'un laissez passer (carte CIMS ou badge - visiteur ou temporaire - attribué nominativement au visiteur pour la durée de la visite) permettant leur identification et attestant de la décision d'accès.

Tous les visiteurs doivent être accompagnés par des personnes habilitées désignées parmi le personnel de la zone réservée, pendant toute la durée de la visite. L'accès des visiteurs aux ISC est strictement limité à ceux dont ils ont le besoin d'en connaître et pour lesquels ils sont habilités au niveau requis.

¹²⁹ C'est-à-dire que l'organisme doit conserver une trace de l'identité du visiteur, du motif de la visite et de la date/heure de la visite.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES**5.2****ELEMENTS CLASSIFIÉS CONSERVÉS « HORS COFFRE »****Références :**

- IGI 1300 – 5.2.2 et annexe 30
- II n° 300 du 24/06/2014 relative à la protection contre les signaux parasites compromettants.

Points clés :

- Les ISC trop grands ou trop volumineux pour être enfermés dans des meubles de sécurité (ISC dits « hors coffre ») doivent bénéficier de mesures de protection compensatoires.
- Les ISC conservés hors coffre dans des moyens mobiles, hors opérations, sont soumis à des règles particulières et doivent être gardés en permanence.

Principes

Compte tenu de leurs dimensions, certains ISC de niveaux *Secret* et *Très Secret* (comme des prototypes, des pièces usinées ou des objets, par exemple) ne peuvent être conservés dans un coffre ou dans une armoire forte, alors que les conditions des textes de référence le prévoient.

Aussi, leur protection physique doit être adaptée pour tenir compte de l'absence de meuble de sécurité. Ces ISC atypiques sont alors conservés dans un local répondant aux normes minimales d'infrastructure définies *infra*. Leurs conditions de conservation/stockage doivent faire l'objet d'une étude au cas par cas avec le concours du service enquêteur. Dans la mesure des possibilités techniques, un dispositif de masquage des ISC doit être installé (exemple : rideaux, diffusion d'une fumée opacifiante sur détection d'intrusion).

Les ISC conservés dans des moyens mobiles doivent être, quant à eux, gardés en permanence. Enfin, il peut exceptionnellement exister des ISC qui ne sont ni mobiles ni conservés dans un local. Leur protection doit être étudiée au cas par cas en liaison avec le service enquêteur.

1. ISC atypiques de niveau Secret

Le local est au moins de type « c » avec un dispositif de détection-alarme indépendant de ceux de l'emprise/bâtiment et répond aux normes suivantes :

- le bâtiment ou l'emprise dans lequel il est situé est au moins 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.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES

5.2

Classe de l'emprise / bâtiment	Classe du local			
	a	b	c	d
1	autorisé	autorisé	autorisé	interdit
2	autorisé	autorisé	autorisé	interdit
3	autorisé	autorisé	autorisé	interdit
4	interdit	interdit	interdit	interdit

2. ISC atypiques de niveau *Très Secret*

Les ISC trop grands ou trop volumineux pour être enfermés dans des meubles de sécurité doivent être situés dans une zone réservée (cf. fiche 5.1) et stockés dans un local renforcé correspondant aux caractéristiques suivantes :

- l'emprise 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/bâtiment pour la classe 2.

Classe de l'emprise / bâtiment	Classe du local			
	a	b	c	d
1	autorisé	autorisé	interdit	interdit
2	autorisé (1)	autorisé (1)	interdit	interdit
3	interdit	interdit	interdit	interdit
4	interdit	interdit	interdit	interdit

(1) Le local ZR et l'emprise sont équipés de dispositifs de détection alarme indépendants.

3. Moyens mobiles du MINARM

ISC de niveau *Secret* et *Très Secret* hors classification spéciale

La protection des ISC abrités dans des moyens mobiles en opération n'est pas traitée dans la présente fiche et fait l'objet d'une directive technique particulière.

Pour les mobiles (aéronefs, navires, véhicule, etc.) abritant des ISC de niveau *Secret* et *Très Secret* hors classification spéciale en déplacement en dehors de leur entité de rattachement, les modalités de protection suivantes sont à appliquer.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES
5.2

	En terrain militaire sur le territoire national	Hors terrain militaire sur le territoire national	Zone civile sur un territoire étranger	Zone militaire sur un territoire étranger
Gardiennage par des agents du MINARM ¹³⁰ ou des FSI	Autorisé (1)	Autorisé (1)	Autorisé (1)	Autorisé (1)
Gardiennage par des sociétés en contrat avec le MINARM ou avec un OIV du MINARM	Autorisé (1)	Autorisé (1)	Interdit (2)	Interdit (2)
Autres cas	Interdit (2)	Interdit (2)	Interdit (2)	Interdit (2)

(1) à la condition de verrouiller les accès au mobile¹³¹.

(2) conservation des ISC sur l'homme en permanence (uniquement pour le Secret) ou à la mission de défense de l'ambassade.

¹³⁰ Ou, pour le CEA exclusivement, des forces locales de sécurité (FLS).

¹³¹ Le verrouillage des accès d'un aéronef consiste à la mise en œuvre d'un dispositif de verrouillage mécanique à clé et l'apposition de scellés de sûreté.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES**5.3****ACTIVITÉS NÉCESSITANT L'ACCÈS À DES INFORMATIONS ET SUPPORTS CLASSIFIES EN DEHORS DE LEUR LIEU ABRITANT****Référence :**

IGI 1300 – 5.4.3 et annexe 35

Points clés :

- Le lieu abritant **temporairement** une réunion, une conférence, une présentation de matériel mettant en œuvre des ISC ne nécessite pas l'émission d'un avis d'aptitude physique par le service enquêteur.
- Pour une réunion, tous les participants assument la pleine responsabilité de la protection de leurs documents de travail et de leurs notes, qui sont à classifier au niveau correspondant à celui des informations recueillies. Ces documents sont détruits par leurs soins dès qu'ils ont cessé d'être utiles.

1. Principes

Dès lors que des ISC sont manipulés en dehors du lieu les abritant en temps normal (dans le cas, par exemple, d'une réunion, d'une conférence ou d'une présentation de matériel), l'autorité organisatrice applique les recommandations suivantes avant, durant et après la communication des ISC. Sa responsabilité pénale est, en cas de compromission, susceptible d'être engagée sur le fondement de l'article 413-10 du code pénal. Cela ne désengage cependant pas le détenteur de sa responsabilité. Le lieu dans lequel se déroule l'activité doit être sécurisé et son accès contrôlé. Il peut s'agir d'un lieu dédié au traitement des ISC ou d'un lieu « neutre ». Néanmoins, pour ce dernier, le niveau maximal de classification des informations évoquées au cours de la réunion ne doit pas dépasser les capacités de protection de la salle accueillant la réunion. Aucun avis préalable d'aptitude physique n'est cependant requis lorsque le lieu n'est pas dédié.

2. Choix du lieu pour l'activité

Le local prévu pour la séance au cours de laquelle sont manipulés des ISC doit répondre à des contraintes d'isolement, d'accès et de protection physique. Ainsi il est recommandé :

- d'éviter un local donnant sur l'extérieur ;
- de préférer un local à l'abri des écoutes indirectes, à l'écart des voies d'accès desservant le bâtiment ou les constructions voisines, sans mitoyenneté vulnérable sur les façades ;
- de ne pas indiquer la destination du local ;
- que le local dispose de fenêtres protégées, d'un accès unique avec une porte en bois plein ou blindée, rappel automatique et serrure de sûreté sans poignée extérieure ;
- que le local ne soit accessible qu'aux personnes autorisées pour interdire toute intrusion avant la réunion ;
- d'éviter tout élément de rangement (tiroir, meuble) ou matériel qui ne soit pas utile au déroulement de l'activité.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES

5.3

Un contrôle des lieux est effectué sous la responsabilité de l'autorité organisatrice avant, éventuellement pendant, et après l'activité.

Une attention particulière est portée aux opérations de nettoyage, d'entretien, et de réparation du local comme à ses installations annexes et aux pièces mitoyennes. L'accompagnement permanent des personnes intervenant au titre des maintenances diverses doit impérativement être mis en œuvre afin d'éviter tout piégeage des lieux.

3. Préparation de l'activité au cours de laquelle sont manipulés des ISC

Dès lors que le niveau de classification, les limites et le degré de précision à apporter dans les échanges sont connus, il faut veiller à ce que l'organisateur :

- les précise sur les invitations des participants, pour permettre la désignation de personnes habilitées au niveau requis et ayant besoin d'en connaître ;
- demande aux invités d'adresser en temps utile leurs noms et fonctions ainsi que leur niveau d'habilitation afin que puisse être établie la liste de toutes les personnes participant à la séance, à quelque titre que ce soit : auditeurs, conférenciers, assistants, techniciens chargés des projections ou essais, etc. ;
- rappelle dans l'invitation, la nécessité pour les invités d'être en possession des pièces justificatives le jour de la visite (certificat de sécurité, carte d'identité).

4. Protection des ISC au cours de l'activité

L'autorité organisatrice :

- fait accompagner les visiteurs (participants extérieurs) ;
- s'assure de l'identité et du niveau d'habilitation de chacun des participants présents au vu des certificats de sécurité (cf. fiche 3.6) ;
- s'assure que personne ne détienne d'appareils non agréés au niveau requis par l'activité permettant la captation, la réémission et l'enregistrement d'informations (téléphone mobile, ordinateur portable, objets connectés...) ¹³² ;
- peut interdire toute prise de note ou tout enregistrement des interventions par les auditeurs ;
- veille, en application des principes stricts de cloisonnement de l'information classifiée, en particulier pour le niveau *Très Secret*, dont les classifications spéciales, à ce que la communication demeure limitée à l'objet de l'activité ;
- autorise les participants à quitter le local pendant les pauses, si la sécurité des ISC qui y sont laissés est assurée ;
- prohibe les discussions relatives aux informations classifiées en dehors du local prévu ;
- notifie toute faille dans la sécurité à l'officier de sécurité qui en informe les participants.

5. A l'issue de l'activité

En cas de communication d'informations de niveau *Très Secret*, l'organisateur consigne, dans un procès-verbal succinct, à classifier éventuellement, les domaines d'information qui ont été exposés, les mesures prises pour en assurer la protection ainsi que la liste des participants avec mention de la justification de leur habilitation.

¹³² Dans le respect de la législation (Article L. 33-3 du code des postes et communications électroniques) l'usage de brouilleurs est possible.

**TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIES****5.3**

L'autorité organisatrice de l'activité veille à :

- la récupération et à la mise en sécurité des informations ou supports classifiés éventuellement mis à la disposition des auditeurs ;
- la destruction des supports provisoires et préparatoires ;
- la sensibilisation des participants sur leurs obligations en matière de protection du secret de défense¹³³.

¹³³ Tous les participants assument la pleine responsabilité de la protection de leurs documents de travail et de leurs notes, qui sont classifiés au niveau correspondant à celui des informations recueillies. Ces documents sont détruits par leurs soins dès qu'ils ont cessé d'être utiles.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES**5.4****MATERIEL D'IMPRESSION, DE REPRODUCTION ET DE DESTRUCTION DES INFORMATIONS ET SUPPORTS CLASSIFIES****Références :**

- IGI 1300 – 7.2.4 et 7.5.1
- PSSI-E – Item « Sécurisation des imprimantes et des copieurs multifonctions »

Point clé :

L'impression, la reproduction et la destruction d'ISC doivent être effectuées sur des appareils conformes et idéalement centralisés dans un même lieu.

Les procédures de destruction, d'impression et de reproduction d'ISC doivent répondre à des normes strictes. Le matériel de destruction et d'impression/reproduction de la documentation classifiée de niveau *Très Secret* ou *Secret* doit être centralisé chaque fois que cela est possible.

Il faut placer des signalisations interdisant la destruction ou l'impression/reproduction sur les appareils non conformes ou non retenus pour la destruction de la documentation classifiée.

Une note interne est rédigée sur la gestion des ISC sous forme de fiches réflexes à destination des secrétariats et du personnel, spécifiant les procédures d'impression/reproduction et de destruction des ISC (cf. fiches 7.9 et 7.13).

1. Matériel de destruction des ISC

Le moyen le plus couramment utilisé pour détruire les documents papier est le déchiquetage, qui consiste à réduire le support en lambeaux (particules de moins de 10 mm² et de largeur inférieure à 1 mm).

Le matériel utilisé doit respecter la norme DIN 66399 classe 3, dont seules les catégories P6 et P7 sont adaptées aux exigences de sécurité pour les documents de niveaux *Secret* et *Très Secret*.

L'ancienne norme DIN 32757 reste également valable mais pour sa seule catégorie P5.

2. Matériel d'impression et de reproduction des ISC

De nombreux périphériques de réseaux modernes utilisent des disques durs sur lesquels sont stockées les données à traiter (comme les photocopieurs numériques, par exemple). Afin d'assurer une protection efficace des données traitées par ces équipements et des réseaux qui les mettent en œuvre, il est vivement recommandé d'adopter les mesures suivantes :

- ces appareils sont physiquement protégés pour en limiter l'emploi aux seules personnes autorisées ;
- ils doivent être gérés par les directions informatiques ; une vigilance particulière s'impose de la part des responsables de la sécurité des systèmes d'information ;
- dès lors que des informations sensibles, *Diffusion Restreinte* ou classifiées transitent par ce type d'appareil, l'ensemble des recommandations et réglementations relatives aux systèmes d'information traitant des informations de cette nature s'applique. Si

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES**5.4**

ces matériels sont connectés à un système d'information, ils sont intégrés dans le périmètre d'homologation du système d'information ;

- il convient de limiter au maximum le nombre de photocopieurs dédiés et autorisés à reproduire les documents sensibles, *Diffusion Restreinte* et/ou classifiés (une note interne fixant ce nombre est recommandée, de même que l'utilisation de pictogramme). Ces imprimantes/photocopieurs doivent être soit isolés, soit reliés à un réseau de même niveau de classification que l'ISC reproduit ;
- lorsque cela est possible, systématiser, en lien avec les organismes en charge de l'externalisation des prestations liées aux photocopieurs, imprimantes et autres scanners, le marquage des impressions et numérisations des documents sensibles, *Diffusion Restreinte* ou classifiés (date, heure, et référence du poste d'impression), Le recours à une identification par code/badge permet cette traçabilité ;
- les contrats de location et de maintenance doivent inclure des clauses relatives à la sécurité (rétention des disques durs, notamment) ;
- la télémaintenance est à proscrire : aucun modem ne doit être installé dans le copieur (à défaut, il doit être physiquement désactivé) ;
- l'option fax permettant un accès vers l'extérieur est proscrite : aucune carte fax ne doit être installée dans le copieur (à défaut, elle doit être physiquement désactivée) ;
- l'utilisation par le technicien de la société de maintenance d'un moyen permettant le stockage d'informations (ordinateur portable, graveur de cédéroms, disquettes, outils de stockage USB,...) est interdite. Si nécessaire, l'entité utilisant le copieur doit mettre à disposition du technicien un ordinateur sans graveur de cédéroms sur lequel sont installés les logiciels et applicatifs de maintenance nécessaires ;
- avant toute opération de maintenance, le copieur doit être débranché du réseau. Il est procédé à la photocopie de quelques feuilles contenant des informations non sensibles, puis à l'arrêt complet du copieur (mise hors tension quelques minutes) ;
- en cas de problème sur le disque dur du périphérique, celui-ci est soit réparé sur place, soit remplacé par un nouveau matériel ; l'élément remplacé doit être remis à l'OS du site pour destruction ;
- le copieur ne doit pas posséder de lecteur extérieur ou de port actif (RS 232, USB, Firewire, Wifi,...) permettant une connexion non prévue vers l'extérieur (à défaut, il doit être physiquement désactivé) ;
- pendant toute l'opération de maintenance des copieurs du site, un personnel est présent afin de contrôler l'application des règles ci-dessus ;
- ces règles doivent être affichées, de manière visible, à proximité de chaque photocopieur numérique.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET 5.5 SUPPORTS CLASSIFIES

PROTECTION CONTRE LES COMPROMISSIONS VIA LES EQUIPEMENTS ELECTRONIQUES

Référence :

IGI 1300 – 6.5.1

Points clés :

- Les équipements électroniques sont des vecteurs possibles pour capter des informations sensibles, *Diffusion Restreinte* ou classifiées par piégeage. Le piégeage de certains équipements électroniques (exemple smartphone) est considéré comme facile sans nécessiter l'accès à l'équipement.
- Il est de la responsabilité de l'officier de sécurité de fixer les règles applicables au sein de son organisme.
- Dans les zones réservées les équipements électroniques personnels (ou assimilés) sont interdits, les équipements électroniques professionnels peuvent être acceptés ou tolérés sous certaines conditions.
- Un affichage doit être mis en place et permettre de s'assurer que chacun connaît les règles applicables.

1. Vulnérabilités spécifiques des équipements électroniques

Les équipements électroniques sont des vecteurs possibles pour capter des informations sensibles, *Diffusion Restreinte* ou classifiées et sont susceptibles d'être piégés et en capacité d'exfiltrer les données classifiées, *Diffusion Restreinte* ou sensibles (échanges verbaux, fichiers informatiques, images...) à l'insu de l'utilisateur, en temps réel ou en temps différé.

Il s'agit principalement de traiter les vulnérabilités dues aux équipements électroniques munis d'un dispositif technique de captation sonore ou vidéo (ordinateurs portables, téléphones mobiles, tablettes, montres, dictaphone, écouteurs/micro sans fils, caméra,...) connectés à l'espace cybernétique (Internet, GSM, WIFI, Bluetooth, indirectement par synchronisation ou mise à jour,...).

Pour exemple, il peut s'agir d'une application pour smartphone, a priori banale, disponible en téléchargement sur un « store » et installée par le propriétaire du téléphone qui se révèle être malveillante en déclenchant un enregistrement audio sur mot-clé ou dès que le téléphone est mis en mode avion ou lorsqu'elle détecte une absence de réseau GSM (entrée en cage de faraday), l'enregistrement étant transmis dans un second temps. Ce piégeage est considéré comme facile et ne nécessite pas d'accès à l'équipement électronique. Il est également possible d'utiliser une vulnérabilité ou une porte dérobée préexistantes.

Les équipements professionnels, voire ayant fait l'objet d'un agrément par l'ANSSI (*Diffusion Restreinte* ou classifié), entrent également dans le champ de cette menace, même si leur vulnérabilité est moindre en raison des dispositions techniques ou organisationnelles prises.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET 5.5 SUPPORTS CLASSIFIES

2. Définitions

Parmi les équipements électroniques, on distinguera :

- les équipements informatiques : ordinateurs portables, tablettes-PC et tablettes. Ces objets sont généralement très connectés (WiFi, Bluetooth, réseau GSM) et sont « encombrants » (ne tiennent pas dans la poche) ;
- les équipements mobiles : téléphone, smartphone. Ces objets sont connectés à des réseaux publics et sont peu encombrants (tiennent dans la poche) ;
- les objets connectés (et assimilés) : objets munis d'un moyen de captation sonore ou vidéo et pouvant être connectés directement à un réseau public (GSM, WiFi,...) ou indirectement (synchronisation ou mise à jour *via* un ordinateur ou un smartphone).

Les équipements électroniques utilisés à des fins médicales sont exclus.

Pour chacun de ces types d'équipements électroniques, on distinguera l'usage :

- personnel : l'utilisateur est propriétaire et seul responsable de sa gestion ou de sa sécurisation
- professionnel : l'organisme a procédé à la sécurisation de l'objet et a procédé à une démarche d'homologation pour du sensible, du *Diffusion Restreinte* ou du classifié ; l'utilisateur ne peut pas modifier la configuration du système.
- professionnel « non encadré » : les équipements professionnels n'entrant pas dans la catégorie précédente.

3. Cadre général

D'un point de vue général, il est de la responsabilité de l'officier de sécurité de définir les règles en fonction de la sensibilité des activités de son entité¹³⁴. Les mesures mises en place sont proportionnées et adaptées aux spécificités et au fonctionnement de l'organisme, mais aussi des emprises, des bâtiments ou des locaux qu'elle occupe.

L'officier de sécurité peut mettre en place un zonage (par exemple *via* l'identification des bâtiments ou des bureaux et salles de réunion dans lesquels sont traitées les activités sensibles) permettant d'adapter au mieux les règles à chaque zone.

Lorsque la sensibilité des activités le nécessite, l'officier de sécurité proscrit les équipements électroniques personnels et professionnels non encadrés.

Il est mis en place des dispositifs pour permettre le stockage des équipements proscrits en nombre suffisant et aux localisations nécessaires, notamment pour rendre les conditions de travail acceptables (proximité entre les employés et leurs moyens de communication professionnels ou personnels) ou permettre l'accueil des visiteurs en toute sécurité.

Un affichage est mis en place par l'officier de sécurité pour que les règles en vigueur soient connues de tous, y compris des éventuels visiteurs.

4. Spécificités applicables pour la protection du classifié

En dehors des produits agréés pour traiter des informations classifiées, les équipements électroniques ne doivent en aucun cas être à moins de 2 mètres d'un équipement traitant d'informations classifiées.

¹³⁴ La sensibilité d'une activité dans le cadre de la présente fiche se mesure par la sensibilité des informations traitées et le volume d'informations classifiées ou *Diffusion Restreinte* traitées.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET 5.5 SUPPORTS CLASSIFIES

Dans les salles de réunion (ou autre local utilisé momentanément comme salle de réunion), les équipements électroniques non agréés (hors équipements informatiques professionnels nécessaires) sont proscrits lorsque la réunion est classifiée. Les équipements mobiles professionnels peuvent être exceptionnellement tolérés lorsqu'ils répondent à une nécessité (exemple : astreinte).

Il est également proscrit de réaliser une visioconférence avec des moyens non classifiés dans un environnement classifié afin d'empêcher la captation vidéo d'une information classifiée visible dans l'environnement.

5. Spécificités applicables aux zones réservées

Seuls les systèmes d'informations dont l'installation est prévue dans la zone réservée et homologués peuvent être présents dans la zone réservée.

Les objets personnels et les objets professionnels non encadrés sont interdits en zone réservée. L'officier de sécurité peut déroger à cette règle si une organisation est formalisée et mise en place au sein de la zone réservée pour que les activités relevant du *Très Secret* soient réalisées en l'absence d'objet personnels ou professionnels non encadrés.

Il revient à l'officier de sécurité de fixer les règles propres à la zone réservée en fonction de la classe de la zone réservée et de la nature des activités réalisées dans la zone réservée et de l'usage de chaque pièce. Les équipements électroniques professionnels peuvent être tolérés en zone réservée. Par exemple :

- un équipement électronique homologué pour le traitement d'informations de niveau *Très Secret* (exemple : ordinateur portable) ou un produit agréé *Très Secret* (exemple : TEOREM) peut être accepté ;
- un équipement mobile professionnel pour une personne devant rester joignable à tout moment (par exemple dans le cadre d'une astreinte) peut être toléré selon des conditions à définir ;
- un équipement informatique professionnel peut être toléré (exemple : ordinateur portable de travail) ;
- le téléphone professionnel d'une personne travaillant dans le service peut être toléré, par exemple lorsque cette personne n'est pas présente dans un local dans lequel du *Très Secret* est cours de traitement (i.e. audible ou visible) et qu'il peut à tout moment le déposer rapidement dans un lieu sûr en cas de besoin.

6. Autres dispositions

La localisation d'une emprise ou l'appartenance d'une personne à un organisme sont des informations qui peuvent être jugées sensibles au regard de la protection des informations. Dans ce cas, le personnel concerné est sensibilisé aux risques de géolocalisation induits par les équipements électroniques, qu'ils soient équipés d'un dispositif de géolocalisation (GPS) ou non, notamment au regard de l'usage qu'il peut en être fait, comme le suivi géolocalisé par des applications sportives. Si cette information est classifiée, une interdiction est envisagée.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES**5.6****CONTROLES D'APTITUDES PHYSIQUE A LA DETENTION D'INFORMATIONS ET SUPPORTS CLASSIFIES****Références :**

- IGI 1300 – 4.4.1.5, 5.3.3, annexes 29 à 32
- Pour les établissements du MINARM, ses établissements publics sous tutelle et les INID du CEA : IM 1544/DEF/CAB/DR du 17 janvier 2017, version du 10 août 2020, relative à la défense-sécurité des activités, moyens et installations relevant du ministère de la défense
- IM 7326/ARM/CAB (édition n°2) du 25 juin 2018 relative à la politique de sécurité des systèmes d'information du ministère des armées.

Points clés :

- La détention d'ISC dans un local est conditionnée à l'obtention d'une aptitude physique.
- L'aptitude physique est un préalable impératif à :
 - la détention d'ISC *Secret* en dehors d'une zone militaire.
 - la détention d'ISC *Très Secret*, y compris ceux faisant l'objet d'une classification spéciale au sein d'une ZR (zone réservée).
- L'aptitude physique est vérifiée par le service enquêteur et renseigne les autorités contractantes et d'habilitation sur le niveau de protection du secret atteint dans l'établissement ou l'organisme qui va exécuter les travaux classifiés.

1. Généralités

Les organismes traitant des ISC doivent au préalable obtenir un **avis technique d'aptitude physique** (ATAP). Ce dernier est obtenu après évaluation de l'aptitude des locaux. Le service enquêteur s'assure notamment que les mesures de protection physique des locaux sont cohérentes avec l'analyse de risque réalisée par l'établissement ou l'organisme. Ces mesures, qu'elles soient réglementaires ou compensatoires, doivent permettre d'entraver une atteinte à la protection du secret. Il s'assure également que le SI de sûreté fait l'objet d'une homologation de sécurité.

Enfin, dès la réception d'un ATAP, l'organisme bénéficiaire émet une « attestation de conformité physique » certifiant que les mesures de protection dont bénéficie le local sont conformes à l'ATAP.

- Pour le niveau *Secret* :

Répondant à des normes de protection imposées par les documents en référence, les locaux de stockage ou de traitement des ISC *Secret* des entités ministérielles ou à la direction des applications militaires du CEA (CEA/DAM) situées dans une zone militaire ou au CEA/DAM ne sont pas concernés par les demandes d'avis d'aptitude.

Les autres locaux que ceux évoqués précédemment doivent faire l'objet d'une demande d'avis, à l'instar des établissements disposant de locaux prévus pour détenir des ISC *Secret* dans le cadre de contrats ou des lieux abritant des ISC *Secret* au sein du MINARM situés en dehors d'une zone militaire.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES**5.6****- Pour le niveau *Très Secret* :**

Les zones réservées (militaires ou non), qui abritent des ISC *Très Secret*, y compris ceux faisant l'objet d'une classification spéciale, doivent sans exception faire l'objet d'un ATAP.

2. Le dossier d'aptitude

Dans le cas d'un contrat avec détention d'ISC, les entités candidates sont informées par l'autorité contractante des normes physiques et informatiques (cf. introduction du titre 5) imposées par la détention d'ISC auxquelles elles doivent satisfaire et des obligations induites par la détention de tels informations et/ou supports.

Un dossier d'aptitude est déposé pour chaque lieu d'exploitation ou de détention de travaux classifiés afin de solliciter un ATAP du service enquêteur.

Pour les organismes ministériels ainsi que le CEA/DAM, ce dossier comprend :

- le plan de la ZR et du bâtiment/emprise ;
- l'organisation et les moyens de protection et de gardiennage ;
- l'identification et la description de la protection, actuelle et envisagée, du local ou des locaux où sont exécutés les travaux protégés. Ceci inclut l'analyse de risque et la liste des organismes assurant l'installation et la maintenance des SI de sûreté concourant à la protection du local ainsi que l'analyse de risque réalisée dans le cadre de l'homologation de ces mêmes SI.

Pour les organismes liés au MINARM par contrat ou convention, la constitution du dossier peut prendre deux formes :

- un dossier d'aptitude complet si l'entité envisage de réaliser les travaux classifiés dans un local n'ayant pas au préalable fait l'objet d'un avis d'aptitude « sans réserve » ou si le local a fait l'objet de modifications rendant caducs les avis d'aptitude précédemment émis.
- un dossier d'aptitude allégé comprenant les copies des avis d'aptitude déjà obtenus, accompagnés des attestations de conformité correspondantes ainsi que de l'attestation de non-changement des conditions qui ont amené la délivrance de l'avis d'aptitude, si l'entité envisage de faire les travaux classifiés du contrat dans des locaux ayant précédemment fait l'objet d'avis d'aptitude physique.

Le règlement de la consultation¹³⁵ indique les documents nécessaires à la constitution du dossier d'aptitude (cf. [annexe 5](#)). Ces documents sont fournis à l'autorité contractante avec l'offre dans les délais fixés dans le règlement de la consultation.

3. Evaluation et décision d'aptitude

Dès le choix de l'attributaire, l'autorité contractante informe l'autorité d'habilitation et le service enquêteur. L'autorité d'habilitation transmet le dossier de demande d'aptitude correspondant au service enquêteur. Lors de la notification du contrat et après étude du dossier d'aptitude, le service enquêteur et l'autorité contractante établissent un

¹³⁵ « Qui pourra télécharger le règlement de consultation ? » : <https://www.ixarm.com/fr/Qui-pourra-telecharger-un>

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES**5.6**

calendrier permettant de déterminer une date de début des travaux classifiés. Ce calendrier comprend notamment :

- une date d'évaluation initiale d'aptitude physique ;
- une date d'émission d'avis d'aptitude physique.

Au sein du MINARM, l'organisme transmet son dossier d'aptitude au service enquêteur. Ils fixent ensemble le calendrier d'évaluation et d'émission de l'avis.

L'évaluation initiale de l'aptitude prend en compte un certain nombre de mesures de protection relatives au bâtiment et à l'emprise contenant le local, le local lui-même et le meuble de sécurité contenant les ISC (cf. introduction du titre 5). Elle se conclut par l'émission (cf. [annexe 6](#)) :

- d'un avis technique d'aptitude physique « sans objection », lorsque le niveau de sûreté répond aux exigences de protection des ISC. Le chef d'organisme établit alors une attestation de conformité physique (cf. IGI 1300 – annexe 26) ;
- d'un avis technique d'aptitude physique « avec réserve », lorsque le niveau de sûreté atteint ne permet pas de répondre totalement aux exigences de protection des ISC. L'avis décrit les mesures compensatoires à mettre en œuvre afin d'atteindre le seuil minimal de protection ;
- d'un avis technique d'inaptitude physique, lorsque le service enquêteur constate des carences graves dans le dispositif de sécurité. L'organisme ne peut alors pas détenir des ISC dans ses locaux.

Un avis d'inaptitude interdit formellement à l'autorité contractante de transmettre des ISC au titulaire du contrat. Il est aussi interdit à celui-ci de produire des ISC.

En cas d'avis d'aptitude « avec réserve », le chef d'organisme s'engage à effectuer une mise en conformité avant le début des travaux classifiés. Il transmet par la suite un certificat de mise aux normes de sécurité physique (cf. IGI 1300 – annexe 27) au service enquêteur, qui procède, s'il le décide, à un nouveau contrôle.

Si ces avis sont « sans réserve », les travaux classifiés attendus peuvent alors débiter.

Les ATAP et attestations d'aptitude sont transmis à l'autorité publique contractante et à l'autorité d'habilitation et sont notifiés à la personne morale afin d'autoriser le début des travaux classifiés.

L'avis d'aptitude « sans réserve » est émis avec la mention DR et, pour les organismes liés par convention ou contrat, renseigné dans SOPHIA. Dans ces conditions, les éléments constitutifs de l'avis sont renvoyés dans une annexe qui est classifiée *Secret*.

L'avis « avec réserve » est classifié *Secret*, le descriptif des mesures compensatoires y figure, et à plus forte raison dans le cas d'un avis « défavorable », où les vulnérabilités sont listées.

Si le titulaire d'un contrat ne peut pas conserver dans ses locaux un avis classifié *Secret*, il est informé oralement des mesures recommandées par le service enquêteur, qui conserve le document classifié.

Si les attestations ne sont pas parvenues dans le délai prédéfini ou si des carences sont constatées lors des contrôles effectués par le service enquêteur, une mise en demeure de se conformer aux prescriptions de la présente instruction est effectuée par l'autorité

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES**5.6**

publique contractante. Le défaut d'exécution des travaux de mise en conformité engage la responsabilité du représentant légal de la personne morale.

Les éléments constitutifs de l'ATAP sont :

- un liminaire présentant la zone et le local ;
- une première partie présentant les éléments de l'analyse de risque réalisée par l'organisme puis les constats suivant les niveaux présentés dans la fiche introductive du titre 5 : emprise/bâtiment, local, meuble ;
- une deuxième partie donnant la conclusion du service enquêteur ;
- une troisième partie (optionnelle) dédiée aux points de vigilance et aux mesures compensatoires nécessaires pour les avis avec réserve.

4. Modification de locaux ayant fait l'objet d'un ATAP

Toute modification (transformation des locaux, déménagement dans un autre local ou modification du dispositif de protection,...) implique une reconsidération de l'aptitude détenue. Le service enquêteur doit être informé de la démarche le plus tôt possible. Les éléments d'actualisation du dossier d'aptitude sont transmis au service enquêteur qui décide, si nécessaire, d'effectuer un nouveau contrôle.

Pour les organismes liés au MINARM par contrat ou convention, la modification est signalée à l'autorité contractante par le titulaire qui fournit les éléments d'actualisation du dossier d'aptitude. L'autorité contractante saisit, le cas échéant, le service enquêteur pour diligenter, si nécessaire, un nouveau contrôle d'aptitude.

Dans l'attente du nouvel avis d'aptitude, l'entité quelle qu'elle soit prend les mesures nécessaires pour assurer la permanence de la protection des ISC.

5. Commission de mise en conformité

Le titulaire du contrat peut se retrouver dans le cas où il dispose d'un local ne pouvant répondre entièrement aux dispositions réglementaires et aux clauses contractuelles de protection des ISC. Dans ce cas, à la demande du contractant et après accord de l'autorité contractante, une commission de mise en conformité réunissant le contractant, l'autorité d'habilitation, l'autorité contractante et le service enquêteur peut se réunir afin de déterminer les conditions de délivrance d'un avis d'aptitude exceptionnel et soumis à conditions.

A l'issue de cette commission, une autorisation d'exploitation, sous réserves ou à titre dérogatoire, peut être délivrée exceptionnellement si l'avis d'aptitude ne peut être prononcé et si les risques encourus sont acceptables pour toutes les participants de la commission.

Cette autorisation (cf. [annexe 7](#)) indique les conditions qui lui sont associées, à savoir :

- la date limite de validité ;
- les réserves ;
- les mesures dérogatoires autorisées par l'autorité contractante ;
- les procédures mises en œuvre pour pallier les réserves ;
- les actions à mener en vue de l'émission d'un avis d'aptitude ultérieur ;
- les échéances à respecter.

**TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIES****5.6**

Cette autorisation peut être remise en cause par une inspection, un contrôle, un audit de sécurité ou une évolution du système d'information ou du besoin.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES**5.7****ACCES DE PERSONNES NON QUALIFIEES AUX LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES****Références :**

- Code pénal – art. 413-9 à 413-12, 121-2 et 414-7
- Code de la défense – art. D. 3126-5 à 9 et D. 1221-6
- Code du travail – art. L. 8112-1, L. 8123-1, L.8123-4, L. 8114-1 et 2
- IGI 1300 – 5.3.2 et annexe 33

Points clés :

- L'accès aux lieux abritant des ISC à des personnes non qualifiées (personne non habilitée et/ou ne disposant pas du besoin d'en connaître) est possible dans les cas et conditions suivants :
 - le personnel d'intervention en matière de secours, de sécurité ou d'incendie, agissant dans des cas d'urgence, est autorisé à procéder aux opérations requises par la situation sans être soumis aux formalités ordinaires ;
 - les personnes procédant aux inspections sont autorisées par l'autorité responsable de l'emprise à pénétrer dans les zones dans lesquelles sont traités des ISC et font préalablement l'objet d'une vérification d'identité et d'un contrôle de leur qualité ;
 - l'intervention pour une prestation de service n'est autorisée que dans le cadre d'un contrat sensible justifiant une enquête administrative préalable et comportant une clause de protection du secret.
- Si, dans ces circonstances, l'une de ces personnes accède fortuitement à un document classifié et en prend connaissance, elle s'expose, en cas de divulgation, aux peines prévues aux articles 413-11 et 413-12 du code pénal.

L'accès de personnes **non qualifiées**¹³⁶ aux lieux abritant des ISC, qu'elle soit accompagnée ou non, n'est envisageable qu'en raison :

- de l'exécution d'une opération de secours, de sécurité ou d'incendie ;
- d'une mission de visite ou de contrôle prévue par la réglementation française, dont celle relative au travail ;
- d'inspections internationales effectuées en application d'une convention ;
- pour l'exécution d'une prestation de service ;
- dans le cadre d'une réquisition judiciaire (cf. fiche 5.8).

Ces personnes, en leur qualité particulière et pour l'exercice d'attributions conférées par la loi, ou dans un cadre contractuel, peuvent avoir à pénétrer dans les zones abritant des secrets **sans pour autant avoir la qualité ni la nécessité d'accéder à ces secrets**.

¹³⁶ Personne qualifiée : personne disposant du besoin de connaître une information classifiée dans le cadre de sa mission et faisant l'objet d'une décision d'habilitation au niveau requis en cours de validité.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES

5.7

1. Cas envisagés

a. Généralités

Aucun organisme ne doit faire obstacle aux missions d'inspection, d'enquête ou de contrôle par les personnes disposant pour l'exercice de leurs attributions :

- du droit d'entrer dans les lieux où travaillent des salariés ;
- de la possibilité d'effectuer les prélèvements aux fins d'analyse ;
- de se faire présenter les livres, registres et documents utiles à l'accomplissement de leur mission.

Cependant, lorsque l'organisme détient des ISC, seul le responsable de l'organisme visité peut les autoriser à pénétrer dans les zones où sont traités des ISC, et ce après contrôle de la qualité et vérification de l'identité de ces personnes. Ces personnes ne sont nullement autorisées à accéder ou prendre connaissance d'ISC. Si, dans des circonstances exceptionnelles, l'un de ces intervenants accède fortuitement à des ISC, il est tenu de ne pas les divulguer, sous peine de s'exposer aux dispositions des articles 413-11 et 413-12 du code pénal. L'OS de l'entité visitée rappelle préalablement à ces personnes les règles de protection du secret.

b. Cas d'une mission de contrôle

Les personnes procédant aux inspections (inspecteurs et contrôleurs, médecins ou inspecteurs du travail, ingénieurs de prévention, instances représentatives du personnel, etc.) et nécessitant de pénétrer dans une zone où sont traités des ISC doivent être autorisées par l'autorité responsable du site, après avoir préalablement fait l'objet d'une vérification d'identité et d'un contrôle de leur qualité. Ces personnes ne sont nullement autorisées à accéder ou prendre connaissance d'ISC.

c. Cas de l'exécution d'une opération 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.

d. Autres cas

Dans tous les autres cas, l'intervention, pour une prestation de service, de personnes non qualifiées, dans un lieu abritant des éléments couverts par le secret de la défense nationale, n'est autorisée que dans le cadre d'un contrat sensible conclu par son employeur et comportant une clause de protection du secret.

Dans le cadre de l'exécution de prestation prévue par un **contrat sensible** (cf. fiche 4.3), par exemple gardiennage de lieux abritant des éléments couverts par le secret de défense nationale, entretien ou maintenance dans de telles zones, ce contrat comporte une clause de protection du secret conforme à celle figurant à l'annexe 33 de l'IGI 1300. L'autorité contractante peut compléter ou adapter la clause selon les spécificités du contrat.

La personne morale peut faire l'objet d'une enquête administrative pour le renseignement et la sûreté préalable. Les personnes physiques associées en font l'objet systématiquement (cf. fiche 3.9). L'autorité contractante peut écarter la candidature de

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES **5.7**

la personne morale concernée à condition que l'avis ait été motivé par l'identification d'une interdiction de soumissionner¹³⁷.

Seules les personnes appartenant à l'entreprise titulaire du contrat ont le droit d'exécuter ce contrat sous réserve d'avoir fait l'objet, au préalable, d'une enquête administrative pour le renseignement et la sûreté. Les contrats de travail des personnes exécutant un contrat sensible comportent une clause de protection du secret présentée en annexe 33 de l'IGI 1300. Lorsqu'un salarié exécutant un contrat de travail ordinaire se trouve soumis aux conditions applicables aux contrats sensibles, un avenant est introduit dans son contrat de travail.

2. Action en cas de compromission

Si une personne physique non qualifiée a eu accès à un ISC (malveillance, espionnage industriel, présence dans des lieux classifiés sans raison, ...), il y a suspicion de compromission. La procédure à mettre en œuvre est la même que celle relevant d'une compromission avérée (cf. titre 8) et le service enquêteur est alerté au plus tôt.

¹³⁷ Articles 2, 45 et 46 de l'ordonnance n° 2015-899 du 23 juillet 2015 relative aux marchés publics, articles 37, 40 I 3°, 41, 42 et 47 du décret n° 2016-361, ainsi que le 14° du I de l'article 3 de l'arrêté du 29 mars 2016 fixant la liste des renseignements et des documents pouvant être demandés aux candidats aux marchés publics. L'acheteur peut tenir compte des garanties offertes en matière de sécurité des approvisionnements et des informations par les opérateurs économiques au cours du processus de sélection des candidatures ou des offres. Il peut également imposer des conditions particulières d'exécution du marché public de défense ou de sécurité.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES**5.8****ACCES DES MAGISTRATS AUX INFORMATIONS ET SUPPORTS CLASSIFIES****Références :**

- Code de procédure pénale – art. 56-4, 230-2 et 698-3
- Code de la défense – art. L. 2312-4 à L. 2312-8
- IGI 1300 – 1.2.2.2
- Note n° 331 DEF/CAB/BRES/DR du 14 avril 2011 relative à la procédure à suivre en cas de perquisition dans un lieu abritant des éléments couverts par le secret de la défense nationale ou dans un lieu « neutre ».

