PREMIER
MINISTRE

Liberté
Égalité
Fraternité

Instruction ministérielle sur la protection du secret de la défense nationale

1er décembre 2021

TABLE DES MATIERES

INTRODUCTION

La présente instruction sur la protection du secret et des informations « Diffusion Restreinte » décline pour les services du Premier ministre les orientations énoncées dans l'instruction générale interministérielle 1300 (IGI 1300), dans l'instruction générale interministérielle n° 2102 pour ce qui est de la protection en France des informations classifiées de l'Union européenne et de l'instruction interministérielle n° 2100 pour ce qui est de la protection en France des informations classifiées de l'organisation du traité de l'Atlantique nord.

Cette instruction est principalement destinée à l'usage des officiers de sécurité, maillons essentiels de la chaîne de protection du secret. Elle doit permettre, plus largement, une meilleure sensibilisation aux enjeux de la protection du secret au sein des services du Premier ministre.

A cette fin, elle reprend les récentes évolutions de la règlementation, notamment la nouvelle nomenclature de classification (*Secret, Très Secret*), le renforcement du suivi des informations et supports classifiés tout au long de leur cycle de vie et les nouvelles dispositions applicables en matière de déclassification.

Elle apporte par ailleurs les précisions nécessaires relatives aux enquêtes administratives, aux missions et tâches de l'officier de sécurité et à la contribution de sécurité des systèmes d'information à la protection du secret.

Elle évoque également les informations protégées par la mention de protection *Diffusion Restreinte* et celles, sans être classifiées ou protégées, qui peuvent néanmoins revêtir un caractère sensible.

Elle s'applique au périmètre de compétence du haut fonctionnaire de défense et de sécurité auprès du Premier ministre, tel que défini par le décret n° 2012-383 du 20 mars 2012[1]. Elle s'applique ainsi aux autorités administratives indépendantes autorisées par la loi à accéder à des informations et supports classifiés et à la Cour des comptes.

Sa mise à jour, en fonction des évolutions législatives ou réglementaires, voire pratiques, est effectuée par le moyen d'instructions modificatives du HFDS/PM.

[1] Pour rappel, le SGDSN et ses entités rattachées (services et établissement public) ne relèvent pas de la compétence du haut fonctionnaire de défense et de sécurité auprès du Premier ministre.

REFERENCES

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.

Code de la défense, et notamment les articles L. 1111-1, L. 1131-L L. 1332-1 et suivants, L. 2311-1. L. 2312-1 à L. 2312- 8, L. 2362-1, L 4121-2, R.* 1132-1 à R.* 1132-3 ; R. 1143-1, R. 1143-2, R. 1143-5, R. 1143-6, R. 1143-8, R. 2311-1 à R. 2311-9-1, R. 2311-10 à R. 2311-11, D.* 2311-12, R. 2312-1, R. 2312-2.

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

Code pénal, et notamment les articles 121-2, 226-13 et 14 (atteinte au secret professionnel), 411-6 à 411-8, 413-7, 413-9 à 413-12 (atteinte au secret de la défense nationale), 414-5 à 414-9, 434-4, R. 413-1 à R. 413-5 et 444-1 à 444-9.

Code civil, art.22.

Code de procédure pénale, article 56-4.

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

Code de la commande publique, et notamment les articles L. 2141-1 et suivants, R. 2300-1, R. 2332-8, R. 2343-4, R. 2343-5, R. 2343-13, R. 2351-14, R. 2396-6, R. 3123-3.
Code du commerce, article L. 210-3.

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

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

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

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.

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

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.

Décret n° 2019-1271 du 2 décembre 2019 relatif aux modalités de classification et de protection du secret de la défense nationale.

Arrêté du 9 août 2021 portant approbation de l'instruction générale interministérielle 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)

Instruction interministérielle n° 50/SGDN/SSD/DR sur la protection du secret dans les rapports entre la France et les États étrangers du 9 janvier 1971.

Instruction interministérielle n° 910/SGDSN/ANSSI relative aux articles contrôlés de la sécurité des systèmes d'information du 22 octobre 2013.

Instruction générale interministérielle n° 6600/SGDSN/PSE/PSD relative à la sécurité des activités d'importance vitale du 7 janvier 2014.

Instruction interministérielle n° 901/SGDSN/ANSSI sur la protection des systèmes d'information sensibles du 28 janvier 2015.

1. PRINCIPES GENERAUX

1.1. Le secret de la défense nationale

Selon l'article 413-9 du Code pénal, *« Présentent un caractère de secret de la défense nationale au sens de la présente section, les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès.*

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

Ainsi, le secret de la défense nationale ne constitue pas qu'un enjeu de défense « militaire », dans la mesure où la défense nationale concerne toutes les administrations responsables de ressources essentielles à la vie du pays (conception globale de la défense envisagée dès l'ordonnance du 7 janvier 1959). La défense nationale s'inscrit en effet dans le contexte plus vaste, transversal et interministériel, de la stratégie de sécurité nationale, qui a pour objet *« d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République, et de déterminer les réponses que les pouvoirs publics doivent y apporter*[2] *»*.

Sous réserve des dispositions en vigueur, les services et entités rattachés au Premier ministre peuvent produire, avoir connaissance et échanger des informations qui ressortent du secret de la défense nationale.

A titre d'illustration, ces informations peuvent :

- concerner les activités et les travaux du cabinet civil, du cabinet militaire du Premier ministre et du secrétariat général du Gouvernement ainsi que des directions et services qui y contribuent ;

- être issues des conseils de défense et de sécurité nationale et de réunions interministérielles classifiées ;

- concerner la protection contre la malveillance sous toutes ses formes visant les services du Premier ministre.

1.2. 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 à la sauvegarde des intérêts fondamentaux de la Nation.

[2] Article L. 1111-1 du code de la défense.

Elle est régie par les principes suivants :

1.2.1. Le principe de la matérialité du secret

Selon l'article 413-9 du code pénal, peuvent présenter un caractère secret de la défense nationale « les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers ».

L'information classifiée prend corps dans un document et le cas échéant, mise sous format électronique, s'incarne dans un support numérique (une clef USB, par exemple).

Cette matérialité de l'information permet de lui apposer un marquage (un timbre de classification) et lui confère la protection du code pénal. Elle conduit à manipuler l'information selon des mesures de protection spécifiques, à protéger le document en le conservant dans des meubles de sécurité ou utiliser des systèmes d'information (SI) homologués.

La dématérialisation croissante des informations classifiées exige une collaboration très étroite entre les officiers de sécurité et les acteurs de la chaîne fonctionnelle de sécurité des systèmes d'information (cf. paragraphes 2.2.3 à 2.2.5).

1.2.2. Le principe du contrôle de confiance préalable

L'accès au secret de la défense nationale par une personne ne peut se faire que s'il existe un certain degré de confiance. Ce principe de confiance s'incarne dans le processus d'habilitation destiné à vérifier que la personne physique ou morale peut sans risque pour la défense et la sécurité nationale, accéder à des informations et supports classifiés (ISC).

L'habilitation doit être justifiée dans un catalogue d'emploi, établi par le chef d'organisme, qui confirme le « besoin d'en connaître » et implique une enquête administrative préalable sur la personne qui doit accéder à des ISC. Cette exigence réglementaire résulte de l'article R. 2311-7 du code de la défense qui dispose que « *[…] nul n'est qualifié pour connaître d'ISC s'il n'a fait au préalable l'objet d'une décision d'habilitation et s'il n'a besoin au regard du catalogue des emplois justifiant une habilitation, […] de les connaître pour l'exercice de sa fonction ou l'accomplissement de sa mission* ».

1.2.3. Le principe de cloisonnement des ISC

Pour que les ISC ne circulent qu'auprès de personnes habilitées ayant le « besoin de les connaître », il faut en limiter l'accès et en contrôler le partage. C'est le principe du cloisonnement qui impose de prendre connaissance d'une information dans le cadre strict de l'exercice d'une fonction ou l'accomplissement d'une mission.

Le cloisonnement se traduit :

- *pour les données sur un système d'informations classifié, par une gestion stricte des droits d'accès ;*

- *pour le stockage d'ISC dans une armoire forte commune à plusieurs services, par une séparation physique stricte.*

1.2.4. Le principe de traçabilité des ISC

En application du § 7.2 de l'IGI 1300, les ISC sont tracés depuis leur rédaction/création jusqu'à leur détention finale et à leur destruction/archivage en passant par leurs copies et leur distribution.

La perte d'une information ou d'un support classifié, y compris par la chaîne de protection du secret, est considérée comme une possible compromission.

Pour respecter ce principe, les responsables d'organismes doivent veiller en particulier à préciser dans leur politique de protection du secret les consignes pour la reproduction et l'impression des ISC (cf. paragraphe 4.8).

1.3. La sanction des atteintes au secret de la défense nationale

La divulgation à un tiers non qualifié (personne physique ou morale) d'ISC peut avoir des conséquences extrêmement préjudiciables. Les ISC constituent en effet de potentielles cibles pour les services étrangers ou pour toute organisation ou individu souhaitant déstabiliser l'État en s'attaquant à sa population ou à son tissu économique et industriel. 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.