Points clés :

- Une perquisition ne peut être effectuée que par des magistrats ou des officiers de police judiciaire, selon les cas. Ils peuvent saisir des ISC mais ne sont pas autorisés à en prendre connaissance à ce stade de la procédure.
- Les éléments utiles à la justice sont déclassifiés avant d'être versés à la procédure. Seul le ministre de la défense peut prendre une décision de déclassification¹³⁸.
- Pour saisir des ISC dans un lieu abritant, le magistrat doit être accompagné du président de la commission du secret de la défense nationale (CSDN) ou de son représentant ou de son délégué dûment habilité.
- Seul le président de la CSDN, son représentant¹³⁹, et, s'il y a lieu, les personnes qui l'assistent peuvent prendre connaissance d'éléments classifiés et vérifier s'ils concernent les infractions sur lesquelles portent les investigations.
- Les autorités responsables des lieux abritant des ISC sont tenues de diffuser à l'intention de leurs personnels les consignes prescrivant la conduite à tenir en cas de perquisition, afin de faciliter le déroulement des opérations.
- Lors d'une audition, aucun personnel n'est autorisé à s'exprimer au sujet d'une information classifiée avant que celle-ci ne soit déclassifiée.

Il n'est pas tenu compte dans la présente fiche de l'exception que constituent les magistrats de la formation spécialisée du Conseil d'Etat chargée du contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'Etat et la défense (cf. IGI 1300 – 1.2.2.2.b).

1. Compétences

Le détenteur d'une information classifiée a le devoir d'en refuser la communication à un tiers, même s'il s'agit d'un magistrat ou d'un officier de police judiciaire (OPJ). Pour être consultés par un magistrat ou un OPJ, les éléments classifiés sont au préalable déclassifiés sur décision du ministre¹⁴⁰ (après avis de la CSDN).

¹³⁸ A l'exception des ISC dont il n'est pas l'autorité émettrice.

¹³⁹ Membre de la commission ou un délégué choisi sur une liste établie par la commission.

¹⁴⁰ A l'exception des ISC dont il n'est pas l'autorité émettrice.

TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIES 5.8

a. Lieux abritant des éléments couverts par le secret de la défense nationale

Une perquisition envisagée dans un lieu précisément identifié comme abritant des éléments couverts par le secret de la défense nationale, ne peut être effectuée que par un magistrat. Il est accompagné du président de la CSDN (ou son représentant ou délégué dûment habilité). Nul ne peut s'opposer à l'action de ce dernier pour aucun motif que ce soit. Ils peuvent être chacun accompagnés de personnes les assistant pour procéder aux investigations. **Le chef d'établissement accompagné de son OS, son délégué, ou le responsable du lieu sont présents pendant la perquisition.**

Seul le président de la CSDN, son représentant ou son délégué dûment habilité et, s'il y a lieu, les personnes qui l'assistent peuvent prendre connaissance d'éléments classifiés découverts sur les lieux. Le magistrat et les personnes qui l'assistent (y compris des OPJ habilités pour d'autres missions) ne peuvent en aucun cas prendre connaissance d'éléments classifiés : l'administration a le devoir de s'opposer à une telle communication qui constituerait une compromission. L'accès par le magistrat à un ISC dématérialisé est traité comme l'accès à un ISC papier : seul le représentant de la CSDN est autorisé à accéder au système d'information et les modalités techniques de constitution des scellés sont adaptées.

b. Lieux « neutres »

Une perquisition dans un lieu dit « neutre » est effectuée selon les règles de droit commun, par les OPJ ou le magistrat. Au cours de la perquisition, l'enquêteur ne peut prendre connaissance d'éléments classifiés en cas de découverte fortuite d'ISC. Le magistrat, s'il n'est pas présent, en est avisé sans délai. Il prévient alors le président de la CSDN. Les opérations sont suspendues tant que ce dernier, ou son représentant, n'est pas présent. Si ce dernier, ou son représentant, ne peut se déplacer pour assister physiquement à la perquisition, le magistrat ou l'OPJ transmettent à la CSDN les documents placés sous scellés par tout moyen en conformité avec la réglementation applicable au secret de la défense nationale.

Le déroulement d'une procédure de perquisition est précisé à l'article 56-4 du CPP et dans l'IGI 1300 (§ en référence).

2. Conduite à tenir en cas de perquisition

L'autorité responsable du site – ou son OS - transmet aux personnes affectées sur le site des consignes relatives à la conduite à tenir en cas de perquisition, tout particulièrement lorsqu'il s'agit d'un lieu référencé comme « abritant » des ISC. Elles visent à faciliter le bon déroulement de l'opération tout en garantissant la protection du secret :

- a. Demander au magistrat la **décision de perquisition** qui doit être écrite et motivée : elle doit indiquer la nature des infractions sur lesquelles portent les investigations, les raisons et l'objet de la perquisition et les lieux précisément visés par la perquisition.
- b. **Relever l'identité** des personnes et s'assurer que les lieux perquisitionnés sont bien ceux inscrits sur la décision de perquisition (des confusions sont possibles).

**TITRE 5 : SECURITE DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIES****5.8**

- c. S'il s'agit d'un lieu abritant, s'assurer de la présence du magistrat et du président de la CSDN (ou de son représentant ou délégué dûment habilité). Les opérations de perquisition ne peuvent débuter qu'en leur présence.
- d. **Informé dans les meilleurs délais sa hiérarchie** de la démarche judiciaire.
- e. **Cas 1** : Si le magistrat saisit des originaux dans un lieu abritant, **des copies doivent être laissées** à leur détenteur. Les éléments éventuellement saisis sont remis au président de la CSDN ou son représentant ou délégué dûment habilité et placés sous scellés durant les opérations, sans que le magistrat ait pu prendre connaissance de leur contenu. Ils ne peuvent être versés à la procédure qu'après déclassification.

Cas 2 : Si des ISC sont découverts dans un lieu neutre, l'OPJ avise immédiatement le magistrat mandant. Le président de la CSDN est alerté et les documents saisis lui sont transmis. **Des copies des documents doivent être laissées** à leur détenteur. Les ISC sont placés sous scellés durant les opérations, sans que le magistrat ou l'OPJ ait pu prendre connaissance de leur contenu. Ils ne peuvent être versés à la procédure qu'après déclassification.
- f. **Rendre compte à sa hiérarchie** du déroulement de la perquisition.

3. Cas particulier des auditions

Aucune autorité administrative ne peut autoriser l'un de ses agents à s'exprimer au sujet d'une information classifiée avant que celle-ci ait été préalablement déclassifiée. Si une autorité judiciaire interroge une personne sur des éléments couverts par le secret de la défense nationale, celle-ci doit donc refuser de répondre en rappelant les dispositions applicables en matière de protection du secret de la défense nationale.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE

REMARQUES GENERALES

Le présent titre 6 ne s'applique qu'aux seules entités contractantes du MINARM et du CEA/DAM pour les systèmes d'information qu'elles exploitent pour l'exécution du contrat, quel qu'en soit le niveau de classification. Il s'inscrit en complément des réglementations en vigueur (IGI1300, II901, dispositif SAIV, etc.) sans se substituer à ces dernières. Il apporte certaines précisions sur ces différentes réglementations, vise à apporter une harmonisation et à préciser les interactions entre les entités contractantes et le ministère des armées. Dans certains cas, lorsque le ministère l'a jugé utile, il rappelle certaines mesures de la réglementation et peut apporter des mesures complémentaires.

En ce qui concerne les systèmes livrés par les entités contractantes, les dispositions spécifiques prévues au contrat s'appliquent, qu'il s'agisse de méthodologie ou de mesures spécifiques. Sauf disposition prévue par le contrat, le système livré doit être conforme à la réglementation pour le niveau de classification des informations qu'il traitera en exploitation par le ministère.

Les plates-formes représentatives ou de qualification des systèmes d'armes sont généralement construites dans le cadre du processus d'ingénierie. Contrairement aux autres systèmes détenus par l'industriel, la sécurité de ces plates-formes est fixée par les dispositions contractuelles, notamment les questions de représentativité du système d'arme ou de conformité à la réglementation.

Les entités relevant du ministère doivent appliquer l'IM7326 (politique de sécurité des systèmes d'information). Les entités publiques sous tutelle du ministère appliquent également l'IM7326, sous couvert de l'autorité du ministère responsable de la tutelle qui pourra en préciser les éventuelles modalités d'application.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.1****CARTOGRAPHIE DES SYSTEMES D'INFORMATION DES ENTITES CONTRACTANTES****Références :**

- Code de la défense – Art. L.1332-6-1 à L.1332-6-6
- IGI 1300 – 6.1
- II n°901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles
- Cartographie du système d'information, guide de l'ANSSI d'élaboration en 5 étapes

Points clés :

- La cartographie permet une connaissance complète des systèmes d'information de l'entité.
- Son contenu est décrit dans la PSSI de l'entité contractante.

La cartographie apporte une connaissance complète de l'environnement du système d'information (SI), de ses interactions avec l'extérieur et de toute son infrastructure technique. Cette connaissance détaillée permet de réagir plus efficacement en cas d'incident (cf. fiche 8.2).

La cartographie des SI est établie sous la responsabilité de l'autorité qualifiée. Elle fournit la connaissance du système d'information global de l'entité (**classifié et non classifié**) et permet notamment d'appréhender les principaux risques sur son activité. Cette cartographie est également nécessaire à l'identification initiale des Systèmes d'Information d'Importance Vitale (SIIV) et des systèmes d'information traitant des informations sensibles, *Diffusion Restreinte* ou classifiées.

L'autorité qualifiée en SSI de l'entité contractante précise dans la PSSI le contenu exact de la cartographie qui comprend au moins selon les recommandations de l'ANSSI :

- la description fonctionnelle et les lieux d'installation du SI et de ses différents sous-réseaux et, le cas échéant, les plages d'adresses associées aux différents sous-réseaux composant le système d'information ;
- la description fonctionnelle des points d'interconnexion du SI et de ses différents sous-réseaux avec des réseaux tiers, notamment la description des équipements et des fonctions de filtrage et de protection mis en œuvre au niveau de ces interconnexions ;
- l'inventaire et l'architecture des dispositifs d'administration du SI permettant de réaliser notamment les opérations d'installation à distance, de mise à jour, de supervision, de gestion des configurations, d'authentification ainsi que de gestion des comptes et des droits d'accès ;
- la liste des comptes disposant de droits d'accès privilégiés au SI. Cette liste précise pour chaque compte le niveau et le périmètre des droits d'accès associés ;
- les équipements d'import et d'export de données ;
- l'inventaire, l'architecture et le positionnement des services de communication et d'accès distant mis en œuvre par le SI.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.1**

Les éléments de cartographie ainsi réunis sont des documents sensibles susceptibles de contenir des informations couvertes par le secret de la défense nationale.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.2****LE PROCESSUS D'HOMOLOGATION****Références :**

- Directive européenne « NIS¹⁴¹ » (Network and Information Security - directive sur la sécurité des réseaux et des systèmes d'information »)
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, dite « loi informatique et libertés » (LIL), reste applicable, dans une version remise à jour par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, complétée par ses décrets d'application
- Articles L.1332-6-1 à L.1332-6-6 du code de la défense
- IGI 1300 – 6.1
- Il n°901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles
- Référentiel général de sécurité - version 2.0 du 13 juin 2014

Points clés :

- L'homologation d'un SI consiste à évaluer les risques encourus afin de les traiter ou de les accepter. Elle fournit un niveau de confiance dans l'usage et la protection des informations et du système d'information.
- La démarche d'homologation est un préalable à toute mise en service d'un SI, quel que soit son niveau de sensibilité ou de classification.
- La démarche d'homologation est globale : elle doit prendre en compte l'écosystème métiers et IT, aussi bien interne qu'externe, dans lequel le SI concerné s'intègre dans toutes ses phases de vie.

1. La démarche d'homologation

La démarche d'homologation s'intègre dans le cycle de vie d'un système d'information (SI). Elle repose sur une analyse de risque globale et prend en compte tous les éléments indispensables au fonctionnement et à la sécurité du système. Elle permet de s'assurer que les risques pesant sur ce système au regard des objectifs de sécurité, dans son contexte d'emploi, sont connus et maîtrisés. À cet effet, elle consiste à trouver le juste équilibre entre les risques résiduels acceptables, les actions à conduire pour la sécurisation et les contraintes techniques ou organisationnelles, en prononçant les arbitrages nécessaires, de manière formelle, par un responsable qui a autorité pour le faire.

L'homologation de sécurité d'un SI correspond à une démarche globale : le périmètre du SI à homologuer comporte tous les éléments indispensables au fonctionnement et à la sécurité du système. Il inclut les éléments fonctionnels et d'organisation, les éléments techniques, ainsi que le périmètre géographique et physique. L'homologation tient compte de l'environnement numérique du système d'information comme les systèmes en interface, les équipements externes pouvant être connectés au système, notamment lors d'opération de maintenance, etc.

La démarche d'homologation débute par la définition de la stratégie d'homologation qui a pour objectif de préciser :

¹⁴¹ http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.FRA&toc=OJ.L:2016:194:TOC

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.2**

- la cible de l'homologation (le périmètre du système, le ou les référentiels réglementaires applicables) ;
 - les étapes de la démarche d'homologation ;
 - les acteurs concernés, les actions à réaliser et les livrables attendus ;
 - la liste des documents constituant le dossier d'homologation.
- Remarque : La stratégie d'homologation peut être commune à plusieurs systèmes d'information, permettant ainsi de mettre en place une démarche d'homologation cohérente sur un système plus global.

La démarche d'homologation doit être adaptée aux enjeux et éviter la « sur-sécurité » ou encore la multiplication de documents fastidieux, inadaptés ou inefficaces. Il convient donc de catégoriser les systèmes d'information pour éviter de conduire des démarches d'homologation complexes, coûteuses et finalement inadaptées à leurs besoins de sécurité. La catégorisation du SI dépend essentiellement de deux paramètres : son exposition et sa criticité.

- L'exposition d'un SI se mesure par le nombre de point d'entrées et de chemins d'attaques ouverts à un attaquant. L'exposition est directement liée au nombre d'interactions avec d'autres SI et à l'accessibilité depuis des milieux plus ou moins maîtrisés. Elle est au contraire réduite par un isolement des réseaux mais aussi grâce à la sécurisation de l'environnement du SI (réseau support, hébergement et politiques de sécurisation associées, organisation de la SSI, sensibilisation, sécurité physique, etc.). Ainsi, un SI hébergé dans un environnement sécurisé et conforme aux exigences de ce dernier ne présentera qu'une faible surface d'attaque limitant ainsi les besoins d'étude de risques.
- La criticité d'un SI est directement liée à l'impact qu'une attaque pourrait avoir sur les missions et les activités de l'entreprise et celles de l'autorité contractante, les personnes et les biens.

Les méthodes et critères précis de catégorisation sont définis par l'autorité qualifiée d'un SI. La catégorisation d'un SI est validée formellement par l'autorité qualifiée, en accord avec l'autorité contractante.

Afin de simplifier le processus, l'opérateur privé peut définir des stratégies types d'homologation adaptées à la catégorisation des SI choisie.

La démarche d'homologation pourra distinguer une homologation de référence du SI et une ou des homologations de déploiement. L'homologation de déploiement est la décision préalable à l'exploitation du SI en contexte opérationnel attestant de la conformité à l'homologation de référence et, le cas échéant, du traitement des non-conformités.

La rédaction de la stratégie d'homologation peut s'appuyer sur le guide de l'ANSSI¹⁴².

La stratégie d'homologation doit faire l'objet d'une validation formelle par l'autorité d'homologation. Pour les systèmes d'information classifiés et pour les systèmes *Diffusion Restreinte* les plus exposés et critiques (cf. catégorisation des SI mentionnée ci-dessus), la validation de la stratégie d'homologation est faite en accord avec l'autorité

¹⁴² <https://www.ssi.gouv.fr/guide/lhomologation-de-securite-en-neuf-etapes-simples/>

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.2**

contractante sur avis de la DRSD. La validation de la stratégie d'homologation doit intervenir au plus tôt du cycle de vie du système, idéalement dès la phase de conception. La démarche d'homologation s'appuie sur une analyse de risque qui décrit et caractérise particulièrement :

- la menace cyber contextualisée pesant sur le SI, notamment les sources de risque intentionnel (profils d'attaquant, objectifs visé, etc.)
- le niveau de dangerosité des parties prenantes de l'écosystème du fait des interactions métiers et IT qu'elles entretiennent avec le SI dans ses différentes phases de vie ;
- les scénarios de risques intentionnels décrivant les chemins d'attaque et les modes opératoires susceptibles d'être orchestrés par les sources de risque, y compris *via* les parties prenantes de l'écosystème (attaques par rebond, *supply chain attacks*, etc.).

Il est recommandé de réaliser l'analyse de risque selon la méthode EBIOS Risk Manager de l'ANSSI.

2. L'autorité d'homologation

Pour les systèmes d'information appartenant ou mis en œuvre par un opérateur privé, l'autorité d'homologation est désignée dans les conditions suivantes :

- dans le cas où le système d'information traite d'informations classifiées au niveau *Très Secret* « classification spéciale », le SGDSN est l'autorité d'homologation ;
- dans le cas où le système d'information est amené à traiter des informations classifiées de l'UE, y compris au niveau R-UE/EU-R, ou de l'OTAN, l'autorité d'homologation est désignée par le SGDSN ;
- dans le cas d'une interconnexion entre un système d'information *Secret* ou *Très Secret* et un système d'information d'un niveau de classification différent ou non classifié, si l'utilisation de dispositifs agréés est impossible, l'autorité d'homologation est l'ANSSI ou toute autorité qu'elle désigne ;
- dans le cas d'une passerelle entre un système d'information *Secret* ou *Très Secret* et un système d'information qui n'est pas sous maîtrise nationale, si l'utilisation de dispositifs agréés est impossible, l'autorité d'homologation est l'ANSSI ou toute autorité qu'elle désigne ;
- dans les autres cas, notamment lorsque le système d'information traite d'informations non classifiées ou classifiées au niveau *Secret* ou *Très Secret*, la désignation de l'autorité d'homologation relève de la responsabilité de l'autorité qualifiée de l'opérateur privé.

L'autorité d'homologation est responsable de prendre la décision d'accepter les risques résiduels ; à ce titre, lorsque cela est possible, elle doit en principe être l'autorité chargée de l'emploi du système ou dans la chaîne d'emploi du système.

Il est possible de distinguer l'autorité d'homologation qui prononcera l'homologation de référence d'un système et l'autorité (ou les autorités) d'homologation qui prononcera les homologations de déploiement.

3. Réglementation applicable

Certaines procédures et mesures de sécurité sont imposées, *a priori*, sur le système par la loi ou la réglementation afin d'instaurer un socle jugé minimal de sécurité pour les systèmes d'information :

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.2**

- d'importance vitale (SIIV) ;
- essentiels (SE) [NIS] ;
- sensibles ou *Diffusion Restreinte* (II901) ou classifiés (IGI1300) ;
- établissant des échanges entre administrations ou réalisant des télé-services au profit des citoyens [RGS] ;
- traitant de données à caractère personnel (DCP), [Loi I&L] ;
- relevant des dispositions de la présente instruction.

En fonction de la nature du système d'information objet de l'homologation, il peut être parfois impossible pour des raisons techniques ou opérationnelles de se conformer à certaines mesures de sécurité. Par exemple, l'authentification forte de l'utilisateur sur un système d'arme comme un missile air-air peut apparaître peu pertinente. Les non conformités éventuelles doivent figurer dans le dossier d'homologation, doivent y être justifiées et les éventuels risques associés doivent être identifiés.

Lorsque plusieurs réglementations s'appliquent sur un même SI, la démarche d'homologation et la décision d'homologation sont uniques et couvrent l'ensemble des réglementations applicables.

4. Le dossier d'homologation

La composition du dossier d'homologation est fixée dans la stratégie d'homologation. Il contient généralement une sélection des documents suivants :

- une description du système d'information (son utilité, son cadre d'emploi, les composants matériels et logiciels, l'architecture réseau logique et physique, les utilisations, administrateurs et responsables de sécurité, les références des plans contractuels) ;
- les objectifs de sécurité du système d'information ;
- la politique de sécurité du système d'information¹⁴³ ;
- les procédures d'exploitation de la sécurité (PES) ;
- 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 de sécurité à destination des utilisateurs et des administrateurs ;
- 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 risque et les mesures de mitigation envisagées.

Pour les SI classifiés, le dossier d'homologation doit contenir :

- les avis techniques d'aptitude physique (ATAP) ;
- sauf dérogation de la DRSD et de l'autorité contractante, l'avis technique d'aptitude informatique (ATAI) (Cf. fiche 6.3)

¹⁴³ Généralement, il s'agit de la politique de sécurité des systèmes d'information applicable au sein de l'organisme éventuellement complété d'éléments propre au système d'information considéré.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.2**

- et les autres documents prévus par l'IGI1300.

Conformément à l'IGI1300, la nécessité du versement de chacun de ces documents au dossier d'homologation est évaluée et justifiée au regard des enjeux du système d'information. Si un document n'est pas versé au dossier d'homologation, la justification associée y figure.

Le dossier d'homologation, particulièrement la politique de sécurité du SI et le plan d'amélioration continue de la sécurité, présente les mesures de sécurité en profondeur suivantes :

- protection : mesures visant à réduire les vulnérabilités et facteurs d'exposition du SI (surface d'attaque) ;
- défense : mesures visant à superviser le SI, détecter les événements de sécurité et anticiper la réponse à un incident ;
- résilience : mesures visant à gérer les situations de crise et à assurer la continuité et reprise d'activité ;
- gouvernance : mesures visant à définir une organisation de management des risques cyber adaptée, agile et réactive pour le SI.

5. 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. Une telle commission comprend notamment des représentants des utilisateurs du système et des responsables de l'exploitation et de la sécurité du système.

Pour les SI classifiés, la DRSD¹⁴⁴ est membre de droit de la commission. Pour les autres SI, la DRSD est systématiquement informée et membre de la commission si nécessaire. Les autorités contractantes sont membres de droit des commissions d'homologation. Si elles le jugent nécessaire, elles peuvent solliciter le FSSI du Ministère des Armées. Afin de leur permettre d'apprécier la nécessité de leur participation, l'autorité d'homologation les informe, dans un délai raisonnable, de la date de la commission et leur transmet, le cas échéant, le dossier d'homologation.

Au titre de la maîtrise du risques cyber au sein de l'industrie de défense, la DGA doit pouvoir accéder aux informations concernant l'état de cybersécurité de leurs SI et participer aux commissions d'homologation de ces SI.

En tant qu'autorité nationale en matière de sécurité des systèmes d'information, l'ANSSI conserve la possibilité de participer à toute commission d'homologation d'un SI classifié. Elle en est membre de droit lorsque le SGDSN est l'autorité d'homologation.

6. Décision d'homologation

La décision d'homologation constitue le premier aboutissement de la démarche d'homologation, le cas échéant après avis de la commission d'homologation. Elle se traduit par l'attestation formelle de l'autorité d'homologation et précise les éventuelles conditions d'emploi, que le SI considéré est protégé conformément aux objectifs de

¹⁴⁴ Ou la DGSE, le cas échéant.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.2**

sécurité fixés. Ces objectifs sont généralement exprimés en termes de confidentialité, d'intégrité, de disponibilité et de traçabilité.

L'autorité d'homologation accepte les risques résiduels de sécurité, en pleine connaissance des vulnérabilités du système d'information qui sont liées notamment :

- aux usagers
- aux interconnexions avec d'autres systèmes ;
- aux supports amovibles ;
- aux accès à distance par des utilisateurs « nomades » ;
- aux moyens de visualisation et d'hébergement des informations classifiées ;
- aux opérations de maintenance, d'exploitation ou de télégestion du système, notamment lorsqu'elles sont effectuées par des prestataires externes.

Un SI classifié protège des informations classifiées soit transmises par le ministère pour l'exécution du contrat, soit élaborées dans le cadre du contrat au profit du ministère. La compromission de ces informations est de nature à remettre en cause les intérêts fondamentaux de la nation. Par ailleurs, la perte d'intégrité d'information sur des SI protégeant des informations de niveau *Diffusion Restreinte* ou classifié peut entraîner le sabotage d'un système d'armes (rendre le système d'armes non fonctionnel, non conforme aux performances attendues, non intègre, permettre sa prise de contrôle par un attaquant). Ainsi, de façon exceptionnelle, pour les SI classifiés ou protégeant des informations de niveau *Diffusion Restreinte*, si le niveau de risque est jugé inacceptable par la DRSD et par l'autorité contractante, et pourrait mettre en péril la confidentialité, la disponibilité ou l'intégrité d'informations *Diffusion Restreinte* ou classifiées de défense, alors l'autorité d'homologation n'est pas autorisée à prononcer l'homologation du SI. Dans ce cas exceptionnel, avec l'accord de la DRSD et de l'autorité contractante, une « Autorisation Provisoire d'Emploi » (APE) peut être proposée à l'autorité d'homologation. La durée de validité d'une APE est de 6 mois maximum et est renouvelable au plus une fois.

La décision d'homologation doit intervenir avant la mise en service opérationnelle du système.

La décision d'homologation est prononcée pour une durée maximale :

- de cinq ans pour un SI traitant de données non protégées, sensibles ou *Diffusion Restreinte* ;
- de trois ans pour un SI au niveau *Secret* ;
- de deux ans pour un SI au niveau *Très Secret* ou traitant d'informations classifiées au niveau *Très Secret* « classification spéciale ».

Cette durée d'homologation peut être réduite par une réglementation plus contraignante, comme celle concernant les systèmes d'information d'importance vitale.

Dans le cas d'une Autorisation Provisoire d'Emploi peut être proposée à l'autorité d'homologation. La durée de validité d'une APE est de 6 mois maximum et est renouvelable au plus une fois.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.2**

La DRSD et l'autorité contractante sont destinataires de toute décision d'homologation¹⁴⁵ ou d'autorisation provisoire d'emploi. Elles peuvent demander le dossier d'homologation correspondant.

7. Contrôle et renouvellement de l'homologation

Conformément aux instructions de la PSSI de l'opérateur privé, l'autorité d'homologation fixe les conditions du maintien de l'homologation de sécurité au cours du cycle de vie du système d'information. Elle contrôle régulièrement que le système fonctionne effectivement selon les conditions qu'elle a approuvées, en particulier après des opérations de maintien en condition opérationnelle et de maintien en condition de sécurité (MCS).

L'autorité d'homologation examine le besoin de renouvellement de l'homologation avant le terme prévu sur la base du dossier tenu à jour par le Responsable de la Sécurité du SI.

Une nouvelle décision d'homologation est nécessaire lorsque :

- les conditions d'exploitation du système ont été significativement modifiées ;
- des nouvelles fonctionnalités ou applications ont été installées ;
- le système a été interconnecté à de nouveaux systèmes ;
- des problèmes d'application des mesures de sécurité ou des conditions de maintien de l'homologation ont été révélés ;
- les menaces sur le système ont évolué ;
- de nouvelles vulnérabilités ont été découvertes ;
- le système a fait l'objet d'un incident de sécurité ;
- un ATAI défavorable ou, à la demande de la DRSD et de l'autorité contractante, un ATAI avec réserve.

Le Responsable de la Sécurité du SI analyse les événements pouvant remettre en cause l'homologation et, en fonction des impacts, il sollicite ou non l'autorité d'homologation via la commission d'homologation pour la conduite à tenir.

L'autorité d'homologation est responsable de contrôler le niveau de sécurité atteint du système (cf. fiche 6.4).

La DRSD, l'autorité contractante ou l'autorité d'habilitation peuvent contrôler eux-mêmes ou faire contrôler le niveau de sécurité atteint et la maîtrise des risques du système. Dans le cas d'un système classifié, si ce contrôle est réalisé par la DRSD, il donne lieu à un ou plusieurs ATAI. Dans un système *Diffusion Restreinte*, le contrôle donne lieu à un avis sur le niveau de sécurité et si besoin des recommandations.

Sauf dérogation de la DRSD et de l'autorité contractante, le renouvellement d'une homologation nécessite un nouvel avis technique d'aptitude informatique (ATAI).

¹⁴⁵ Les décisions d'homologation relatives aux entités contractantes avec la DGSE répondent à une procédure spécifique.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.3****CONTRÔLE D'APTITUDE AU TRAITEMENT D'INFORMATIONS NUMERIQUES CLASSIFIEES****Références :**

- IGI 1300 – annexe 30
- DTM 63
- II 300, directives 485 et 495
- Guide DGA de rédaction DSSI

Points clés :

- Les systèmes d'information classifiés sont homologués pour être utilisés. Dans ce cadre, un avis technique d'aptitude informatique (ATAI) est nécessaire sauf dérogation prévue par la présente fiche.
- L'ATAI est émis par la DRSD et informe les autorités contractantes et l'autorité d'homologation du niveau de protection du secret atteint sur le système d'information de l'entité.

1. Généralités

Pour les SI classifiés intéressant la défense, la DRSD contrôle le niveau de sécurité et s'assure que les risques cyber sont maîtrisés. Ce contrôle donne lieu à un ou plusieurs avis d'aptitude informatique (ATAI). Un ATAI est généralement nécessaire dans le cadre de l'homologation ou des renouvellements d'homologation.

Afin de produire un ATAI, la DRSD¹⁴⁶ s'assure en particulier que :

- Pour les contrats classifiés intéressant la défense, le niveau de classification du système d'information est conforme aux prescriptions du plan contractuel de sécurité du contrat.
- Les constituants physiques du système d'information sont situés dans des locaux ayant fait l'objet d'un avis technique d'aptitude et que, le cas échéant, les liens informatiques cheminant hors de ces locaux font l'objet d'une approbation conformément à la fiche 6.10.
- Les mesures de protection contre les signaux parasites compromettants sont conformes.
- Les personnes ayant accès au système d'information ou à ses constituants physiques sont habilitées au niveau idoine.
- Les supports numériques classifiés (ISC) sont dûment marqués et enregistrés

Pour les systèmes d'information de niveau *Très Secret*, la DRSD s'assure de plus que :

- les résultats de mesures d'atténuation électromagnétiques (Tempest) réalisées par un organisme accrédité identifient les locaux utilisés comme aptes à traiter des informations numériques classifiées au niveau *Très Secret* en fonction des caractéristiques des équipements présents.
- les locaux identifiés sont érigés en zone réservée incluse dans une zone protégée.

¹⁴⁶ Ou la DGSE pour les contrats qui la concernent.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.3**

L'élaboration de l'avis d'aptitude informatique est réalisée à partir d'une *évaluation in situ* préparée à partir de documents prévus dans le dossier d'homologation (notamment le document de description du système d'information et des informations du DSSI¹⁴⁷).

2. Évaluation de l'aptitude technique informatique

La DRSD réalise *in situ* et en tant que de besoin des contrôles sur les conformités réglementaires et la bonne application de l'état de l'art en matière de sécurité informatique. Elle apprécie l'efficacité et la complétude des mesures de sécurité déployées par l'entité visant à amener les risques identifiés à un niveau acceptable. La DRSD notifie l'avis qu'elle a élaboré à l'entité et à l'autorité contractante.

a. Avis favorable

Le niveau de sécurité est jugé satisfaisant et les risques cyber semblent maîtrisés. Un avis favorable peut également être émis si le plan d'actions de l'entité contractante apporte un niveau de confiance suffisant dans l'atteinte d'un niveau satisfaisant et dans la maîtrise des risques cyber.

b. Avis avec réserves

Lorsque le niveau de sécurité n'est pas jugé satisfaisant ou que la maîtrise des risques cyber doit être améliorée, un avis avec réserves est émis. Il définit un plan d'action supplémentaire en vue de diminuer ou d'annuler les risques identifiés et jalonne la mise en conformité des SI concernés en complément des actions élaborées dans le cadre de l'homologation.

Des réserves peuvent être formulées en cas de :

- absence de fourniture par l'entité d'un ou plusieurs documents nécessaires à l'évaluation du système d'information par la DRSD dans des délais compatibles avec l'exécution du contrat classifié ;
- non-conformité réglementaire ;
- identification de lacunes techniques ou organisationnelles faisant peser sur les informations classifiées de défense un risque non négligeable.

Un délai compatible avec l'exécution du contrat est défini par la DRSD afin que les mesures soient prises par l'entité, permettant de lever les réserves avant l'homologation du système d'information.

Au terme du délai imparti, la DRSD procède aux contrôles visant à lever les réserves. Un avis favorable peut alors être émis si les contrôles sont positifs. Dans le cas contraire, les réserves existantes sont notifiées à l'autorité contractante.

¹⁴⁷ Le DSSI est un dossier d'identité et de description d'un SI. Il n'a pas besoin d'être tenu à jour, mais les informations qui le constituent doivent être tenues à jour par ailleurs. Une version à jour doit pouvoir être fournie à la demande de l'autorité contractante, de l'autorité d'habilitation ou du service enquêteur. Le DSSI contient les informations nécessaires pour connaître le système d'information et en évaluer la sécurité dans le cadre d'une inspection, d'un contrôle, d'un audit, d'un ATAI : informations sur la société, l'établissement concerné, et sur le SI ou réseau concerné (en particulier sa description et l'ensemble des procédures de sécurité applicables, qu'elles soient particulières au SI ou relevant de l'établissement ou de la société concernés). Le format du DSSI est précisé dans les contrats et le modèle par défaut et disponible sur le site IXARM. Afin de ne pas dupliquer des informations qui seraient déjà demandées au titre du dossier d'homologation, le DSSI peut référencer des pièces du dossier d'homologation sans les reproduire.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.3****c. Avis défavorable**

La mise en lumière de vulnérabilités graves ou de non conformités réglementaires mettant en péril la confidentialité, la disponibilité ou l'intégrité d'informations classifiées de défense peuvent conduire la DRSD à émettre un avis défavorable.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.4****LES AUDITS DE SECURITE****Références :**

- Code de la défense – Art. L.1332-6-1 à L.1332-6-6
- IGI 1300 – 6.9
- II n°901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles
- II n°910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)

Points clés :

- Les audits de sécurité interviennent aux moments critiques du cycle de vie d'un SI :
 - lors de l'homologation initiale ou à l'occasion du renouvellement de cette dernière ;
 - à des fins de maintien en condition de sécurité du SI.
- Les audits peuvent être externalisés notamment auprès de prestataires qualifiés par l'ANSSI - les prestataires d'audit SSI.
- L'externalisation des audits de systèmes d'information classifiés est possible après analyse de risque et avec l'accord de l'autorité contractante.

En complément des tâches de maintien en condition de sécurité, l'autorité d'homologation réalise ou fait réaliser périodiquement des contrôles ou des audits¹⁴⁸ de sécurité des systèmes d'information. Pour les systèmes les plus importants (cf. fiche 6.2 pour la catégorisation des SI), un audit de sécurité est obligatoire avant l'homologation et chaque renouvellement d'homologation.

Une autorité qualifiée d'entreprise peut s'appuyer sur des prestataires de services internes ou externes pour la réalisation d'audits SSI. En ce qui concerne les systèmes classifiés de défense, l'externalisation est possible après analyse de risque et avec l'accord de l'autorité contractante.

Sauf dérogation de l'autorité contractante, les auditeurs d'un système d'information *Diffusion Restreinte* doivent être habilités au niveau *Secret*. Les auditeurs d'un système d'information classifié doivent être habilités au niveau *Très Secret*. Lorsqu'il s'agit d'un auditeur interne, ce niveau d'habilitation est sans incidence sur le niveau d'habilitation de la personne morale. En cas de sous-traitance de la prestation d'audit, le contrat doit comporter un plan contractuel de sécurité validé par l'autorité contractante.

Ces audits de sécurité doivent, en plus de la conformité aux règles en vigueur, évaluer le niveau de robustesse des systèmes visés face à l'état de l'art des menaces informatiques.

Les auditeurs réalisant l'audit de sécurité utilisent les outils logiciels, des outils matériels et des privilèges qu'ils estiment nécessaires à la réalisation des activités d'analyse technique à l'état de l'art.

¹⁴⁸ Processus systématique, indépendant et documenté en vue d'obtenir des enregistrements, énoncés de faits ou autres informations qui se rapportent aux critères de contrôle ou d'audit et sont vérifiables et de les évaluer de manière objective pour déterminer dans quelle mesure les critères de sécurité sont satisfaits. Un audit de sécurité comporte un audit d'architecture, un audit de configuration, un audit de code source, un audit organisationnel et un test d'intrusion. Un contrôle de sécurité comporte un audit de configuration et un audit de conformité à la documentation applicable au système d'information.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.4**

Les conditions d'utilisation des équipements nécessaires à l'audit doivent respecter la fiche 6.7 relative à la mobilité et aux supports amovibles.

Pour un système *Diffusion Restreinte* ou classifié, en cas de recours à un prestataire, celui-ci doit être qualifié « Prestataire d'Audit de la Sécurité des Système d'Information » (selon la nature du système d'information : PASSI ou PASSI-LPM¹⁴⁹). Le plan contractuel de sécurité du sous-contrat doit préciser comment la prestation d'audit doit être réalisée (il peut prévoir l'impossibilité pour les auditeurs de récupérer des informations issues du système d'information audité, la mise à disposition par l'entreprise auditée des moyens d'audit ou des moyens pour rédiger le rapport d'audit, la réalisation complète de la prestation dans les locaux de l'entreprise auditée, l'exécution des outils d'audit par les administrateurs du système et non par les auditeurs, la réalisation de la totalité de la prestation par des moyens logiciels et/ou matériels propres aux auditeurs mais avec des mesures de contrôle et de surveillance particulières, ...).

Les rapports d'audit sont classifiés selon les dispositions prévues par l'[annexe 9](#) de la présente instruction.

L'audit porte au moins sur :

- l'application des dispositions réglementaires et des directives particulières de l'AQSSI responsable ;
- le respect des conditions organisationnelles et techniques prévues par l'homologation ou l'autorisation provisoire d'emploi du système ;
- l'adéquation des règles d'exploitation (contrôle des procédures d'exploitation de sécurité) ;
- la protection du personnel ;
- les mesures de sauvegarde en cas d'incident ou d'accident ;
- la planification des mesures particulières relatives aux situations de crise ;
- l'évaluation des conséquences des risques acceptés ;
- le respect des dispositions réglementaires relatives à la gestion des ACSSI ;
- la protection contre les signaux parasites compromettants.

Les conditions de mise à disposition des outils, des privilèges et de communication des relevés techniques nécessaires à la réalisation de l'audit de sécurité doivent figurer dans une charte d'audit spécifique au système visé, quel que soit son niveau de classification et sans préjudice des dispositions de la présente instruction. Cette charte d'audit entre l'entité du système d'information visé et celui réalisant l'audit précise ces conditions et le périmètre de l'audit.

¹⁴⁹ Prestataire d'audit qualifié par l'ANSSI au sens des articles L.1332-6-1 à L.1332-6-6 du code de la défense.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.5****SOUS-CONTRACTANCE A UN TIERS EN MATIERE INFORMATIQUE****Références :**

- Décret n° 2016-361 du 24 mars 2016 relatif aux marchés de défense et de sécurité
- IGI 1300 – 6.3
- Guide de l'externalisation¹⁵⁰, par l'ANSSI

Points clés :

- Pour les systèmes d'information classifiés ou *Diffusion Restreinte*, le recours par un contractant du MINARM à une sous-contractance informatique doit être explicitement autorisé par le plan contractuel de sécurité initial.
- Préalablement à la mise en place d'une sous-contractance, une analyse de risque doit être menée.
- La contractualisation par l'entreprise à un tiers d'activités sur des systèmes d'information sensibles, *Diffusion Restreinte* ou classifiés impose de formaliser les objectifs de sécurité dans des documents dédiés et d'appliquer les mesures de protection associées.

La sous-contractance informatique consiste à confier à un tiers tout ou partie de l'activité dans le domaine des systèmes d'information. Il peut s'agir, entre autres, de MCO (maintien en condition opérationnelle), de MCS (maintien en condition de sécurité), de TMA (tierce maintenance applicative), d'ASP (Application Service Provider - fournisseur d'applications en ligne), de SAAS (Software as a service - logiciel en tant que service), de MSSP (Managed Security Service Provider - fournisseur de service de sécurité géré), etc.

Toute entreprise sous contrat avec le MINARM traitant des informations *Diffusion Restreinte* ou classifiées est tenue d'appliquer les présentes dispositions. **Le recours à une sous-contractance doit être explicitement autorisé par le plan contractuel de sécurité.**

Le cas échéant, les activités peuvent être identifiées comme des tâches essentielles¹⁵¹ qui ne peuvent faire l'objet d'un sous-contrat. En particulier, les prestations d'administration de la sécurité d'un système d'information classifié ne peuvent pas faire l'objet d'un sous-contrat.

1. Analyse de risque préalable par l'autorité contractante.

Une analyse de risque est nécessaire pour formaliser des objectifs de sécurité ainsi que des mesures adaptées au contexte. Cette analyse de risque permettra à l'autorité d'homologation d'autoriser ou non la sous-contractance.

L'entreprise doit veiller à conserver la maîtrise du système d'information (gouvernance, dépendance technologique, etc.).

Trois sources de risques principales liées à la démarche de sous-contractance à un tiers doivent être envisagées :

¹⁵⁰ https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf

¹⁵¹ Au sens de l'article 133 du décret de référence.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.5**

- les interventions à distance (liaisons permanentes avec droits privilégiés, télé-administration de passerelles de sécurité, interconnexions non sécurisées, mots de passe faibles, etc.) ;
- l'externalisation de l'hébergement (isolation défailante, effacement incomplet ou non sécurisé, etc.).
- l'exposition à des réglementations extraterritoriales (exemple : Cloud Act adopté en mars 2018 par les Etats-Unis).

Si la prestation est effectuée à distance, et selon la complexité et les enjeux de sécurité du système d'information, elle pourra être complétée par les documents suivants :

- un document de procédures d'exploitation de sécurité, fixant les modalités générales d'exploitation de sécurité des dispositifs de télémaintenance ;
- des fiches réflexes permettant de garantir la bonne application des procédures d'exploitation de sécurité par le personnel en charge de l'utilisation ou de l'administration des dispositifs de télémaintenance ;
- un protocole d'accord entre le client et la société en charge de la télémaintenance pour formaliser des procédures spécifiques.

Si l'analyse de risque fait apparaître un risque pour l'autorité contractante, alors l'autorité contractante doit en être informée.

2. Processus contractuel d'externalisation par l'entreprise.

Le contrat de sous-contractance à un tiers comprendra les clauses de sécurité – y compris celles devant s'appliquer aux sous-traitants en cascade – et celles relatives à la réversibilité. Le contrat précisera la possibilité d'effectuer des audits de sécurité à son niveau ou par l'administration. Le périmètre d'intervention du prestataire doit y être établi par une délimitation claire de ses fonctions et responsabilités – notamment en matière de sécurité – vis-à-vis de celles conservées par le donneur d'ordre.

Tout contrat de sous-contractance nécessitant un accès à des ISC est soumis à l'autorisation explicite de l'autorité contractante. Ce contrat :

- obéit aux règles de l'IGI 1300 et de l'IM 900,
- comporte des clauses de protection du secret (cf. IGI 1300 - annexes 9 et 10),
- implique l'habilitation préalable des personnes physiques et morales,
- nécessite les aptitudes physiques des locaux et des systèmes d'information support de la prestation.

Ces contrats avec détention ou accès à des ISC font alors l'objet d'un plan contractuel de sécurité qui décline les objectifs de confidentialité (fiche 4.8 de la présente instruction).

Toute prestation d'infogérance nécessitant un accès à des informations *Diffusion Restreinte* devra se conformer aux règles du guide de l'ANSSI « Externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques », au « Recueil de mesures de protection des systèmes d'information traitant d'informations sensibles non classifiées de défense de niveau *Diffusion Restreinte* » et à l'annexe 3 de l'IGI 1300. Il sera porté une attention particulière à la localisation géographique de l'hébergement des données et à l'homologation *Diffusion Restreinte* du système d'information.

Il est recommandé de demander aux candidats de recenser et de justifier les dispositifs de télémaintenance qu'ils envisagent de mettre en œuvre sur le système du client.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.5**

Il doit leur être également demandé un descriptif des dispositifs de télémaintenance et des mesures de sécurité techniques et organisationnelles proposées :

- la sécurité de la liaison : réseau public ou ligne spécialisée, type de VPN, etc. ;
- les dispositifs techniques de sécurité : filtrage des accès réseau, droits d'accès, etc. ;
- les mesures organisationnelles, les procédures retenues pour déclencher une intervention ;
- les mécanismes d'authentification des techniciens assurant le support ;
- la traçabilité des actions ;
- la protection des accès aux données confidentielles en cas d'utilisation sur un système de production ;
- les éventuels rapports d'audit et plans d'action afférents

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.6****PRISE EN COMPTE DE LA SECURITE DANS LE CYCLE DE VIE DES SYSTEMES D'INFORMATION****Référence :**

IGI 1300 – 6.6.

Point clé :

La sécurité doit être prise en compte dans tout le cycle de vie d'un système d'information depuis la phase de conception/développement en passant par la phase d'exploitation (maintien en condition opérationnelle et de sécurité) jusqu'au retrait de service. Elle est à la charge de l'entité contractante.

1. Développement**a. Principes**

Afin de prévenir les attaques informatiques, les systèmes d'information et les applications « métier » doivent être développés de manière robuste et sécurisée conformément à l'état de l'art. La sécurité doit être prise en compte dès la conception d'un système. Cette précaution relève du responsable de l'organisme. Le RSSI de l'organisme est chargé d'en organiser la mise en œuvre.

A cet effet, l'ANSSI fournit des guides et recommandations. Il s'agit de guides et recommandations concernant la méthodologie pour intégrer la sécurité dans le développement d'un système d'information, concernant la maîtrise des risques cyber ou concernant la configuration et la sécurité des solutions disponibles sur étagère.

b. Dispositions particulière concernant les supports physiques intégrés dans des équipements

Une grande partie des équipements constitutifs des systèmes d'information est équipée de supports physiques de stockage rémanent (mémoires de masse de type disque dur magnétique, SSD, mémoire flash, ...). On les retrouve au sein d'équipements tels que les serveurs, ordinateurs individuels, robots de sauvegarde, périphériques de stockage, copieurs multifonctions, « ordiphones », vidéoprojecteurs, systèmes de visioconférence, des matériels de téléphonie et équipements de réseau.

Les actes contractuels d'approvisionnement et de maintenance d'équipements qui intègrent des supports physiques pour traiter des informations classifiées ou *Diffusion Restreinte* doivent comprendre des clauses de non-retour de ces supports chez les fournisseurs, applicables dès lors que ces supports ont traité des informations classifiées ou *Diffusion Restreinte*.

Sur les SI classifiés, ces supports physiques contiennent des informations classifiées et doivent être traités, si les informations ne sont pas chiffrées par un dispositif agréé, comme étant des ISC physiques, soit de façon unitaire, soit au niveau de l'équipement. A chaque étape de la vie du système, la traçabilité et la gestion réglementaire de ces ISC doit être assurée.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.6****c. Authentification**

L'authentification forte de l'utilisateur (exemple : par carte à puce ou *token*) est obligatoire pour tout système d'information traitant des informations *Diffusion Restreinte* ou classifiées. Elle est fortement recommandée pour les systèmes d'information traitant des données sensibles. Les dérogations à cette règle sont possibles mais doivent être justifiées dans le dossier d'homologation.

2. Exploitation et administration**a. Homologation**

L'homologation est un prérequis pour la mise en service d'un système d'information. Cf. fiche 6.2.

b. Habilitation des personnes accédant au SI

Une personne disposant de droits d'accès administrateur d'un SI *Secret* ou *Très Secret* doit être habilitée au niveau *Très Secret*.

Une personne disposant de droits d'accès administrateur d'un SI *Diffusion Restreinte* doit être habilitée au niveau *Secret*.

Une personne ne possédant pas de compte administrateur est habilitée au même niveau que le SI.

Les exigences ci-dessus concernant le niveau d'habilitation des administrateurs sont sans incidence sur le niveau d'habilitation de la personne morale.

c. Gestion des privilèges

Le principe du « moindre privilège » doit être appliqué. A cet effet, le nombre d'administrateur sera réduit autant que possible et des revues périodiques des droits seront menées, au moins annuellement.

Les comptes d'administration doivent être attribués individuellement et ne doivent être utilisés qu'à des fins d'administration. L'utilisation du système d'information se fait exclusivement avec des privilèges restreints d'utilisateur.

Les utilisateurs ne doivent pas pouvoir modifier les paramètres de configuration de démarrage de leur poste.

d. Procédure de transfert de données entre deux réseaux de classifications différentes

Le transfert d'information entre deux réseaux de classifications différentes se fait idéalement par une passerelle agréée par l'ANSSI ou homologuée et prévue à cet effet (généralement équipée d'une ou de plusieurs diodes). A défaut, le transfert d'information peut être effectué *via* un support amovible exclusivement dédié à cet effet selon une procédure fixée par l'entité contractante qui permet de vérifier l'innocuité du transfert d'information et de maîtriser les supports amovibles utilisés pour de tels transferts.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.6****3. Maintien en condition opérationnelle (MCO)**

Les opérations de maintenance sur un système d'information classifié doivent obligatoirement être tracées et imputées.

Interventions de maintenance :

Avant chaque intervention de maintenance, il est obligatoire de s'assurer de la mise en place des mesures de préservation des informations à protéger et des équipements classifiés, sensibles ou *Diffusion Restreinte* (une procédure d'effacement pourra être mise en œuvre avant toute intervention de la société de maintenance). Après l'intervention, la configuration du système est vérifiée afin de s'assurer de sa conformité avec l'état requis. En particulier, il est vérifié que les modifications apportées n'altèrent pas le niveau de sécurité pour lequel une homologation a été prononcée. Si l'intervention est associée à une évolution significative du système et notamment de sa configuration, celle-ci donne lieu à une nouvelle homologation du système.

Seuls les composants matériels mis à disposition ou administrés par l'organisme dont dépend un système classifié ou explicitement autorisés dans le dossier d'homologation du SI peuvent être connectés à des SI classifiés.

Une personne en charge de la maintenance ayant potentiellement accès à des informations classifiées et ne possédant pas de compte administrateur est habilitée au même niveau que le SI sur lequel elle est amenée à effectuer une opération de maintenance. Si elle n'est pas habilitée à ce niveau, elle est accompagnée pendant toute l'opération par un agent habilité et ayant des compétences suffisantes pour s'assurer que la personne en charge de la maintenance n'ait pas accès à des informations classifiées et n'introduise pas d'élément non maîtrisé dans le SI traitant d'informations classifiées.

4. Maintien en condition de sécurité (MCS)**a. Généralités**

Le MCS est l'ensemble de mesures organisationnelles et techniques concourant à maintenir le niveau de sécurité accepté lors de l'homologation tout au long du cycle de vie du SI.

Le MCS est de la responsabilité de l'entité contractante qui exploite le système. Elle approuve les modifications ou installations de patches et peut avoir à requérir l'avis formel du ministère.

Tout système doit prévoir les dispositions requises pour permettre de couvrir les risques tout au long de la vie du système. Des moyens techniques et organisationnels sont prévus et mis en place pour valider puis diffuser les mesures correctrices requises. Ces procédures de MCS font partie du périmètre d'homologation du système.

L'entité contractante se tient informée des vulnérabilités ou mesure correctrices diffusées par les fournisseurs de solutions ou des centres de prévention et d'alerte en matière de cyber sécurité.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.6****b. Configuration et mise à jour de sécurité**

Le système d'information doit utiliser des logiciels soutenus par les éditeurs et régulièrement mis à jour.

Les ressources logicielles et matérielles font l'objet d'une procédure de gestion de configuration, définie dans le cadre de l'homologation. Sauf difficulté technique ou opérationnelle justifiée, l'installation des mises à jour de sécurité est planifiée après vérification de l'origine de la version et de son intégrité. Lors d'une décision de ne pas installer la mise à jour, des mesures techniques et organisationnelles sont mises en œuvre pour réduire les risques liés à l'utilisation de cette version obsolète ou vulnérable.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.7****EQUIPEMENTS MOBILES ET SUPPORTS AMOVIBLES****Références :**

- IGI 1300 – 6.7 et 6.8
- Instruction interministérielle relative à la protection des systèmes d'information sensibles n°901/SGDSN/ANSSI¹⁵².
- Guide ANSSI-PA-054 recommandations sur le nomadisme numérique

Points clés :

- Le chiffrement permet d'assurer la protection des informations traitées par des équipements mobiles ou stockées sur des supports amovibles, particulièrement en dehors des locaux protégés. Ce chiffrement doit être qualifié (standard ou renforcé) ou agréé en fonction du niveau de protection des informations.
- Les équipements utilisés et leur configuration doivent être gérés logistiquement et administrés par l'entité conformément aux procédures d'exploitation de la sécurité définies lors de la démarche d'homologation.

1. Généralités

Le traitement d'informations sensibles, *Diffusion Restreinte* ou classifiées, en dehors des locaux adaptés, nécessite la mise en place de mesures techniques et organisationnelles afin de sécuriser l'accès aux données et aux matériels. Ces mesures visent à atteindre un niveau de sécurité le plus proche possible du SI interne de l'entité.

L'exploitation d'informations *Secret* sur un poste mobile est conditionnée par l'existence d'une zone permettant de respecter le besoin d'en connaître de l'information traitée. En conséquence, elle est interdite dans un espace ouvert au public (aéroport, train, ...). Les périphériques (clavier, souris, ...) sans fils et les protocoles et technologies de communication sans fil susceptibles d'induire des signaux compromettants sont interdits¹⁵³.

Pour l'exploitation d'informations *Secret* sur un poste mobile en dehors des locaux de l'entreprise prévus à cet effet, il est recommandé de privilégier le fonctionnement sur batterie et non sur secteur. Par ailleurs, un éloignement d'un mètre des sources de conduction (radiateurs, réseaux électriques, réseaux informatiques ou téléphonique, ... doit être respecté.

Pour mémoire, l'exploitation d'information *Très Secret* n'est possible qu'en zone réservée.

2. Protection des informations contre la perte ou le vol

Les informations doivent être chiffrées avec un produit agréé¹⁵⁴, tout en appliquant des règles de sécurité particulières liées à la mobilité ou aux supports amovibles.

¹⁵² <http://circulaires.legifrance.gouv.fr/index.php?action=afficherCirculaire&hit=1&retourAccueil=1&r=39217>

¹⁵³ Exception possible : cage de Faraday.

¹⁵⁴ Utilisation de ACID, de Cryhod... jusqu'au niveau *Diffusion Restreinte* et stockage sur un support amovible de type Globull par exemple pour le niveau *Secret*.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.7****3. Gestion de la protection des matériels et supports amovibles**

Les équipements mobiles et supports amovibles doivent être considérés comme étant partie intégrante du ou des systèmes auxquels ils peuvent être connectés. Ils sont inclus dans l'analyse de risque et explicitement autorisés dans le dossier d'homologation. L'autorité d'homologation doit veiller à la mise en œuvre des mécanismes et des fonctions de sécurité adéquats et ces équipements doivent être fournis et administrés par l'entité.

En dehors des locaux de l'organisme, les équipements doivent rester sous la surveillance permanente de l'utilisateur.

Pour le niveau *Secret*, à l'étranger, la surveillance permanente de l'utilisateur est systématiquement recherchée, par le dépôt du poste dans une représentation française (consulat, ambassade, coopération, opération extérieure, ...). Par mesure de précaution, des solutions physiques (étiquettes ou enveloppes de sécurité, ...) permettent de détecter une tentative d'accès frauduleux au poste ou une atteinte à son intégrité.

Un équipement mobile pour du classifié doit faire l'objet de vérifications régulières de sa configuration physique, en particulier avant qu'il soit reconnecté sur le système d'information homologué de son organisme d'appartenance.

4. Branchement de supports amovibles sur les systèmes d'information

Les supports amovibles classifiés ne doivent pas être connectés à un matériel non classifié ou de classification inférieure. Les supports amovibles *Diffusion Restreinte* ne doivent pas être connectés à un matériel de niveau de sensibilité inférieure. Les échanges entre les supports de l'entreprise et les supports extérieurs à l'entreprise (qui ne peuvent détenir que des informations qui ne soient ni sensibles ni classifiées) se font sur une station blanche - avec rupture de support - ou *via* les interconnexions de réseaux en adoptant les dispositifs de protection adéquats (exemple : transmission des fichiers par courriel, *via* une passerelle ou un sas homologué).

Les ports USB des systèmes d'information classifiés et *Diffusion Restreinte* doivent faire l'objet d'un verrouillage ou d'un contrôle afin de prévenir les extractions non autorisées, tracer l'utilisation des supports externes et éviter les compromissions¹⁵⁵ du fait de mauvaises manipulations.

5. Cas particulier de la mobilité *via* Internet

Un service de mobilité peut être mis en œuvre entre un utilisateur et son entité d'appartenance *via* Internet (filaire ou sans fil) jusqu'au niveau *Diffusion Restreinte* à la condition de se conformer aux exigences de l'II 901, complétées par les recommandations de l'ANSSI.

Les mesures spécifiques à ce type de mobilité doivent être définies dans la PSSI de l'entité.

En particulier, il est impératif de :

- maîtriser la gestion des utilisateurs et des équipements de mobilité ;
- former et sensibiliser les utilisateurs sur leurs obligations face aux risques et menaces ;

¹⁵⁵ Cf. définition au paragraphe 1 de la fiche introductive du titre 8.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.7**

- appliquer des restrictions d'usage (séquence de démarrage, filtrage internet, désactivation des services et applications inutiles, ...) afin de réduire la surface d'attaque ;
- mettre à disposition des moyens de protection (chiffrement, filtre écran, scellés, verrous sur les ports USB, ...);
- mettre en œuvre un tunnel VPN (exemple : IPSEC agréé) à l'état de l'art entre le SI de l'entité et les équipements de mobilité et maîtriser les flux réseau ;
- assurer l'authentification forte de l'utilisateur et de l'équipement ;
- assurer le MCO et le MCS, la supervision, la journalisation et la détection.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.8****SUPERVISION DE SECURITE D'UN SYSTEME D'INFORMATION****Références :**

- IGI 1300 – 6.6.4
- Instruction interministérielle n°901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles

Point clé :

La supervision de sécurité d'un système d'information est un élément clé de la cybersécurité, qu'il soit ou non classifié.

Sauf mention contraire, la présente fiche concerne les systèmes d'information classifiés, tels que décrits dans le chapitre 6 de l'IGI 1300, et *Diffusion Restreinte*, au sens de l'II 901 citée en référence.

1. Journalisation des événements

A 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 selon les recommandations de l'ANSSI. La journalisation porte sur :

- la gestion des accès,
- les modifications,
- les enregistrements,
- tout élément permettant l'investigation en cas d'incident de sécurité.

Les événements enregistrés par le système de journalisation¹⁵⁶ sont horodatés. Les composantes du système doivent être synchronisées pour assurer un horodatage cohérent des événements enregistrés.

Ils sont, pour chaque système d'information, centralisés et archivés pour une durée d'au moins cinq ans. Le format d'archivage des événements permet de réaliser des recherches automatisées sur ces événements.

Dans l'éventualité où, pour un système d'information classifié, certains événements ne pourraient être enregistrés, le dossier d'homologation doit préciser les éventuelles mesures organisationnelles palliatives mises en place.

L'autorité d'homologation s'assure de la définition de procédures d'exploitation des événements enregistrés par le système de journalisation et de leur application.

2. Systèmes de détection

La supervision de la sécurité des systèmes d'information s'appuie notamment, en complément de la journalisation des événements, sur des systèmes de détection de type « sonde d'analyse de fichiers et de protocoles », qui font l'objet d'une stratégie de

¹⁵⁶ Le système de journalisation est une fonction indépendante du système d'information, qui enregistre les événements relatifs au fonctionnement du système et à sa gestion.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.8**

déploiement et d'une stratégie d'exploitation approuvées par l'AQSSI. La stratégie de déploiement s'assure notamment que l'ensemble des flux de données échangé avec d'autres systèmes d'information est analysé.

L'architecture de déploiement des systèmes de détection ne doit pas remettre en cause la sécurité du système d'information. Les systèmes de détection journalisent l'ensemble des éléments qu'ils détectent.

Si la mise en œuvre des systèmes de détection de type « sonde d'analyse de fichiers et de protocoles » est impossible pour des raisons techniques ou organisationnelles ou 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, après accord de l'autorité contractante, la non mise en place d'un système de détection. La justification figure dans le dossier d'homologation.

3. Déclaration des incidents

En cas d'incident détecté, l'opérateur privé doit le déclarer à l'administration, notamment si la confidentialité, l'intégrité ou la disponibilité peut être impactée. De plus, il se doit de déclarer tout incident survenant dans le périmètre d'un SI classifié, *Diffusion Restreinte* ou sensible ou ayant une adhérence ou une proximité avec celui-ci. Une campagne d'appui à la détection de compromission¹⁵⁷ peut être initiée par le service enquêteur voire un audit conseil.

Sauf cas particulier (contrôle gouvernemental ou si l'autorité contractante est la DGSE, etc.), la déclaration initiale d'incident se fait de façon unique à l'administration, c'est-à-dire avec l'usage d'un même formulaire (formulaire type ANSSI) qui est transmis à l'ANSSI, copie DRSD et DGA/SSDI.

Suite à un incident ou dans le cadre d'une suspicion de compromission¹⁵⁸, la DRSD et la DGA/SSDI¹⁵⁹ peuvent mener, en coordination avec l'ANSSI et le COMCYBER, des contrôles sur les SI classifiés ou *Diffusion Restreinte* ainsi que les systèmes sensibles ou non protégés qui appartiennent à l'environnement d'un réseau classifié ou *Diffusion Restreinte*.

¹⁵⁷ Cf. définition au paragraphe 1 de la fiche introductive du titre 8.

¹⁵⁸ Idem

¹⁵⁹ Ou la DGSE pour son périmètre de compétence.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.9****LES ACSSI****Références :**

- IGI 1300 – 6.6.3.3
- II n°910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)¹⁶⁰
- II 500 bis /SGDN/TTS/SSI/DR du 18 octobre 1996 relative au chiffre dans la sécurité des systèmes d'information.
- Directive n°34/DEF/DGSIC du 10/03/2015 relative aux articles contrôlés de la sécurité des systèmes d'information du ministère de la défense

Points clés :

- La qualification d'article contrôlé de la sécurité des systèmes d'information (ACSSI) garantit la traçabilité comptable et géographique de ces éléments contribuant à la sécurité des SI.
- La qualification comme ACSSI ne préjuge pas de la classification de cet objet (qui peut être aussi NP ou DR).
- Pour manipuler des ACSSI, une décision d'accès est nécessaire (DACSSI). Elle est délivrée après une formation spécifique.

1. Définitions

Certains moyens, tels que des dispositifs de sécurité ou leurs composants, et certaines informations relatives à ces moyens (spécifications algorithmiques, documents de conception, clés de chiffrement, rapports d'évaluation, etc.) peuvent nécessiter la mise en œuvre d'une gestion spécifique visant à assurer leur traçabilité tout au long de leur cycle de vie. Ces moyens qui, par leur intégrité ou leur confidentialité, contribuent à la sécurité d'un système d'information, sont dénommés « articles contrôlés de la sécurité des systèmes d'information » (ACSSI).

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

La qualification ACSSI et la classification procèdent de deux logiques différentes. La qualification ACSSI vise à apporter une assurance de traçabilité (la localisation doit être connue à tout moment), la protection physique, logique et juridique de l'ACSSI étant apportée par son niveau de classification. Ainsi, les ACSSI classifiés sont à la fois ACSSI et classifiés *Secret* (ACSSI S) ou *Très Secret* (ACSSI TS). Les ACSSI non classifiés sont *Diffusion Restreinte* (ACSSI DR) ou *Non protégé* (ACSSI NP).

¹⁶⁰ <http://circulaire.legifrance.gouv.fr/index.php?action=afficherCirculaire&hit=1&r=37647>

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.9****2. Règles générales**

Les éléments du présent paragraphe correspondent aux règles générales de gestion des ACSSI. La décision d'agrément du dispositif de sécurité ou la décision d'homologation peut inclure des règles additionnelles, des dérogations aux règles générales ou des règles différentes.

Les ACSSI portent un marquage spécifique identifiant, en plus, le cas échéant, leur mention de classification. Le marquage est définitif jusqu'à la destruction du dispositif (ou éventuellement la décision de retirer le marquage ACSSI par l'autorité qui en avait décidé le marquage).

L'accès à un ACSSI nécessite une décision d'accès aux ACSSI (DACSSI). Pour les industriels de la défense, hors contractants avec la DGSE, elle n'est délivrée qu'après une formation organisée par le CISIA.

Stockage : les ACSSI classifiés sont stockés comme des ISC de même niveau de classification¹⁶¹. Les ACSSI non classifiés sont stockés dans des armoires ou des locaux fermés à clé afin de garantir en permanence leur intégrité.

Utilisation : les ACSSI doivent être manipulés et protégés conformément à la classification des informations qu'ils protègent.

Transport physique d'ACSSI classifiés :

- Il est réalisé selon les mêmes conditions que le transport d'ISC de même niveau de classification.
- Vers l'étranger, le convoyeur dispose d'une lettre de courrier.

Transport physique d'ACSSI non classifiés (cas des équipements de cryptographie) :

- Il est réalisé selon les règles applicables au *Secret*.
- Vers l'étranger, le convoyeur dispose d'une lettre de courrier.

Transport physique d'ACSSI non classifiés (hors équipement cryptographique) :

- Il est réalisé selon les règles applicables au *Diffusion Restreinte*.
- L'ACSSI est mis sous double enveloppe (si ses dimensions le permettent).

Dans tous les cas :

- Les convoyeurs ne sont pas tenus d'avoir une DACSSI.
- Le transport d'ACSSI donne lieu à un ABB' permettant de s'assurer de la bonne réception de l'ACSSI et de son intégrité.

Selon les destinations et le type d'ACSSI non classifié, l'emploi de conteneurs approuvés par l'Etat est recommandé afin de s'affranchir d'une surveillance permanente. L'usage d'un tel conteneur est obligatoire pour un transport vers l'étranger.

Certains matériels ACSSI sont transportés (y compris à l'étranger) par l'utilisateur lui-même. Pour les règles d'utilisation, de stockage et de transport il est nécessaire de se référer à la décision d'agrément ou d'homologation.

Maintenance : les opérations de maintenance d'un moyen ACSSI doivent être soigneusement tracées. Elles font partie intégrante de l'historique de l'ACSSI.

¹⁶¹ Lorsque des ACSSI sont stockés dans le même meuble que des ISC, ils doivent être spécifiquement marqués de façon à être immédiatement visibles par l'utilisateur.

TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES DE DROIT PRIVE**6.9****3. Responsabilité et gestion des ACSSI**

Les opérateurs privés sont responsables, sous l'autorité de la DGA, de la mise en œuvre des procédures réglementaires prescrites pour la gestion des ACSSI par l'IGI 1300 et par l'II 910. Les ACSSI non classifiés (DR et NP), sous réserve que l'agrément ne l'interdise pas, peuvent être suivis en gestion locale ; cependant, l'échelon central doit pouvoir accéder à leurs informations de suivi pour permettre de fournir, autant que de besoin, une vision globale à la DGA, voire au niveau ministériel.

Le suivi d'un ACSSI consiste à :

- pouvoir déterminer la position géographique d'un ACSSI à tout instant,
- pouvoir déterminer l'exploitant, l'utilisateur, le comptable ou le gestionnaire central/local d'un ACSSI à tout instant (à partir des actes de comptabilité ACSSI),
- pouvoir déterminer le statut d'un ACSSI, notamment pour un bien matériel (bien en exploitation, bien disponible, bien non disponible et ses sous-statuts), l'applicabilité de ce statut étant étendue aux informations ACSSI pour lesquelles cela est pertinent.

Des inspections programmées ou inopinées sont menées par la DGA. Elles témoignent de la bonne tenue et de l'efficacité du suivi spécifique et du respect des mesures de protection. L'inspection se limite à des constats visuels, sans porter atteinte à l'intégrité ou aux fonctions de sécurité des ACSSI. Il s'agit en effet d'une inspection relative à la gestion des ACSSI.

4. La gestion des incidents de sécurité

Selon l'II 910, un incident de sécurité concernant un ACSSI est un événement indésirable ou inattendu présentant une probabilité forte de porter atteinte à la confidentialité, l'intégrité ou la disponibilité des informations ou des systèmes protégés par les ACSSI. Un incident de sécurité peut conduire à une compromission¹⁶². En revanche, une compromission est nécessairement tracée sous la forme d'un incident de sécurité. La perte (même temporaire) ou le vol d'un ACSSI, le blocage ou le dysfonctionnement d'un équipement cryptographique ACSSI, le constat d'un défaut d'intégrité d'un ACSSI sont des exemples d'incident de sécurité.

Tout incident de sécurité affectant un ACSSI doit faire l'objet d'un compte-rendu immédiat via la chaîne SSI. Un inventaire des incidents sera adressé annuellement, par l'opérateur privé, à la DGA (même en cas d'état néant), qui retransmet une synthèse des incidents sur son périmètre de responsabilité au FSSI.

Tout incident de sécurité doit conduire à la mise en œuvre des mesures techniques et organisationnelles, qu'elles soient immédiates (exemple : révocation d'une clé) ou qu'elles soient le fruit d'une analyse par la chaîne ACSSI, le FSSI, le HFCDS ou l'ANSSI.

¹⁶² Cf. définition au paragraphe 1 de la fiche introductive du titre 8.

**TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES
DE DROIT PRIVE****6.10****SECURITE DU CABLAGE ET CIRCUITS APPROUVES****Référence :**

IGI 1300 – 6.4.1

Point clé :

Sous réserve de conditions techniques et d'environnement, les circuits approuvés permettent de faire circuler de façon permanente et en clair des informations classifiées tout en assurant leur protection.

L'installation du câblage d'un réseau transportant des informations classifiées respecte les exigences de la réglementation relative à la protection contre les signaux parasites compromettants¹⁶³.

Le câblage véhiculant en clair des informations classifiées est confiné à l'intérieur de l'environnement de sécurité local et, à minima, selon les dispositions prévues par le titre 5 de la présente instruction. Il permet de constituer des réseaux physiquement dissociés et autorise le contrôle de l'infrastructure de câblage.

Pour un système d'information homologué au niveau *Secret*, dans le cas où l'autorité d'homologation prend la responsabilité d'utiliser des circuits approuvés¹⁶⁴ entre différents environnements de sécurité locaux implantés au sein de la même emprise physique, en remplacement de la mise en œuvre de moyens de chiffrement agréés, une cartographie précise du câblage est détenue par l'officier de sécurité des systèmes d'information et l'officier de sécurité. Le câblage de chaque circuit approuvé doit pouvoir être contrôlé. Les locaux, volumes ou cheminements doivent être protégés soit physiquement, soit par un système d'alarme, soit par un dispositif permettant de vérifier l'intégrité du circuit approuvé comme de la réflectométrie. En complément de ces dispositions, les informations *Spécial France* ne peuvent circuler sans chiffrement que dans le cas où le circuit approuvé est sous maîtrise et utilisation nationale. Des procédures spécifiques d'exploitation de la sécurité sont établies (contrôles d'intégrité du câblage, etc.). Il est de la responsabilité de l'autorité qualifiée d'inspecter régulièrement les moyens de protection physique, d'assurer la mise en œuvre des systèmes d'alarme, de contrôler l'intégrité de l'infrastructure de câblage et de s'assurer que les interventions soient effectuées par du personnel habilité (ou accompagné par des agents habilités). **L'utilisation d'un circuit approuvé doit faire l'objet de l'accord de l'autorité contractante.** Les éléments relatifs au circuit approuvé (cartographie, mesures de sécurité, procédures d'exploitation, ...) sont transmis à l'autorité contractante sur simple demande.

¹⁶³ Directive n° 495/ANSSI/DR du 20 novembre 2013 de zonage TEMPEST – protection contre les signaux parasites compromettants et directive n° 495/SGDN/TTS/SSI du 20 novembre 2013 relative à l'installation des sites et systèmes d'information pour la protection contre les signaux parasites compromettants.

¹⁶⁴ Un circuit approuvé est un circuit qui fait l'objet de mesures spécifiques de protection physique et visuelle afin de permettre son emploi pour la transmission d'informations classifiées de défense sans protection par des moyens de chiffrement agréés.

**TITRE 6 : SECURITE DES SYSTEMES D'INFORMATION POUR LES ENTITES
DE DROIT PRIVE****6.10**

Pour un système d'information homologué au niveau *Très Secret*, l'usage de circuits approuvés est interdit, le câblage véhiculant en clair des informations classifiées *Très Secret* est confiné à l'intérieur de la zone réservée.

TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES TOUT AU LONG DE LEUR CYCLE DE VIE

PRINCIPES ET DEFINITIONS

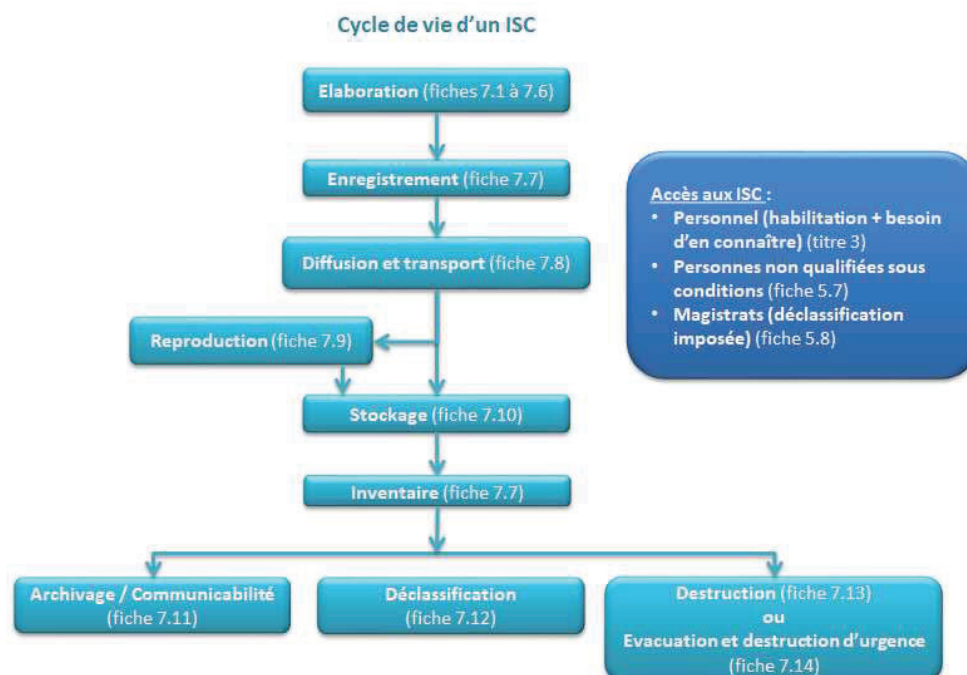
Références :

- Code de la défense - art. R. 2311-7
- IGI 1300 – Introduction, chap. 1, 7

Points clés :

- La sauvegarde des intérêts fondamentaux de la Nation doit être le seul motif présidant à la décision de classification.
- Classifier un document ou un support lui offre une protection pénale.
- Il existe deux niveaux de classification : *Secret* et *Très Secret*. Des classifications spéciales viennent compléter le niveau *Très Secret* ; leur traitement fait l'objet de textes spécifiques du SGDSN.
- Les ISC créés avant le 1^{er} juillet 2021 conservent leur marquage d'origine (CD, SD) et la protection juridique afférente. Les règles applicables au *Secret* décrites dans la présente IM s'appliquent également aux ISC *Confidentiel défense* et celles applicables également au *Très Secret* s'appliquent aux ISC *Secret défense*.

1. Principes



TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES TOUT AU LONG DE LEUR CYCLE DE VIE

La protection du secret de la défense nationale assure la sauvegarde des intérêts fondamentaux de la nation en empêchant la divulgation, intentionnelle ou non, d'informations pouvant leur porter atteinte ou ayant des conséquences exceptionnellement graves pour eux.

La classification d'une information place celle-ci sous la protection de dispositions spécifiques du code pénal. Cette protection comprend des autorisations nécessaires pour accéder à cette information, des mesures physiques pour limiter l'accès à cette information et des règles de gestion particulières (enregistrement, inventaire, déclassification, destruction, etc.).

Les différents niveaux de classification correspondent à des mesures de protection plus ou moins renforcées et adaptées au risque encouru en cas de compromission du secret de la défense nationale.

La classification peut être augmentée (reclassement), réduite (déclassement) ou supprimée (déclassification), à l'échéance obligatoirement indiquée sur le document ou à l'échéance de la durée maximum de classification (préalablement officiellement établie ou sur décision particulière).

Les règles à suivre concernant la classification et le suivi des ISC sont décrites dans les fiches 7.1 à 7.14.

Les locaux et meubles et systèmes d'informations (SI) contenant des ISC doivent respecter des normes de protection particulières et adaptées (cf. fiches du titre 5 jusqu'à 5.4).

Toute personne visant ou occupant un poste pour lequel le besoin d'une habilitation est avéré et qui refuserait de se soumettre à la procédure d'habilitation ne peut exercer les fonctions prévues et est écartée (cf. fiche 3.1 et suivantes).

Dans le cadre des marchés, le besoin d'en connaître est défini dans le plan contractuel de sécurité suivant les prescriptions des fiches 4.3 et 4.4.

2. Définitions et champs d'application

Informations et supports classifiés (ISC): 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 aux ISC, il faut être habilité et avoir le besoin d'en connaître (cf. IGI 1300 – 3.1.1).

« 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

TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES TOUT AU LONG DE LEUR CYCLE DE VIE

protéger les informations relatives aux priorités gouvernementales en matière de défense et de sécurité nationale (cf. fiche 7.6).

3. Correspondance des niveaux de classification pour les ISC marqués avant le 1^{er} juillet 2021 (date d'entrée en vigueur de l'IGI 1300 édition 2020)

Niveau *Confidentiel Défense* : Tout ISC marqué « *Confidentiel Défense* » conserve son marquage et la protection juridique associée. Il est traité et protégé selon les mesures de protection applicables aux informations et supports classifiés au niveau « *Secret* ».

Niveau *Secret Défense* : Tout ISC marqué « *Secret Défense* » conserve son marquage et la protection juridique associée. Il est traité et protégé selon les mesures de protection applicables aux informations et supports classifiés au niveau « *Très Secret* ».

L'équivalence des niveaux de classification avec les protections étrangères est validée avec les Autorités Nationales de Sécurité (ANS) des pays partenaires.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.1****ELABORATION D'INFORMATIONS ET SUPPORTS CLASSIFIES****Références :**

- Code pénal – Art. 413-9 et suivants
- IGI 1300 – 7.1, annexes 36 à 38

Points clés :

- Les règles d'élaboration et de marquage des ISC permettent d'assurer leur traçabilité et leur prise en compte par les détenteurs habilités.
- En raison de la possibilité technique de faire réapparaître des informations en principe effacées, un support informatique contenant des informations classifiées conserve toujours le niveau de classification des informations qu'il détient ou qu'il a détenues, sauf si celles-ci ont toutes été déclassifiées préalablement.
- **Il convient de ne classifier uniquement que ce qui est nécessaire en se référant aux guides de classification.**

1. Décision de classifier

Le ministre, en tant qu'autorité émettrice, énonce les critères de classification. Il veille à ce que le niveau de classification soit approprié à l'information ou au support concerné, c'est-à-dire à ce qu'il soit à la fois nécessaire et suffisant. Il cherche ainsi à limiter la prolifération de documents classifiés, à éviter les classifications abusives ou, au contraire, les sous-classifications (cf. guide de classification en [annexe 8](#)). Pour le département ministériel, chaque ADS rédige une instruction précisant le guide de classification cité *supra*. Il précise les consignes de déclassification à appliquer aux ISC.

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. Il procède à l'analyse de l'importance de l'information au regard de son contexte et eu égard aux directives de classification applicables.

2. Elaboration

Elaborer un ISC consiste à apposer un timbre de classification visible. Cette classification a pour conséquence de le placer sous la protection des dispositions spécifiques du code pénal¹⁶⁵.

L'élaboration d'un ISC est obligatoirement effectuée dans un lieu abritant par un personnel détenant une habilitation de niveau au moins équivalent à celui de l'information ou du document considéré. Le système d'information servant à l'élaboration des documents ou fichiers classifiés fait l'objet d'une homologation au minimum du niveau de classification de l'information concernée. En l'absence de système homologué, l'ISC est créé sur un poste isolé, hors réseaux, spécifiquement dévolu à cet usage.

¹⁶⁵ Articles 413-9 et suivants du code pénal.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.1**

L'élaboration d'un ISC de niveau *Très Secret* se fait impérativement en zone réservée (ZR) (cf. fiche 5.1). Il est recommandé d'élaborer des ISC de niveau *Secret* au sein d'une zone protégée (cf. IGI 1300 – 5.3.1.1).

3. Cas particuliers

- o Classification de l'objet du document : par principe, l'objet d'un document classifié est lui-même classifié (au même niveau que le document) sauf si son auteur en décide autrement.

- o Les agrégats : Un ensemble d'informations ou supports, dit parfois « agrégat », est classifié si le regroupement des informations ou supports qui le composent le justifie, alors même qu'aucun de ses éléments, pris isolément n'est classifié. Un agrégat d'ISC peut également être classifié à un niveau supérieur à celui des ISC qu'il contient.

Tout agrégat (pages, paragraphes, annexes, appendices, pièces jointes) contenant des informations classifiées à des niveaux différents est classifié lui-même au niveau le plus élevé des informations qu'il contient.

- o Les documents composites : 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. modèle dans IGI 1300 annexe 36). Cela revient à marquer entre crochets en tête de paragraphe le niveau de protection de l'information¹⁶⁶:

« [S-SF] texte du paragraphe.

[NP] texte du paragraphe. »

Si une partie complète du document présente un niveau de protection homogène alors la mention de protection est située au début du titre de la partie :

« [S-SF] texte du titre.

Texte des paragraphes. »

Pour faciliter la manipulation de ces documents, le bon sens recommande, lorsque cela est possible, d'isoler sur des pages particulières les informations d'un même niveau.

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 illisibles, de manière irréversible, les paragraphes classifiés ou classifiés au niveau supérieur.

Le niveau de classification des informations (notices, plans, etc.) concernant un matériel peut être différent du niveau de classification de ce dernier.

Un extrait d'information classifiée conserve le niveau de classification de l'information elle-même, à moins que le chef d'organisme de l'auteur du document n'en décide autrement. En l'absence d'indication contraire, la diffusion séquentielle d'extraits non classifiés par découpage de l'information classifiée est interdite. Lorsque des extraits

¹⁶⁶ En l'absence de ce marquage, l'information est considérée classifiée au niveau du document. En particulier, en l'absence de ce marquage, l'objet d'un document classifié est lui-même réputé classifié au même niveau que le document.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.1**

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.

- Les supports préparatoires : Les supports préparatoires ayant servi à l'élaboration du document classifié (brouillons, impressions sur papier, matériels informatiques nomades : clés USB, disquettes, CD, CD-ROM...) doivent porter la mention du niveau de classification adapté, ils sont placés sous la responsabilité de celui qui les a élaborés ou modifiés. Ils doivent être détruits ou effacés selon les conditions décrites dans la fiche 7.13 le plus rapidement possible dès qu'ils sont devenus sans objet et en tout état de cause, au plus tard lorsque le document classifié est émis.
- Les informations dématérialisées :
Pour les SI, la décision d'homologation du système vaut décision de classification.
En raison de l'impossibilité technique actuelle 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 du ou des documents qu'il aura contenus au cours de son cycle de vie. Il ne peut être déclassé ou déclassifié qu'à la condition que toutes les informations qu'il contient ou a contenues aient elles-mêmes préalablement fait l'objet d'une telle mesure.