L'atteinte au secret de la défense nationale est ainsi sanctionnée au plan pénal. Elle constitue un délit prévu aux articles 413-10 et 413-11 du code pénal. Ces articles différencient les sanctions selon la qualité de la personne qui peut être « *toute personne dépositaire, soit par état ou profession, soit en raison d'une fonction ou d'une mission temporaire ou permanente* » d'un tel secret (art. 413-10) ou bien un tiers quelconque (art. 413-11).

Une personne dépositaire ou non, agissant volontairement ou non, se rend coupable d'un délit de compromission lorsqu'une information ou un support classifié est détruit, détourné, soustrait, reproduit sans autorisation ou divulgué c'est-à-dire rendu accessible ou porté à la connaissance d'une ou plusieurs personnes non qualifiées.

La caractérisation du délit, sa répression et la procédure à suivre en cas de compromission sont détaillées au § 1.4.2 de l'IGI 1300.

1.4. Les niveaux de classification

La classification d'une information la place sous la protection de dispositions du code pénal. Cette protection comprend un mécanisme d'autorisation pour accéder à cette information (l'habilitation, cf. paragraphe 3), des règles de gestion particulières (enregistrement, inventaire, déclassification, destruction, cf. paragraphe 4) et des mesures physiques pour limiter l'accès à cette information (cf. paragraphe 5).

Les différents niveaux de classification correspondent à des mesures de protection graduées et proportionnées aux risques encourus en cas de compromission du secret de la défense nationale.

On distingue deux niveaux de classification, les niveaux *Secret* et *Très Secret* :

- *Secret* : réservé aux informations et supports dont la divulgation ou auxquels l'accès non autorisé 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 non autorisé aurait des conséquences exceptionnellement graves pour la défense et la sécurité nationale.

Des « classifications spéciales » existent pour le niveau *Très Secret* afin de protéger les informations relatives aux priorités gouvernementales en matière de défense et de sécurité nationale[3]. Depuis le 1er juillet 2021, ces classifications spéciales recouvrent les anciennes classifications spéciales du *Très Secret Défense*.

NB : La mise en place des niveaux de classification, « Secret » et « Très Secret », ne signifie nullement que les anciens documents marqués « Confidentiel Défense » ou « Secret Défense » sont à marquer de nouveau ou qu'ils perdent toute protection.

A compter du 1er juillet 2021, les règles suivantes sont à appliquer :

- *tout ISC élaboré à partir de cette date porte les nouveaux timbres (Secret ou Très Secret) ;*

- *les ISC élaborés avant cette date (et stockés dans les armoires fortes) conservent leur marquage « Confidentiel Défense » et « Secret Défense » et la protection juridique associée. L'ensemble des règles des niveaux « Secret » et « Très Secret » définies dans la nouvelle IGI 1300 et la présente instruction leur sont applicables[4].*

1.5. La mention « Diffusion Restreinte » et la mention « Spécial France »

1.5.1. La mention « Diffusion Restreinte »

Traitée par le § 1.4.3 de l'IGI 1300, la mention « *Diffusion Restreinte » (DR)* n'est pas un niveau de classification mais une mention de protection. Elle a pour but d'imposer à l'utilisateur d'être discret dans la gestion des informations couvertes par cette mention.

Susceptible, par exemple, de porter atteinte au secret des délibérations du Gouvernement, à la sécurité d'une installation, à la notoriété d'un service public, à la vie privée de ses agents, une information protégée par la mention DR ne doit pas être rendue publique mais peut être communiquée aux personnes devant en connaître dans l'exercice de leurs fonctions ou dans l'accomplissement de leurs missions.

[3] La protection de ces ISC est organisée dans le cadre d'une réglementation particulière du SGDSN, qui complète les dispositions de l'IGI 1300 ; elle s'opère dans le cadre d'une chaîne de sécurité distincte de celle décrite au chapitre 2.
[4] Cf. article 11 du décret n° 2019-1271 du 2 décembre 2019 sur les modalités de classification et de protection du secret de la défense nationale.

Dans la mesure où il ne s'agit pas d'ISC, les règles de gestion sont moins contraignantes. La divulgation intentionnelle ou par négligence d'un document protégé par la mention DR ne constitue pas une compromission au sens du code pénal. Elle peut cependant constituer une faute professionnelle et exposer la personne responsable à des sanctions administratives et disciplinaires ainsi qu'éventuellement pénales au titre de la violation du secret professionnel.

1.5.2. La mention complémentaire « Spécial France »

Classifiées ou « Diffusion Restreinte », les informations marquées « *Spécial France* » (SF) ne peuvent être transmises qu'à des personnes physiques ayant la nationalité française et à des personnes morales établies en France ayant le besoin d'en connaître.

1.6. Les informations sensibles et le devoir de discrétion des agents publics

1.6.1. Les informations sensibles

Certaines informations, sans être classifiées ou protégées par la mention de protection *Diffusion Restreinte*, peuvent néanmoins revêtir un caractère sensible. Au sens de cette 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 pourrait nuire à l'image ou aux intérêts des services du Premier ministre (SPM), des organismes placés sous son autorité, sous sa tutelle ou liés par contrat ou convention, ou à leur personnel 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) ;

- consistait en un document falsifié.

Ainsi, dans le champ d'application de la présente instruction, sont considérées comme sensibles :

- les informations couvertes par le secret des délibérations du Gouvernement ;

- les données à caractère personnel ;

- plus largement, les informations stratégiques et organisationnelles, les informations techniques et technico-commerciales, les informations commerciales et les données économiques et financières.

1.6.2. Le devoir de discrétion des agents publics

La discrétion professionnelle est requise au sein des SPM afin d'éviter la divulgation non maîtrisée d'informations relatives notamment à l'activité ou au fonctionnement des sites et des entités rattachées au Premier ministre.

La discrétion professionnelle est définie à l'alinéa 2 de l'article 26 du statut général des fonctionnaires : *« Les fonctionnaires doivent faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont ils ont connaissance dans l'exercice ou à l'occasion de l'exercice de leurs fonctions. En dehors des cas expressément prévus par la réglementation en*

vigueur, notamment en matière de liberté d'accès aux documents administratifs, les fonctionnaires ne peuvent être déliés de cette obligation de discrétion professionnelle que par décision expresse de l'autorité dont ils dépendent ».

Ce devoir de discrétion concerne les informations qui n'ont pas vocation à être communiquées au public. Cette obligation s'applique à l'extérieur de l'environnement professionnel (notamment sur les réseaux sociaux), mais également à l'égard du personnel qui n'a pas besoin d'en connaître même s'il appartient au même service.

Tout manquement à cette obligation peut donner lieu à des sanctions administratives et disciplinaires.

2. STRUCTURES, INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.1. Le pilotage de la protection du secret

2.1.1. Le SGDSN

Sous l'autorité du Premier ministre, le secrétariat général de la défense et de la sécurité nationale (SGDSN) définit et coordonne sur le plan interministériel la politique de sécurité en matière de protection du secret de la défense nationale, y compris en matière de sécurité des systèmes d'information, avec l'assistance de l'agence nationale de la sécurité des systèmes d'information (ANSSI).

Au niveau national, le SGDSN veille notamment à la mise en œuvre des mesures relatives aux classifications spéciales pouvant être associées au niveau de classification « Très Secret ».

Au plan international, le SGDSN est l'autorité nationale de sécurité (ANS) pour le secret de la défense nationale[5]. A ce titre, il joue un rôle dans les habilitations[6] des personnes morales et physiques dans le cadre international, qu'elles soient étrangères en France ou françaises à l'étranger. Il assure la sécurité des ISC confiés à la France, qu'ils soient étrangers ou d'organisations interalliées (OTAN et UE, par exemple). L'ANS peut nommer des autorités de sécurité déléguées (ASD), chargées de mettre en œuvre ses missions dans un domaine particulier.

2.1.2. Le Premier ministre à l'égard de ses services

Le Premier ministre est responsable de la protection du secret de la défense nationale pour l'ensemble des organismes qui lui sont rattachés 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.

Au sens de l'IGI 1300, le Premier ministre est « autorité émettrice » pour les ISC aux niveaux *Secret* et *Très Secret* dont l'élaboration est nécessaire à l'exercice de ses missions, celles de son cabinet ou celles dévolues aux services et entités placés sous son autorité.

[5] Code de la défense, art. 2311-10-1.

[6] Pour les autres missions de l'ANS, se référer au § 2.1.1.2 de l'IGI 1300.

Conformément aux consignes de classification de la présente instruction, les autorités suivantes, à la condition qu'elles aient été elles-mêmes dûment habilitées, décident, sous la responsabilité du Premier ministre, de la classification des informations produites chacun dans leur périmètre de responsabilité :

- le directeur de cabinet,
- le directeur adjoint de cabinet,
- le chef du cabinet militaire,
- le secrétaire général du Gouvernement,
- les directeurs de l'administration centrale et les chefs de service de rang équivalent.

NB : Les autorités administratives indépendantes, autorisées par la loi à accéder au secret de la défense nationale, et la Cour des comptes sont également des « autorités émettrices » au sens de l'IGI 1300.

Le Premier ministre est l'autorité d'habilitation aux niveaux *Secret* et *Très Secret*, ainsi qu'aux niveaux équivalents de l'Union européenne (UE) et de l'organisation du traité de l'Atlantique nord (OTAN), pour les services et organismes qui lui sont rattachés. Cette compétence s'étend aux personnes morales liées contractuellement à ces services et ayant à connaître d'ISC dans ce cadre (cf. paragraphe 3.7).