4. Marquage

Une information doit pouvoir être identifiée comme étant classifiée avant sa consultation. L'apposition d'un timbre de classification visible constitue le seul moyen de conférer la protection des dispositions spécifiques du code pénal. Le marquage constitue une marque de l'autorité publique permettant de vérifier l'authenticité du support.

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 (cf. modèles en [annexe 9](#)).

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 9](#)). 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 sous le timbre de classification de l'information en page de garde ou directement à droite du timbre.

Les abréviations indiquant la classification ou le niveau de protection ainsi que les mentions complémentaires peuvent être utilisées pour préciser le niveau de classification des paragraphes du texte. Les abréviations sont les suivantes :

- Non protégé : NP ;

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.1**

- Diffusion restreinte : DR ;
- Secret : S ;
- Très Secret : TS ;
- Spécial France : SF

Ces abréviations ne remplacent pas la mention de classification inscrite en toutes lettres sur le document papier ou dématérialisé.

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 9](#)) ;
- l'échéance de la classification. Le cas échéant, la mention de déclassément ou de déclassification est apposée sur cette même page (cf. [annexe 9](#)) ;
- 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 ;
- le niveau de protection ou de classification de l'objet (cf. [annexe 13](#)).

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".

Marquage d'un support immatériel, d'éléments constitutifs d'un SI classifié ou de supports de stockage amovible

Dans la mesure du possible, les règles de marquage d'un support immatériel doivent respecter les règles de marquage d'un support papier.

Le marquage d'un support immatériel d'information classifiée (message ou fichier électronique, base de données, etc.), des éléments constitutifs d'un système

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.1**

d'information classifié¹⁶⁷ ou d'un support de stockage amovible d'informations classifiées 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. Il peut contenir la mention *Spécial France* si l'information ne peut être divulguée qu'aux seuls ressortissants français ;
- une identification assurée par l'inscription des références et, le cas échéant, du volume de chacune des informations enregistrées.

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 ou la documentation utilisateur. Pour les supports de stockage amovible agréés, le marquage doit être réalisé dans les conditions prévues par les instructions d'emploi du support, mentionnées dans sa décision d'agrément.

¹⁶⁷ Tout périphérique d'entrée non doté d'un élément mémorisant ou de communication sans fil peut être exempté de marquage (ex. claviers, souris, etc.). Cette exemption doit être mentionnée dans le dossier d'homologation.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.2****MENTION DE PROTECTION *DIFFUSION RESTREINTE*****Références :**

- IGI 1300 – 1.3.2 et annexe 1
- Instruction ministérielle n° 26209/ARM/SGA/DAJ du 16 août 2017 relative à la communication par les services du ministère des armées des documents administratifs aux citoyens
- Code des relations entre le public et l'administration (Livre III)

Points clés :

- En France, la mention *Diffusion Restreinte* (DR) n'est pas un niveau de classification mais une mention de protection apposée par une autorité ministérielle.
- Cette mention ne confère pas aux informations concernées la protection pénale propre au secret de la défense nationale, mais leur divulgation au public est considérée comme un manquement à la discrétion professionnelle.
- Le personnel ne respectant pas les règles de discrétion pour cette mention de protection peut faire l'objet d'une sanction administrative, voire pénale¹⁶⁸.
- La mention DR ne fait toutefois pas obstacle à la communication d'un document sur le fondement du code des relations entre le public et l'administration si elle n'est pas accompagnée d'une autre mention spécifique propre à rendre incommunicable le document (cf. fiche 7.5 sur les mentions spécifiques).

La mention *Diffusion Restreinte* indique que l'information ne doit pas être rendue publique et ne doit être communiquée qu'aux personnes ayant besoin de la connaître dans l'exercice de leur fonction ou dans l'accomplissement de leur mission. Cette mention n'est pas, pour la France¹⁶⁹, un niveau de classification mais une mention de protection. Son objectif principal est de sensibiliser l'utilisateur à la nécessaire discrétion dont il doit faire preuve dans la manipulation des informations couvertes par cette mention.

1. Teneur des informations *Diffusion Restreinte*

Au sein du MINARM, l'utilisation de cette mention relève de la nécessité d'éviter la divulgation d'informations dont le regroupement ou l'exploitation peuvent :

- conduire à la découverte d'un secret de la défense nationale ou compromettre la protection et la sécurité de la défense ;
- porter atteinte à la sécurité ou à l'ordre public, au renom des armées, à la vie privée de ses ressortissants ;
- porter préjudice aux intérêts économiques ou financiers de sociétés privées ou d'établissements publics du fait de leurs activités à caractère militaire.

Doivent notamment recevoir au minimum la mention « DR » les informations et documents :

¹⁶⁸ Abus de confiance, violation du secret professionnel ou de non-respect des règles relatives au traitement des données à caractère personnel.

¹⁶⁹ Certains alliés de la France ou des organisations internationales (OTAN, UE) considèrent le DR comme un premier niveau de classification. Pour en savoir plus, cf. fiche 9.4.

TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES TOUT AU LONG DE LEUR CYCLE DE VIE

7.2

- définissant, en termes généraux, les objectifs, options, critères de choix retenus dans les différents domaines de l'activité militaire française, opérationnelle ou technique ;
- relatifs à l'ordre public (comptes rendus d'événements...) ;
- couverts par cette mention à la suite d'un accord de sécurité conclu avec un pays étranger ;
- d'exercice dont la confidentialité défense n'a qu'un intérêt limité et temporaire ;
- ou informations émanant d'un autre ministère dont la diffusion n'est pas jugée souhaitable par ce ministère.

Bien que la mention « DR » ne soit pas destinée à protéger des informations à caractère personnel, son utilisation reste possible dans le cas de rapport sur le moral ou de compte rendu d'événements, etc.

2. Autorités habilitées à décider de l'emploi de la mention *Diffusion Restreinte*

Sous l'autorité du MINARM, sont autorisés à apposer sur des informations et supports la mention *Diffusion Restreinte* et à y accéder :

- les armées directions et services ;
- les établissements publics placés sous sa tutelle ;
- les opérateurs d'importance vitale relevant des DNS AME et ID ;
- 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*.

Tout signataire d'un document contenant des informations répondant aux critères précisés ci-dessus est responsable de l'attribution de 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 (cf. [annexe 10](#)).

Les informations DR du ministère ne doivent être communiquées qu'aux personnes qui ont le besoin d'en connaître. **Une divulgation de ces informations au-delà de ce cercle est considérée comme un manquement à la discrétion professionnelle et peut entraîner des sanctions disciplinaires ou professionnelles pour le personnel l'ayant causée** (cf. fiche 3.10).

Toutefois, la mention DR ne fait pas obstacle à elle-seule à la communication d'un document administratif à une personne qui en ferait la demande selon les dispositions législatives du code des relations entre le public et l'administration, à moins que leur

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.2**

communication ne porte atteinte entre autres¹⁷⁰ au secret industriel et commercial (aspects stratégiques) ou au secret médical¹⁷¹.

3. Élaboration et marquage

L'élaboration des documents DR 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 DR doivent être identifiés sur la première page avec les références de l'organisme émetteur, la date d'émission, et le numéro d'enregistrement.

Ils portent le marquage suivant :

DIFFUSION RESTREINTE

- sur chaque page, le timbre « Diffusion Restreinte » apposé avec de l'encre de couleur rouge, au milieu du haut de la page (cf. IGI 1300 - annexe 1) ;
- pour les messages et autres documents informatiques, la mention *Diffusion Restreinte* doit être rappelée en début de chaque page ;
- pour les documents reliés, le timbre *Diffusion Restreinte* doit être apposé au milieu de la page de garde et de la couverture.

4. Conservation, destruction et impression/reproduction

Les documents DR sont enregistrés au départ et à l'arrivée selon les règles appliquées à tous documents administratifs non classifiés.

Ils doivent être conservés dans des meubles offrant des garanties de sécurité suffisantes (cf. fiche introductive du titre 5).

Leur destruction irréversible a lieu sous la responsabilité des détenteurs, sans mention particulière sur les documents d'enregistrement du courrier, ni procès-verbal¹⁷².

Leur impression/reproduction doit rester limitée aux seuls besoins du service.

5. Expédition et circulation

La transmission interne des documents DR peut être effectuée :

- à l'intérieur d'un local, d'une enceinte ou d'un bâtiment relevant des autorités habilitées à décider de l'emploi du DR, sans précaution particulière si le convoyeur est une personne autorisée à en connaître ou sous pli fermé dans le cas contraire, par toute personne de ce ministère ou par toute entreprise privée autorisée par le ministère ;
- vers l'extérieur ou par un tiers :

¹⁷⁰ Cf. les dispositions législatives du CRPA, art. L. 311-5 A8 et L. 213-2 du code du patrimoine.

¹⁷¹ En cas de difficultés, les services peuvent se rapprocher de la direction des affaires juridiques (DAJ/D2P/DPSP).

¹⁷² Cf. les dispositions prévues par l'instruction n°101/DEF/SGA/DMPA/DPC du 29 juillet 2011 relative à la politique et à l'organisation générale de l'archivage du ministère de la défense et des anciens combattants.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.2**

- la transmission s'effectue sous double enveloppe, l'enveloppe intérieure portant la mention DR et les références du document, l'enveloppe extérieure ne comportant que les indications nécessaires à la transmission ;
- l'envoi est acheminé en recommandé avec accusé de réception par voie postale en France métropolitaine, vers les départements et collectivités d'outre-mer (DROM, COM) et vers l'étranger ;
- lorsqu'ils sont destinés à des personnels du ministère en poste au sein d'une mission diplomatique ou consulaire, les plis sont transmis au BCAC qui les achemine par la voie de la VD en « toute valise-recommandé » (TVR)¹⁷³.

La transmission par moyen électronique garantit la protection des informations. Les règles suivantes sont applicables :

- sur un réseau de transmission homologué « DR » ou plus, la transmission peut se faire en clair¹⁷⁴ ;
- dans les autres cas, les informations sont chiffrées à l'aide d'un dispositif ayant fait l'objet d'une qualification ou d'un agrément de l'ANSSI (outil Acid pour le MINARM).

¹⁷³ Le pli ou colis voyage au minimum en valise non accompagnée et au maximum en valise accompagnée.

¹⁷⁴ Le DRSF doit être cependant chiffré.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.3****MENTION DE PROTECTION *SPECIAL FRANCE*****Références :**

- Code de la défense - art. R. 2311-4
- IGI 1300 – 7.1.1.3.a et annexe 37

Points clés :

- La mention *Spécial France* n'est pas une mention de classification.
- Elle est apposée sur les documents nationaux, en complément d'autres timbres.
- Il est interdit aux ressortissants et militaires étrangers insérés, même habilités, de prendre connaissance, en aucune circonstance, des documents portant la mention *Spécial France*.
- Le personnel ne respectant pas les règles de discrétion pour cette mention de protection peut faire l'objet d'une sanction administrative.

1. Champ d'application

La mention *Spécial France* n'intéresse que les documents d'ordre strictement national traitant de sujets que l'autorité estime ne pouvoir être communiqués qu'aux nationaux. Elle est employée pour les informations et supports classifiés ou portant la mention *Diffusion Restreinte* que l'autorité émettrice estime devoir n'être divulgués qu'aux seuls ressortissants français relevant d'entités de droit français et qui ne sauraient, en aucune circonstance, être communiqués, en tout ou partie, à un État étranger ou à l'un de ses ressortissants, organisation internationale ou personne morale de droit privé étrangère, même s'il existe un accord de sécurité avec ces États ou cette organisation.

Elle peut être apposée sur des ISC mais aussi sur des documents faisant l'objet de la mention de protection *Diffusion Restreinte*. Dans l'objectif d'une passation de marché public, la mention *Spécial France* doit être étudiée et portée après l'acceptation des parties, de l'entité contractante et l'occupant bénéficiaire de la prestation. Cette mention n'est pas une mention de classification. Elle peut ne concerner que certaines parties d'un document.

Lorsque des informations marquées *Spécial France* sont classifiées, elles doivent, outre satisfaire aux mesures de sécurité appropriées à leur degré de protection, n'être transmises qu'à des personnes physiques et morales françaises dûment habilitées et ayant le besoin d'en connaître. Ce principe implique un cloisonnement très strict des réseaux, si elles sont véhiculées par voie électronique.

2. Marquage

Le timbre est de couleur bleue. Il est apposé en haut de page, immédiatement à droite ou au-dessous du timbre de classification (ou de la mention de protection DR) s'il existe.

SPECIAL FRANCE

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.3****3. Mesures de sécurité**

Les mesures de sécurité à appliquer sont déterminées par la mention de protection DR ou de classification du document ou du support. Leur acheminement se fait par des voies nationales. Ils ne figurent en aucun cas sur des inventaires ou répertoires prescrits par les règlements de sécurité relatifs aux accords internationaux.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.4****MENTION DE PROTECTION COMMUNICABLE A [SERVICES, ETATS,
ORGANISATIONS INTERNATIONALES, INSTITUTIONS, ORGANES OU
ORGANISMES DE L'UE]****Référence :**

IGI 1300 – 7.1.1.3.b

Points clés :

- La mention *Communicable* à n'est pas une mention de classification.
- Elle est apposée sur les documents nationaux, en complément d'autres mentions.
- Le personnel ne respectant pas les règles de discrétion pour cette mention de protection peut faire l'objet d'une sanction administrative.

1. Champ d'application

La mention « *Communicable à.....* » intéresse les documents traitant de sujets que l'on estime ne pouvoir communiquer qu'à certains services, Etats, organisations internationales, institutions, organes ou organismes de l'Union Européenne. Elle 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. Elle est apposée par l'auteur du document sous la responsabilité de l'autorité émettrice. Elle est employée pour les informations et supports classifiés ou portant la mention *Diffusion Restreinte* et conformément aux accords de sécurité avec ces services, États ou organisations.

Elle peut être apposée sur des documents classifiés ou faisant l'objet d'une confidentialité spécifique. La mention « *Communicable à.....* » n'est pas une mention de classification. Elle concerne la totalité d'un document.

Lorsque des informations marquées « *Communicable à.....* » sont classifiées, elles doivent, outre satisfaire aux mesures de sécurité appropriées à leur degré de protection, n'être transmises qu'à des personnes physiques et morales dûment habilitées et ayant le besoin d'en connaître. Ce principe implique un cloisonnement très strict des réseaux, si elles sont communiquées par voie électronique.

2. Marquage

Le timbre est de couleur rouge. Il est apposé en haut de page immédiatement à droite ou au-dessous du timbre de classification, s'il existe. Il précise explicitement les services, Etats, organisations internationales, institutions, organes ou organismes auxquels le document est communicable.

COMMUNICABLE A**3. Mesures de sécurité**

Les mesures de sécurité à appliquer sont déterminées par la mention de protection ou de classification du document ou du support. Leur acheminement est réalisé de façon à garantir le respect du périmètre de diffusion délimité.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.5****MENTIONS DE CONFIDENTIALITE SPECIFIQUES****Références :**

- Code de la défense - art. L. 4137-1 et R. 2311-4
- Code des relations entre le public et l'administration – art. L. 311-5 et L. 311-6
- Instruction ministérielle n° 26209/ARM/SGA/DAJ du 16 août 2017 relative à la communication par les services du ministère des armées des documents administratifs aux citoyens.

Points clés :

- Les mentions de confidentialité spécifiques n'ont pas pour objet de protéger des informations qui relèvent du secret de la défense nationale.
- Le personnel ne respectant pas les règles de discrétion pour ces mentions de confidentialité peut faire l'objet d'une sanction disciplinaire, professionnelle, voire pénale¹⁷⁵.
- Les règles de protection *Diffusion Restreinte* sont également applicables aux documents portant une mention de confidentialité spécifique.
- Le *Confidentiel Industrie* ou *Technologie* peut être utilisé par le personnel du MINARM et les entreprises si elles le jugent nécessaire, dans le cadre, notamment, des négociations menées avec l'Etat qui n'ont pas nécessairement vocation à constituer des informations stratégiques relevant du secret des affaires.
- Les mentions de confidentialité spécifiques ne font pas obstacle à elles-seules à la communication d'un document administratif à une personne qui en ferait la demande selon les dispositions législatives du code des relations entre le public et l'administration, à l'exception de ceux dont la communication porterait atteinte à un secret protégé par la loi.

1. Généralités

Les mentions de confidentialité spécifiques ne relèvent pas du secret de la défense nationale mais contribuent au respect des autres secrets protégés par la loi ainsi qu'à la protection des informations sensibles en apportant le marquage nécessaire pour attirer l'attention du détenteur et des personnes ayant accès au document.

Leur objectif principal est de sensibiliser l'utilisateur à la nécessaire discrétion dont il doit faire preuve dans la manipulation des informations couvertes par ces mentions.

La divulgation non autorisée de ces informations peut être de nature à compromettre gravement les intérêts de l'entité concernée en portant atteinte à son potentiel scientifique et technique, à ses positions stratégiques, à ses intérêts commerciaux ou financiers, son personnel, l'organisation d'examens ou de concours, ou à sa capacité concurrentielle. Elles permettent d'indiquer le domaine couvert par la protection : *Confidentiel Personnel*, *Confidentiel Médical*, *Confidentiel Technologie*, *Confidentiel Industrie*, *Confidentiel Commercial*, *Confidentiel Concours*,...

¹⁷⁵ Abus de confiance, violation du secret professionnel ou de non-respect des règles relatives au traitement des données à caractère personnel.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.5**

L'obligation de confidentialité et de discrétion qu'imposent les mentions de confidentialité spécifiques, à l'exception du secret médical et en cas de violation du secret professionnel n'est pas soumise au code pénal. La violation d'une mention spécifique de protection n'est donc pas assortie de sanctions pénales et ne constitue pas une compromission. Les sanctions sont alors de deux ordres :

- disciplinaire (avertissement, mise à pied, mutation, ou licenciement, avertissement, consigne, réprimande, blâme, arrêt, etc.) ;
- professionnelle (retrait notamment partiel ou total, temporaire ou définitif d'une qualification professionnelle, prononcée par décret en Conseil d'Etat pour les militaires).

L'attribution de ces mentions de confidentialité spécifiques relève des autorités définies au paragraphe 2, qui définissent le champ des informations couvertes par chacune de ces mentions de confidentialité et les personnes ayant besoin d'en connaître. Elles fixent les règles dans une note.

Une information particulière des personnes internes ou extérieures à l'organisme ayant besoin d'en connaître doit être réalisée par l'OS. Une attestation de responsabilité est signée par les personnes concernées ; elle est conservée par l'OS. Le contrat de travail ou de stage comprend une clause de confidentialité pour les personnes ayant accès à ces informations.

Les supports de l'information confidentielle portent le marquage de la mention de confidentialité spécifique. Hormis le timbre portant la mention de confidentialité spécifique, toutes les règles définies pour la mention *Diffusion Restreinte* sont applicables à ces mentions de confidentialité. **Le timbre doit être de couleur rouge et n'être apposé sur les documents papier qu'en haut de la page.**

2. Nature des différentes mentions de confidentialités spécifiques et détermination des autorités habilitées à décider de l'emploi de ces mentions**a. Confidentiel Médical**

Pour les informations relevant du secret médical concernant une personne, la décision relève du directeur du service de santé des armées. Le secret médical est défini par l'article R. 4127-4 du code de la santé publique comme étant le secret professionnel institué dans l'intérêt des patients et qui s'impose à tout médecin. Le secret médical entre dans le cadre de l'article 226-13 du code pénal, qui définit le secret professionnel (cf. fiche 3.10).

Besoin d'en connaître : le personnel médical, paramédical et médico-administratif du MINARM assujetti aux obligations du secret professionnel médical, dans les limites de ses responsabilités au sein du service de santé des armées. Les intéressés ont la possibilité de consulter les dossiers les concernant.

b. Confidentiel Personnel

Pour les informations relatives à la vie privée ou professionnelle des personnels militaires et civils du ministère : notations, travaux d'avancement, déroulement de carrière, enquêtes sociales ; cette mention peut être complétée en précisant la catégorie de personnel concernée, par exemple : *confidentiel personnel sous-officier, confidentiel*

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.5**

officiers généraux. La décision relève des autorités responsables de la gestion du personnel au sein des différents EMDS.

Besoin d'en connaître : les autorités hiérarchiques de la personne concernée, les personnels chargés de l'administration des ressources humaines, les services contentieux et les intéressés dans la limite autorisée par les procédures de gestion (il ne peut être fait obstacle à une demande de communication de ces informations que si elle est de nature à porter atteinte à la protection de la vie privée ; cf. 1^{er} de l'article L. 311-6 du CRPA).

c. Confidentiel Protection Personnel

Pour les informations qui, dans le cadre des procédures d'instruction des dossiers de contrôle de sécurité, ne sont pas couvertes par le secret de la défense nationale. La décision relève du directeur du service enquêteur.

Besoin d'en connaître : le personnel du service enquêteur, les autorités compétentes pour décider des habilitations ainsi que les OS, les directions de personnels et organismes de gestion pour ce qui concerne les décisions.

d. Confidentiel Concours

L'inscription de la mention est de la responsabilité des organisateurs, dans le cadre de l'organisation des concours, des examens, des épreuves de sélection au sein du ministère.

Besoin d'en connaître : les autorités hiérarchiques en charge de l'organisation, le personnel chargé de préparer les sujets et/ou de corriger les copies, le personnel chargé de surveiller le bon déroulement des épreuves. Les convoyeurs en charge du transport des sujets ou des copies ne sont pas autorisés à en prendre connaissance.

e. Confidentiel Industrie

Pour les informations dont la divulgation peut porter préjudice à des établissements publics ou privés lorsqu'elles ressortent du secret en matière industrielle hors contrat avec détention ou avec accès aux ISC. Cette mention peut couvrir :

- l'acquisition de certains matériels ;
- la politique industrielle ;
- les rapports des commissaires du gouvernement ;
- les données industrielles des directions et services techniques de la défense ;
- les échanges entre le service enquêteur et les autorités d'habilitation ou contractantes dans le cadre des procédures d'habilitation des établissements industriels.

Cette mention peut être complétée par le nom de la société ou de l'organisme d'État lorsqu'il s'agit de protection des droits de propriété industrielle.

f. Confidentiel Technologie

Pour les informations dont la divulgation peut porter atteinte au secret en matière de recherche ou de technologie, dans la mesure où elles ne relèvent pas du secret de

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.5**

défense¹⁷⁶. Cette mention peut être complétée par le nom de la société ou de l'organisme d'État lorsqu'il convient de sauvegarder l'identité de ces derniers ou leurs droits sur les résultats des recherches, en vue de leur exploitation ultérieure.

g. Confidentiel Commercial

Pour les informations relatives à des négociations commerciales menées pour le compte d'établissements industriels de la défense ou effectuées dans le cadre d'exportation de matériels d'armement dont il convient de préserver la confidentialité¹⁷⁷.

L'attribution de ces trois dernières mentions de protection relève du DGA, du SGA, du chef du contrôle général des armées, des autorités responsables de la gestion des matériels dans les états-majors et grandes directions ainsi que de la DRSD dans le cadre de la protection du patrimoine de l'industrie de défense.

Besoin d'en connaître (Confidentiel Industrie, Confidentiel Technologie et Confidentiel Commercial) : dans la limite de leurs responsabilités et de leurs attributions dans les domaines concernés notamment en matière de recherches, de programmes ou de passation des contrats :

- pour les personnels de la DGA, du SGA, de la DRSD, des ADS directement intéressés ;
- pour les personnels d'entreprises ou de laboratoires du secteur nationalisé ou privé dans le cadre des contrats passés avec des organismes relevant du ministère.

3. Élaboration et marquage

L'élaboration des documents de confidentialité spécifique doit être effectuée dans les locaux des autorités directement concernées, et sous leur responsabilité, par des personnes présentant les garanties de discrétion de par leur statut ou leur lien contractuel avec ces autorités.

Les documents de confidentialité spécifique doivent porter les marquages suivants :

- sur la première page, les références : organisme émetteur, date d'émission, numéro d'enregistrement;
- sur chaque page, le timbre adapté avec encre rouge, apposé au milieu du haut ;
- pour les documents reliés, le timbre adapté est placé au milieu du bas de la page de garde de la couverture.

4. Circulation et expédition

A l'intérieur d'un service, la transmission de ces documents s'effectue sans précaution particulière si le convoyeur est une personne autorisée à en connaître ou sous pli fermé dans le cas contraire.

Vers l'extérieur et/ou par un tiers, la transmission des documents doit respecter les règles suivantes :

- sous double enveloppe, soit par voie postale, soit par porteur autorisé (cf. fiche 7.8) ;

¹⁷⁶ Protection du secret en matière commerciale et industrielle ; cf. 1^o de l'article L. 311-6 du CRPA et paragraphe 2.4 de l'instruction n° 26209/ARM/SGA/DAJ du 16 août 2017 relative à la communication par les services du ministère des armées des documents administratifs aux citoyens.

¹⁷⁷ *Idem*

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.5**

- l'enveloppe intérieure porte la mention de "confidentialité spécifique" et les références du document ;
- l'enveloppe extérieure ne porte que les indications nécessaires à sa transmission.

L'envoi doit être acheminé en recommandé avec accusé de réception :

- en France métropolitaine et vers les DROM-COM par voie postale ;
- vers l'étranger par voie postale et par valise diplomatique.

L'utilisation de bordereaux récapitulatifs de pièces est préconisée ; il appartient à l'expéditeur d'en apprécier l'opportunité en fonction de la nature de l'envoi et des moyens d'acheminement utilisés.

La transmission des informations de confidentialité spécifique par moyen électronique doit appliquer la même procédure que pour le DR (cf. fiche 7.2). Celle-ci fait l'objet de mesures particulières portant sur l'identification des correspondants, l'approbation des circuits ou la protection des données par moyen de chiffrement qualifié au niveau adéquat.

5. Conservation, impression/reproduction et destruction

Les documents de confidentialité spécifique sont enregistrés au départ et à l'arrivée.

Ils doivent être conservés dans des locaux ou dans des meubles offrant des garanties de sécurité suffisantes (*a minima* fermés à clés) pour éviter leur divulgation aux personnes non autorisées.

Comme pour les documents *Secret*, leur impression/reproduction est laissée à l'initiative du destinataire et sous sa responsabilité, sauf mention contraire de l'autorité d'origine.

Le destinataire est responsable de leur destruction par des moyens ou procédés offrant toute garantie de sécurité.

Les livrets médicaux détenus par le service de santé des armées ne font pas l'objet d'une mention de confidentialité spécifique mais sont couverts par le secret médical. Ils sont conservés de manière à empêcher tout accès à des personnes n'ayant pas le besoin d'en connaître. Des dispositions de protection mécanique sont nécessaires pour assurer la sécurité des locaux conservant ces livrets. Ils sont, complétés par des dispositifs de protection électronique, si nécessaire.

6. Communication des informations de confidentialité spécifique

Ces documents ne sont communicables qu'aux personnes ayant strictement le besoin d'en connaître. Toutefois, les documents à caractère nominatif peuvent être portés à la connaissance des intéressés (ou de leurs ayants droit) dans le respect des prescriptions légales et réglementaires¹⁷⁸.

Toutefois, ces mentions ne font pas obstacle à elles-seules à la communication d'un document administratif à une personne qui en ferait la demande selon les dispositions législatives du code des relations entre le public et l'administration, à moins que leur

¹⁷⁸ Les documents comportant des mentions de confidentialité spécifique ne deviennent librement communicables qu'à l'expiration des délais prévus par l'article L.213-2 du code du patrimoine, et peuvent être communicables selon les dispositions prévues par l'article L.213-3 du code du patrimoine.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.5**

communication ne porte atteinte entre autres¹⁷⁹ au secret industriel et commercial (aspects stratégiques) ou au secret médical¹⁸⁰

¹⁷⁹ Cf. les dispositions législatives du CRPA, art. L. 311-5 A8 et L. 213-2 du Code du patrimoine.

¹⁸⁰ En cas de difficultés, les services peuvent se rapprocher de la direction des affaires juridiques (DAJ/D2P/DPSP).

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.6****CAS PARTICULIER DES INFORMATIONS ET SUPPORTS CLASSIFIES
TRES SECRET « CLASSIFICATION SPECIALE »****Références :**

- Code de la défense – Art. R. 2311-1 à 2311-5
- IGI 1300 – 1.3.1

Points clés :

- La protection des ISC *Très Secret* « classification spéciale » est organisée dans le cadre d'une réglementation particulière du Premier ministre, qui complète les dispositions de caractère général de l'IGI 1300 ; elle s'opère dans le cadre d'une chaîne de sécurité distincte de celle des OS.
- L'élaboration, le traitement, le stockage, l'acheminement, la présentation ou la destruction des ISC au niveau TS « classification spéciale » nécessitent une autorisation du SGDSN.

1. Principes

Le *Très Secret* « classification spéciale » est réservé aux ISC concernant des priorités gouvernementales en matière de défense et de sécurité nationale. Les modalités de protection et de gestion de ces ISC sont déterminées par le Premier ministre.

Aucun service ni organisme ne peut élaborer, traiter, stocker, acheminer, présenter ou détruire des informations ou supports classifiés TS « classification spéciale » sans y avoir été préalablement autorisé par le SGDSN. De plus, leur impression/reproduction totale ou partielle ainsi que leur numérisation sont formellement interdites aux détenteurs (elles ne peuvent être effectuées que par l'antenne émettrice).

Le versement aux archives des ISC TS « classification spéciale » n'est possible qu'après une procédure, obligatoire et préalable, de déclassement ou de déclassification.

2. Une chaîne de protection du secret distincte de la chaîne classique

Les prérogatives générales dévolues aux officiers de sécurité ne s'exercent pas sur les classifications spéciales qui répondent à une autre hiérarchie.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.7****ENREGISTREMENT ET INVENTAIRE****Référence :**

IGI 1300 – 7.2.2 et 7.4

Points clés :

- Les règles d'enregistrement et d'inventaire des ISC permettent d'assurer leur traçabilité et leur prise en compte par les détenteurs habilités.
- Le niveau de classification des systèmes d'enregistrement est équivalent au niveau de classification des documents qu'ils référencent lorsque leur objet est mentionné et est lui-même classifié¹⁸¹.
- Un inventaire contradictoire est effectué à chaque changement de détenteur.
- Un inventaire des ISC « papier » et des supports numériques est effectué chaque année¹⁸². Celui des informations classifiées dématérialisées n'est pas obligatoire.
- Un inventaire est classifié au niveau des ISC qu'il inventorie lorsque l'objet des documents y figure et est lui-même classifié.
- Une période ouvrée doit être banalisée et spécifiquement dédiée à l'inventaire annuel ou lors du départ du détenteur.

1. Enregistrement

Le but de l'enregistrement est d'établir sans ambiguïté l'attribution d'un ISC à un détenteur, c'est-à-dire une personne physique clairement identifiée. Tout ISC est enregistré, dans l'ordre chronologique, dans un système d'enregistrement spécifique, manuel ou informatisé (le système ou fichier doit alors être régulièrement sauvegardé notamment sur un support externe), dont l'accès est restreint aux personnes ayant le besoin d'en connaître. Si l'objet des documents est classifié et est mentionné dans le système d'enregistrement (manuel ou informatisé), celui-ci est classifié au même niveau que les documents qu'il référence. S'il est classifié, les personnes qui le manipulent doivent être habilitées au niveau requis et le SI qui l'héberge, le cas échéant, homologué à ce niveau. Si l'auteur a précisé que l'objet du document n'était pas classifié, le système d'enregistrement n'est pas nécessairement classifié.

Pour les informations classifiées dématérialisées, l'enregistrement est assuré automatiquement par le système d'information, conformément aux obligations de traçabilité qui lui sont imposées par l'IGI 1300. La matérialisation d'une information classifiée dématérialisée (impression, CDROM, ...) est tracée. De même, les transferts d'un SI classifié à un autre SI classifié sont tracés (éventuellement par une passerelle).

Pour les ISC matériels (papiers et supports numériques), le nombre et le numéro des supports attribués à chaque destinataire ainsi que le numéro des exemplaires conservés par l'émetteur sont inscrits dans le système d'enregistrement. Ce numéro apparaît sur chaque ISC. Le détenteur assume alors la responsabilité de la protection du support. Cet enregistrement est la seule référence de cette attribution de responsabilité. Pour un

¹⁸¹ 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.

¹⁸² Les services d'archives définitives et intermédiaires du MINARM répondent à des dispositions qui leurs sont propres.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.7**

support numérique, dans la mesure du possible, le numéro d'enregistrement est assorti d'une fiche où sont inscrites les références des informations contenues.

La position des supports classifiés est suivie sans discontinuité, notamment dans le système d'enregistrement des supports classifiés (cf. [annexe 11](#) - modèle de fiche de position).

Enfin, pour chaque support classifié, il est précisé dans le système d'enregistrement l'échéance de classification fixée par l'auteur de l'information.

Un modèle des renseignements qui doivent se trouver dans le système d'enregistrement (papier ou dématérialisé) est donné en [annexe 12](#).

a. Au niveau Secret

Un système d'enregistrement, mis en place par le responsable de l'organisme avec l'appui de l'OS, est tenu par le service en charge de la gestion des ISC de ce niveau (BPS, le cas échéant). Il peut être relié à une base de gestion du courrier sous réserve que l'accès à la base soit restreint et qu'elle permette de tracer les détenteurs jusqu'au document final.

b. Au niveau Très Secret

Chaque support d'informations classifiées à ce niveau fait l'objet d'une double numérotation présentée sous la forme d'une fraction comportant le numéro d'enregistrement de l'émetteur sur le numéro d'enregistrement du bureau de protection du secret chargé de leur traitement (cf. modèle - [annexe 13](#)).

2. L'inventaire

L'inventaire consiste à vérifier la concordance entre le stock physique et réel d'ISC et ceux listés dans les registres. Il est classifié au même niveau que les documents qu'il inventorie lorsque l'objet des documents y figure et est lui-même classifié. Les services d'archives répondent à des dispositions d'inventaire qui leurs sont propres.

Sur les consignes du service émetteur, le détenteur procède à l'examen de la pertinence de la conservation ou du maintien en classification de l'ISC. Au moment de l'inventaire, chaque organisme détenteur vérifie, en outre, dans la base interministérielle des décisions de déclassification (cf. fiche 7.12) si les supports qu'il détient ont fait l'objet d'une déclassification et procède, le cas échéant, à leur déclassification.

Un document de travail (ex : brouillon, courriel...) est identifié, protégé et suivi mais ne nécessite pas d'être inventorié (cf. fiche 7.1).

L'inventaire des informations classifiées dématérialisées au sein d'un système d'information n'est pas nécessaire, leur suivi étant assuré par la traçabilité interne du système d'information renforcée par les exigences organisationnelles et logiques prévues par la PSSI ministérielle (pour le département ministériel) ou par la présente instruction pour les entreprises contractantes.

L'inventaire est réalisé lors d'une mutation ou annuellement :

- lors du changement de titulaire d'un emploi figurant au catalogue des emplois, il est procédé à un inventaire détaillé contradictoire entre les titulaires montant et descendant et signé des deux personnes. Cet inventaire est enregistré et conservé au

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.7**

niveau de l'organisme et permet de connaître le responsable actuel de l'ISC (cf. [annexe 14](#)).

- un inventaire des ISC matériels (support et documents papiers) est réalisé chaque année et arrêtée au 31 décembre. Les dates d'expiration de validité sont vérifiées aux fins de déclasserement ou de déclassification : la réévaluation du niveau de protection des ISC est réalisée et, le cas échéant, leur destruction ou leur versement aux archives est étudié.

a. Au niveau Secret

L'inventaire annuel est effectué par chaque détenteur sous la supervision de l'officier de sécurité ou du bureau de protection du secret s'il existe.

b. Au niveau Très Secret

L'inventaire annuel est effectué par les détenteurs sous la supervision du 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 échéant, de l'une ou l'autre des pièces administratives suivantes :

- un bordereau de prise en compte ;
- un procès-verbal de destruction (fiche 7.13) ;
- une fiche de suivi du support (IGI 1300 – 7.3.2.1.a et fiche 7.8) ;
- un procès-verbal de versement à un dépôt d'archives.

Banalisation d'une période dédiée à l'inventaire :

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.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.8****DIFFUSION ET TRANSPORT DES INFORMATIONS ET SUPPORTS
CLASSIFIES****Références :**

- IGI 1300 – 7.3. et annexes 41 à 44
- Instruction n° 132/ARM/SGA/SPAC du 14/12/2017 relative au traitement des valises diplomatiques vers ou depuis l'étranger pour le compte du ministre des armées.
- Instruction n° 133/ARM/SGA/SPAC du 14/12/2017 relative à la transmission des courriers classifiés en partance ou en provenance des départements ou régions français d'outre-mer et collectivités d'outre-mer.

Points clés :

- La transmission physique d'ISC répond à des modalités précises, différenciées suivant le niveau de classification et le lieu de destination.
- La transmission dématérialisée d'informations classifiées via un système d'information homologué doit être privilégiée à l'envoi de supports physiques (papier, CD-Rom...).
- Quel que soit le mode de transport, la traçabilité de l'ISC est toujours assurée.

1. Cas général de transmission physique d'un ISC

Lorsqu'une information classifiée ne peut être diffusée via un système informatique homologué, une transmission physique n'est possible que selon les modalités décrites dans les tableaux présentés dans cette fiche.

- Si la diffusion de l'information se fait lors d'une réunion, les prescriptions de la fiche 5.3 doivent être appliquées.
- **L'expédition par voie postale d'ISC de niveau Très Secret est interdite.**
- **Pour l'expédition par voie postale d'ISC de niveau Secret :**
 - L'emploi du recommandé de niveau R3 avec accusé de réception est privilégié.
 - La preuve de dépôt du recommandé ainsi que la preuve de distribution du recommandé est archivée par le BPS ou le bureau courrier en charge des ISC.
 - Si le BPS ou le bureau courrier en charge des ISC passe par un vaguemestre pour l'envoi postal, une prise en charge de l'enveloppe est assurée (notion de traçabilité).
 - Si un bureau courrier ou un secrétariat reçoit un recommandé contenant des ISC, il doit pouvoir le stocker provisoirement (de plusieurs heures à plusieurs jours) dans un meuble et un local adaptés (cf. fiche introductive du titre 5), avant de pouvoir le remettre au destinataire final.
- **Les supports marqués *Spécial France* ne peuvent sortir des frontières du territoire que par la valise diplomatique (VD), ou en cas d'urgence par lettre de courrier¹⁸³ délivrée**

¹⁸³ La "lettre de courrier de cabinet" garantit l'immunité diplomatique à son porteur pour la durée de la mission. Elle est nominative et doit être sollicitée auprès du BCAC.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.8**

par le ministère de l'Europe et des affaires étrangères (MEAE). Les expéditions vers l'outre-mer impliquent parfois un transit par des pays étrangers et un incident peut amener un vol direct à faire une escale imprévue dans un pays étranger. Dès lors, les expéditions vers ces destinations doivent bénéficier du même niveau de protection qu'un courrier à destination de l'étranger.

- Les procédures d'expédition permettent de respecter des délais compatibles avec le degré d'urgence, d'assurer le suivi et de garantir l'intégrité physique du support classifié grâce à un conditionnement spécial.
- Avant toute diffusion d'un ISC, le service émetteur 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 à l'ISC.

a. Emission

Les autorités d'expédition sont :

- au niveau *Secret*, les personnes en charge de la gestion des ISC à ce niveau (par exemple : le bureau de protection du secret) ;
- au niveau *Très Secret*, le bureau de protection du secret (BPS, cf. fiche 2.7).

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, cf. fiche 7.11). A l'intérieur d'un site ou d'une même emprise, une fiche de suivi, établie pour chaque support classifié au niveau *Très Secret*, permet d'en contrôler la position et est élargée 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*.

Après marquage et enregistrement de chaque support, il est procédé aux opérations suivantes :

Conditionnement :

L'envoi de supports classifiés se fait sous double enveloppe présentant des garanties de solidité de nature à assurer au maximum l'intégrité physique des supports :

- l'enveloppe extérieure : renforcée et plastifiée, 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 ou de protection, la référence des supports transmis, le cachet de l'autorité expéditrice, le

La VD ainsi transportée ne peut être adressée qu'à une représentation diplomatique française ou à un poste diplomatique ou consulaire, à l'exclusion de toute autre destination militaire ou civile située sur le territoire étranger. Seul un personnel militaire ou civil habilité de la défense peut en être le bénéficiaire. Ces convois doivent se conformer aux mêmes règles de sécurité que celles imposées aux courriers de cabinet par le MEAE.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.8**

nom et la fonction du destinataire ainsi que l'indication de l'entité dans laquelle il est affecté.

Suivi de l'envoi :

L'expéditeur reste responsable de l'ISC transporté jusqu'à sa prise en compte par le destinataire.

Le bordereau d'envoi, sans timbre de classification ni indication de l'objet des informations envoyées, comporte **trois feuillets détachables si possible de couleurs différentes A, B et B'** (cf. IGI 1300 - annexe 41), signés par le responsable de l'autorité expéditrice ou une personne désignée par lui :

- les feuillets A (blanc) et B (vert) sont placés dans l'enveloppe intérieure de sécurité et sont adressés au destinataire qui conserve le premier (A) comme élément de preuve et renvoie le second (B) à titre d'accusé de réception ;
- le feuillet B' (rose) est conservé par l'expéditeur jusqu'à réception du feuillet B qui lui est alors substitué.

La différence de couleur des bordereaux permet une visualisation rapide par l'expéditeur des accusés de réception (volets B) manquants.