2.1.3. Le haut fonctionnaire de défense et de sécurité auprès du Premier ministre

Le Premier ministre est assisté du secrétaire général du Gouvernement, haut fonctionnaire de défense et de sécurité auprès du Premier ministre (HFDS/PM). Les attributions du HFDS/PM sont précisées dans le décret n° 2012-383 du 20 mars 2012.

Ainsi, en matière de protection du secret de la défense nationale, le HFDS/PM a autorité sur l'ensemble des services du Premier ministre. Cependant, en application du décret du 20 mars 2012, le SGDSN, l'ANSSI, l'OSIIC[7], le GIC[8], l'IHEDN[9] et l'Académie du renseignement sont exclus de son périmètre de compétences[10].

Par arrêté et à leur demande, le HFDS/PM peut assister les juridictions et autorités administratives indépendantes autorisées à accéder au secret de la défense nationale et rattachées pour leur gestion administrative et budgétaire au Premier ministre.

Sa compétence s'étend aux personnes morales candidates ou parties à un contrat de la commande publique, à un contrat de sous-traitance, à un sous-contrat, à un contrat de la commande publique, à un contrat de subvention émanant des SPM dès que des ISC sont transmis ou échangés.

---

[7] Opérateur des systèmes d'information interministériels classifiés.

[8] Groupement interministériel de contrôle.

[9] Institut des hautes études de défense nationale.

[10] Le Service de vigilance et de protection contre les ingérences numériques étrangères, nouvellement créé au sein du SGDSN par le décret n° 2021-922 du 13 juillet 2021, est également exclu du périmètre de compétence du HFDS/PM.

Le HFDS/PM anime et coordonne la politique de défense et de sécurité pour les services relevant du Premier ministre. Le Premier ministre lui délègue sa signature en matière d'habilitation des personnes physiques et morales aux niveaux *Secret* et *Très Secret* (hors classifications spéciales qui relèvent du SGDSN), ainsi qu'aux niveaux équivalents de l'UE et de l'OTAN. Le HFDS/PM est chargé des relations avec le SGDSN et avec les hauts fonctionnaires de défense et de sécurité des autres ministères.

Le HFDS/PM est assisté par **le chef de la mission d'organisation des services du Premier ministre, haut fonctionnaire adjoint de défense et de sécurité auprès du Premier ministre** (HFDSa/PM) et chef du service du HFDS.

Pour le compte du HFDS/PM, le HFDSa/PM anime les chaînes fonctionnelles de la protection du secret et de la sécurité des systèmes d'information. Il dispose d'un **fonctionnaire de sécurité de défense** (FSD) et d'un **fonctionnaire de sécurité des systèmes d'information** (FSSI).

2.1.4. Le fonctionnaire de sécurité de défense des SPM

Le fonctionnaire de sécurité de défense des services du Premier ministre (FSD/PM) est désigné par le HFDS/PM et placé auprès du HFDSa/PM. Sous son autorité, il anime la chaîne fonctionnelle de protection du secret. À ce titre, il définit les mesures de protection des ISC, ceux protégés par la mention de protection *Diffusion Restreinte* ou les informations et supports sensibles. Il en fait contrôler l'application sur l'ensemble des entités relevant du champ de compétences des services du Premier ministre. Il a la charge de leur mise en œuvre dans l'ensemble du périmètre.

Pour l'assister dans l'exécution de ses attributions, le FSD/PM s'appuie sur le réseau des officiers de sécurité (OS) et travaille en lien avec le fonctionnaire de sécurité des systèmes d'information auprès du Premier ministre (FSSI/PM).

Ses attributions sont précisées en annexe II de la présente instruction.

2.1.5. Le fonctionnaire de sécurité des systèmes d'information auprès du Premier ministre

Le fonctionnaire de sécurité des systèmes d'information auprès du Premier ministre (FSSI/PM) est nommé par le Premier ministre et placé auprès du HFDSa/PM. Il a la charge d'animer la chaîne fonctionnelle « sécurité des systèmes d'information » (SSI) dans le périmètre des SPM (hors SGDSN qui conserve son autonomie). Sa compétence s'étend aux services numériques interministériels et aux infrastructures transverses [11] de la compétence de la direction interministérielle du numérique (DINUM).

A ce titre, le FSSI/PM :

- porte la réglementation interministérielle à la connaissance des différents organismes ;
- définit les mesures concernant la sécurité des systèmes d'information, notamment classifiés, en définissant pour chaque type de système d'information les mesures de

[11] Notamment, le réseau interministériel de l'Etat (RIE).

protection précisées dans la politique de sécurité des systèmes d'information (PSSI) des SPM ;

- 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.