En cas de convoyage, l'expéditeur s'assure de la date et de l'heure de livraison. Il en avise aussitôt le service destinataire par courrier électronique. Pour les envois postaux, il indique au service destinataire le bureau de dépôt du courrier et les références du support, à l'exclusion de leur objet et de leur caractère secret. La traçabilité physique ou logique doit être assurée en permanence. En cas de retard anormal, il y a suspicion de compromission. Le bureau de protection du secret ou le service destinataire met alors en œuvre les dispositions à suivre en cas de compromission (cf. titre 8).

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. Si l'ISC ne transite pas par valise diplomatique, le porteur doit être muni d'un certificat de courrier (cf. définition en [annexe 17](#)).

Pour le cas d'envoi via un système d'information, l'accusé de réception type signature ACID doit être mis en place. Les modalités de suivi (bordereaux, etc.), décrites ci-dessus, ne concernent que les supports expédiés par voie physique, et non les informations transmises de façon dématérialisée.

TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES TOUT AU LONG DE LEUR CYCLE DE VIE 7.8

Transport de documents DR et d'ISC sur le territoire national

	Détenteur	Personne du service de courrier interne	Personnel MINARM habilité au niveau Secret OU Convoyeur autorisé MINARM	Personnel autre organisme détenteur habilité au niveau Secret OU Convoyeur autorisé d'un autre organisme détenteur	Voie postale (opérateur autorisé ¹⁸⁵)	Valise diplomatique Porteur muni d'une lettre de courrier ¹⁸⁶
Au sein de l'emprise	DR	X	X	X	Sans objet	Sans objet
	DRSF	X	X	X	Sans objet	Sans objet
	S	X	X	X	Sans objet	Sans objet
	TS	X	X	X	Sans objet	Sans objet
En métropole	DR	Sans objet	X	X	X	Sans objet
	DRSF	Sans objet	X	X	X	Sans objet
	S	Sans objet	X	X	X	Sans objet
	TS	Sans objet	X	X	Interdit	Sans objet
De et vers l'outre-mer	DR	Sans objet	X	X	X ¹⁸⁶	X
	DRSF	Sans objet	Interdit	Interdit	Interdit	X
	S	Sans objet	+ certificat de courrier ¹⁸⁷	+ certificat de courrier ¹⁸⁷	X ¹⁸⁶	X
	S-SF	Sans objet	Interdit	Interdit	Interdit	X
	TS	Sans objet	+ certificat de courrier ¹⁸⁷	+ certificat de courrier ¹⁸⁷	Interdit	X
	TS-SF	Sans objet	Interdit	Interdit	Interdit	X

¹⁸⁴ 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.

¹⁸⁵ Le service « courrier convoyé » (CC) est une déclinaison au sein du ministère des armées du service « valise diplomatique » mis en œuvre par le MEAE. Il vise à étendre le périmètre de la « valise diplomatique » à des destinations non couvertes par le MEAE. Chaque « courrier convoyé » est soumis aux mêmes exigences qu'une « valise diplomatique », mais le convoyeur est un agent du ministère des armées ou du ministère de l'intérieur, désigné par le ministère des armées, ce dernier étant responsable du transport.

¹⁸⁶ A la condition impérative de confier le transport à La Poste ou une de ses filiales répondant aux conditions du transport postal en métropole. Il est fait usage du service prioritaire « recommandé international », sous réserve que l'instruction de sécurité du programme l'autorise.

¹⁸⁷ Sont exclus du domaine d'utilisation du certificat de courrier en raison de ses limites d'emploi les documents, équipements et/ou composants classifiés de l'OTAN ; dans ce cas, le certificat de courrier est remplacé par un ordre de mission de courrier établi selon les dispositions des directives OTAN AC/35-D/2002 (appendice 1 à son annexe) et AC/35-D/2003 (appendice 8).

7.8

TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES TOUT AU LONG DE LEUR CYCLE DE VIE

Transport de documents DR et d'ISC de et vers l'étranger

		Détenteur	Personnel MINARM habilité au niveau Secret OU Convoyeur autorisé MINARM	Personnel autre organisme détenteur habilité au niveau Secret OU Convoyeur autorisé d'un autre organisme détenteur	Voie postale (opérateur autorisé ¹⁸⁴)	Valise diplomatique Porteur muni d'une lettre de courrier ¹⁸⁵
OTAN / UE	DR	X	X	X	X ¹⁸⁶	X
	DRSF	interdit	interdit	interdit	interdit	X
	S	+ certificat de courrier ¹⁸⁷	+ certificat de courrier ¹⁸⁷	+ certificat de courrier ¹⁸⁷	X ¹⁸⁶	X
	TS	+ certificat de courrier ¹⁸⁷	+ certificat de courrier ¹⁸⁷	+ certificat de courrier ¹⁸⁷	interdit	X
	S ou TS-SF	interdit	interdit	interdit	interdit	X
De et vers l'étranger (avec AGS)	DR	X	X	X	X ¹⁸⁶	X
	DRSF	interdit	interdit	interdit	interdit	X
	S	Si prévu par accord + certificat de courrier	Si prévu par accord + certificat de courrier	Si prévu par accord + certificat de courrier	Si prévu par accord ¹⁸⁶	X
	TS	Si prévu par accord + certificat de courrier	Si prévu par accord + certificat de courrier	Si prévu par accord + certificat de courrier	interdit	X
	S ou TS-SF	interdit	interdit	interdit	interdit	X
De et vers l'étranger (sans AGS)	DR	interdit	interdit	interdit	X ¹⁸⁶	X
	DRSF	interdit	interdit	interdit	interdit	X
	S	interdit	interdit	interdit	interdit	X
	TS	interdit	interdit	interdit	interdit	X
	S ou TS-SF	interdit	interdit	interdit	interdit	X

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.8****b. Réception**

La réception est assurée au niveau *Secret* par le service en charge de la gestion des ISC ou, à défaut, par le destinataire de l'envoi, ou au niveau *Très Secret*, par le BPS de l'entité destinataire, suivant la procédure suivante :

- l'intégrité de l'emballage est vérifiée afin de déceler une éventuelle compromission ;
- l'enveloppe intérieure ne doit être ouverte que par le BPS (obligatoire pour le TS), ou par le service en charge de la gestion des ISC à ce niveau ou le destinataire du courrier (S).
- au niveau *Secret*, le destinataire fait procéder à son enregistrement, ou au niveau *Très Secret*, le BPS enregistre l'ISC :
- pour le support physique, le feuillet B du bordereau d'envoi est signé et renvoyé à titre d'accusé de réception. Le bureau de protection du secret transmet l'information classifiée *Très Secret* au destinataire.

Ces règles s'appliquent à la réception, par voie physique, des ISC devant faire l'objet d'un enregistrement (cf. fiche 7.7). Dans le cas d'une information classifiée dématérialisée, la réception est assurée par les obligations de traçabilité des SI 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.

2. Cas particuliers**a. Transport d'informations classifiées sur un support de stockage numérique**

Les informations classifiées stockées sur un support amovible sont, lorsqu'elles sont transportées en dehors d'une zone protégée, acheminées conformément aux règles décrites ci-dessus.

L'utilisation d'un produit ou d'un mécanisme de chiffrement agréé par l'ANSSI, dans le respect des instructions d'emploi associées à cet agrément, permet, conformément aux directives de l'agrément, de déroger aux dispositions du paragraphe relatif au transport de supports classifiés.

b. 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.

Pour le niveau *Secret*, à l'étranger, la surveillance permanente par l'utilisateur est systématiquement recherchée par le dépôt du poste dans une représentation française (consulat, ambassade, coopération, opération extérieure,...). Par mesure de précaution, des solutions physiques (étiquettes ou enveloppes de sécurité, etc.) permettent de détecter une tentative d'accès frauduleux au poste ou une atteinte à son intégrité.

Un équipement mobile traitant d'informations classifiées fait l'objet de vérifications régulières de sa configuration physique, en particulier avant qu'il soit reconnecté sur le système d'information homologué de son organisme d'appartenance.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.8**

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 concernant le nucléaire de défense tenue à jour par le ministère des armées, il convient de se reporter aux dispositions particulières¹⁸⁸.

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.

Les exigences liées au suivi de l'envoi de supports classifiés (bordereau, etc.) sont applicables aux matériels classifiés.

Le transport des matériels classifiés est effectué, sauf impossibilité absolue ou opération conjointe, par des moyens nationaux. A défaut, ils sont convoyés et toutes les dispositions sont prises pour que la sécurité soit assurée sans discontinuité pendant toute la durée du transport. Le recours par voie contractuelle à un transitaire agréé par les autorités portuaires ou aéroportuaires peut être requis lorsqu'il existe des restrictions d'accès à certaines zones aéroportuaires ou maritimes. Dans ce cas, le matériel est placé sous la responsabilité du transitaire qui en assure le suivi (voire le stockage temporaire) entre le moyen de transport (soute de l'avion ou du navire) et la zone où il sera remis au représentant du Ministère. Avant tout transfert de matériel classifié, un certificat de courrier (cf. IGI 1300 - annexes 43 et 44) est établi pour le porteur. Un plan de transport peut être exigé par l'ANS ou l'ASD compétente, en fonction du poids ou des dimensions du matériel.

¹⁸⁸ 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.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.9****IMPRESSION/REPRODUCTION DES INFORMATIONS CLASSIFIEES****Références :**

- IGI 1300 – 7.2.4 et annexes 39 et 40
- IM n° 7326/ARM/CAB du 25 juin 2018, relative à la PPSI du MINARM.

Points clés :

- La reproduction et l'impression d'informations classifiées sont placées sous la responsabilité du détenteur.
- Les ISC reproduits doivent être obligatoirement tracés :
 - la traçabilité des ISC papier est organisée par l'OS, via la tenue d'un registre (manuel ou informatisé) ;
 - la traçabilité des ISC dématérialisés est considérée comme étant automatique sur les SI classifiés homologués grâce au niveau élevé d'exigences que doivent remplir ces SI en matière de traçabilité et d'imputabilité des actions réalisées.
- Les matériels utilisés pour ces actions doivent répondre à des conditions de protection physique et d'homologation pour les matériels connectés sur des systèmes d'information.

Le détenteur est responsable de la reproduction ou de l'impression des informations classifiées qu'il détient.

Les matériels utilisés pour la reproduction d'informations classifiées (photocopieurs, télécopieurs, systèmes informatiques, etc.) sont physiquement protégés afin d'en limiter l'emploi aux seules personnes autorisées. Si ces matériels sont connectés à un SI, ils sont intégrés dans le périmètre d'homologation de ce SI et doivent être homologués au même niveau. Les opérations de maintenance sur ces matériels sont effectuées dans des conditions permettant de garantir la sécurité des informations classifiées qui ont été reproduites, dans le respect des dispositions de la présente instruction. Il en est de même pour leur mise au rebut, qui doit garantir la destruction des mémoires de ces appareils. Le détenteur veille à limiter la diffusion au strict besoin d'en connaître.

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 ISC à ce niveau, la trace du nombre et des destinataires des exemplaires papiers reproduits (enregistrement et suivi suivant les règles décrites dans la fiche 7.7). Pour les informations classifiées dématérialisées, cette obligation de conservation est assurée automatiquement grâce aux obligations de traçabilité interne du SI.

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.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.9****2. Au niveau *Très Secret***

La reproduction totale ou partielle des ISC de ce niveau n'est possible qu'avec l'autorisation écrite préalable de l'autorité émettrice.

Le détenteur de l'information papier ou sur support classifié qui souhaite en effectuer une reproduction adresse une demande motivée (cf. IGI 1300 - annexe 39) à cette autorité *via* son bureau de protection du secret (BPS, cf. fiche 2.7), en précisant le nombre d'exemplaires. Si l'autorité émettrice consent à la reproduction (cf. IGI 1300 - annexe 40), elle porte mention de cette reproduction sur l'exemplaire en sa possession. Le BPS 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 BPS :

- 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.

Des extraits d'informations classifiées à ce niveau peuvent être reproduits et sont enregistrés selon les conditions indiquées ci-dessus.

Pour les informations classifiées dématérialisées, ce suivi est assuré par les obligations de traçabilité du SI précisées dans la PSSI (entités ministérielles) ou dans la présente instruction.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.10****STOCKAGE DES INFORMATIONS ET SUPPORTS CLASSIFIES****Références :**

- Code du patrimoine – Art. L. 212-2 et L. 212-3 (destruction)
- IGI 1300 – 7.2.3
- IM n°7326-2/DEF/CAB du 25 juin 2018 relative à la politique de sécurité du système d'information du ministère de la défense

Points clés :

- La responsabilité de la conservation des ISC incombe à leur détenteur
- Les ISC « physiques » sont stockés dans des meubles et locaux adaptés
- Les ISC « dématérialisées » sont stockées sur un système d'information classifié homologué au même niveau ou au niveau supérieur

1. Règles générales relatives au stockage des ISC

Chaque ISC est suivi de son élaboration à sa déclassification ou à sa destruction. Le responsable d'organisme met en place des moyens de conservation sécurisés et pérennes. La responsabilité de la conservation des ISC incombe au détenteur, sous la supervision du BPS ou des personnes en charge de la gestion des ISC.

Le traitement ou la conservation d'ISC classifiés TS ne peut intervenir dans des locaux, sauf en cas d'impossibilité majeure, qu'après l'avis technique d'aptitude physique (ATAP, cf. fiche 5.6) du service enquêteur sur l'aptitude de ces locaux à conserver des ISC de ce niveau.

Les **ISC « physiques »** sont stockés, en dehors des périodes d'utilisation, dans des meubles et locaux adaptés. Les combinaisons des meubles sont changées tous les ans et à chaque fois, en cas de mutation des utilisateurs, d'identification d'un risque ou de suspicion de compromission. Les prescriptions sont définies par l'IGI 1300 et précisées dans la présente instruction. Pour garantir le cloisonnement, les ISC émis par les États étrangers ou par des organisations internationales sont conservés de façon séparée des informations nationales (cf. fiche 9.4).

Les **ISC « dématérialisées »** sont stockées sur un système d'information (SI) classifié homologué au même niveau ou au niveau supérieur. Les prescriptions sont définies par la PSSI ministérielle ou précisées au titre 6 pour les organismes qui ne sont pas soumis à cette dernière. Les exigences de sécurité relatives à la sécurité du système d'information de l'organisme prévoient des moyens et des procédures de sauvegarde et de conservation sécurisés et pérennes des informations classifiées contenues au sein des SI classifiés utilisés. Ces moyens et procédures respectent le besoin d'en connaître.

Les systèmes d'information appelés à traiter des informations classifiées doivent faire l'objet d'une homologation (cf. fiches 6.2 et 6.3).

2. Cas particuliers

- Les **ISC dites hors coffres** : certains ISC de grande dimension (prototypes ou objets classifiés, par exemple) ne peuvent pas être conservés dans les meubles prescrits pour

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.10**

leur niveau de classification. Dans ces conditions, les règles particulières à appliquer sont précisées dans la fiche 5.2 de la présente instruction.

- Les **moyens mobiles** (aéronefs, navires, etc.) susceptibles de faire escale ou s'implanter temporairement à l'étranger et dans lesquels des informations et supports classifiés sont stockés doivent se conformer aux principes de la fiche 5.2 de la présente instruction (hors opérations, qui répondent à des procédures particulières).

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.11****VERSEMENT DANS UN SERVICE D'ARCHIVES****Références :**

- IGI 1300 – 7.5.4 et 7.5.5 et annexe 46
- Code du patrimoine – Art. L. 212-2 et L. 212-3 (destruction)
- Arrêté du 5 novembre 2012 fixant la liste des dépôts d'archives du ministère de la défense
- Instruction n°101/DEF/SGA/DMPA/DPC du 29 juillet 2011 relative à la politique et à l'organisation générale de l'archivage du ministère de la défense et des anciens combattants

Points clés :

- Les archives intermédiaires et définitives, dont les ISC (TS classification spéciale exclus), sont versées dans des services d'archives relevant du ministère.
- Un ISC ne peut être isolé du dossier auquel il appartient et doit par conséquent être versé dans le même fond d'archives. Les services d'archives définitives (SHD pour les archives papier et électronique, ECPAD pour l'audiovisuel) sont sollicités pour connaître les lieux de versement.
- Les ISC émis par les États étrangers ou dans le cadre d'organisations internationales doivent être archivés de façon à les séparer clairement des informations nationales.

Avant leur versement, les ISC sont correctement marqués et répertoriés. En outre, le chef d'organisme de l'auteur des ISC vérifie systématiquement la pertinence de la classification et sa durée de vie et décide le cas échéant de les déclassifier, de les déclasser (éventuellement de les reclasser) (cf. fiche 7.12). Le service versant consulte la base interministérielle¹⁸⁹ des décisions de déclassification 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. A l'occasion du versement, le service d'archives peut, s'il le juge opportun, proposer au service émetteur la déclassification ou le déclassement d'un document. Le service émetteur reste compétent pour décider du niveau de classification des ISC qu'il a produits.

1. Versement aux archives des documents classifiés

On distingue :

- les **archives courantes**, lorsque les documents sont d'utilisation habituelle pour l'activité des services ;
- les **archives intermédiaires**, lorsque, n'étant plus considérées comme archives courantes, les documents ne peuvent encore en raison de leur intérêt administratif faire l'objet d'un tri ou d'une élimination ;

¹⁸⁹ Lorsque cette dernière sera mise en service. Les procédures d'emploi de cette base restent à définir à ce jour.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.11**

- les **archives définitives**, lorsque les documents ont subi les tris et éliminations nécessaires et sont à conserver sans limitation de durée¹⁹⁰.

Les ISC présentant une utilité administrative ou un intérêt historique ou scientifique sont, à l'issue de leur période d'usage courant, versés dans un service d'archives intermédiaires ou définitives. Les autres documents sont détruits (cf. fiche 7.13) après avoir reçu un visa d'élimination conformément à l'article L. 212-2 du code du patrimoine.

Le versement dans un service d'archives s'effectue conformément aux principes énoncés par les textes de référence, en suivant les directives données par l'administration des archives et selon les modalités définies par les textes techniques propres à chaque ADS.

Les ISC ne peuvent être isolés du dossier auxquels ils appartiennent et du reste de leur fonds d'archives, afin de conserver l'intégrité des informations. Il convient de consulter les services d'archives définitives (SHD pour les archives papier et électronique, ECPAD pour l'audiovisuel) pour connaître les lieux de versement déterminés par l'administration des archives (en fonction du type de fonds, de leur intérêt ou de leur ancienneté).

2. Conservation des archives classifiées

Le niveau de classification maximal des ISC qui peuvent être détenus par les différents services d'archives varie d'un service à l'autre, mais aucun n'est en mesure d'abriter les ISC de niveau TS faisant l'objet d'une classification spéciale. Ceux-ci doivent faire l'objet d'une procédure de déclasserement ou de déclassification.

- a) Le SHD et l'ECPAD conservent les archives définitives et des archives intermédiaires.
- b) Les ISC peuvent également être conservés dans des services d'archives intermédiaires sous contrôle scientifique et technique de la DPMA/DPC¹⁹¹.
- c) Certains ISC peuvent enfin être versés dans un service ne relevant pas du MINARM, comme les Archives nationales ou le service d'archives des Affaires étrangères¹⁹².

¹⁹⁰ Instruction en référence.

¹⁹¹ Les services d'archives intermédiaires sont désignés par arrêté du ministre (en référence).

¹⁹² Les services du Président de la République, du Premier ministre et des ministères autres que celui des Armées reçoivent des ISC émis par le MINARM dans le cadre de leurs fonctions, et les dossiers où ils figurent sont versés par la suite aux Archives nationales ou aux Affaires étrangères.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.12****DECLASSIFICATION OU DECCLESEMENT D'UNE INFORMATION
CLASSIFIEE****Références :**

- Code du patrimoine – Art. L. 213-1 et suivants
- IGI 1300 – 7.6

Points clés :

- La date ou l'évènement entraînant la déclassification du document doit être indiqué en couverture du document lors de sa classification.
- Les ISC qui ne comportent pas une telle mention sont déclassifiés après décision de déclassification par le service auteur ou son héritier, par le HFCDS ou par le service historique de la Défense pour les documents qu'il conserve.
- Le ministre a toute latitude pour organiser et déléguer le traitement des procédures de déclassification du ministère.
- Pour les ISC étrangers, seule l'autorité étrangère émettrice peut procéder à une déclassification ou à un déclassement.

1. Définitions

La **déclassification** consiste à supprimer toute mention de classification. La déclassification d'un document peut résulter d'une décision de commandement (à l'initiative de l'autorité émettrice ou du service auteur, à la demande d'un destinataire, lors de révisions annuelles ou lors du versement aux archives), être provoquée par une requête en déclassification judiciaire (cf. fiche 5.8), par une demande de communication d'archives ou intervenir à l'issue du délai mentionné lors de la classification du document. La déclassification à date n'exonère pas de l'obligation de procéder, avant toute communication, à un examen individualisé du document. Il s'agit de s'assurer que celui-ci soit effectivement devenu communicable de plein droit et, dans le cas où la classification peut encore être prolongée, que sa communication ne soit pas de nature à porter atteinte à la défense et à la sécurité nationale.

Le **déclassement** est la modification, par abaissement, du niveau de classification d'une information ou d'un support classifié (ne s'applique qu'aux niveaux *Très Secret* et *Très Secret classification spéciale*).

Le **reclassement** consiste à apposer sur un document le niveau de classification supérieur.

2. Echéance de la classification et communicabilité

Lors de l'élaboration d'ISC, la date ou l'évènement défini précisant sa déclassification ou, exceptionnellement, la date ou le délai au terme duquel le niveau de classification doit être réévalué, est porté sur cet ISC.

Des directives techniques rédigées par les ADS encadrent les modalités de déclassification et précisent, pour chaque grande catégorie de documents, les délais de déclassification recommandés (cf. fiche 7.1).

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.12**

La déclassification d'un support n'entraîne pas pour autant automatiquement la libre communicabilité de ce support ou des informations qu'il contient. Ainsi, l'administration saisie d'une demande de communication d'une information ou d'un support régulièrement déclassifié doit s'assurer qu'aucun autre motif d'incommunicabilité ne trouve à s'appliquer en vertu des articles L. 213-2 et suivants du code du patrimoine.

Il convient, à cet égard, de souligner que les délais d'incommunicabilité mentionnés à l'article L. 213-2 sont, pour la plupart d'entre eux, décomptés à partir « de la date du document ou du document le plus récent inclus dans le dossier ». Tel est notamment le cas du délai de 50 ans prévu pour les documents dont la communication porte atteinte au secret de la défense nationale. Ces dispositions doivent être interprétées comme prescrivant un décompte à partir de la date du document demandé, quand celui-ci est isolé, et à partir de la date du document le plus récent inclus dans le dossier, dans le cas contraire.

Le « dossier », au sens de l'article L. 213-2 du code du patrimoine, ne doit pas être assimilé au carton d'archives, en tant que pièce matérielle, au sein duquel se trouve le document dont la communication est sollicitée. Il doit être regardé comme l'ensemble des pièces présentant un lien suffisamment marqué avec le document demandé. Une telle interprétation implique une appréciation, par l'administration, sous le contrôle du juge administratif, du caractère suffisant du lien en question.

Par dérogation aux dispositions de l'article L. 213-1 et du I de l'article L. 213-2, les informations classifiées dont la divulgation est susceptible d'entraîner la diffusion d'informations permettant de concevoir, fabriquer, utiliser ou localiser des armes nucléaires, biologiques, chimiques ou toutes autres armes ayant des effets directs ou indirects de niveau analogue ne comporte aucune échéance de classification et ne peuvent être déclassifiées ni communiquées.

3. Procédures de déclassification

Les dispositions qui suivent s'appliquent aux seuls ISC qui ne comportent pas mention de la date ou de l'événement défini précisant leur déclassification, ou aux documents déclassifiés avant la date d'échéance de classification.

a. Organisation de la fonction de déclassification

L'organisation de la fonction de déclassification s'exerce selon les modalités suivantes.

Les ISC étrangers :

Pour les ISC étrangers, seule l'autorité étrangère émettrice peut procéder à leur déclassification ou déclassement. Pour les ISC élaborés dans le cadre de coopérations incluant la France, seuls les pays émetteurs peuvent procéder à leur déclassification ou au déclassement.

Déclassification par le service auteur ou le service héritier :

La décision de déclassifier un ISC appartient à l'autorité émettrice, qui peut déléguer cette responsabilité au service auteur. Ce dernier peut également prendre toutes les mesures justifiées visant à déclasser ou reclasser les ISC.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.12**

Le service auteur évalue la sensibilité des informations classifiées avant de procéder éventuellement à la déclassification du document ou de l'ensemble des documents.

Lorsque le service auteur n'existe plus, la responsabilité de la décision de déclassifier, déclasser ou reclasser les ISC revient à un service identifié comme héritier¹⁹³ ou, à défaut, au HFCDS, qui a toute latitude pour organiser la fonction de déclassification du ministère.

En cas d'absence de réponse du service auteur dans les deux mois à compter de la demande de déclassification, le HFCDS peut évaluer lui-même la sensibilité des ISC et prendre la décision de les déclassifier, déclasser ou reclasser.

Documents conservés dans un service d'archives :

Toute demande de communication d'un support classifié ou d'un ensemble de supports classifiés est adressée au service détenteur des archives, qui saisit le service auteur.

Par dérogation aux dispositions énoncées ci-dessus, le SHD peut prendre toutes les mesures justifiées visant à déclasser, reclasser ou déclassifier les ISC qui figurent dans les archives qui lui sont confiées et qui sont émises par le ministère des Armées, selon les modalités suivantes :

- pour les documents de plus de cinquante ans, à l'exception de ceux relatifs à des thématiques revêtant une sensibilité particulière et qui sont listées ci-dessous, sur décision du chef du SHD ;
- pour les documents de moins de cinquante ans ou pour les documents de plus de cinquante ans relatifs à certaines thématiques revêtant une sensibilité particulière (armes nucléaires, biologiques ou chimiques, dispositifs de dissuasion, programmes d'armement encore en activité, infrastructures sensibles encore en usage), après autorisation du service auteur ou héritier, ou, à défaut, du HFCDS.

Le SHD peut également décider de classer tout ou partie des fonds entrés par voies extraordinaires dont il est dépositaire ainsi que des entretiens qu'il peut être amené à recueillir dans le cadre de sa collecte de témoignages oraux. La classification est en effet justifiée lorsque les fonds déposés contiennent des informations dont la divulgation est de nature à compromettre le secret de la défense nationale.

Les Archives nationales et le service d'archives des Affaires étrangères peuvent solliciter la DPMA pour demander la déclassification de documents conservés dans ces services mais émanant du ministère (cf. fiche 7.11). La DPMA sollicite alors le service auteur des documents.

Pour les documents de moins de 50 ans, les décisions de déclassification sont consignées dans la base interministérielle des décisions de déclassification (selon des procédures qui restent à définir à ce jour).

b. Le marquage de déclassification

Le document déclassifié avant la date d'échéance ou ne comportant pas de date d'échéance fait obligatoirement l'objet d'un marquage de déclassification spécifique

¹⁹³ Les autorités héritières sont désignées par le ministre des Armées (note n°5158/ARM//CAB/CM1/NP du 31 juillet 2018 relative à la définition des services héritiers).

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.12**

comportant la date et les références de la décision, à l'exception des documents antérieurs au 1^{er} août 1954 conservés au SHD, pour lesquels ce dernier est habilité à opérer une déclassification « au carton ». Le document déclassé ou reclassé fait lui aussi l'objet d'un marquage analogue comportant la date et les références de la décision (cf. modèle en [annexe 9](#)).

La déclassification au carton n'exonère pas de l'obligation d'examiner pièce à pièce les documents concernés. Un marquage de déclassification est, le cas échéant, apposé sur chaque page avant toute reproduction.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.13****DESTRUCTION DES INFORMATIONS ET SUPPORTS CLASSIFIES ET
DES INFORMATIONS *DIFFUSION RESTREINTE* OU SENSIBLES****Références :**

- Code du patrimoine – Art. L. 212-2 et L. 212-3 (destruction)
- IGI 1300 – 7.5.1 et 7.5.2 et annexe 45
- Instruction n° 101/DEF/SGA/DMPA/DPC du 29 juillet 2011 relative à la politique et à l'organisation générale de l'archivage du ministère de la défense et des anciens combattants

Points clés :

- La destruction est réalisée par des personnes habilitées au niveau des ISC.
- Après destruction des ISC, un procès-verbal est dressé.
- Les moyens d'impression / reproduction et de destruction des ISC doivent dans la mesure du possible être centralisés.
- Aucune destruction d'archives ne peut être réalisée sans le visa d'élimination de l'administration des archives concernée.
- De manière générale, tout document papier, même non protégé, est broyé, *a fortiori* s'il présente un caractère sensible.

1. Documents classifiés

- Les documents classifiés sont soumis à la règle commune en matière d'élimination d'archives¹⁹⁴.

Lorsque des ISC sont périmés ou devenus inutiles, il est procédé à leur destruction selon les directives données par la DPMA. Afin d'établir la distinction entre les documents à détruire et ceux nécessitant une conservation, il est nécessaire de prendre contact avec le Service Historique de la Défense (SHD) ou l'Etablissement de de Communication et de Production Audiovisuelle de la Défense (ECPAD). La DPMA, le SHD ou l'ECPAD pourront délivrer dans certains cas des visas d'élimination par anticipation (éliminations très fréquentes de documents d'un même type).

- La destruction ne peut être réalisée que par des personnes habilitées. Il est recommandé de centraliser la destruction et la reproduction de la documentation classifiée de niveau *Secret* ou *Très Secret* chaque fois que cela est possible. Un marquage est placé de façon visible indiquant les appareils conformes pour ces opérations. De même, il est recommandé de placer des signalisations interdisant la destruction sur les appareils non conformes ou non retenus pour la destruction des ISC.
- La destruction des ISC est effectuée de façon à rendre impossible toute reconstitution, même partielle, des informations contenues sur les supports. Les principales formes de destruction sont :
 - l'incinération ou le brûlage¹⁹⁵ ;

¹⁹⁴ IM de référence.

¹⁹⁵ L'incinération consiste à réduire l'ISC en cendres, le brûlage pour sa part est incinération incomplète qui ne permet pas de reconstituer ou de prendre connaissance de l'information.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.13**

- le broyage ;
- le déchiquetage ;
- la surtension électrique¹⁹⁶.

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*. Les modèles de procès-verbal figurent en annexe 45 de l'IGI 1300. Ceux-ci sont conservés pendant cinq ans.
- Au niveau *Très Secret*, le détenteur du document sollicite officiellement le service auteur et lui rend compte, sauf avis contraire de sa part, qu'il procédera à la destruction du support ([annexe 15](#)). Sans réponse dans un délai de deux mois, le service détenteur procède à la destruction du support et en rend compte au service auteur en lui adressant une copie du procès-verbal¹⁹⁷. Une copie de ce procès-verbal est transmise au bureau de protection du secret. Cette procédure n'est pas requise pour le niveau *Secret*.
- Tout support de stockage électronique classifié mis au rebut est préalablement effacé selon des procédés employant, dans la mesure du possible, des produits certifiés/qualifiés par l'ANSSI pour l'effacement (par exemple, un produit d'effacement sécurisé pour la mention *Diffusion Restreinte*). Le support électronique est ensuite détruit physiquement, selon un procédé qui rend impossible la reconstitution de tout ou partie de l'information classifiée ou sensible contenue sur ce support (si possible conforme aux recommandations du SGDSN).

2. Informations *Diffusion Restreinte* ou sensibles

Par prudence, tous les documents papiers considérés comme sensibles, ainsi que ceux portant la mention de protection *Diffusion Restreinte* et une mention de confidentialité spécifique doivent recevoir le traitement suivant :

- tous les supports papiers seront jetés dans une corbeille à papier, distincte de la poubelle de bureau, laquelle n'est destinée qu'à recueillir les gobelets, bouteilles d'eau, résidus alimentaires, etc. ;
- ces corbeilles seront vidées chaque soir par leur détenteur et leur contenu broyé (les broyeurs existants, destinés aux ISC, peuvent être utilisés).

Ces dispositions permettent de réduire le risque de *TrashInt* (*Trash Intelligence*), qui renvoie à un procédé d'espionnage réalisé par l'analyse d'informations sensibles recueillies dans les corbeilles à papier des organismes.

¹⁹⁶ Les normes techniques sont arrêtées par le SGDSN, après expertise des services compétents.

¹⁹⁷ 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 S-HFDS du ministère compétent.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.14****EVACUATION ET DESTRUCTION D'URGENCE****Références :**

- Code pénal – art. 414-7
- IGI 1300 – 7.5.3

Points clés :

- Pour faire face à des circonstances exceptionnelles, l'organisation d'une éventuelle évacuation ou destruction d'urgence est planifiée en amont.
- Lors de la rédaction des plans afférents, il est nécessaire de prendre en compte le volume des ISC à transporter ou à détruire.

1. Plan d'évacuation et de 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 ISC, des plans d'évacuation et de destruction d'urgence sont établis par chaque service ou entité qui détiennent des ISC. Ces plans prévoient notamment les procédures d'accès, en toute circonstance, aux locaux et donc aux ISC.

Les modalités d'exécution pratiques de ces plans figurent sur des fiches placées dans chaque coffre contenant des ISC. Elles précisent :

- les autorités désignées pour donner l'ordre de destruction ou d'évacuation ;
- la liste des personnes pouvant accéder aux locaux et ouvrir les meubles de sécurité pendant et hors heures ouvrables ;
- la liste et la localisation des ISC 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 au minimum tous les trois ans par l'OS de l'organisme. Ce contrôle fait l'objet d'un compte rendu diffusé aux personnes concernées, il précise les points qui doivent être modifiés. Il est conservé par l'OS de l'organisme concerné.

2. Ordre de destruction ou d'évacuation d'urgence

L'ordre de destruction ou d'évacuation d'urgence est transmis suivant les cas par :

- note écrite (ou message) revêtue de la signature de l'autorité désignée ;
- téléphone : dans ce cas l'ordre est authentifié par rappel de l'autorité désignée pour donner l'ordre de destruction, ou par tout autre moyen permettant de s'assurer de la réalité de l'ordre donné. Dans la mesure du possible l'ordre téléphonique est suivi d'une note ou d'un message ;
- de vive voix, par l'autorité désignée ou l'officier de permanence ou assimilé, notamment en cas de catastrophe naturelle.

Dans la mesure du possible, les cahiers d'enregistrement, les procès-verbaux d'inventaires, de destruction, les fiches de position des documents sont conservées. Après application des directives, il est procédé à :

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.14**

- un procès-verbal de destruction ;
- un compte rendu d'exécution.

Ces documents sont adressés à l'OS et au BPS de l'entité.

TITRE 8 : GESTION ET REPRESSION DES ATTEINTES AU SECRET DE LA DEFENSE NATIONALE

GENERALITES

Références :

- Code pénal – Art. 121-2, 413-10 à 12, 414-7 à 9
- Code de justice militaire – Art. L. 332-2
- IGI 1300 – 1.2.2.2, 1.4.1 et 1.4.2
- II n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information
- II n° 500 bis/SGDN/TTS/SSI/DR du 18 octobre 1996 relative au chiffre dans la sécurité des systèmes d'information
- Directive n° 911/DISSI/SCSSI/DR du 20 juin 1995 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)
- Directive n° 485/SGDN/TTS/SSI du 20 novembre 2013 relative à l'installation des sites et systèmes d'information pour la protection contre les signaux parasites compromettants
- IM n° 133/DEF/SEC/DIR/SIC du 18 mars 2002 modifiée, relative à la politique de sécurité des systèmes d'information du ministère de la défense
- IM n° 7326-2/DEF/CAB du 25 juin 2018 relative à la politique de sécurité du système d'information du ministère de la défense

Point clé :

La compromission se caractérise par l'accès à un ISC d'une personne non habilitée ou qui ne dispose pas du besoin d'en connaître. Elle peut être intentionnelle ou non intentionnelle.

1. Définition

Une information ou un support classifié est compromis lorsqu'une personne non habilitée ou n'ayant pas le besoin d'en connaître est susceptible d'en avoir pris connaissance. Il convient de considérer que la compromission est possible dès qu'un ISC a échappé au contrôle continu de la personne qui assure sa protection. Le compte-rendu de cette dernière est immédiat.

Cette compromission peut découler autant d'un vol, d'une consultation illicite, d'une perte, d'une erreur de traitement ou de protection que de l'exploitation de moyens électroniques, informatiques, audio et techniques. Sont ainsi punis de cinq ans d'emprisonnement et de 75 000 euros d'amende : la destruction, le détournement, la soustraction, la reproduction non autorisée d'un ISC, 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 à une ou plusieurs personnes n'étant pas qualifiées pour y accéder.

Outre des sanctions pénales, l'auteur d'un acte, commis délibérément ou non, qui compromet un secret de la défense et de la sécurité nationale, encourt l'abrogation de sa décision d'habilitation, la révision de son avis de sécurité et des sanctions disciplinaires.

TITRE 8 : GESTION ET REPRESSION DES ATTEINTES AU SECRET DE LA DEFENSE NATIONALE

Les personnes morales sont pénalement responsables des faits de compromission qui leur sont imputables et encourent, outre une peine d'amende, l'interdiction d'exercer dans le domaine d'activité dans lequel l'infraction a été commise.

2. Indices révélateurs d'une compromission

Outre le vol, la disparition ou la perte de contrôle de l'ISC, une compromission peut découler :

- d'un incident réel ou supposé d'un système d'information (SI) ou de la découverte d'un piégeage pouvant remettre en cause la confidentialité d'une information (II 910) ;
- de la modification non autorisée d'un élément de protection d'un SI (directive 911) ;
- d'un incident ou accident affectant un système d'information classifié de défense (IM 133) ;
- d'une exploitation de signaux électromagnétiques compromettants (directive 485, guide 960)
- de la pénétration dans des lieux abritant ou des locaux techniques, ou de la détention d'un moyen pouvant contribuer à la fuite d'information (téléphones portables par exemple).

**TITRE 8 : GESTION ET REPRESSION DES ATTEINTES AU SECRET DE LA
DEFENSE NATIONALE****8.1****TRAITEMENT DES COMPROMISSIONS****Référence :**

IGI 1300 – 1.4.2.3

Points clés :

- La compromission se caractérise par l'accès à un ISC d'une personne non habilitée ou qui ne dispose pas du besoin d'en connaître. Elle peut être intentionnelle ou non intentionnelle.
- En cas de suspicion de compromission, le chef d'entité prend sans délai toute mesure conservatoire et informe la DRSD¹⁹⁸, qui effectue une investigation et analyse les faits.
- Si le doute n'est pas levé sur la compromission, la DRSD¹⁹⁹ informe et transmet les éléments à la DGSI pour enquête.

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

La « suspicion de compromission » est le terme à employer lorsque la divulgation d'un ISC a été rendue possible.

La « compromission avérée » signifie qu'il est établi qu'un ISC a été porté à la connaissance d'une personne non qualifiée.

1. Action de l'autorité hiérarchique

Dès qu'un personnel d'un organisme découvre une compromission possible, il rend compte immédiatement à son autorité hiérarchique et à son officier de sécurité.

Lorsqu'une compromission est avérée ou lorsqu'il s'agit d'une suspicion de compromission, le chef d'entité se conforme en tout point à la procédure décrite ci-dessous.

Le chef d'organisme veille à faire prendre les mesures conservatoires appropriées et à informer la DRSD. En liaison étroite avec elle, les mesures suivantes sont appliquées :

- Pour les ADS uniquement, un message « FLASHEVENT », adressé à :
 - o pour action : au Cabinet du ministre (CAB/BRES), au HFCDS, aux autorités hiérarchiques à laquelle l'unité est rattachée, au directeur de la DRSD et à l'OS de niveau 1 ;Ces dispositions s'appliquent également aux cas de compromissions et de divulgations d'informations classifiées étrangères détenues par la France (cf. fiche 8.3) du fait :
 - 1/ de sa coopération avec les États de l'Alliance atlantique et de l'UE,

¹⁹⁸ Ou la DGSE, le cas échéant.

¹⁹⁹ *Idem.*

**TITRE 8 : GESTION ET REPRESSION DES ATTEINTES AU SECRET DE LA
DEFENSE NATIONALE****8.1**

2/ d'accords de sécurité bilatéraux conclus avec les États amis qui ne sont membres ni de l'une ni de l'autre de ces deux organisations et d'accords portant sur les informations classifiées échangées avec des organisations internationales.

- o pour info : à l'entité DRSD compétente localement (poste et direction régionale concernée), au délégué d'armée représentant local de l'armée considérée.
- Pour tous (ADS et entreprises contractantes) : un compte rendu détaillé dans les trente jours.
Le délai est impérativement respecté même si tous les éléments n'ont pas pu être apportés. Ils sont adressés par la suite lors d'un message complémentaire.

En cas de compromission avérée ou de suspicion de compromission, le chef de cabinet militaire du ministre, en tant que HFCDS, informe le SGDSN.

Lors d'une mission effectuée en isolé (personne seule ou en petit groupe) à l'étranger, en cas de perte ou de vol d'ISC, il convient de prévenir le plus rapidement l'ambassade de France ou le consulat, de rendre compte à sa hiérarchie, civile ou militaire et, selon les directives reçues, d'informer les autorités de police du pays.

2. Préservation des preuves et investigation

Des mesures de préservation de l'objet, du système ou des traces nécessaires à l'enquête doivent être prises dès que possible. Ces mesures conservatoires font l'objet de l'[annexe 16](#). Il est toutefois rappelé que toute investigation ou action, quelle qu'elle soit, susceptible de modifier ou détruire des éléments de preuve et de compromettre la valeur des traces informatiques est formellement proscrite. La non-observation de cette règle est susceptible d'exposer le responsable de l'action menée à des sanctions pénales (article 434-4 du code pénal).

Dans certains cas (atteinte d'un serveur ou d'un élément actif d'un réseau par exemple), les nécessités de l'enquête peuvent conduire à suspendre le fonctionnement du système d'information (II 920, IM 7326-2). Il appartient aux responsables de ce dernier de prévoir et d'adopter des solutions de secours permettant d'assurer à cette occasion une continuité de service adaptée (II 500 bis). Les mesures correspondantes doivent être décrites dans la procédure d'exploitation de sécurité du système.

Tous les éléments recueillis sont mis à la disposition de la DRSD, dans les plus brefs délais, pour la conduite de son enquête.

3. Action de la DRSD

La DRSD est le service du MINARM compétent pour le traitement des compromissions (hors DGSE). A ce titre, elle est sollicitée dès que les indices suivants sont constatés :

- dégradations d'emballage contenant des ISC ;
- disparition, définitive ou temporaire, partielle ou totale de supports susceptibles de contenir des ISC ;
- traces d'effraction dans un lieu abritant ;
- découverte d'un dispositif illicite permettant de recueillir ou d'accéder à des informations classifiées.

TITRE 8 : GESTION ET REPRESSION DES ATTEINTES AU SECRET DE LA DEFENSE NATIONALE

8.1

Informé par le chef d'organisme concerné par une compromission avérée ou une suspicion de compromission, le représentant de la DRSD, après avoir procédé aux investigations nécessaires, rédige un avis d'enquête.

Lorsque les investigations confirment la suspicion ou avèrent la compromission, la DRSD, après avoir informé le chef de l'organisme concerné et la chaîne des officiers de sécurité, transmet le dossier à la DGSI (ou à la gendarmerie prévôtale sur les théâtres d'opérations extérieures ou n zone de stationnement des forces françaises), qui procède à l'enquête judiciaire.



Les organismes liés au MINARM ou au CEA/DAM par contrat ou par convention saisissent l'entité DRSD compétente, qui rend compte à son tour à sa direction centrale. Cette dernière informe l'autorité contractante (DGA, par exemple).

**TITRE 8 : GESTION ET REPRESSION DES ATTEINTES AU SECRET DE LA
DEFENSE NATIONALE****8.2****COMPROMISSION AFFECTANT UN SYSTÈME D'INFORMATION****Référence :**

IGI 1300 – 1.4.2.4

Points clés :

- Tout support informatique potentiellement affecté par une compromission cesse d'être utilisé et est conservé dans un endroit sécurisé.
- L'OS et l'OSSI sont les acteurs agissant dans la mise en œuvre de la procédure.
- La DRSD est saisie et procède aux investigations en liaison avec l'ANSSI avant transmission éventuelle à la DGSi.

La présente fiche complète la fiche 8.1 dans le cas où la compromission (cf. définition au paragraphe 1 de la fiche 8.1) concerne un système d'information, qu'il s'agisse d'une suspicion de compromission ou d'une compromission avérée. Les dispositions prévues par la fiche 8.1 sont applicables (« FLASHEVENT », ...).

1. Réactions immédiates

Il convient de :

- Préserver le support numérique susceptible d'être affecté par une compromission (cesser d'utiliser ou de travailler sur le support, etc.) ;
- Saisir l'Officier de Sécurité, qui saisit l'Officier de Sécurité des Systèmes d'Information ainsi que la DRSD, qui prend en charge les investigations et informe l'ANSSI ;
- Le cas échéant, pour les ADS, informer l'Officier de Sécurité de la DIRISI ;
- Rassembler les éléments techniques et humains en rapport avec l'incident en cours²⁰⁰ ;

Dans le cas où les services spécialisés de la DIRISI découvrent qu'un système d'information est affecté par une compromission, ils doivent saisir la DRSD et l'officier de sécurité de l'organisme concerné qui est alors responsable de conduire les actions relatives à cette compromission.

Toutes les actions entreprises entrent dans le cadre d'une première réponse sur incident. Elles doivent impérativement être répertoriées et horodatées dans un registre dédié.

L'OSSI de l'entité concernée prend toutes les mesures nécessaires pour garantir la sauvegarde et l'intégrité des preuves techniques. Toute intervention de personnel non qualifié forensic (visualisation du contenu d'un message, fichier ou répertoire, etc.) sur la machine est de nature à laisser des traces sur le disque dur et ainsi à rendre la preuve judiciairement irrecevable. Seules des interventions justifiées par l'état de nécessité sont autorisées.

²⁰⁰ Pour préserver la validité de futures investigations judiciaires, les éléments de preuve (messages, documents...) ne doivent pas être effacés mais conservés dans des fichiers spécifiques ou à défaut sur un support classifié dédié à cette conservation. L'OS et l'OSSI doivent conserver la trace de leurs actions visant à faire cesser au plus vite la compromission.

TITRE 8 : GESTION ET REPRESSION DES ATTEINTES AU SECRET DE LA DEFENSE NATIONALE **8.2**

2. Règles de base applicables par l'organisme touché par une compromission possible (OSSI ou OS)

a. Suspicion de compromission sur une machine isolée

Si l'équipement est en fonctionnement :

- laisser la machine en fonctionnement ;
- ne pas retirer les médias amovibles connectés, s'il y en a ;

Si l'équipement a été éteint :

- ne pas rallumer la machine.

Si la machine est reliée à un serveur de stockage, appliquer les consignes *supra* au serveur.

b. Suspicion de compromission sur machine connectée au réseau

Appliquer les mêmes dispositions que celles prévues pour une machine isolée.

En complément :

- noter le numéro de la prise murale du réseau ;
- débrancher le câble réseau ;
- demander aux administrateurs du système de mettre à disposition du service enquêteur les journaux d'événements des différents équipements liés (serveurs, commutateurs,...).

3. Premières constatations et investigations

Au-delà des règles de base ci-avant, les premières constatations et les investigations ultérieures doivent être réalisées par un inspecteur de la DRSD²⁰¹ dès qu'une suspicion de compromission affectant un système d'information est signalée.

²⁰¹ Ou un agent de la DGSE, le cas échéant.

**TITRE 8 : GESTION ET REPRESSION DES ATTEINTES AU SECRET DE LA
DEFENSE NATIONALE****8.3****COMPROMISSION D'INFORMATIONS CLASSIFIEES ETRANGERES****Références :**

- Code pénal – Art. 414-8 et 9
- IGI 1300 – 1.4.2.3
- II n°910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)

Points clés :

- Les faits de compromission d'ISC étrangers doivent être signalés à l'ASD compétente ou à l'ANS.
- Il convient de bien distinguer les ISC nationaux des ISC étrangers dans l'armoire forte.

Lorsqu'une suspicion de compromission ou compromission avérée porte sur des informations classifiées d'origine étrangère (ou sur des informations classifiées communes partagées dans le cadre de programmes/projets en coopération), des dispositions complémentaires aux fiches 8.1 et 8.2 de la présente instruction s'appliquent, sous réserve des dispositions de l'accord de sécurité conclu avec l'Etat correspondant :

- le détenteur rend compte le plus rapidement possible à l'ASD compétente ou à l'ANS (cf. fiche 9.1). Sur le territoire national, l'ASD informe la DRSD (en charge de caractériser la compromission) et le SGDSN de la constatation d'une compromission possible d'informations classifiées et des mesures immédiates prises ;
- pour les compromissions sur des informations classifiées du niveau *Très Secret* ou équivalent, le SGDSN assure seul la relation avec les autorités de sécurité étrangères, sur la base du compte rendu adressé dans les meilleurs délais par l'ASD française compétente ;
- pour les compromissions sur des ISC allant jusqu'au niveau *Secret* ou équivalent (ce qui peut inclure le niveau DR au sens des accords et règlements de sécurité internationaux), l'ASD informe, le plus rapidement possible, le pays d'origine de l'information (ou le pays partenaire en cas de projet/programme en coopération) de la compromission avérée ou suspectée. Le rapport d'enquête final rédigé par la DRSD est transmis aux autorités étrangères (avec copie au SGDSN) au plus tard 31 jours ouvrables après le constat avéré de la compromission.
- Pour les compromissions touchant aux ACSSI étrangers, l'agence nationale de distribution (AND) de la DIRISI coordonne la remontée d'information vers les autorités de sécurité étrangères avec la chaîne de sécurité afin de préserver la cohérence de l'action du ministère des armées et d'assurer l'information du service enquêteur du ministère.

Afin d'éviter le risque de compromission d'informations étrangères et, sauf dispositions contraires dans l'accord de sécurité, les documents d'origine étrangère sont marqués au moins sur la première page, selon le timbre équivalent français.

TITRE 8 : GESTION ET REPRESSION DES ATTEINTES AU SECRET DE LA DEFENSE NATIONALE

8.3

Ces dispositions sont applicables aux actes commis au préjudice :

- des puissances signataires de l'OTAN ou d'une institution ou d'un organe de l'OTAN²⁰² ;
- d'un État étranger ou d'une organisation internationale en vertu d'un accord de sécurité, régulièrement approuvé et publié, relatif à la protection des informations classifiées conclu entre la France et un État étranger ou une organisation internationale ;
- d'une institution, d'un organe ou d'un organisme de l'UE en vertu des règles de sécurité de ces derniers qui ont fait l'objet d'une publication au Journal officiel de l'Union européenne²⁰³.

A titre d'information, pour connaître toute équivalence, il y a lieu de consulter les accords ou règlements de sécurité des principales organisations internationales dont la France fait partie ou l'accord de sécurité avec le pays considéré et à défaut, de prendre contact avec le bureau DIE de la DAJ.

Enfin, les documents classifiés relevant d'une organisation internationale sont conservés dans des meubles de sécurité, ou coffres, séparément du classifié national ou étranger, afin de ne pas compromettre l'information nationale ou étrangère lors d'une inspection éventuelle des organismes de contrôle de ces organisations (application du principe du besoin d'en connaître – cf. fiches 7.10 et 9.4).

²⁰² Article 414-8 du code pénal.

²⁰³ Article 414-9 du code pénal.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES

PRINCIPES DE LA PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES

La fiche 1 précise les responsabilités du secrétariat général de la défense et de la sécurité nationale (SGDSN), autorité nationale de sécurité (ANS), relatives à la protection du secret dans les relations internationales ainsi que celles de la Direction générale de l'armement (DGA), en tant qu'autorité de sécurité déléguée (ASD), pour le domaine concernant la coopération ou l'exportation en matière d'armement, impliquant notamment l'industrie de défense.

Les fiches 2 à 5 établissent les règles de protection des informations classifiées, *Diffusion Restreinte ou sensibles* à observer par les agents des entités étatiques du ministère de la défense, des organismes et écoles sous sa tutelle, et de l'industrie de défense, dans le cadre des échanges internationaux, des missions accomplies à l'étranger en dehors des opérations, des visites en France de personnel étranger.

Elles précisent également les dispositions à prendre dans le cadre d'accords avec les organisations internationales (OTAN, OCCAr, UE, EDIR/FA)²⁰⁴.

Les dispositions spécifiques relatives à la protection du potentiel scientifique et technique de la nation, définies dans le décret n° 2011-1425 du 2 novembre 2011, ne sont pas traitées dans cette instruction²⁰⁵.

Enfin, la fiche 6 traite des missions et séjours à l'étranger. Dans ce domaine, il est crucial d'intégrer que le contexte international géopolitique et économique actuel de montée des tensions peut accroître les vulnérabilités des personnes morales et physiques. Il incombe à tous les acteurs – militaires et civils de la défense, OS, chefs d'organisme etc.- d'appliquer la réglementation et d'accomplir ces missions avec la plus grande rigueur et vigilance.

²⁰⁴ Organisation du Traité de l'Atlantique Nord, Organisation conjointe de coopération en matière d'armement, Union européenne, European Defense Industry Restructuring/Framework Agreement.

²⁰⁵ Pour les règles relatives à la PPST, se reporter à l'Instruction ministérielle n° 298 du 5 mars 2014 relative à la mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation par le ministère de la défense

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.1****AUTORITE NATIONALE DE SECURITE ET AUTORITE DE SECURITE DELEGUEE****Références :**

- IGI 1300 - 2.1.1.2.b.
- Code de la défense - art. R. 2311-10-1

Points clés :

- Le secrétariat général de la défense et de la sécurité nationale (SGDSN) est l'autorité nationale de sécurité (ANS) en matière de protection du secret. A ce titre, il est le seul organisme, sauf délégation, responsable de la négociation et de la conclusion des traités et accords intergouvernementaux en matière d'échange et de protection réciproque des ISC, appelés aussi accords généraux de sécurité (AGS).
- La direction générale de l'armement (DGA) est l'autorité de sécurité déléguée (ASD) par le SGDSN pour le domaine concernant la coopération ou l'exportation en matière d'armement impliquant notamment l'industrie de défense. Elle apporte son soutien et son expertise au SGDSN pour la rédaction et la négociation des accords de sécurité qui encadrent des coopérations ou des exportations en matière d'armement. En appui du SGDSN, elle est une interlocutrice des ANS et ASD étrangères pour la mise en œuvre des dispositions des accords de sécurité bilatéraux ou conclus avec les organisations internationales, la définition des mesures de protection à apporter aux informations et supports classifiés échangés lors des coopérations ou des exportations en matière d'armement, l'échange d'informations sur les habilitations de sociétés ou de personnes et la mise en œuvre des processus et règles en matière de sécurité industrielle internationale, définies par les accords ou les documents de sécurité complétant ces accords.

1. Autorité nationale de sécurité (ANS)

L'ANS est, pour le secret de la défense nationale, l'entité gouvernementale interministérielle chargée des relations avec les autres États et les structures internationales en matière d'habilitation de personnes et de 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** (SGDSN).

L'agence nationale de la sécurité des systèmes d'information (ANSSI), service à compétence nationale rattaché au SGDSN, est l'autorité nationale de défense et de sécurité des systèmes d'information. Elle est chargée d'assister le SGDSN pour l'exercice de ses attributions.

L'ANS :

- négocie les accords intergouvernementaux encadrant l'échange d'informations classifiées et protégées avec des États partenaires ou des organisations internationales ;

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.1**

- supervise la négociation par le MINARM, des accords intergouvernementaux encadrant l'échange d'informations classifiées et protégées avec des Etats partenaires ou des organisations internationales dans le domaine spécifique de la défense ou, plus restreint, de l'armement;
- est l'interlocuteur des autorités nationales de sécurité étrangères ;
- assure, en application des accords internationaux en vigueur, la sécurité des ISC confiés à la France, détermine les procédures d'habilitation requises pour permettre l'accès à ces informations et organise, dirige et contrôle les réseaux à mettre en place pour les ISC OTAN et UE ;
- 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.

2. Autorité de sécurité déléguée (ASD)²⁰⁶

L'ASD est l'autorité responsable devant l'ANS de la mise en œuvre de la politique de sécurité du secret de la défense nationale dans un domaine particulier. Elle est désignée par l'ANS (SGDSN) sur proposition du ministre. Au sein du ministère des armées, le **service de la sécurité de défense et des systèmes d'information** (SSDI) de la **DGA** est l'autorité de sécurité déléguée dans le domaine de la coopération ou l'exportation en matière d'armement impliquant notamment l'industrie de défense.

La DGA en tant qu'ASD et pour son domaine de compétence :

- coordonne, dans le domaine de l'armement, la mise en œuvre des dispositions des accords de sécurité bilatéraux ou conclus avec les organisations internationales ;
- définit, en concertation avec ses homologues, et valide les mesures de protection à apporter aux informations et supports classifiés échangés (instructions de sécurité programme, assurances de sécurité,..) ;
- instruit et valide les annexes de sécurité internationales ;
- procède aux échanges d'informations sur les habilitations de sociétés ou de personnes ;
- instruit, établit et valide les actes administratifs relevant de la sécurité industrielle internationale (transports classifiés, visites classifiées, certificats de courrier) ;
- instruit, en liaison avec les ASD partenaires, les demandes d'habilitation des personnels étrangers employés par les entreprises françaises ou les entités étatiques ;
- fait connaître aux personnes morales de droit privé ou aux entités étatiques de son périmètre de compétence la politique et les règles à appliquer en matière de sécurité industrielle internationale et apporte conseil et assistance pour leur mise en œuvre ;
- participe, avec ses partenaires étrangers, à l'élaboration des réglementations au sein des comités de sécurité des organisations internationales, en soutien au SGDSN ou dans le cadre de sa délégation.

²⁰⁶ En anglais : DSA : Designated Security Authority.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.2****CONDITIONS POUR ECHANGER DES INFORMATIONS ET SUPPORTS CLASSIFIES AVEC L'ETRANGER****Références :**

- IGI 1300 – 4.4.1.4.f, 4.4.1.4.g et 7.2.1.3
- II n° 50/SGDN/SSD/DR du 9 janvier 1971 sur la protection du secret dans les rapports entre la France et les États étrangers

Points clés :

- Les échanges d'ISC avec l'étranger se font sur la base d'un accord de sécurité signé entre les gouvernements des deux Etats.
- Les accords de sécurité identifient les équivalences des niveaux de protection dans chacun des pays et instaurent la réciprocité de la protection des ISC.
- Le SGDSN pilote la négociation des accords généraux de sécurité (AGS).
- La direction des affaires juridiques (DAJ) pilote la rédaction et la négociation des accords de sécurité dans le domaine de la défense (ASDD) au MINARM, en lien avec le SGDSN. Quand ces accords encadrent des coopérations ou des exportations d'armement, l'ASD DGA/SSDI participe à la négociation.
- DGA/SSDI en tant qu'ASD est le point d'entrée du MINARM pour toutes les questions des entreprises liées au MINARM par contrat ou par convention et impliquées dans des coopérations, exportations d'armement.

1. Règlementation et dispositions préalables

Une information classifiée ne peut être communiquée à un gouvernement étranger ou à l'un de ses ressortissants, que dans le cadre d'un accord de sécurité signé entre le gouvernement de cet État et le gouvernement de la République française. Plusieurs types d'accords peuvent être conclus en fonction de la nature des échanges d'informations classifiées :

- accords généraux de sécurité applicables à tous les ministères ;
- accords de sécurité dans le domaine de la défense, ou d'armement, applicables au seul MINARM.

En l'absence des accords de sécurité mentionnés ci-avant, peuvent également être mis en place des accords par échange de lettres ou de notes verbales signées par les gouvernements applicables à un projet particulier et généralement pour la seule transmission d'informations classifiées vers le pays demandeur.

Pour l'exécution d'une coopération dans un domaine donné (programme d'armement, coopérations militaires ou industrielles) ou d'une opération d'exportation, d'autres clauses dans les accords relatifs à cette coopération et dans les contrats qui en résultent ou des documents spécifiques (instruction de sécurité programme) peuvent compléter ou décliner les dispositions de sécurité des accords de sécurité.

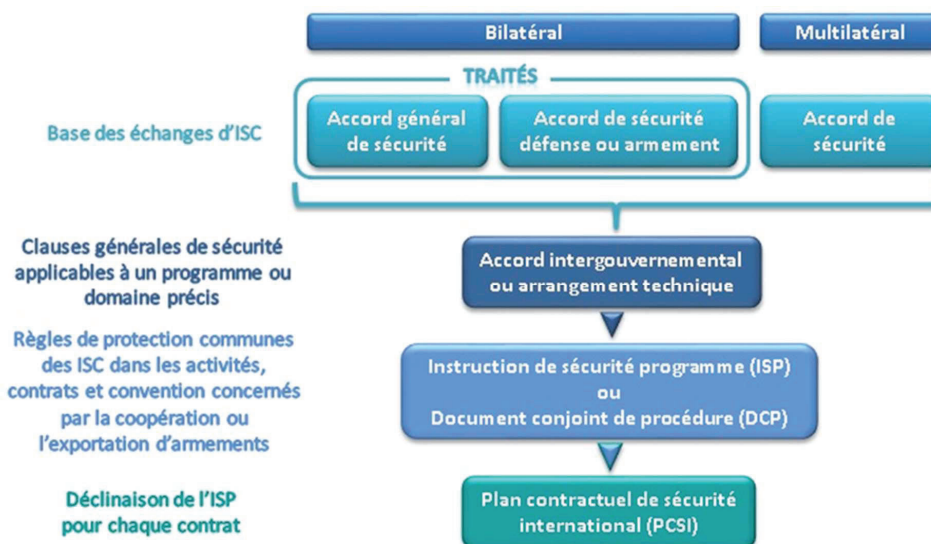
Si l'accord de sécurité intervient dans le cadre d'une organisation internationale (OI), il convient de se référer aux textes de sécurité régissant ladite organisation. Pour l'exécution d'une coopération dans un domaine donné (programme d'armement, coopérations militaires ou industrielles), d'autres clauses ou documents peuvent

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES

9.2

compléter les dispositions de sécurité dans les accords inter gouvernementaux relatifs à cette coopération avec l'OI et dans les contrats qui en résultent.

2. Les différents documents traitant d'ISC à l'international



Une description détaillée du contenu et de la portée des documents présentés ci-dessous figure en [annexe 17](#).

BESOIN	DOCUMENT
Engagement réciproque de deux gouvernements, dans le domaine général ou un domaine particulier	Accord Général de Sécurité Accord de sécurité dans le domaine de la défense Accord de sécurité dans un domaine spécifique (par exemple celui de l'armement)
Échange de lettres entre ministres engageant le ministère rédigeant la réponse pour une affaire ou un programme particulier	Accord/Arrangement Assurance de sécurité s'appliquant dans un cadre OTAN ou OCCAR
Programme Coopération d'État à État	Accord inter gouvernemental ou arrangement technique Clause de non divulgation - Non Disclosure Agreement (NDA) PCSI
Programme Coopération d'État à État impliquant des industriels	Instruction de sécurité programme (ISP) PCSI ou Security Aspect Letter (SAL) lorsque l'Etat étranger adresse des ISC à la France
Vente d'armements à l'export entre un industriel français et un État étranger	Instruction de sécurité programme (ISP) le cas échéant

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES

9.2

	Plan contractuel de sécurité international (PCSI) Clause de non divulgation - Non Disclosure Agreement (NDA)
Sous-traitance à l'étranger entre un industriel français et un industriel étranger	PCSI ou Security Aspect Letter (SAL) lorsque un industriel français est sous-traitant
Attestations internationales de sécurité	
Connaître l'habilitation d'une personne morale, ou entamer une procédure d'habilitation en sa faveur	Formulaire Facility Security Clearance Information Sheet (FSCIS)
Connaître l'habilitation d'une personne physique, ou entamer une procédure d'habilitation en sa faveur	Personnel Security Clearance Information Sheet (PSCIS)
Complément d'enquête de sécurité pour un individu ayant résidé à l'étranger ou pour un ressortissant étranger dont on souhaiterait l'équivalent d'un contrôle élémentaire	Personnel Security Clearance Assurance Request (PSCAR)
Prouver l'habilitation d'un individu pour l'accomplissement d'une mission à l'étranger	Certificat de sécurité ou PSCIS ou RFV (selon le contexte et les règlements applicables)
Acheminement d'ISC par porteur	Certificat de courrier
Acheminement d'ISC par fret	Plan de transport
Visite à l'étranger	
Avec échange d'ISC à partir nominalement du niveau secret ou du niveau diffusion restreinte si les accords ou les règles de sécurité du projet mené le prévoient ou si la réglementation du pays hôte l'exige pour accéder à certains sites sensibles	Formulaire de Demande de visite – Request For Visit (RFV)
Visite depuis l'étranger	
Avec échange d'ISC à partir du niveau secret	Formulaire de Demande de visite – Request For Visit (RFV)

3. Démarche à entreprendre par l'OS

Préalablement à l'échange d'ISC avec l'étranger, il est nécessaire de vérifier les éléments suivants :

- existence d'un cadre juridique avec le pays dont relève son interlocuteur ;
- connaissance des règles prévues dans cet accord par les participants concernés par l'échange d'information ;
- s'il s'agit d'un industriel étranger, l'habilitation de la société et la détention par la société de l'aptitude physique et informatique pour détenir et traiter les informations classifiées qui lui seront confiées ;
- habilitation de l'interlocuteur (selon le contexte et les règlements de sécurité qui couvrent l'échange) ;

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.2**

- existence entre les deux pays d'une liaison électronique sécurisée et homologuée par les ANS/ASD respectives si l'information est transmise par voie numérique ;
- autorisation de la transmission de l'information classifiée par le pays d'origine de l'information ;
- couverture de l'échange par une licence d'exportation (s'adresser à DGA/DI ou EMA/MA).

Les informations relatives aux correspondants étrangers et à leurs autorités d'emploi, en particulier lorsqu'il s'agit de contractants étrangers, sont obtenues par les ANS/ASD en utilisant les formulaires internationaux de demande d'information reconnus par les parties concernées conformément aux stipulations de l'accord de sécurité applicable à l'échange considéré.

L'accès des correspondants étrangers est limité au strict besoin d'en connaître et dans la mesure où ils sont affectés dans un emploi nécessitant l'accès à des ISC, ils sont habilités aux niveaux appropriés. Les conditions générales d'habilitation des ressortissants étrangers sont fixées dans la fiche 3.9.

4. Marquages

Voir [Annexe 9](#).

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.3****CAS SPECIFIQUE DES CONTRATS INTERNATIONAUX : PLAN CONTRACTUEL DE SECURITE INTERNATIONAL (PCSI)****Référence :**

IGI 1300 - 4.4.2.3.a

Points clés :

- Un PCSI est établi pour définir les mesures de sécurité applicables et servir de vecteur de transmission des ISC dans le cadre d'un accord intergouvernemental, partenariat, convention ou contrat impliquant l'accès à des ISC entre entités de nationalités différentes. Il est mis en place avant tout échange d'ISC et couvre donc les phases amont telles que les phases précontractuelles.
- Dans le cadre d'un contrat ou d'une phase précontractuelle, le plan contractuel de sécurité international constitue une annexe qui lie les partenaires.
- Les accords de sécurité stipulent la rédaction d'un PCSI pour tout projet, contrat classifié²⁰⁷ qui implique un échange d'ISC.

Un plan contractuel de sécurité international (PCSI)²⁰⁸ est établi pour définir les mesures de sécurité à appliquer dans le cadre d'un accord intergouvernemental, d'un partenariat, d'une convention ou d'un contrat impliquant l'échange d'ISC entre une entité française, étatique ou privée, et des entités étrangères, étatiques ou privées. Dans la pratique, quand on rédige un PCSI pour couvrir les échanges d'ISC, on y ajoute les informations de niveau *Diffusion Restreinte* qui sont également transmises ou échangées.

En cas d'accord de sécurité, si l'accord le spécifie ou si l'accord ne mentionne aucune disposition en fonction du contexte, de la sensibilité du projet, de la nature ou du volume des ISC échangés, il revient à l'entité française émettrice de saisir son ANS/ASD pour définir la conduite à tenir. Le PCSI est élaboré par l'industriel ou l'Etat français (partie émettrice) dans le cadre d'une phase de négociation précontractuelle, d'un contrat, ou d'une opération de coopération internationale. Il précise au partenaire étranger, étatique ou industriel (partie destinataire), les instructions à prendre pour assurer la protection des ISC échangés.

Dès le stade de demande de délivrance de licence de transfert ou d'exportation, l'industriel, ou l'étatique concerné, prépare le plus en amont possible, avec l'appui du service du ministère concerné par le matériel exporté, la rédaction du PCSI.

Pour les contrats (y compris ceux en sous-traitance), il s'applique essentiellement aux types suivants :

- ceux passés par une autorité contractante française (étatique ou privée) avec un industriel ou titulaire étranger ;
- les contrats « export » conclus par un industriel français ou l'Etat français avec un État étranger ou avec un industriel étranger.

Le PCSI permet d'assurer quatre fonctions :

²⁰⁷ Désigné par le terme « classified contract » dans les textes internationaux.

²⁰⁸ L'appellation internationale est SAL (Security Aspect Letter)

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.3**

- constituer la partie d'un contrat contenant les éléments relatifs à la sécurité, dont la référence à la base juridique de protection des ISC (l'accord de sécurité) ;
- permettre le contrôle de la cohérence des informations transmises avec les termes de la licence d'exportation ;
- lister les ISC et leur niveau de classification et de protection à transmettre à l'étranger ;
- informer les ANS/ASD étrangères sur l'envoi d'ISC françaises à des entités de leur pays et les responsabiliser sur le fait qu'elles doivent s'assurer, dans leur domaine de responsabilité, du respect de la base juridique de protection des ISC conformément aux dispositions des accords de sécurité signés.

Le PCSI est validé par l'ASD avant recueil par la partie émettrice de la signature de la partie destinataire. Il est signé par les parties émettrices et destinataires.

Il comprend obligatoirement :

- un guide de classification de sécurité (Security Classification Guide en anglais) s'inspirant du guide de classification de l'ISP lorsqu'elle existe ;
- la référence aux accords applicables ;
- la référence de la licence d'exportation ;
- les coordonnées des autorités de sécurité étrangères ;
- les coordonnées des destinataires de l'information ;
- les lieux d'exécution des travaux classifiés ;
- une clause contraignante pour que ses dispositions soient également répercutées auprès des sous-traitants du destinataire étranger.

Une copie du PCSI est adressée pour information à :

- l'ANS française (SGDSN) et l'ANS/ASD étrangère, pour surveillance du contrat selon les stipulations de l'accord de sécurité ;
- la DRSD, pour information et lien éventuel avec l'opération protégée mère dont il peut découler.

Le formulaire de PCSI est disponible sur IXARM (<https://ep.ixarm.dga.defense.gouv.fr>).

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.4****ÉCHANGES D'INFORMATIONS ET SUPPORTS CLASSIFIÉS AVEC LES ORGANISATIONS INTERNATIONALES****Références :**

- IGI 1300 – 7.2.1.3
- Instruction interministérielle n° 2100 du 01/12/1975 pour l'application en France du système de sécurité de l'OTAN
- Instruction interministérielle n° 2102 du 13/07/2013 sur la protection en France du système de sécurité de l'UE

Points clés :

- Les échanges d'ISC avec les organisations internationales sont encadrés par des accords de sécurité conclus avec celles-ci.
- Les ISC émis par les États étrangers ou dans le cadre d'organisations internationales bénéficient de mesures de protection au moins égales aux ISC français de niveau de classification équivalente²⁰⁹.
- La France met en place une organisation permettant la protection des informations classifiées de l'UE et de l'OTAN et en particulier un réseau de bureaux de contrôle (OTAN) ou bureaux d'ordre (UE).
- Les informations classifiées ou protégées OTAN, UE ou étrangères doivent être conservées de façon séparée des informations nationales.

1. Généralités

Les directives générales sur la sécurité fixées par les organisations internationales sont rappelées dans des accords de sécurité spécifiques. Ces accords déterminent les obligations de chacun des États membres en matière de sécurité. Ils rappellent les niveaux de classification équivalents dans chacun d'entre eux. Un comité de sécurité est généralement chargé de surveiller la bonne exécution des engagements pris.

L'accord de sécurité est généralement complété par un règlement de sécurité (équivalent de l'IGI 1300 au niveau international).

Les principaux accords ou règlements de sécurité applicables sont :

- le C-M 2002/49 du 17 juin 2002 modifié et ses directives AC35/35-D2000 à D2005 modifiées, portant sur le règlement de sécurité de l'OTAN ;
- l'accord entre les États membres de l'Union européenne, réunis au sein du Conseil, relatif à la protection des informations classifiées échangées dans l'intérêt de l'Union européenne (2011/C 202/05), signé le 4 mai 2011 ;
- l'accord-cadre EDIR/FA chapitre IV et son annexe (décret 2001-1075 du 16 novembre 2001) portant publication de l'accord-cadre relatif aux mesures visant à faciliter les restructurations et le fonctionnement de l'industrie européenne de défense ;
- l'accord de sécurité de l'OCCAr du 25 mars 2004 et son règlement de sécurité (notamment OMP 11 « OCCAr security regulations » et OMP 12 « Handling of unclassified sensitive information ») ;

²⁰⁹ Loi n° 2007-288 du 5 mars 2007, modifiant les articles 414-8 et 414-9 du Code pénal.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.4**

- l'accord entre les Etats parties à la Convention portant création d'une Agence spatiale européenne et l'Agence spatiale européenne concernant la protection et l'échange d'informations classifiées, fait à Paris le 19 août 2002 et le règlement de sécurité de l'Agence (ESA/REG/004 rev. 2, ou toute version ultérieure).

Les atteintes au secret des ISC émis par les États étrangers confiés à la France dans le cadre d'accords bilatéraux ou internationaux sont réprimées comme des atteintes au secret de la défense nationale dans les conditions prévues aux articles 413-9 à 413-12 du code pénal.

Par ailleurs, la livraison d'informations étrangères, OTAN et UE, à une puissance étrangère est réprimée dans les conditions prévues aux articles 411-6 à 411-11 du code pénal. Les peines prévues peuvent atteindre 15 ans de détention criminelle et 225 000 € d'amende.

Les sanctions disciplinaires définies par le statut général des fonctionnaires et par le code de la défense, en cas de manquement au devoir de discrétion professionnelle concernant les informations de la défense nationale, s'appliquent également en cas d'indiscrétion relative aux informations classifiées étrangères ou relevant d'organisations internationales dont la France est membre (cf. fiche 8.3).

Les ISC émis par les États étrangers ou dans le cadre d'organisations internationales doivent être conservés de façon séparée des informations nationales (ils peuvent néanmoins être conservés dans le même meuble). Cette séparation matérialise les exigences du besoin d'en connaître et permet une inspection des documents, sans qu'un inspecteur de l'État étranger ou de l'organisation internationale ne puisse avoir accès à des informations classifiées ou protégées françaises.

2. L'Organisation du traité de l'Atlantique nord (OTAN)

Les dispositions particulières suivantes relatives au système de sécurité de l'Organisation du traité de l'Atlantique nord (OTAN) s'appuient sur l'instruction interministérielle n° 2100 du 1er décembre 1975 pour l'application en France du système de sécurité de l'OTAN²¹⁰.

a. Principes généraux de sécurité de l'OTAN

Aux termes de la Convention sur la sécurité, les États signataires du Traité de l'Atlantique nord se sont mutuellement engagés à :

- garantir la sécurité des informations protégées de l'OTAN ;
- ne faire part de ces informations à aucune autre organisation internationale, ni à aucun État non membre du Traité de l'Atlantique nord, sans l'accord de l'autorité d'origine.

Les informations protégées de l'OTAN restent propriété de l'autorité d'origine. Cependant, elles peuvent être diffusées à l'intérieur de l'OTAN, selon le principe du besoin d'en connaître, et sans qu'il en soit référé à l'autorité d'origine.

²¹⁰ En cours de révision par le SGDSN.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.4****b. Application en France**

L'application se traduit par :

- la concentration des responsabilités en matière de sécurité sous la direction d'une ou plusieurs autorité(s) nationale(s) de sécurité, couvrant les secteurs civil et militaire ;
- l'organisation d'un réseau hiérarchisé civil et militaire de « bureaux de contrôle » (bureaux d'ordre) des documents protégés de l'OTAN de niveau SECRET OTAN ou supérieur en compte dans les organismes nationaux ;
- l'habilitation du personnel devant avoir accès aux informations de l'OTAN ;
- un ensemble de mesures destinées à la protection des informations.

c. Niveaux de classification OTAN

La protection des informations de l'OTAN²¹¹ comporte des niveaux comparables à ceux utilisés dans le système national français :

- Très Secret COSMIC (en anglais : COSMIC Top Secret) : « Informations dont la divulgation non autorisée a des conséquences exceptionnellement graves pour l'OTAN ».
 - Secret OTAN (en anglais : NATO Secret) : « Informations dont la divulgation non autorisée a des conséquences graves pour l'OTAN ».
 - Confidentiel OTAN (en anglais : NATO Confidential) : « Informations dont la divulgation non autorisée est préjudiciable aux intérêts de l'OTAN ».
 - Diffusion Restreinte OTAN (en anglais : NATO Restricted) : « Informations dont la divulgation non autorisée porte préjudice aux intérêts ou à l'efficacité de l'OTAN ».
- L'OTAN définit le niveau Diffusion Restreinte OTAN (DRO) comme une classification.

Les informations de l'OTAN sont conservées de façon séparée des informations nationales.

Tout système d'information traitant des informations DRO fait l'objet d'une homologation. Faute d'homologation, il est admis de s'appuyer sur l'homologation au niveau *Diffusion Restreinte*, avec le respect de la mesure complémentaire suivante : chiffrage systématique des informations DRO au moyen d'un produit de chiffrage agréé.

De même, l'envoi de fichiers électroniques DRO se fait à l'aide d'un moyen reconnu par l'OTAN ou par l'ANSSI, avant tout envoi sur des réseaux non maîtrisés (comme Internet).

Enfin, les informations ne nécessitant pas de protection particulière portent parfois la mention Non Classifié OTAN (en anglais : NATO Unclassified). Celles-ci restent toutefois soumises à contrôle²¹² : elles ne sont pas diffusables hors de l'OTAN sans autorisation, conformément au document C-M(2002)60 sur la gestion des informations OTAN non classifiées du 23 juillet 2002, sauf si elles sont marquées « diffusable au public ».

L'organisation du réseau OTAN est détaillée en [annexe 18](#).

²¹¹ Les documents OTAN peuvent être libellés dans l'une des deux langues officielles, l'anglais ou le français, les documents les plus importants étant rédigés dans les deux langues.

²¹² Document C-M(2002)60 sur la gestion des informations OTAN non classifiées du 23 juillet 2002.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.4****3. L'Union européenne**

Les dispositions particulières suivantes relatives au système de sécurité de l'UE s'appuient sur l'instruction interministérielle n° 2102 du 13 juillet 2013 sur la protection en France du système de sécurité de l'UE²¹³.

a. Principes généraux de sécurité de l'UE

La France s'est engagée à assurer la sécurité des ICUE et veille à ce que ces informations ne soient pas :

- déclassées ou déclassifiées sans le consentement préalable écrit de l'autorité émettrice ;
- utilisées à d'autres fins que celles qui sont fixées par l'autorité émettrice ;
- divulguées à un pays tiers ou à une organisation internationale en l'absence d'un accord ou d'un arrangement approprié de protection des informations classifiées conclu entre l'UE et le pays tiers ou l'organisation internationale en question et sans le consentement préalable écrit de l'autorité émettrice.

Les ICUE s'entendent comme tout « matériel et toute information dont la divulgation non autorisée porte atteinte à des degrés divers aux intérêts de l'UE, que ces informations aient leur origine à l'intérieur de l'UE ou dans les États membres, des États tiers ou des organisations internationales ».

b. Application en France

Elle se traduit par :

- la responsabilité, au nom de la France, d'une autorité nationale de sécurité en matière de sécurité des ICUE ;
- l'organisation d'un réseau hiérarchisé composé de bureaux d'ordre des documents classifiés de l'UE en compte dans les organismes nationaux ;
- l'habilitation du personnel devant avoir accès aux ICUE ;
- un ensemble de mesures destinées à la protection des informations.

c. Niveaux de classification UE

Les niveaux de classification de l'UE sont établis comme suit :

- TRÈS SECRET UE/EU TOP SECRET : ce niveau de classification s'applique aux informations et matériels dont la divulgation non autorisée pourrait causer un préjudice exceptionnellement grave aux intérêts de l'UE ou d'un ou de plusieurs de ses États membres ;
- SECRET UE/EU SECRET : ce niveau de classification s'applique aux informations et matériels dont la divulgation non autorisée pourrait nuire gravement aux intérêts essentiels de l'UE ou d'un ou de plusieurs de ses États membres ;
- CONFIDENTIEL UE/EU CONFIDENTIAL : ce niveau de classification s'applique aux informations et matériels dont la divulgation non autorisée pourrait nuire aux intérêts essentiels de l'UE ou d'un ou de plusieurs de ses États membres ;

²¹³ En cours de révision par le SGDSN.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.4**

- RESTREINT UE/EU RESTRICTED : cette classification s'applique aux informations et matériels dont la divulgation non autorisée pourrait être défavorable aux intérêts de l'UE ou d'un ou de plusieurs de ses Etats membres.

Points particuliers :

- Le RESTREINT UE/EU RESTRICTED est un niveau de classification pour l'UE. Il est traité et protégé selon les règles applicables en France au niveau de protection DR ;
- Les institutions, organes et organismes de l'Union traitent et protègent les informations classifiées de niveau « CONFIDENTIEL DEFENSE » et « SECRET DEFENSE » émises par la France avant le 1^{er} juillet 2021 respectivement conformément aux mesures de protection des niveaux de classification « SECRET UE/EU SECRET » et « CONFIDENTIEL UE/EU CONFIDENTIAL ».

Les informations de l'UE sont conservées de façon séparée des informations nationales.

Tout système d'information traitant des informations R-UE/EU-R fait l'objet d'une homologation UE. Faute d'homologation, il est admis de s'appuyer sur une homologation au niveau *Diffusion Restreinte*, avec le respect de la mesure complémentaire suivante : chiffrage systématique des informations R-UE/EU-R au moyen d'un produit de chiffrage agréé.

De même, l'envoi de fichiers électroniques R-UE se fait à l'aide d'un moyen reconnu par l'UE ou par l'ANSSI, avant tout envoi sur des réseaux non maîtrisés (comme Internet).

L'organisation du réseau UE est détaillée en [annexe 18](#).

4. L'European defence industry restructuring / framework agreement (EDIR/FA)

Les dispositions visant à faciliter les restructurations et le fonctionnement de l'industrie européenne de défense, entre la France, l'Allemagne, le Royaume-Uni, l'Espagne, l'Italie et la Suède sont précisées dans un accord-cadre particulier, l'accord EDIR/FA.

a. Champ d'application

L'EDIR/FA s'applique aux ISC jusqu'au niveau *Secret* ou son équivalent relevant de la classification française ou de celle d'un autre pays membre. Il inclut également les informations protégées du niveau DR. Les informations classifiées ou protégées relevant d'une classification multinationale continuent à être traitées conformément aux dispositions du règlement de sécurité dont elles relèvent (OTAN, OCCAr, UE, etc.).