En lien étroit avec les responsables des entités relevant des SPM, il met en œuvre la politique ministérielle de sécurité du numérique.

Dans le cadre de ses attributions, il apporte son concours aux acteurs de la chaîne fonctionnelle de protection du secret, en définissant les mesures de protection des systèmes d'information classifiés et des articles contrôlés de la sécurité des systèmes d'information (ACSSI) pour les services du Premier ministre.

Ses attributions sont précisées en annexe III de la présente instruction.

2.2. La mise en œuvre de la protection du secret

La protection du secret repose sur un réseau de confiance qui impose à chacun la nécessité de protéger le secret au profit de l'intérêt général. Les acteurs de ce réseau qui détiennent des ISC sont les responsables d'organisme et le personnel de ces organismes en qualité de détenteur final.

2.2.1. Le responsable d'organisme

Le responsable d'organisme est le responsable local 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[12], 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 et de la sécurité des systèmes d'information. A cet effet, il désigne un OS et, si nécessaire, un officier de sécurité des systèmes d'information (OSSI) ainsi que, dans la mesure du possible, un adjoint ou suppléant pour chacun d'eux, au sein de son organisme. A défaut d'OS et/ou d'OSSI, le responsable d'organisme exerce la fonction d'OS et/ou OSSI et se charge lui-même de l'accomplissement des tâches relatives à la protection du secret pour son entité.

Au sens de l'IGI 1300 et de la présente instruction, les responsables d'organisme sont :

- pour les services de l'État (services centraux, services déconcentrés, services à compétence nationale, organismes extérieurs comme les établissements sous tutelle) : le chef du service ou de l'entité ayant accès à des ISC.

[12] La politique de protection du secret de l'organisme est transmise au HFDSa/PM pour approbation.

- pour les personnes morales autres que l'État : le représentant légal de la personne morale.

Pour assumer cette responsabilité, il incombe au responsable d'organisme :

- de doter sa structure de l'organisation et des procédures nécessaires pour garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité des informations et des supports classifiés ;

- d'organiser les chaînes fonctionnelles de protection du secret et de sécurité des systèmes d'information dans son organisme avec la désignation d'un OS et d'un OSSI, le cas échéant ;

- de veiller à la bonne gestion des habilitations, en définissant le besoin d'en connaître au sein de son organisme, en établissant le catalogue des emplois et en faisant habiliter son personnel en conséquence ;

- de faire assurer la protection des ISC conformément à la réglementation en donnant à son personnel les moyens matériels adéquats et en déterminant les sujets devant bénéficier de la protection pénale conférée au secret de la défense nationale.

2.2.2. Le détenteur de l'ISC

Seules les personnes qualifiées peuvent accéder et détenir des informations et des supports classifiés. Cette qualification exige deux conditions cumulatives :

- le besoin d'en connaître ;

- la délivrance d'une habilitation au niveau de classification requis.

Seule, l'habilitation ne permet pas d'accéder sans limite à toutes les informations et à tous les supports classifiés.

Le détenteur d'ISC, personne morale ou physique habilitée et clairement identifiée assume la responsabilité de leur protection, à partir du moment où il lui a été attribué sans ambiguïté[13].

2.2.3. La chaîne fonctionnelle de la protection du secret

En application du § 2.2.2 de l'IGI 1300, la chaîne fonctionnelle de protection du secret des SPM est organisée de façon à veiller à la bonne mise en œuvre des dispositions relatives à la protection du secret, aux informations DR et sensibles au sein de chaque entité et organisme relevant du Premier ministre.

Elle est structurée de façon à :

- veiller à la bonne mise en œuvre des mesures de sécurité applicables aux personnes physiques et morales ;

[13] L'enregistrement du support classifié n'est pas une condition préalable à la responsabilité du détenteur. Celle-ci débute dès la prise en charge du support classifié.

- garantir la protection physique et logiques des ISC, y compris les systèmes d'information classifiés ;
- assurer la gestion des ISC ;

- être en capacité de détecter dans les meilleurs délais toute compromission avérée ou suspectée ;

- veiller au respect des mesures de prévention et de protection, y compris pour les systèmes d'information classifiés ;

- identifier et tracer les informations qui doivent être classifiées ou protégées.

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

2.2.4. L'officier de sécurité

L'officier de sécurité (OS) est le maillon essentiel de la chaîne de protection du secret, des informations DR et sensibles. Son rôle est décrit au § 2.2.2.1 de l'IGI 1300.