Les dispositions de l'EDIR/FA s'appliquent :

- aux établissements industriels se consacrant à l'acquisition de matériels de défense ;
- aux industriels titulaires de contrats de défense ;
- aux laboratoires d'État impliqués dans l'acquisition ou le soutien de matériels de défense ;
- aux établissements d'État impliqués dans l'acquisition ou le soutien de matériels de défense (entités de la DGA, entités des forces armées impliquées dans l'expérimentation et le maintien en condition opérationnelle des matériels).

b. Dispositions particulières

Les dispositions ci-dessous offrent des possibilités pour faciliter la coopération, l'emploi des individus et le fonctionnement de l'industrie entre les différents pays de l'EDIR/FA.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.4**

Lors de la mise en application de ces principes à un cas donné (programme en coopération, contrat, échange d'ISC lors de réunion...), des mesures plus restrictives supplémentaires peuvent être appliquées : elles doivent alors être définies entre les parties impliquées dans un document spécifique (par exemple au sein de l'Instruction de Sécurité Programme).

Habilitation de personnel étranger :

Une habilitation de sécurité individuelle délivrée par l'ANS/ASD d'une « partie » à l'accord EDIR/FA et en cours de validité, est acceptée par l'autorité compétente du ministère concerné, dans le cas d'un emploi nécessitant l'accès à des informations classifiées dans un établissement étatique ou industriel français.

Accès aux informations classifiées :

L'accès à des informations classifiées de niveau *Secret* par une personne physique ayant la nationalité d'une partie est accordé sans autorisation préalable de la partie d'origine, à condition qu'elle détienne le niveau d'habilitation nationale équivalent (cf. fiche 3.9). En revanche, lorsque l'accès à des informations classifiées relatives à un projet/programme est sollicité par des ressortissants qui n'appartiennent pas aux parties, les participants à ce projet/programme doivent s'accorder pour autoriser ou non l'accès. La consultation est alors lancée formellement selon un modèle préétabli²¹⁴, avant le début, ou selon le cas, au cours du projet/programme. La consultation est faite exclusivement par l'intermédiaire de l'ASD compétente.

Visites :

Les visites entrant dans le champ de l'accord-cadre sont traitées directement entre les officiers de sécurité des entreprises sans passer par leurs ANS ou ASD, pour une période d'un an maximum renouvelable. L'ANS/ASD de la partie d'accueil peut exiger de ses établissements d'être préalablement informée d'une visite si celle-ci excède 21 jours.

Lorsque la visite porte sur un projet/programme bien identifié pour lequel une instruction de sécurité de programme a été établie, l'autorisation de visite ouvre droit à l'accès aux informations classifiées du projet/programme.

Les responsables de sécurité des établissements d'accueil ont l'entière responsabilité de la sécurité de la visite. Ils sont en particulier chargés de s'assurer du niveau d'habilitation de leurs visiteurs, et du niveau d'habilitation de l'établissement étranger d'envoi ou d'accueil. Ils s'assurent également de la tenue de registres contenant les informations biographiques des visiteurs et les conservent au moins deux ans.

²¹⁴ Document II de l'EDIR/FA Consultation process.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.5****ECHANGES NUMERIQUES CLASSIFIES AVEC L'ETRANGER****Point clé :**

Les mesures de protection des informations numériques classifiées ou protégées échangées avec l'étranger sont fixées par des accords internationaux ou des documents de sécurité les déclinant et assurent un niveau de protection équivalent au niveau national.

En sa qualité d'ANS, le SGDSN prescrit, coordonne et contrôle l'application des mesures propres à assurer la protection du secret dans les relations entre la France et les États étrangers ou les organisations internationales. A cet effet, il négocie les accords généraux de sécurité qui permettent d'échanger des informations et supports classifiés (cf. fiche 10.1). L'ANS peut déléguer à une ASD (cf. fiche 10.1).

Lorsque des informations classifiées ou protégées *Diffusion Restreinte* françaises sont transmises dans des systèmes d'information relevant de la responsabilité d'États étrangers ou d'organisations internationales, des mesures de protection sont fixées par des accords ou des règlements de sécurité avec ces partenaires, qui assurent à ces informations un niveau de protection au moins équivalent à celui prévu par la norme française.

La protection des systèmes d'information traitant d'informations classifiées ou protégées au niveau équivalent *Diffusion Restreinte* confiées à la France par des États étrangers ou par des organisations internationales est assurée conformément aux accords et aux règlements de sécurité établis avec ces partenaires. Ces accords et règlements font, le cas échéant, l'objet d'instructions complémentaires pour l'application de ces mesures en France. A défaut de tels accords ou règlements, les dispositions de la présente instruction s'appliquent à ces systèmes.

Lorsque des systèmes d'information traitant des informations classifiées ou protégées au niveau *Diffusion Restreinte* sont utilisés en commun avec des partenaires étrangers ou internationaux, ces systèmes font l'objet d'une homologation commune. Une telle homologation ne peut être effectuée que s'il existe un accord de sécurité. Les représentants des autorités d'emploi, de l'autorité de sécurité déléguée (ASD – cf. fiche 9.1), et, le cas échéant des autorités contractantes de référence, sont conviés au comité d'homologation. La protection des informations de tels systèmes est d'un niveau au moins équivalent à celui prévu dans la présente instruction, au titre 6.

Lorsque des méthodes cryptographiques doivent être appliquées pour assurer la protection de la confidentialité, de l'intégrité et de la disponibilité de tels systèmes d'information, ces méthodes ou les produits associés sont expressément approuvés pour chaque cas précis par l'ANSSI.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.6****MISSIONS ET SEJOURS A L'ETRANGER****Référence :**

Circulaire n° 2527/DEF/CAB/SDBC/CPAG du 21/02/2003 relative aux conditions dans lesquelles les militaires peuvent franchir les limites du territoire métropolitain

Points clés :**Missions et déplacements professionnels avec détention ou consultation d'ISC :**

- Les demandes de visite à l'étranger impliquant du classifié sont adressées par le chef d'entité à l'autorité de sécurité compétente (DGA pour les industriels ou son personnel au titre de son rôle d'Autorité de Sécurité Déléguée, Etats-majors pour les autres personnels), qui les fait suivre à l'ambassade de France du pays d'accueil pour transmission à l'ANS/ASD étrangère.
- L'autorité de sécurité compétente atteste du niveau d'habilitation du missionnaire.

Séjours :

- Les permissions du personnel militaire à l'étranger font l'objet de mesures particulières, notamment pour les pays de certaines catégories.
- Lorsque les circonstances l'exigent, le commandement peut restreindre l'exercice de la liberté de circulation pour le personnel militaire.
- Le personnel civil relevant du MINARM ou des entités contractantes n'est pas assujéti à ces deux dernières obligations mais informe son OS, qui le renseignera sur les bonnes pratiques à adopter.

Dans tous les cas :

- En cas d'incident durant une mission ou un séjour, l'OS fait rédiger par l'intéressé un compte rendu à destination du service enquêteur.

1. Missions à l'étranger**a. Demandes de visite impliquant du classifié**

Les demandes de visites impliquant du classifié sont prévues dans les accords de sécurité. Hors de ce cadre et mis à part certains cas particuliers (pour certains programmes, ou visites vers des pays de l'EDIR/FA), les demandes de visites de ressortissants français pour l'étranger impliquant du classifié sont adressées par l'ASD ou l'autorité de sécurité française compétente à l'ambassade de France dans le pays d'accueil (mission de défense), qui fait suivre la demande à l'ANS/ASD du pays d'accueil, ou à l'ANS/ASD étrangère si l'accord de sécurité le précise, en utilisant le formulaire prévu soit dans l'accord ou le règlement international lorsqu'il existe, dans les documents du projet, programmes fixant les règles de sécurité (instruction de sécurité programme) soit celui du GMSI²¹⁵.

²¹⁵ GMSI ou groupe multinational de sécurité industrielle (angl. MIWSG) est un groupe informel qui établit des documents de sécurité dont un document sur les visites internationales. Ce document s'appelle RFV « Request For Visit ».

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.6**

La demande de visite est visée par l'autorité de sécurité française compétente afin d'attester du niveau d'habilitation du personnel candidat à la visite.

Pour le MINARM, ces autorités compétentes pour viser ces demandes de visites sont :

- la DGA, en tant qu'ASD²¹⁶, pour les programmes, les coopérations ou l'exportation dans le domaine de l'armement ;
- l'EMA ou les EMx pour les coopérations militaires.

Ces dernières peuvent déléguer leur signature à tout chef de formation militaire ou direction/service subordonné nominativement désigné et à qui elles précisent par écrit les consignes à appliquer.

En l'absence de modalités spécifiques contraires (par exemple, définies dans une instruction de sécurité programme), les demandes de visites de ressortissants étrangers employés par des établissements français de droit privé (industriels de défense) sont également adressées à la DGA/SSDI qui fait suivre les demandes selon la procédure précitée. A défaut d'imprimé imposé par le cadre de coopération (AGS, ISP, etc.), le formulaire standard GMSI peut être utilisé.

Cas particulier pour les visites au sein des entités de l'OTAN : l'accès aux entités fait l'objet de consignes, régulièrement mises à jour, et diffusées via les sous-réseaux COSMIC. Les visiteurs doivent être en possession de leur certificat de sécurité OTAN pendant la durée de leur visite.

Cas particulier de certains programmes, ou visites vers des pays de l'EDIR/FA : ce type de visite s'effectue directement d'OS à OS, lesquels sont chargés de certifier l'habilitation du visiteur auprès de l'établissement visité.

b. Sensibilisation des Français en mission à l'étranger

Afin de limiter les risques, le missionnaire se conforme aux conseils pratiques figurant dans l'[annexe 19](#).

La règle essentielle à suivre en cas d'incident est de rendre compte immédiatement à l'ambassade ou au consulat le plus proche. Il est donc indispensable de posséder les coordonnées des points de contact diplomatiques locaux à alerter en cas de problème. Il lui importe de faire preuve de maîtrise de soi en toute circonstance : réagir avec trop de nervosité devant une provocation complique l'intervention des autorités consulaires ou diplomatiques.

2. Permissions et séjours à l'étranger**a. Personnel militaire**

La circulaire de référence classe les pays en différentes catégories : la catégorie 10, pour laquelle les militaires peuvent librement circuler, et la catégorie 20 qui se subdivise en :

- Catégorie 21 : pays pour lesquels l'autorisation de s'y rendre relève de la décision du ministre après avis de la DRSD ;
- Catégorie 22 : pays pour lesquels l'autorisation de s'y rendre relève de la décision du commandant de formation administrative après avis de la DRSD ;

²¹⁶ Rôle tenu par DGA/SSDI.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.6**

- Catégorie 23 : pays pour lesquels l'autorisation de s'y rendre relève de la décision du commandant de formation administrative.

Pour les catégories 21, 22 et 23, le demandeur complète le formulaire du système d'information SOPHIA, qui peut être téléchargé sur le site Intradef de la DRSD :

- Pour la catégorie 21, l'autorité d'emploi demande par SOPHIA l'avis de la DRSD, qui dispose de deux semaines pour émettre un avis après avoir, selon son appréciation, procédé à une sensibilisation individuelle et adresse la demande au cabinet du ministre pour décision. En cas de procédure d'urgence (cas d'évènement familial grave), le commandant de formation administrative peut adresser directement au cabinet du ministre une demande d'autorisation de permission pour un pays de catégorie 21 ;
- Pour la catégorie 22, l'autorité d'emploi demande par SOPHIA l'avis de la DRSD. Celle-ci dispose de deux semaines pour émettre un avis après avoir vérifié que l'intéressé a joint le formulaire daté et signé attestant qu'il a pris connaissance de la fiche de sensibilisation et de conseils en ligne sur le site DRSD de l'Intradef. La DRSD peut exceptionnellement procéder à une sensibilisation. A défaut de réponse de la DRSD dans un délai de deux semaines à compter de la prise en compte de la demande dans l'application SOPHIA, le commandant de formation administrative peut signer le titre de permission. Il adresse alors une copie du titre de permission au poste RSD compétent ;
- Pour la catégorie 23, le commandant de formation administrative donne son autorisation et signe le titre de permission sans être tenu de solliciter l'avis de la DRSD.

Lorsque les circonstances l'exigent, le commandement peut restreindre davantage l'exercice de la liberté de circulation pour le personnel militaire.

En cas d'incident durant le séjour, le personnel militaire rédigera à son retour un compte-rendu détaillé à l'attention de son OS (en annexe 4 de la circulaire de référence) qui le transmettra au correspondant DRSD.

b. Personnel civil du ministère et des entités liées par contrats ou convention

Le personnel civil du MINARM et des entités contractantes est soumis aux obligations de signalement énoncées précédemment. Le personnel détenteur d'informations sensibles, *Diffusion Restreinte* et/ou habilité se rapproche alors de son OS pour se renseigner sur les zones à risque ou les mesures à adopter lors d'un déplacement ou un séjour. Ce dernier pourra alors utilement se rapprocher de la DRSD si le déplacement concerne un pays des catégories 21 à 23.

Il est également recommandé au personnel civil de consulter l'onglet « conseils aux voyageurs » sur le site du Ministère de l'Europe et des Affaires étrangères²¹⁷ et de s'enregistrer sur la base Ariane²¹⁸ lors de son déplacement.

Les incidents survenus durant le séjour d'un civil peuvent être signalés à l'OS par l'intéressé.

²¹⁷ Consulter le site du Ministère de l'Europe et des affaires étrangères (MEAE) : <https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/>

²¹⁸ Consulter le site du MEAE : <https://pastel.diplomatie.gouv.fr/fildariane/dyn/public/login.html>

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.6**

Tous les échanges relatifs aux demandes d'avis et aux comptes rendus d'incident entre la formation administrative et le poste RSD compétent se font, sauf urgence avérée, par voie électronique Intradef ou Internet sécurisé par Acid.

3. Rôle de l'OS

L'OS doit sensibiliser le personnel de son organisme sur les démarches à suivre en cas de mission ou séjour à l'étranger.

Pour les militaires, l'OS se tient informé des modifications pouvant intervenir dans la catégorisation des pays.

La mise en garde des titulaires de missions à l'étranger dépend de la situation. Elle est complète et s'effectue dans la mesure du possible sous la forme d'un stage d'information ou de sensibilisation, pour une première mission de type donné. Elle peut être plus rapide pour des missions de routine telle que la participation périodique à des réunions de travail faisant suite à un accord. La DRSD peut être sollicitée pour apporter son concours en matière de prévention.

En cas de sensibilisation avant départ ou d'entretien au retour, l'OS facilite le contact entre l'intéressé et son correspondant DRSD. Selon les consignes données par l'autorité d'emploi du missionnaire, un compte rendu peut être établi à l'issue de la mission, et systématiquement, en cas d'incident pendant la mission. Les informations recueillies sont transmises à l'organisme DRSD compétent par l'officier de sécurité (OS) ou l'autorité d'emploi du missionnaire.

Lorsqu'un missionnaire convoie des ISC, il se munit auprès de son OS d'un certificat de courrier validé par une autorité de sécurité compétente (voir §1.a.). Dans ce cas, la sensibilisation au départ de mission et un compte-rendu en fin de mission sont systématiques.

ANNEXES

ANNEXE 1

MODELE DE FICHE CONFIDENTIELLE

SECRET

N°

Reproduction interdite

FICHE CONFIDENTIELLE

exclusivement réservée à l'autorité de décision

Concerne né le à

I – [NP] Informations communicables

[NP] (Qui pourraient au besoin être portées à la connaissance de l'intéressé dans le cas où l'autorité de décision déciderait d'une mise en éveil)

Les informations communiquées supra sont à analyser par l'autorité d'habilitation en fonction de la spécificité du poste et/ou du contexte d'emploi de l'intéressé.

II - Renseignements non communicables (à l'intéressé)

L'intéressé est connu pour :

Les informations de mise en garde, communiquées par le Service, sont à considérer comme une aide à la décision pour l'autorité d'habilitation qui doit statuer sur le niveau de confiance à accorder à l'intéressé, dans le cadre de son accès aux ISC.

Note à l'attention de l'autorité d'habilitation :

Du point de vue de la DRSD, il est nécessaire de sensibiliser l'intéressé quant au comportement qu'il doit adopter au regard de son environnement actuel. Il est donc proposé de procéder à sa mise en éveil afin d'atténuer le risque et d'établir une situation favorable à la prise de décision.

De plus, il est nécessaire de faire connaître la situation actuelle de l'intéressé à son employeur. Ainsi, dans l'hypothèse d'une décision d'admission, ce dernier pourra adopter la posture la plus adaptée. Il est donc proposé de procéder à une mise en garde de l'officier de sécurité de l'organisme employeur de l'intéressé.

CE DOCUMENT DOIT ETRE RESTITUÉ À L'AUTORITÉ D'ORIGINE DES QUE L'AUTORITÉ DE DÉCISION EN AURA PRIS CONNAISSANCE

Renseignements communiqués le à

Par

SECRET

ANNEXE 2

LISTE DES EMPLOIS SENSIBLES

Sont à considérer comme occupant un emploi sensible le personnel :

- Servant dans l'environnement immédiat des hautes autorités²¹⁹ ;
- Servant dans les forces nucléaires ;
- Affecté à la manutention, le transport, la comptabilité de matériels ou de produits présentant un caractère dangereux (armement, munitions et explosifs, carburant, substances toxiques)²²⁰ ;
- Affecté à la préparation, au traitement, au conditionnement et au stockage des expéditions de fret, biens et produits transportés par les aéronefs, bâtiments de surface et sous-marins, utilisés par le ministère des armées ;
- Affecté à la réparation ou l'entretien des matériels considérés comme majeurs par les EMDS ministériels ;
- Transportant des ISC de niveau Secret ou Très Secret sur le territoire national (au titre de la décision de sécurité convoyeur)²²¹ ;
- Affecté au poste de gardien-veilleur civil du MINARM (hors personnel externalisé).

Les appellations utilisées *supra* sont génériques. Chaque état-major, direction ou service (EMDS) ministériel les précisera selon ses spécificités et en liaison avec la DRSD.

Le formulaire de demande à utiliser sur Sophia pour les enquêtes administratives préalable à l'accès à un emploi sensible est le CES (comme *Contrôle Emploi Sensible*) sauf pour le transport d'ISC, pour lequel il faut remplir un formulaire CNV (comme *CoNVoyeur*).

²¹⁹ Conducteur ou personnel de la maison militaire, par exemple

²²⁰ Concerne le personnel spécialisé – armurier ou comptable munitions par exemple - et non le militaire portant ou servant son arme.

²²¹ Selon la mission décrite à l'article 36 de l'IGI de référence e). Le transport du TSD fait l'objet de dispositions particulières.

ANNEXE 3

**MODELE DE DOSSIER DE DEMANDE D'HABILITATION D'UNE PERSONNE
MORALE**

1- À remplir par la personne morale	
Dénomination ou raison sociale (<i>en lettres majuscules, sans acronyme</i>) :	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
2- À remplir par l'autorité contractante/le maître 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 <input type="checkbox"/> SECRET <input type="checkbox"/> TRÈS SECRET, le cas échéant, préciser la classification spéciale :
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 contrat ²²²	
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 :	

²²² Ne concerne que les contrats prévoyant les prestations suivantes : travaux, fournitures, services.

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 :	Date et signature
Nom, prénom et coordonnées de la personne en charge du dossier :	

3- À remplir par l'autorité d'habilitation	
Ministère :	Date et signature
N° de la demande d'habilitation :	
Nom, prénom et coordonnées de la personne en charge du dossier :	

Notice de sécurité personne morale²²³

À renseigner intégralement en utilisant, si nécessaire, l'espace « renseignements complémentaires »

Représentant de la personne morale		
Nom - prénom :		
Date et lieu de naissance :		
Fonction :		
Tél. bureau :	Tél. portable :	Fax :
Email :		
Officier de sécurité (à remplir s'il est différent du représentant de la personne morale)		
Nom - prénom :		
Fonction :		
Tél. bureau :	Tél. portable :	Fax :
Email :		
Officier de sécurité des systèmes d'information		<input type="checkbox"/> Cocher si sans objet
Nom - prénom :		
Fonction :		
Tél. bureau :	Tél. portable :	Fax :
Email :		
Habilitation déjà détenue par la personne morale		<input type="checkbox"/> Cocher si sans objet
La personne morale a-t-elle déjà été habilitée au secret de la défense nationale ?		<input type="checkbox"/> OUI <input type="checkbox"/> 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 ?		<input type="checkbox"/> OUI <input type="checkbox"/> 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 ?		<input type="checkbox"/> OUI <input type="checkbox"/> 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 :		

²²³ À renseigner également par les indépendants, les microentreprises.

Informations relatives à 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 ?

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

1 ^{er} niveau					
Nom (et prénom) 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 pour tout actionnaire détenant 40 % et plus des parts sociales du 1 ^{er} niveau					
Nom (et prénom) du ou des actionnaires	Nationalité(s)	Date et lieu de naissance	N° RCS pour les personnes morales (Kbis à fournir)	% détenu	Droit de vote (%)
3 ^e niveau d'actionnariat pour tout actionnaire détenant 40 % et plus des parts sociales du 2 ^e niveau					
Nom (et prénom) du ou des actionnaires	Nationalité(s)	Date et lieu de naissance	N° RCS pour les personnes morales (Kbis à fournir)	% détenu	Droit de vote (%)

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
- ☐ 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 4**MODELE DE DECISION DE CREATION DE ZONE RESERVEE****Nom de l'organisme, du service**Ville, le
N° /XXX/XXX/NP**DECISION N° XXX/DATE/ORGANISME/SERVICE/DR
PORTANT CREATION D'UNE ZONE RESERVEE**

Nom du chef d'organisme, fonction,

- Vu le code pénal et notamment... ;
- Vu l'arrêté du 13 novembre 2020 approuvant l'IGI 1300 ;
- Vu l'arrêté du (date) portant création de la zone protégée de l'emprise dénommée (nom de l'emprise) ;
- Vu l'instruction ministérielle n° 900/DEF/CABIDR du XXXXX ;
- Vu l'avis technique d'aptitude physique n° (réf. de l'avis) du (date).

DECIDE:

ARTICLE 1 : la pièce XX située au (n° étage) du bâtiment XXXX est érigée en zone réservée de classe XXX.

ARTICLE 2 : cette ZR est intégrée dans la zone protégée désignée par l'arrêté du (date de l'arrêté) susmentionné.

Fait à (ville), le (date).

Nom du chef d'organisme

Fonction

(Signature)

DESTINATAIRES :COPIES :

ANNEXE 5

**LISTE DES PIÈCES CONSTITUTIVES DU DOSSIER D'APTITUDE D'UN ÉTABLISSEMENT
POUR L'EXECUTION D'UN CONTRAT AVEC DETENTION D'INFORMATIONS ET
SUPPORTS CLASSIFIES**

Il y a lieu de constituer autant de dossiers différents qu'il y a de lieux distincts d'exécution des travaux protégés.

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

- Extrait en cours de validité du registre du commerce et des sociétés (modèle L bis) ou copie du bail de location.
- Organigramme fonctionnel et nominatif de l'établissement.
- Notice individuelle de sécurité 94/A (cf. IGI 1300 – annexe 7) et lettre de proposition de chaque OS pressenti.
- Plan de masse de l'établissement.
- Organisation et moyens de protection et de gardiennage de l'établissement.
- Identification et description de la protection, actuelle et envisagée, du local ou des locaux où sont exécutés les travaux protégés. Ceci inclut l'analyse de risque et la liste des organismes assurant l'installation et la maintenance des SI de sûreté concourant à la protection du local.
- Dossier de sécurité des SI.
- Liste des sous-traitants intervenant dans l'établissement, faisant ressortir les entreprises prestataires de services au titre d'un contrat à clause de sécurité ou d'un contrat sensible.
- Lettre du dirigeant de l'entreprise, par laquelle celui-ci s'engage à mettre en place, avant le début des travaux protégés, les dispositions qui sont nécessaires pour garantir la protection des informations et supports classifiés qui lui sont confiés.

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

Plan contractuel de sécurité ou projet de plan contractuel de sécurité.

ANNEXE 6

MODELE D'AVIS TECHNIQUE D'APTITUDE / D'INAPTITUDE PHYSIQUE

DIFFUSION RESTREINTE

DIRECTION DU RENSEIGNEMENT ET
DE LA SECURITE DE LA DEFENSE

....

VILLE, LE

N° /ARM/DRSD/XXX/DR

Le Nom, Prénom, Qualité l'autorité DRSD
compétente
direction du renseignement et de la sécurité
de la défense

à

Entreprise - siège social ou établissement
étatique
A l'attention de l'officier de sécurité
Adresse postale

AVIS TECHNIQUE D'APTITUDE - D'INAPTITUDE PHYSIQUE

REFERENCES : Article 413-9 et R- 413-6 du code pénal
Articles R. 2311-1 à R 2312-2 du code de la défense
IGI 1300 à paraître
IM 900 à paraître

ANNEXE :

Le date de la visite/contrôle, la Direction zonale DRSD a évalué les mesures de protection matérielle dont bénéficie la zone devant accueillir les travaux classifiés de la société XXXX (Numéro SIRET).

Cette étude a permis de constater la présence et la mise en œuvre de moyens suivants :

- Emprise/Bâtiment :

- Local/Zone :

- Meuble de sûreté :

(Cas d'un avis d'aptitude sans objection ou avec réserves)

Cet ensemble de mesures correspond aux seuils minimaux réglementaires de protection matérielle pour la conservation de supports d'un niveau maximal « secret – très secret ». En conséquence, la Direction zonale DRSD émet un avis technique d'aptitude physique « sans objection / avec réserve » pour la zone concernée. Le présent avis est inclus dans le dossier de sécurité de l'entreprise et notifié dans les annexes de sécurité qui concernent le local précité.

Toute modification des mesures définies ci-dessus annule automatiquement le présent avis et nécessite une nouvelle évaluation.

(Cas d'un avis d'inaptitude)

Cet ensemble de mesures ne correspond pas aux seuils minimaux réglementaires de protection matérielle pour la conservation de supports d'un niveau maximal « secret – très secret ». Aucun ISC ne peut être conservé dans ladite zone. En conséquence, pour la zone concernée, la Direction zonale DRSD émet un avis technique d'inaptitude physique.

Il est donc strictement interdit d'y stocker tout ISC jusqu'à la mise en place des mesures définies en annexe et après une nouvelle évaluation de la DRSD.

COPIES :

- Poste RSD compétent
- Direction zonale DRSD
- DRSD Direction centrale – bureau en charge du suivi des ATAP
- Autorité contractante
- Autorité d'habilitation
- Eventuellement donneur d'ordre dans le cas de la sous-traitance industrielle
- Eventuellement autorité hiérarchique centrale pour les établissements étatiques

ANNEXE 7**MODELE D'AVIS D'APTITUDE SUITE A UNE COMMISSION DE MISE EN CONFORMITE**

MINISTÈRE DES ARMÉES

Direction régionale

Paris, date

N° /DEF/DRSD/

Le *autorité DRSD compétente*

Directeur de la

en région

à

Entreprise – Siège social

A l'attention de l'officier de sécurité

Adresse postale

Avis de la commission de mise en conformité

ANNEXE :**REFERENCE :**

- IM 900 / du

Le *date de tenue de la commission*, la commission d'aptitude à laquelle était présent :

- représentant de la DRSD compétente.
- représentant de l'autorité d'habilitation.
- représentant de l'autorité contractante.
- représentant du titulaire du contrat.

a évalué les mesures de protection matérielle dont bénéficie la « *zone devant accueillir les travaux classifiés* » de la société « XXXX » (Code SI).

Il apparaît que cet ensemble de mesures ne correspond pas au seuil réglementaire de protection matérielle pour la conservation de supports d'un niveau maximal «xxx», pour les raisons suivantes :

(Énumération des contraintes empêchant l'émission d'un avis d'aptitude selon les conditions générales)

-
-
-

En conséquence, la commission recommande la mise en place des mesures complémentaires et palliatives suivantes :

- *mesures dérogatoires autorisées par l'autorité contractante;*
- *mesures physiques, technique, humaines, organisationnelles mises en œuvre pour pallier les réserves ;*
- *actions à mener ;*
- *échéances à respecter.*

En regard de l'ensemble des dispositions, y compris la mise en place des mesures palliatives détaillées ci-dessus, la commission émet un avis technique d'aptitude physique « sans objection » pour la zone concernée, étant entendu que ces dispositions devront être effectives avant le « date ».

Le présent avis sera inclus dans le dossier de sécurité de l'entreprise et notifié dans les annexes de sécurité qui concernent le local précité.

Toute modification des mesures définies ci-dessus annulera automatiquement le présent avis et nécessitera une nouvelle évaluation.

Copies:

- Autorité contractante / Officier de sécurité
- Direction régionale/locale DRSD
- DRSD/ SDPS/BIC/DPS1
- DRSD/SDPS/BIC/DPS2
- DGA/SSDI
- Chrono

ANNEXE 8

CONDITIONS D'EMPLOI DES NIVEAUX DE CLASSIFICATION *SECRET* ET *TRES SECRET*

Préambule :

Chaque armée, direction ou service devra décliner un guide de classification spécifique à son périmètre de compétence.

Concernant les installations, moyens et activités de la dissuasion, il existe un guide de classification interministériel édité et mis à jour sous l'égide du SGDSN. Il porte généralement le nom de « charte de l'information concernant les forces nucléaires ». Il est classifié au niveau *Secret* et diffusé aux organismes concernés.

En fonction du sujet traité, la classification peut être assortie de la *mention Spécial France*.

Chapitre 1	Questions d'ordre général.
Chapitre 2	Questions relatives aux opérations
Chapitre 3	Questions relatives au renseignement
Chapitre 4	Questions relatives à la protection
Chapitre 5	Questions relatives à la logistique et à la mobilisation
Chapitre 6	Questions relatives aux systèmes d'information, de communication et de guerre électronique
Chapitre 7	Questions concernant les matériels, les systèmes d'armes et les recherches ou études correspondantes

TRES SECRET	SECRET
1- QUESTIONS D'ORDRE GENERAL	
Les études dans les domaines militaires (stratégiques, opératifs, tactiques, opérationnels et techniques) touchant aux concepts d'emploi des forces en opérations réelles dans le domaine nucléaire et de la guerre électronique.	Certaines études dans les domaines militaires (stratégiques, opératifs, tactiques, opérationnels et techniques) touchant aux concepts d'emploi des forces en opérations réelles à l'exception du domaine nucléaire et de la guerre électronique.
Certaines études nationales ayant trait à la conception, à la sûreté, à l'emploi des forces nucléaires et autres éléments de forces présentant un caractère très sensible.	Les études sur des sujets sensibles ²²⁴ .
	Les instructions particulières sur l'emploi et les conditions réelles d'emploi des forces.

²²⁴ La plupart des documents de doctrine (NRBC exclu) doivent être connus du plus grand nombre. Ils ne doivent pas être classifiés. A l'instar des dispositions réglementaires ils comporteront la mention DR.

	Certaines études dans les domaines militaires (stratégiques, opératifs, opérationnels et tactiques, techniques) touchant aux concepts d'emploi des forces tant que les réflexions ne sont pas figées.
Certaines synthèses d'études sur les plans à long terme et sur l'organisation des forces, en particulier dans les domaines nucléaire et de la guerre électronique..	Certaines synthèses d'études sur les plans à long terme et sur l'organisation des forces à l'exception du domaine nucléaire et de la guerre électronique.
	La plupart des études sur les plans à long terme.
Certaines recherches scientifiques et techniques qui présentent une importance majeure pour la politique de défense. Certains documents de synthèse concernant les orientations technologiques.	
Certaines questions financières susceptibles de dévoiler les intentions gouvernementales et militaires.	La plupart des études financières sur les plans d'équipement des forces.
Les accords militaires et protocoles particuliers.	Les accords militaires et protocoles particuliers après concertation avec les autres signataires.
Certains documents concernant les aspects militaires de négociations inter alliées ou internationales.	Certains documents concernant les aspects militaires de négociations inter alliées ou internationales après concertation avec les autres signataires.
Documents se référant explicitement à des documents, concepts et arguments de pays ou organisations alliées ou amies ayant la classification Secret.	
Documents de relations internationales militaires que nos partenaires étrangers souhaitent classer Secret.	La plupart des accords avec les alliés sur la coopération opérationnelle.
Mesures d'alerte essentielles aux échelons élevés du commandement touchant au domaine nucléaire et à la guerre électronique.	Mesures d'alerte essentielles aux échelons élevés du commandement à l'exception de celles touchant au domaine nucléaire et de la guerre électronique.
	Mémentos d'alerte (MEGAL).

TRES SECRET	SECRET
2 - <u>QUESTIONS RELATIVES AUX OPERATIONS</u>	
	Théâtre européen.
	Planification opérationnelle des unités non nucléaires et d'un niveau inférieur aux grands commandements.
	Attributions des autorités chargées d'un grand commandement opérationnel.
	Procédures opérationnelles sauf celles ayant trait aux questions nucléaires.
	Questions relatives à la géographie militaire.
	Études sur les systèmes d'aide au commandement.
	Schémas directeurs.
	Directives initiales de planification et appréciation stratégique.
	Les plans de défense des grands commandements (hors chapitres spécifiques TS).
	Schéma directeur d'opérations.
	Plans d'emploi et plans d'opérations.
	RESEVAC (Plans d'évacuation des ressortissants)
Plans de défense nationaux. – Les plans de recherches, moyens techniques mis en œuvre et certains aspects renseignements.	Logistique : Plans de desserrement éventuels.
Plans directement liés à la sécurité des forces nucléaires.	Plans directement liés à la sécurité des forces nucléaires stratégiques et tactiques après concertation avec les autres signataires.
Plans d'engagement nationaux ou avec les alliés	Plans d'intervention et de renforcement Outre-mer y compris les aspects énumérés aux §312 et 3120.
	Ensemble des plans de stationnement et des études sur les stationnements futurs.
	Études de déploiement hors d'Europe.
Documents de synthèse concernant l'organisation du commandement en temps de crise : transmissions, infrastructure, implantation des PC, etc.	

Exercices et manœuvres mettant en œuvre les plans alliés, nationaux, les plans de défense (thèmes généraux, moyens mis en œuvre, dispositifs, modalités de montée en puissance, résultats et appréciations) concernant les forces nucléaires et la guerre électronique.	Exercices et manœuvres mettant en œuvre les plans alliés, nationaux, les plans de défense (thèmes généraux, moyens mis en œuvre, dispositifs, résultats et appréciations) à l'exception du domaine nucléaire et de la guerre électronique.
	Ordres d'opérations concernant les exercices et manœuvres ne faisant pas référence à des plans.
	Planification et synthèses d'exercices.
Emploi de certaines forces rares et sensibles (unités de recherche du RENS, etc.)	

TRES SECRET	SECRET
3 - <u>QUESTIONS RELATIVES AU RENSEIGNEMENT</u>	
Études générales des besoins en renseignement.	
Plans de recherche à l'échelon interarmées ou des états-majors d'armées.	Plans de recherche à l'échelon des grands commandements d'emploi.
	Plans de recherches particularisés à un moyen ou à une source.
Certains ordres de recherche.	La plupart des notes d'orientation.
Certaines synthèses de renseignement sur les puissances étrangères.	La plupart des synthèses de renseignement sur les puissances étrangères.
	Certains documents de diffusion du renseignement.
Certaines études critiques sur des matériels ou des procédés techniques étrangers nouveaux ou importants liés à un plan ou à un ordre d'opération.	La plupart des informations liées au risque de prolifération NBC des puissances émergentes (mention spéciale France).
Certains comptes rendus de renseignement.	La plupart des comptes rendus de renseignement.
Certaines informations sur les méthodes employées ou le succès obtenus par les sources secrètes de renseignement et les services de contre-espionnage.	
Certains documents d'étude sur les moyens, le dispositif et les procédures des unités du renseignement militaire et de la guerre électronique.	Certains documents traitant des activités et de l'entraînement des unités et des personnels spécialistes du renseignement.

Dossiers d'objectifs majeurs.	Certains dossiers d'objectifs, d'entraînement, d'exercices ou de simulation.
Renseignements résultant d'une analyse cryptographique quand il n'y a pas de marquage du texte original.	
	Certaines études relatives au moral et au personnel.
Rapports particuliers ou occasionnels sur des sujets pouvant présenter une sensibilité particulière.	Documents de gestion susceptibles de dévoiler des intentions militaires.
	Synthèses partielles (drogue, désertion, antimilitarisme...).

TRES SECRET	SECRET
4 – <u>QUESTIONS RELATIVES A LA PROTECTION.</u>	
	Directives nationales de sécurité.
	Plans de protection et de défense des IPD et PIV.
	Plans de sécurité opérateurs.
	Certaines questions d'infrastructure liées à la sécurité des installations ²²⁵ .
	Rapports d'inspection et comptes rendus d'évaluation ou d'exercices concernant la protection d'un PIV.
Etudes de vulnérabilité, dispositions des mesures et protections militaires face aux menaces de malveillance envers les bâtiments de la marine porteurs de chaufferies et/ou d'armes nucléaires.	
Certaines questions d'infrastructure telles que projets de centres sensibles et plans d'installation de niveau gouvernemental.	Certaines questions d'infrastructure telles que projets de centres sensibles et plans d'installation de niveau gouvernemental à l'exception de celles relatives au domaine nucléaire et de la guerre électronique.
	Mise en place de certains personnels, matériels, dispositifs de protection.
	Rapports avec les autorités civiles concernant la participation des armées en cas de troubles ou d'évènements graves.

²²⁵ Se référer au code de l'environnement.

Certains dossiers et comptes rendus concernant des atteintes graves à la sécurité de la défense.	Les dossiers relatifs à la sécurité des personnes et certains dossiers et comptes rendus concernant les atteintes à la sécurité de la défense.
--	--

TRES SECRET	SECRET
5 - QUESTIONS RELATIVES A LA LOGISTIQUE ET A LA MOBILISATION.	
Travaux et questions domaniales relatives à des décisions classées Très Secret classification spéciale (SSBS, QG nationaux).	
Certains travaux préparatoires aux discussions d'accords logistiques internationaux lorsque la situation politique internationale l'exige.	La plupart des travaux préparatoires aux discussions d'accords ou aux échanges d'informations logistiques internationales.
	La plupart des travaux d'exploitation d'exercices interalliés avec ou sans participation effective des armées.
Certains documents concernant l'aide militaire à des gouvernements étrangers lorsque la situation politique internationale l'exige.	Soutiens logistiques urgents apportés à des armées étrangères.
	La plupart des questions relatives au soutien logistique des forces de présence à l'étranger, des éléments d'assistance rapide des éléments français de forces multinationales et notamment celles traitant de l'organisation du soutien.
	La plupart des travaux concernant les accords passés ou à conclure avec des pays étrangers et liés à une présence militaire française.
Transports de matières nucléaires ainsi que des matériels et des personnels dont le déplacement est couvert par une classification particulière.	Transports d'armement, munitions, matériels sensibles.
	Les plans de remplacement des services publics.
	Certains problèmes logistiques interarmées et notamment ceux relatifs aux stocks de crise et de guerre.
Plans de mobilisation.	Synthèses des plans de mobilisation.
	Catalogue des mesures à prendre.

	Directives et instructions particulières concernant le plan de mobilisation.
	Répertoires généraux relatifs à la mise sur pied des moyens.
Documents de synthèses relatifs à la montée en puissance des personnels.	Analyse de situation sur la montée en puissance (difficultés, actions, lacunes).
	Études particulières sur des vulnérabilités importantes.
Certaines synthèses sur les vulnérabilités des systèmes et des forces.	

TRES SECRET	SECRET
6 - <u>QUESTIONS RELATIVES AUX SYSTEMES D'INFORMATION, DE COMMUNICATION ET DE GUERRE ELECTRONIQUE</u>	
Certains dossiers de sécurité concernant les centres de traitement de l'information en fonction de leur importance pour le commandement, de leur vulnérabilité et de la sensibilité des informations traitées.	Les dossiers de sécurité relatifs aux sites de traitement de l'information, aux réseaux locaux et aux systèmes d'information et de communication lorsqu'ils intègrent les mécanismes de protection mis en œuvre et les vulnérabilités potentielles.
Les rapports d'audit ou d'analyse lorsqu'ils décrivent les éléments particulièrement sensibles en matière de sécurité, notamment les failles ou faiblesses, et qu'ils se rapportent à un centre correspondant au paragraphe 700.	Les rapports d'audit ou d'analyse en matière de sécurité des systèmes d'information, de communication et de guerre électronique. Les éléments et comptes rendus d'incident SSI (compromissions).
Certains états de vulnérabilité des systèmes ou d'équipements (amis/ennemis).	Les études sur des vulnérabilités des systèmes ou d'équipements (amis/ennemis).
Certaines études relatives aux concepts d'emploi, aux plans d'action opératifs ou stratégiques en matière de maîtrise des systèmes d'information et/ou de guerre de l'information.	Les plans d'action en matière de maîtrise des systèmes d'information et/ou de guerre de l'information. 7310- Certains plans d'opérations, études et bases de données en matière de maîtrise des systèmes d'information et de communication.
Les documents de conception détaillée de la plupart des équipements de guerre électronique et de sécurité des systèmes d'information et de communication.	Les dossiers d'architecture technique de la plupart des équipements de guerre électronique et des équipements de sécurité des systèmes d'information et de communication.
	Les documents de conception de nommage et d'adressage complets des réseaux informatiques.

Certaines clés de chiffrement, les éléments d'identification ou de camouflage et les documents concernant l'alerte.	Les clés de chiffrement, les éléments secrets d'identification ou de camouflage et les documents concernant l'alerte.
Certaines informations de mise en place des moyens de guerre électronique et des clés de chiffrement.	Les informations de mise en place des moyens de guerre électronique et des clés de chiffrement.
Certains plans globaux d'attribution des fréquences (fichiers interarmées d'attribution des fréquences) et plans d'attribution des fréquences "guerre" et d'opérations.	Plans globaux d'attribution des fréquences (fichiers interarmées d'attribution des fréquences) et plans d'attributions des fréquences "guerre" et d'opérations.