En liaison avec le HFDSa/PM et le FSD/PM, il élabore la politique de protection de son organisme et travaille en étroite collaboration avec les acteurs de la chaîne fonctionnelle de sécurité des systèmes d'information classifiés, ainsi que les systèmes DR et, le cas échéant, sensibles.

L'OS est chargé de fixer les règles et consignes relatives à la protection du secret et d'en contrôler l'application. Il a également la charge de la gestion des habilitations et du contrôle des accès aux zones protégées ou réservées (cf. paragraphe 5.4).

Il instruit et sensibilise le personnel de son organisme en matière de protection du secret de la défense nationale.

Enfin, si l'organisme détient des ISC de niveau *Très Secret* (TS), l'OS dirige le bureau de protection du secret (BPS)[14], obligatoire pour ce niveau et au sein duquel s'effectuent l'élaboration, le traitement, le marquage, la conservation et la destruction des ISC TS.

L'OS est officiellement nommé par décision écrite de son chef d'organisme, adressée en copie au FSD/PM. Pour être désigné, il doit :

- appartenir de façon stable à l'organisme,

- être habilité au niveau adéquat,

- être formé à la gestion du secret,

- avoir un niveau hiérarchique suffisant et l'autorité fonctionnelle nécessaire,

- disposer des moyens nécessaires pour accomplir ses missions.

[14] Le BPS est décrit au § 7.2.1.2 de l'IGI 1300.

Les différents critères exigés pour la désignation d'un OS sont détaillés au paragraphe 2.2.2.1 de l'IGI 1300.

L'OS suit une formation spécifique[15] dans les 12 mois suivant (à moins qu'il ne détienne un certificat attestant qu'il a suivi une telle formation dans les 5 années précédant sa nomination).

Afin d'éviter toute rupture dans la protection à accorder aux ISC, l'OS peut disposer d'un suppléant ou d'un adjoint répondant pour leur désignation aux mêmes exigences que celles de l'OS.

2.2.5. La chaîne fonctionnelle de sécurité des systèmes d'information et son apport à la protection du secret

Abordée au paragraphe 2.2.3 de l'IGI 1300, la chaîne fonctionnelle de sécurité des systèmes d'information est organisée de manière à veiller à la sécurité de l'ensemble des systèmes d'informations détenus par les entités et organismes relevant des SPM, tout au long de leur vie, y compris les systèmes d'information DR et sensibles.

Son rôle n'est pas spécifique aux systèmes d'information classifiés mais est renforcé en ce qui les concerne. Sous l'autorité du responsable d'organisme, elle contribue ainsi au déploiement et à la traçabilité des articles contrôlés de la sécurité des systèmes d'information (ACSSI).

L'autorité qualifiée en sécurité des systèmes d'information (AQSSI) est chargée de décliner et de mettre en œuvre la politique de sécurité du numérique, au sein de son organisme. Dans ce cadre, elle définit les lignes directrices relatives à la sécurité des systèmes d'information classifiés et en contrôle l'application.

Lorsque des SI classifiés sont utilisés au sein de l'organisme, **un officier de sécurité des systèmes d'information** (OSSI) est désigné.

Correspondant du FSSI/PM, l'OSSI appuie l'action de l'OS et est notamment chargé de :

- concevoir et mettre en œuvre le management de la sécurité des systèmes d'information. A ce titre, il définit les exigences de sécurité applicables au sein de l'organisme et relatives à l'usage des systèmes d'information classifiés utilisés ;

- vérifier la mise en œuvre de la politique de SSI et particulièrement la protection des ISC ;

- s'assurer de la prise en compte des exigences de sécurité numérique à tous les stades du cycle de vie des systèmes d'information (étude, réalisation, utilisation, évolution, démantèlement) ;

- participer à la sensibilisation du personnel en matière de protection du secret de la défense nationale.

[15] Sont notamment reconnues les formations dispensées notamment par :
- l'institut des hautes études du ministère de l'Intérieur (IHEMI),
- le centre d'instruction en sécurité industrielle de l'armement de la délégation générale pour l'armement du ministère des Armées (DGA/CISIA).

Désigné par le chef d'organisme, le responsable de la sécurité des systèmes d'information (RSSI) accompagne tout responsable d'une structure en charge du numérique dans la mise en œuvre opérationnelle de la sécurité du numérique.

A ce titre, il intervient dans le cadre du développement et de l'exploitation d'un système d'information classifié. Ainsi, en lien avec l'OSSI, il pilote l'intégration de la sécurité du système classifié de la phase projet jusqu' à l'homologation initiale. Il assure ensuite le suivi de la sécurité du SI classifié une fois en service. Conseiller de l'autorité d'emploi du système d'information classifié, il est garant de la cohérence des mécanismes et des procédures de sécurité ainsi que du maintien du niveau de sécurité dans le temps.