TRES SECRET	SECRET
7 - <u>QUESTIONS CONCERNANT LES MATERIELS, LES SYSTEMES D'ARMES ET LES RECHERCHES OU ETUDES CORRESPONDANTES.</u>	
Certaines synthèses d'étude sur les plans à long terme.	Plans à long terme en matière d'armement.
	Dossiers préparatoires à la programmation budgétaire et à la loi de programmation militaire.
	Programme pluriannuel des recherches et études.
	Certains programmes d'armement et d'infrastructure des armées.
Certaines études d'ordre technique ou d'ordre opérationnel visant à la conception (concepts, modélisation, technologie des systèmes et des matériaux, composants) et à l'évaluation (performances, vulnérabilité, coûts) des matériels ou systèmes nouveaux.	Informations ou supports d'informations, recherches ou études intéressant la conception, la faisabilité, les essais, la fabrication, la maintenance, le coût des systèmes d'arme ou d'éléments de systèmes d'armes ou de certains matériels (chaufferies nucléaires embarquées, appareils propulsifs,...).
Certains résultats d'études en relation avec l'efficacité et la vulnérabilité des systèmes d'arme en service ou en développement.	
Certaines caractéristiques, certaines performances, certains matériels et leur disponibilité, certains logiciels de système d'arme, certains logiciels de système d'information, en raison du domaine important où ils se situent (satellites d'observation, systèmes d'arme nucléaire, radars, etc.).	Certaines caractéristiques, performances, disponibilité ou modes d'utilisation des matériels ou des systèmes pouvant constituer un indicateur de capacités militaires.
Certains aspects du durcissement des systèmes de transmission.	

Certaines performances des moyens de détection (radars, sonars, détecteurs, IR, autodirecteurs...) ; en particulier celles touchant aux limitations d'emploi et à la vulnérabilité et aux capacités de contre-mesures (CME) et contre-contre-mesures (CCME) électroniques.	
Tout ou partie des signatures (EM-IR acoustiques...) de nos matériels.	
<p>Certaines questions touchant des domaines à protéger particulièrement :</p> <ul style="list-style-type: none"> - techniques d'emploi des matériels de guerre nouveaux et importants ; - amélioration de matériels de guerre majeurs ; - armes chimiques et défense biologique ; - armes nucléaires ; - centres d'expérimentation ; - certains systèmes spatiaux ; - moyens et modèles de simulations. 	Certaines études sur les effets des armes nucléaires.
Certaines études spatiales notamment les résultats et synthèses concernant des applications militaires.	
Certaines inventions et demandes de brevets d'invention.	
Certaines directives très importantes à des représentants à l'étranger.	La plupart des directives à des représentants à l'étranger.

ANNEXE 9**MODELES DE TIMBRES DE CLASSIFICATION, DE PROTECTION, DE DECLASSERMENT
ET DE DECLASSIFICATION DES INFORMATIONS ET SUPPORTS CLASSIFIES**

Le marquage d'un support papier comprend à la fois le timbre, l'identification et la pagination.

1. Couverture et page de garde pour les documents reliés

- Niveau de classification : centré, police Arial, gras, taille 18. Texte : taille 6 ;
- Epaisseur du cadre 3 points.

TRÈS SECRET

Toute personne qui détient ce document sans avoir qualité pour le connaître tombe sous le coup des dispositions du code pénal réprimant les atteintes au secret de la défense nationale

SECRET

Toute personne qui détient ce document sans avoir qualité pour le connaître tombe sous le coup des dispositions du code pénal réprimant les atteintes au secret de la défense nationale

Mention prévoyant la réévaluation du niveau de classification :

Classification à réévaluer le
[date]

Mention prévoyant l'abaissement ou le rehaussement du niveau de classification :

Le déclasserment du niveau *Très Secret*
au niveau *Secret*
intervient le
par décision n°
du

Le reclassement du niveau *Secret*
au niveau *Très Secret*
intervient le
par décision n°
du

Mention prévoyant la déclassification :

Déclassifié le [date]

A déclassifier
sur ordre de l'autorité émettrice

DÉCLASSIFIÉ

Par décision n°
du

2. Pages du document

- Niveau de classification / « Spécial France » : centré, police Arial, gras, taille 18 ;
- Epaisseur du cadre : 2,5 points.



SECRET



TRES SECRET

Exemple de marquage d'information classifiée UE :



SECRET UE/EU SECRET

Le marquage « Spécial France » est apposé uniquement en haut de la page :



SPECIAL FRANCE

ANNEXE 10

**MODELE D'ENGAGEMENT DE NON DIVULGATION DES INFORMATIONS ET
SUPPORTS DIFFUSION RESTREINTE****ATTESTATION DE RECONNAISSANCE DE RESPONSABILITE ET DE NON
DIVULGATION DES INFORMATIONS ET SUPPORTS PORTANT LA MENTION
*DIFFUSION RESTREINTE***

NOM et PRENOM :

Grade ou fonction :

Service employeur :

Je reconnais être dûment informé des responsabilités et obligations qui m'incombent :

- au titre de la protection des intérêts fondamentaux de la nation et plus particulièrement au titre des dispositions des articles 410-3 et suivants du code pénal relatives à l'espionnage et à la trahison et aux atteintes au secret de la défense nationale ;
- au titre des mesures de sécurité déclinées par l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, notamment son paragraphe 1.4.3, ainsi que son annexe 1 ;
- *pour les fonctionnaires ou agents contractuels* : au titre de la discrétion et du secret professionnel tel que défini par l'article 26 de la loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ;
- *pour les militaires* : au titre du statut général des militaires tel que défini par le livre 1^{er} de la partie 4 du code de la défense ;

En conséquence, je m'engage sans réserve :

- à ne pas divulguer, par quelque moyen que ce soit, les informations et supports portant la mention *Diffusion Restreinte* à des personnes physiques ou morales n'ayant pas le besoin d'en connaître ;
- à faire preuve de rigueur dans la gestion des informations et supports portant la mention *Diffusion Restreinte* que je serai amené à traiter.

Signature de l'intéressé

ANNEXE 11

MODELE DE FICHE DE POSITION

FICHE DE POSITION

Référence du document

N°.....en date du.....

Exemplaire n°

Niveau de classification

Détenteur :

Nom Prénom

[illegible]

ANNEXE 12

MODELE DE CAHIER D'ENREGISTREMENT DU COURRIER CLASSIFIE

Arrivée :

Références du document (S)			Echéance de classification	objet du document (éventuellement)	n° BE (A, B, B')	destinataire	émargement	Pièce / Armoire forte
n°	origine	date						
15411	ARM/EMAT	24/08/1970	24/08/2020	PSO	23/01	COL B.	\$	Coffre n°1
25412	EMA/SSA	28/02/1990	28/02/2030	Audit (ex. 3/6)	25/01	Arza M.	~	Coffre n°2
15487	DGA/DSEA/SPN	14/12/2001		Données techniques	28/01	Durant F.	£	Pièce n° 1
	Détruit le 29/01/2021 PV 2021-05/ARM/...							
25413	EMA/OIA/COS	30/06/1976	30/06/2021	Plan transports	29/01	Pierrot D.	@	Pièce 1010 Coffre n°2

Références du document (TS)			Echéance de classification	objet du document (éventuellement)	n° BE (A, B, B')	destinataire	émargement	Pièce / Armoire forte
n°	origine	date						
15920	ARM/DPID	28/07/1987	28/07/2037	Réforme PSDN (ex. 2/4)	31/01	Tief E.	&	Coffre n°2
15921	DEF/EMAT/BTSD	21/05/1968	21/05/2018	Programme SSI	02/02	COL X.	§	Pièce 1009 Coffre n°1

Départ :

Références du document S		Echéance de classification	objet du document (éventuellement)	n° BE (A, B, B')	EX. n°	destinataire	Pièce / Armoire forte
n°	origine						
254	SteX/BCA	21/01/2021		35/01 36/01	1/3 2/3 3/3	DGA SteY Archive OST	
							coffre

Références du document TS		Echéance de classification	objet du document (éventuellement)	n° BE (A, B, B')	EX. n°	destinataire	Pièce / Armoire forte
n°	origine						
14	SteX/BCA	25/01/2021		41/01 42/01	1/3 2/3 3/3	DGA SteY Archive OST	
14	SteX/BSD						coffre

ANNEXE 13

MODELE D'UN ISC DE NIVEAU *TRES SECRET***TRES SECRET****SPÉCIAL FRANCE**

(Logo de la formation)

Déclassifié le [date]

Lieu, le

N° /Timbre/classification

N° /année/BPS/classification

Ex n° /nbre total exemplaires

IDENTIFIANT FORMATION

Division ou Bureau

Bureau ou section

NATURE DU DOCUMENT

OBJET : texte, texte, texte, texte, texte.**RÉFÉRENCES** : a)code ;
b) loi ;
c)décret ;
d)arrêté ;
e)instruction ;
f) directive ;
g)lettre.**ANNEXES** : a)annexe I – titre ;
b) annexe II – titre ; (sous forme numéraire à partir de 4 - ex : Quatre annexes)
c)un projet ;
d)un cédérom.

[NP] Texte, texte (Paragraphe contenant des éléments non protégés).

Texte, texte, texte, texte, texte, texte (Style *TEXTE) (paragraphe TS SF).

Pour le délégataire et par délégation,
le (grade Prénom Nom)
fonction,**TRES SECRET**

Ce document est composé de xx pages dont une annexe de xx pages et.....

1/ nbre de pages en totalité

281

Adresse formation expéditrice– PNIA : xx.xx.xx.xx
prenom.nom@intradef.gouv.fr

TRES SECRET**SPÉCIAL FRANCE***Référence du document***DESTINATAIRE :**

- Identifiant destinataire (ex XX/ *nbre total exemplaires*)

COPIES :

- Identifiant copie (ex XX/ *nbre total exemplaires*)
- Archives générales [exemplaire numérique (ex XX/ *nbre total exemplaires*) ; chrono (ex XX/ *nbre total exemplaires*)]

TRES SECRET

TRES SECRET**SPÉCIAL FRANCE**

ANNEXE I (STYLE *TITRE ANNEXE) à la nature du document
n° (timbre entier du document - n° /année/BPS/classification)
du date du document

STYLES A APPLIQUER (STYLE *TITRE ANNEXE).

TITRE DE PREMIER NIVEAU (STYLE *TITRE1)

Texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, Texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte.

Titre de deuxième niveau (style *TITRE2)

[DR] Texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, Texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte (paragraphe contenant des informations DR).

Titre de deuxième niveau

Titre de troisième niveau (style *TITRE3)

Texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte :

liste à puces de premier niveau (Style *PUCE1) ;

liste à puces de premier niveau :

liste à puces de deuxième niveau (Style *PUCE2) ;

liste à puces de deuxième niveau.

Titre de troisième niveau

Titre de quatrième niveau (Style *TITRE4)

1.2.2.1.1 Titre de cinquième niveau et suivant

Texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, Texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte.

[S] TITRE DE PREMIER NIVEAU

Texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, Texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, texte, (Paragraphe contenant des éléments classifiés Secret).

Cette annexe comprend xx pages

TRES SECRET

3/nbre de pages en totalité
283

TRES SECRET

SPÉCIAL FRANCE

Référence du document

PAGE VIERGE

Cette annexe comprend xx pages

TRES SECRET

4/nbre de pages en totalité
284

ANNEXE 14**MODELE D'INVENTAIRE OCCASIONNEL***Lieu, le date*

N° -----/Timbre/Classification

**PROCES VERBAL D'INVENTAIRE OCCASIONNEL
DE DOCUMENTS CLASSIFIES DE NIVEAU S – TS**Date de l'inventaire : **JJ/MM/AAAA**

Inventaire contradictoire réalisé à l'occasion du changement de titulaire / Inventaire annuel

Nom, grade et fonction du détenteur responsable (descendant) :

Grade Nom Prénom, fonction

Nom, grade et fonction du détenteur responsable (montant) :

Grade Nom Prénom, fonction

Nombre de documents classifiés : XX

Nombre de support numérique classifiés : XX

Numéro du Doc	Timbres	Date du document	N° d'ex.	Intitulés
10100	ARM/EMA	03/05/2018	15/16	Instruction XXXXXXXXXX

Type de support	Référence du support	Nombre de documents
Clef USB	256 – Entité	25 (4,5 Go)

Détenteur responsable (descendant):

Grade Nom prénom

Détenteur responsable (montant):

Grade Nom prénom

DESTINATAIRE(S) :

- Officier de sécurité
- détenteur

ANNEXE 15**MODELE DE DEMANDE DE DESTRUCTION D'ISC *Très Secret****Ministère**Organisme employeur**(timbre)**N° ... /***DEMANDE DE DESTRUCTION
de supports classifiés
*Très Secret*****Support classifié *Très Secret* dont la destruction est demandée :**

- Références :

- numéro d'enregistrement et timbre :

- date de création :

- Numéro de l'exemplaire dont la destruction est envisagée :

Organisme demandeur :**Motif succinct de la demande :**
.....

Sauf avis contraire de sa part, j'envisage de procéder à la destruction du support. Aussi, sans réponse dans un délai de 2 mois, je procéderai à la destruction du support et vous en rendrai compte en vous adressant une copie du procès-verbal.

A , le

*Nom, qualité, signature de l'autorité responsable de la demande
et cachet de l'organisme.*

Destinataires :

ANNEXE 16

**MESURES CONSERVATOIRES ET CONDUITE A TENIR EN CAS DE COMPROMISSION
POSSIBLE AFFECTANT UN SYSTEME D'INFORMATION****1. Principes généraux**

Il convient de mettre en œuvre des dispositions organisationnelles permettant au plus tôt de :

- préserver le support numérique susceptible de contenir une compromission ;
- rassembler les éléments techniques et humains en rapport avec l'incident en cours ;
- informer la DRSD qui prend en charge les investigations.

Rappel :

Toutes les actions entreprises entrent dans le cadre d'une première réponse sur incident. Elles doivent impérativement être répertoriées et horodatées.

Toute intervention (visualisation du contenu d'un message, fichier ou répertoire, etc.) sur la machine est de nature à laisser des traces sur le disque dur et ainsi à compromettre la recevabilité judiciaire de la preuve.

Aussi, dès la découverte d'une compromission possible, seules les interventions techniques dûment mandatées par la DRSD sont autorisées.

2. Règles de base applicables par l'organisme touché par une compromission possible (OSSI ou OS)**a. Compromission possible sur une machine isolée**

Si l'équipement est en fonctionnement :

- laisser la machine en fonctionnement ;
- ne pas retirer les médias amovibles connectés, s'il y en a ;
- prendre une photo de l'écran si un élément anormal ou inhabituel apparaît.

Si l'équipement a été éteint, ne pas rallumer la machine.

b. Compromission possible sur machine connectée au réseau :

Appliquer les mêmes dispositions que celles prévues pour une machine isolée (§2.1).

En complément :

- noter le numéro de la prise murale du réseau ;
- débrancher le câble à l'arrière de celui-ci ;
- demander aux administrateurs du système de mettre à disposition de la DRSD les journaux d'événements des différents équipements liés (serveurs, commutateurs,...).

3. Premières constatations et investigations

Au-delà des règles de base ci-avant, les premières constatations et les investigations ultérieures doivent être réalisées par un inspecteur de la DRSD dès qu'une suspicion de compromission affectant un système d'information est signalée.

ANNEXE 17

**DOCUMENTS TRAITANT D'INFORMATIONS ET SUPPORTS CLASSIFIES A
L'INTERNATIONAL****1. Accord général de sécurité**

Un accord général de sécurité est élaboré dès l'instant où les échanges d'ISC avec l'étranger impliquent plusieurs ministères. Cet accord, bilatéral ou multilatéral, engage les gouvernements concernés. Les accords qui fixent les règles de sécurité applicables à une organisation internationale et aux pays qui y adhèrent entrent dans cette catégorie des accords généraux de sécurité. Ces accords ont valeur de traités internationaux.

En tant qu'ANS, le SGDSN est responsable de l'élaboration et de la mise en application de ces accords. Il en détermine les règles et les priorités pour leur établissement, en concertation avec la DPID, la direction des affaires juridiques (DAJ), la DGA, et l'EMA.

Le SGDSN mène les négociations avec la partie étrangère en y associant la direction des affaires juridiques (DAJ), la DGA, et l'EMA en tant que de besoin.

Ces accords identifient les équivalences des niveaux de protection dans chacun des pays et les ANS responsables de leur mise en application. Ils définissent en particulier:

- les conditions d'accès aux informations classifiées générées en commun ou échangées ;
- leurs modes de transmission ;
- les modalités d'habilitation des personnes physiques et morales nécessaires pour les échanges et/ou l'exécution des contrats en coopération ;
- les règles en matière de visites ;
- les mesures à prendre en cas de compromission d'ISC.

Ils sont établis après analyse et comparaison des réglementations respectives sur la protection du secret de défense.

La signature d'un accord de sécurité avec un partenaire étranger engage celui-ci à protéger les ISC français, communiqués ou échangés, selon des dispositions au moins équivalentes à celles appliquées pour ses propres ISC de même niveau. Par réciprocité, le gouvernement français s'engage à assurer aux ISC d'origine étrangère une protection au moins équivalente à celle appliquée aux informations françaises de même niveau.

La publication d'un tel accord rend celui-ci opposable aux tiers et permet tout recours et application des sanctions prévues au code pénal.

Sauf stipulations contraires figurant dans certains accords multilatéraux, chaque État conserve l'entière responsabilité de la conduite des inspections et audits nécessaires à la vérification des engagements pris en matière de sécurité. Au MINARM, des inspections sont menées par la DRSD dans les organismes ou établissements qui détiennent des ISC transmis par un partenaire étranger. Des audits en sécurité de défense sont aussi conduits par la DGA en tant qu'Autorité de Sécurité Déléguée pour le domaine de la sous-traitance, coopération internationale, exportation d'armement dans les organismes ou établissements en relation avec le MINARM pour s'assurer de la mise en œuvre des dispositions des accords de sécurité et des documents spécifiques (instruction de sécurité programme, annexe de sécurité internationale) et vérifier la protection et la

manipulation des ISC des partenaires étrangers et des organisations internationales confiés à la France.

L'ANS effectue également des audits (ou inspections), notamment pour le sous réseau COSMIC.

2. Accord de sécurité dans le domaine de la défense ou de l'armement

Lorsque les échanges concernent un ensemble de domaines particuliers qui relèvent du MINARM, ou lorsqu'il n'est pas possible d'identifier l'ANS étrangère compétente, un accord de sécurité dans le domaine de la défense ou plus spécifiquement de l'armement peut remplacer un accord général de sécurité. Il est préparé et négocié concomitamment par la DAJ, la DGA et l'EMA, selon leur domaine de compétence, et en concertation avec le SGDSN. Il a valeur de traité international et engage le MINARM à l'égard de son homologue étranger. Il est établi selon les mêmes principes et comprend les mêmes types d'engagements qu'un accord général.

La liste des accords généraux, de défense ou d'armement est tenue à jour par la DAJ (DIE/DIP).

3. Projets ou contrats à l'export

Accord par échange de lettres

En l'absence d'accord de sécurité, dans le cas d'échanges portant sur un domaine spécifique donné, un projet ou un contrat export, un accord par échange de lettres entre les gouvernements peut permettre la transmission ou l'échange d'informations classifiées. Cet accord, rédigé pour des sujets spécifiques, sensibles, ne repose pas sur un tableau d'équivalence, ni ne prévoit de double marquage, mais décrit les mesures de protection à prendre par la partie destinataire pour les informations classifiées françaises. Le pilote de la rédaction est le SGDSN. Les clauses sont définies en fonction de la nature du projet, de sa sensibilité et du contexte local.

Assurance de sécurité

Cette notion relève des réglementations OTAN et OCCAR.

Les contrats avec des titulaires établis dans des pays non OTAN, ou non OCCAR (ci-après désignés organisations internationales – OI) qui impliquent des ISC de ces organisations internationales requièrent l'existence d'un accord de sécurité bilatéral entre l'OI et le pays non OI dont l'ANS/ASD a juridiction sur les titulaires. Il incombe à cette ANS/ASD de faire en sorte que les titulaires assurent le niveau de protection requis pour les contrats impliquant des ISC de l'OI.

En l'absence d'un accord de sécurité bilatéral entre l'OI et le pays non OI concerné, et pour échanger des ISC de l'OI, il faut qu'un accord de sécurité bilatéral existe ou soit conclu entre un pays OI contractant et le pays non OI et que ce pays OI contractant se porte garant²²⁶.

Le pays membre qui se porte garant remet à l'OI une assurance de sécurité écrite signée par un représentant dûment mandaté par le destinataire non OI. L'assurance de sécurité

²²⁶ Notion internationale de *sponsorship* (fr. parrainage).

oblige le destinataire non OI à assurer aux informations OI classifiées un niveau de protection au moins égal à celui des dispositions contenues dans l'accord de sécurité bilatéral pour la protection des informations classifiées du pays OI d'un niveau de classification équivalent.

4. Instruction de sécurité de programme

Lors de la mise en place d'un programme en coopération, l'accord inter gouvernemental, ou l'arrangement technique fixe les clauses générales de sécurité, applicables à ce programme, dans le droit fil de l'accord de sécurité et précise le besoin de rédaction d'une instruction de sécurité programme (ISP) pour décliner et préciser les règles de sécurité.

L'ISP, dont la rédaction est pilotée par la direction de programme (nationale ou leur équivalent pour les organisations internationales) avec le support de leur autorité de sécurité, fixe les règles de protection communes des informations concernant cette coopération. Une ISP contient un guide de classification dûment protégé.

Cette ISP est validée, pour la France, par la DGA, en tant qu'autorité de sécurité déléguée dans le domaine de l'armement, ou par l'EMA pour les coopérations à vocation opérationnelle.

Dans le cadre des contrats, l'ISP est déclinée en France en plans contractuels de sécurité nationaux ou internationaux ou le cas échéant selon le modèle approuvé par les pays participant au programme (OCCAr, EDIR/FA, GMSI²²⁷, etc.) ou opération en coopération internationale. Ce plan contractuel de sécurité est désigné, dans le cadre international, par l'expression « Security Aspect Letter²²⁸ » (ou SAL) ou « security annex ».

Lorsque les titulaires sont identifiés dans l'ISP, et que celle-ci est mentionnée au contrat, elle peut alors être utilisée comme plan contractuel de sécurité (national ou international)²²⁹. Ces titulaires doivent alors faire partie de la diffusion nominale de l'ISP.

Une ISP peut, le cas échéant, être mise en place pour les programmes export complexes. Les ISP sont transmises pour information à la DRSD.

5. Attestations internationales de sécurité

Ces attestations sont communément utilisées entre la France, les pays signataires d'un accord de sécurité, et les organisations internationales.

Il existe trois formulaires types :

Facility Security Clearance Information Sheet (FSCIS)

Littéralement "feuille d'information d'habilitation d'un établissement", ce document validé par les ANS/ASD, sert à informer sur le niveau d'habilitation d'un établissement

²²⁷ Groupe Multilatéral de sécurité Industrielle (groupe informel qui établit des documents de sécurité), aussi dénommé MISWG pour l'acronyme anglais de Multinational Security Working Group.

²²⁸ Terminologie OTAN.

²²⁹ C'est le cas pour certains contrats passés par l'OCCAr au maître d'œuvre principal d'un programme, ou également pour le programme OTAN du NH90.

d'une personne morale, avec son aptitude physique et capacité à traiter de l'information numérique ; mais aussi, si demandé, à initier une procédure d'habilitation.

Ce document est renseigné par l'OS de l'organisme demandeur (étatique ou privé) et transmis à son ANS/ASD pour traitement. Il est ensuite transmis à l'ANS/ASD homologue dont ressort la personne morale objet de la requête pour réponse vers l'ANS/ASD requérante.

Personnel Security Clearance Information Sheet (PSCIS)

Littéralement "feuille d'information d'habilitation d'un personnel", ce document validé par les ANS/ASD, sert à informer sur le niveau d'habilitation d'une personne physique ; mais aussi, si demandé, à initier une procédure d'habilitation.

Ce document est renseigné par l'OS de l'organisme demandeur (étatique ou privé) et transmis à son ANS/ASD pour traitement. Il est ensuite transmis à l'ANS/ASD homologue du pays du ressortissant objet de la requête pour réponse vers l'ANS/ASD requérante.

Personnel Security Clearance Assurance Request (PSCAR)

Littéralement "demande d'attestation de sécurité d'un personnel", ce document sert à compléter l'enquête de sécurité d'un individu ayant vécu à l'étranger lorsque le temps de présence de l'individu sur le territoire n'est pas suffisant pour les besoins de l'enquête (règle otanienne des 5 ans notamment), aux fins de savoir qu'il n'y a pas d'information défavorable sur l'intéressé qui empêcheraient la délivrance d'une habilitation de sécurité nationale par le pays d'appartenance.

Le document est complété par l'OS de l'entité privée ou étatique requérante à la demande de l'autorité d'habilitation.

Il est adressé par l'ANS/ASD dont relève la partie requérante à l'ANS/ASD du pays d'origine, ou du pays de dernière résidence de la personne impliquée, qui le complète et le valide et le retourne à l'ANS/ASD requérante.

Ce processus peut aussi être utilisé pour un ressortissant pour constituer l'équivalent d'un contrôle élémentaire par exemple pour pouvoir entrer sur des sites sensibles ou mener des activités qui ne nécessitent pas une habilitation.

Ces formulaires sont disponibles sur le site ixarm.

6. Certificat de courrier

Le certificat de courrier est destiné au porteur, habilité ou ayant la qualité de convoyeur autorisé, chargé du transport du courrier, pour attester auprès des autorités de la police des frontières et des douanes du caractère officiel du transport des documents, équipements et/ou composants couverts par le certificat. Il est utilisé pour éviter les inspections directes des éléments convoyés par le porteur ou, si une inspection est inévitable, obtenir qu'elle soit effectuée dans des conditions de sécurité satisfaisantes, telles que décrites dans le formulaire (par exemple, dans une zone hors de vue des personnes qui n'ont pas une nécessité d'accès aux informations et en présence du courrier).

Le recours à un certificat de courrier ne peut avoir lieu que lorsque les procédures d'acheminement (valise diplomatique, courrier militaire spécialisé) provoquent un retard affectant, à un niveau inacceptable, la négociation ou la réalisation d'un projet, d'un programme ou d'un contrat.

L'utilisation d'un certificat de courrier pour le transport d'ISC est autorisée entre la France et un ou plusieurs pays coopérant à un projet, un programme ou un contrat gouvernemental.

Le certificat de courrier peut être utilisé pour le convoyage d'ISC à l'étranger dans le cadre d'une opération extérieure, d'un exercice multinational, d'une mission en isolé. Les ISC transportés doivent être accompagnés en permanence par un porteur autorisé.

Il existe deux types de certificats de courrier :

- le certificat de courrier « monovoyage », utilisable pour un seul transport. Un aller et retour avec les mêmes documents équivaut à un seul transport (cf. IGI 1300 – annexe 43) ;
- le certificat de courrier « multivoyages », permettant au porteur d'effectuer plusieurs transports (plusieurs aller et retour entre l'expéditeur et le destinataire) pendant une période de temps donnée (cf. IGI 1300 – annexe 44).

Pour le domaine de la coopération, export ou sous-traitance armement, les certificats de courrier sont délivrés par l'Autorité de Sécurité Déléguée (DGA/SSDI).

Sont exclus du domaine d'utilisation du certificat de courrier en raison de ses limites d'emploi :

- les documents, équipements et/ou composants classifiés de l'OTAN ; dans ce cas, le certificat de courrier est remplacé par un ordre de mission de courrier établi selon les dispositions des directives OTAN AC/35-D/2002 et AC/35-D/2003 ;
- les documents marqués *Spécial France*.

Limites d'emploi du certificat de courrier :

- le certificat de courrier ne confère pas au porteur l'immunité diplomatique au sens de la convention de Vienne (le courrier peut donc être ouvert en douane) ;
- les gouvernements des pays destinataires doivent avoir signé avec la France un arrangement ou un accord de sécurité prévoyant une procédure de transport avec de tels certificats ;
- les certificats de courrier relatifs au transport des ACSSI font l'objet de directives particulières.

Conditions de choix des porteurs autorisés :

- les porteurs autorisés sont des employés permanents de l'entité expéditrice. Il n'est en aucun cas fait appel à des intérimaires, à des transitaires ou à leur personnel, ou à des courriers indépendants ;
- les porteurs autorisés font l'objet d'une décision d'admission aux informations classifiées de niveau au moins égal à celui des informations à convoyer ;
- ces porteurs sont désignés par le chef d'entité et mentionnés dans le certificat de courrier.

Modalités de délivrance du certificat de courrier :

- toute demande de certificat de courrier est formulée par écrit et transmise à l'autorité de délivrance compétente ;

- cette demande, dûment justifiée par l'OS de l'établissement expéditeur, comporte les renseignements indispensables à l'édition du certificat de courrier ;
- la nationalité des porteurs ne peut être différente de celles d'un des pays émetteur et destinataire.

7. Plan de transport

Lorsque le contrat prévoit le transport transfrontalier de matériel classifié en tant que fret, les dispositions suivantes sont prises en compte :

- le degré de protection accordé à un envoi est déterminé en fonction du niveau de classification le plus élevé du matériel qu'il contient ;
- la société assurant le transport possède une habilitation du niveau approprié, sauf exception justifiée auprès de l'ANS/ASD. Dans tous les cas, le personnel accompagnant l'envoi est habilité au niveau approprié et muni d'un certificat de courrier conforme aux dispositions de l'IGI 1300 ;
- avant tout transfert de matériel classifié, un plan de transport est dressé par l'expéditeur et approuvé par les ANS/ASD compétentes. Le modèle de plan de transport à utiliser va dépendre du cadre duquel relève ce transport classifié (OTAN, UE, OCCAR, bilatéral) ;
- les trajets sont aussi directs et rapides que les circonstances le permettent.

Pour le domaine de la coopération, export ou sous-traitance armement, les plans de transport sont approuvés par l'Autorité de Sécurité Déléguée (DGA/SSDI) qui les transmet à ses homologues des pays traversés et du pays destinataire. Le chef d'état-major des armées est l'autorité de délivrance compétente pour signer les plans de transport de son périmètre d'activités. Il précise dans une instruction les conditions et les modalités de mise en place et d'utilisation des autorisations de transport relevant de sa compétence ainsi que le contrôle des autorisations délivrées.

Le chef d'état-major des armées peut déléguer aux chefs d'état-major d'armées la mise en place de ces autorisations, sous leur responsabilité.

Modalités de délivrance du plan de transport :

- toute demande de plan de transport est formulée par écrit et transmise à l'autorité de délivrance compétente ;
- cette demande, dûment justifiée par l'OS de l'établissement expéditeur, comporte les renseignements indispensables, requis dans l'instruction éditée par l'autorité, à l'édition du plan de transport.

ANNEXE 18

ORGANISATION DES RESEAUX OTAN ET UE**1. Réseau OTAN****a. Organisation de la sécurité à l'OTAN**

Au niveau du conseil de l'Atlantique Nord, le comité de sécurité comprend un représentant de chacun des pays membres et se réunit périodiquement au siège du conseil de l'OTAN. Il a pour mission :

- d'étudier les questions relatives à la politique de sécurité de l'OTAN ;
- d'examiner les problèmes de sécurité qui peuvent lui être soumis par le conseil, les pays membres, le secrétaire général, le comité militaire, les grands commandements et autres organismes civils ou militaires de l'OTAN ;
- de formuler des recommandations à l'intention du conseil.

Le bureau de sécurité (organisme du secrétariat international) agit sous l'autorité du comité de sécurité et relève directement du secrétaire général de l'OTAN. Il est en relation étroite avec les autorités nationales de sécurité des pays membres, le comité militaire, les grands commandements et organismes de l'OTAN. Son directeur préside le comité de sécurité.

Ce bureau est chargé :

- d'élaborer des procédures en vue d'améliorer la sécurité de l'OTAN ;
- d'assurer la coordination générale en matière de sécurité ;
- de veiller à l'exécution des décisions concernant la sécurité ;
- de coopérer avec les autorités nationales de sécurité dans les enquêtes menées en cas de compromissions.

En France, l'organisation de la sécurité OTAN est du ressort du bureau central COSMIC dont la fonction est exercée par le SGDSN²³⁰.

Cette autorité dispose, pour l'accomplissement de sa mission :

- de l'organisation française de sécurité OTAN, appelée par usage « réseau COSMIC » ;
- de l'ASD, chargée, pour les entités relevant de son périmètre (DGA, écoles sous tutelle DGA, organismes de recherche sous tutelle DGA, industrie de défense) d'informer de la politique nationale couvrant tous les aspects de la politique de sécurité industrielle de l'OTAN et de fournir les orientations et l'assistance nécessaires pour que cette politique soit appliquée.

b. Responsabilités du bureau central COSMIC

Le SGDSN :

- fait assurer la sécurité des informations protégées de l'OTAN dans les organismes nationaux, civils et militaires, situés en France et à l'étranger, conformément aux dispositions adoptées en commun par les pays membres ;
- organise le fonctionnement interne du réseau COSMIC français, notamment en prenant les décisions de création, de rattachement ou de suppression de bureaux de contrôle et en informe le bureau de sécurité de l'OTAN ;

²³⁰ Article R. 2311-11 du code de la défense.

- effectue ou peut faire effectuer des inspections périodiques, notamment par les services enquêteurs pour vérifier notamment l'application des mesures de protection du secret pour :
 - o l'habilitation des personnes ;
 - o les garanties offertes par les installations physiques et informatiques pour la détention des ISC ;
 - o les plans d'évacuation ou de destruction en cas d'urgence ;
- définit la procédure d'habilitation de sécurité à mettre en œuvre pour les ressortissants français appelés à connaître des informations protégées de l'OTAN ;
- soumet au bureau de sécurité de l'OTAN les propositions de modification des procédures de sécurité de l'OTAN et les questions impliquant une coordination entre les services de sécurité des pays membres et les organismes de l'OTAN.

c. Organisation du réseau COSMIC français

Le réseau COSMIC comprend principalement :

- un bureau central COSMIC (SGDSN) ;
- des bureaux COSMIC principaux ;
- des bureaux COSMIC isolés, directement rattachés au Bureau central COSMIC ;
- des bureaux COSMIC secondaires, rattachés aux bureaux COSMIC principaux ;
- des bureaux d'ordre SECRET OTAN, rattachés à un bureau principal ou subordonnés à un bureau secondaire, créés au sein d'organismes recevant des documents de l'OTAN et dont le niveau de classification ne peut pas dépasser le niveau SECRET OTAN.

Chaque bureau COSMIC principal est chargé de mettre en place une organisation qui répondent aux exigences du bureau central COSMIC, et par voie de conséquence, de celles de l'OTAN.

2. Organisation du réseau UE

a. Organisation de la sécurité des ICUE en France

Les Etats membres sont tenus, en application de l'Accord de 2011, de s'assurer que le niveau de protection accordé par leur droit national aux informations classifiées qui lui sont soumises soit équivalent à celui qui leur est accordé par les règles de sécurité du Conseil. L'IGI n° 2102 met en application cette obligation.

Aussi, chaque Etat membre de l'UE est dans l'obligation de protéger les ICUE et de mettre en place un système de sécurité adapté et efficace. Le secrétaire général de la défense et de la sécurité nationale, en qualité d'autorité nationale de sécurité (ANS), veille à la mise en œuvre des mesures de protection des ICUE en France.

b. Responsabilités de l'autorité nationale de sécurité et de ses délégataires dans le cadre contractuel

L'ANS ou, par délégation, l'autorité de sécurité déléguée (ASD) ou toute autre autorité compétente de chaque Etat membre veille, autant que le permettent les dispositions législatives et réglementaires nationales, à ce que les contractants et les sous-traitants immatriculés sur le territoire dudit Etat prennent toutes les mesures appropriées pour

protéger les ICUE dans le cadre de négociations précontractuelles et lors de l'exécution d'un contrat classifié.

L'ANS, l'ASD ou toute autre autorité compétente de chaque État membre veille, conformément aux dispositions législatives et réglementaires nationales, à ce que les contractants et les sous-traitants immatriculés sur le territoire dudit État, qui participent à des contrats classifiés ou à des contrats de sous-traitance nécessitant l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET au sein de leurs établissements, soient en possession, lors de l'exécution desdits contrats ou durant la phase précontractuelle, d'une habilitation nationale de sécurité d'établissement (HSE) du niveau de classification correspondant.

Lorsque les membres du personnel d'un contractant ou d'un sous-traitant doivent, en raison de leurs fonctions aux fins de l'exécution d'un contrat classifié, accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, l'ANS/ASD ou toute autre autorité de sécurité compétente leur délivre une habilitation de sécurité du personnel (HSP), conformément aux dispositions législatives ou réglementaires nationales.

c. Organisation du réseau UE français

Le réseau UE est l'organisation française de sécurité responsable du traitement des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau supérieur.

Le réseau UE comprend principalement :

- un bureau central UE (ci-après « bureau central UE ») ;
- des bureaux TRES SECRET UE/EU TOP SECRET (ci-après « bureaux TS-UE »), principaux, isolés ou subordonnés, chargés du traitement des informations classifiées TRES SECRET UE/EU TOP SECRET ;
- des bureaux de protection des ICUE (ci-après « bureaux ICUE ») pour le traitement des informations classifiées SECRET UE/EU SECRET et CONFIDENTIEL UE/EU CONFIDENTIAL.

Le SGDSN, en tant qu'ANS, est responsable de l'organisation et du fonctionnement du réseau UE. Il fait office d'autorité centrale de réception et de diffusion des informations classifiées TRES SECRET UE/EU TOP SECRET tel que prévu par la Décision 2011/292/UE et dispose, pour l'accomplissement de sa mission, du bureau central UE.

Chaque ministère est chargé de proposer au SGDSN l'organisation des bureaux TS-UE et des bureaux ICUE qui relèvent de son autorité. Cette organisation peut prendre la forme d'un sous-réseau, constitué d'un bureau principal et de plusieurs bureaux subordonnés.

Les personnes qui mettent en œuvre le réseau UE peuvent être les mêmes que celles qui mettent en œuvre les réseaux de gestion des secrets de la défense nationale ou ceux de l'OTAN. Toutefois, le principe de cloisonnement exige que les ICUE soient détenues séparément et enregistrées sur des supports spécifiques.

ANNEXE 19

MISE EN GARDE DES FRANÇAIS EN DEPLACEMENT OU EN MISSION A L'ÉTRANGER

Pour les déplacements à l'étranger, il convient de prendre en compte les recommandations suivantes :

- Se munir uniquement des pièces d'identité et des documents techniques, notes ou fichiers informatiques strictement indispensables à la mission ou déplacement, à l'exclusion de tous autres, tels que carnets d'adresses, de notes..., susceptibles d'être photographiés ou même confisqués.
- Observer strictement les formalités d'entrée et de séjour, en évitant, toute atteinte à la réglementation sur l'importation et l'exportation des devises.
- L'importation d'objets, livres, revues, voire de denrées doit se limiter aux seuls besoins personnels dans les pays où leur détention est réglementée. Les propositions d'achat ou de troc sont parfois provoquées par la police.
- Le transport de lettres ou de paquets à titre « service amical » peut motiver une inculpation pour espionnage ou activité subversive. L'acceptation de présents de mains d'inconnus ou de personnes avec lesquelles il n'est pas entretenu des relations professionnelles normales et sûres est également susceptible de faire encourir un risque. Ces envois ou cadeaux peuvent être effectués dans une intention de compromission.
- Éviter de voyager seul ; cependant on n'est jamais trop prudent dans le choix de ses compagnons de voyage. En cas d'accident lors d'un déplacement, en informer immédiatement nos services diplomatiques²³¹.
- Tous les pays veillent avec un soin jaloux à la protection de leurs installations militaires. Le stationnement à proximité des casernes ou d'autres établissements des forces armées de certains pays, la circulation sur un itinéraire non explicitement autorisé, peuvent être interprétés comme une tentative d'espionnage. Dans le même souci d'éviter l'incident, l'utilisation d'appareils photographiques est déconseillée.
- Éviter de prendre des notes en dehors de l'objet de la mission au cours des visites d'établissements scientifiques ou industriels ; cette pratique attire systématiquement l'attention des services de sécurité.
- Le transport de documents classifiés lorsqu'il est nécessaire doit se faire conformément aux règles de sécurité par le moyen de la valise diplomatique (en s'assurant au préalable des délais) ou exceptionnellement en cas d'urgence et lorsque l'accord de sécurité avec le pays de destination le prévoit, par le missionnaire muni d'un certificat de courrier établi conformément aux dispositions prévues au §6 de l'annexe 17 de la présente instruction.

²³¹L'adresse internet du MAE pour connaître les coordonnées des ambassades et consulats http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs_909/index.html

- Les postes nomades (ordinateurs portables, PDA, téléphones portables) et les supports informatiques (clés USB, CD-ROM,...) doivent faire l'objet d'une attention permanente²³².
- Les locaux d'hébergement, chambre d'hôtel ou logement chez un particulier, ne garantissent pas contre les indiscrétions ; il faut éviter d'y avoir des conversations importantes ou confidentielles. Ne ranger en aucun cas des documents de travail dans des bagages laissés sans surveillance.
- Une attention toute particulière doit être portée aux relations d'apparence amicales qui peuvent se nouer à l'occasion de ces voyages. Les services spécialisés n'hésitent pas à utiliser de tels moyens d'approche.

²³² La mise en application des préceptes de l'ANSSI relatifs au départ en mission avec son téléphone mobile, son assistant personnel ou son ordinateur portable est recommandée : <http://www.securite-informatique.gouv.fr/partirenmission/>