3. LES MESURES DE SECURITE APPLICABLES AUX PERSONNES

En application de l'article R. 2311-7 du code de la défense, « *Nul n'est qualifié pour connaître des informations ou supports classifiés s'il n'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* ».

3.1. Le catalogue des emplois

L'appréciation du « besoin d'en connaître » est fondée sur le principe selon lequel une personne ne peut avoir accès à des ISC 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 service ou d'une entité.

Le besoin d'en connaître se traduit par l'inscription de l'emploi sur un catalogue *ad hoc* et est attesté par la demande d'habilitation, adjointe à la notice individuelle de sécurité (NIS), incluse dans le dossier d'habilitation (cf. IGI 1300 - annexes 5 et 7). Le numéro d'inscription au catalogue des emplois figure dans ce dossier.

L'autorité d'emploi, qu'il s'agisse d'une entité des SPM ou d'un organisme lié par contrat ou convention avec ce dernier, établit pour chaque nature et niveau d'habilitation un catalogue des emplois qui précise, *via* l'octroi d'un numéro de poste, les fonctions et missions impliquant nécessairement l'accès à des ISC de niveau *Secret* ou *Très Secret* (hors classifications spéciales et, y compris le cas échéant, aux niveaux d'habilitation de l'UE et de l'OTAN) ainsi que les nom et prénom des personnes physiques les occupant.

Une copie du catalogue des emplois est adressée au HFDSa/PM.
Les demandes d'habilitation sont établies en référence au catalogue des emplois. Lorsqu'une demande d'habilitation lui parvient, l'OS vérifie l'inscription de la fonction concernée dans le catalogue des emplois correspondant.

Les catalogues sont mis à jour au moins une fois par an et à l'occasion de chaque réorganisation. Ils peuvent faire l'objet d'un contrôle par le HFDSa/PM afin de vérifier notamment si les

titulaires des fonctions répertoriées ont effectivement eu accès à des ISC pour le niveau concerné.

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

3.2. La demande d'habilitation

Le chef d'organisme employeur via son OS s'assure en premier lieu que la demande d'habilitation est justifiée par le besoin d'accéder à des ISC pour exercer une fonction ou accomplir une mission inscrite au catalogue des emplois.

L'OS 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.

3.2.1. La procédure de droit commun

L'OS donne au candidat l'accès à une notice individuelle de sécurité (NIS) sous format dématérialisé. Le candidat la complète et la signe[16], télécharge le formulaire au format *PDF actif* et l'envoie, selon la procédure établie, à son OS. Cette pièce officielle, dont la complétude et la cohérence sont vérifiées par l'OS, est transmise au FSD/PM qui initie la demande d'habilitation. L'OS conserve une copie de la NIS.

La notice est insérée dans le dossier d'habilitation complet, conservé par le FSD/PM. Elle est détruite un an après la fin de validité de l'avis de sécurité émis par le service enquêteur.

Le dossier d'habilitation comporte :

- une demande d'habilitation renseignée et signée par le chef d'organisme ou l'OS attestant le besoin de connaître des ISC à un niveau donné ;

- la notice individuelle de sécurité renseignée intégralement et signée[17] par le candidat ;

- une photographie récente (moins de trois mois, format identique à celui demandé pour la carte nationale d'identité) numérisée.

Les demandes d'habilitation au niveau *Très Secret* faisant l'objet d'une classification spéciale, sont transmises selon une procédure spécifique et sont 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.

[16] S'il n'est pas possible de signer de manière dématérialisée, une copie de la dernière page de la notice est conservée par l'OS en plus de la version dématérialisée.
[17] La dernière page de la notice peut être imprimée et signée de manière manuscrite. Elle fait partie intégrante du dossier d'habilitation.

En accord avec le FSD/PM, une copie du dossier d'habilitation peut être conservée par l'OS jusqu'à la fin de validité de la décision d'habilitation émise par l'autorité d'habilitation. A cette date, l'OS renvoie la copie du dossier au FSD/PM.

3.2.2. La 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. L'officier de sécurité de l'entité dont relève le candidat à l'habilitation, doit justifier l'urgence de la demande. Si le besoin est avéré, la NIS est alors transmise au service enquêteur selon une procédure d'urgence.

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 lors de la demande, rester exceptionnelle et en aucun cas pallier un manque de planification des organismes demandeurs.

3.2.3. La procédure simplifiée

A titre exceptionnel, un agent des SPM peut être habilité au niveau *Secret* par l'autorité d'habilitation dont il relève sans intervention du service enquêteur.

Cette procédure dérogatoire ne peut être utilisée qu'en cas de nécessité avérée et pour des habilitations d'une durée inférieure ou égale à trois mois (stages, vacations, formations, emploi provisoire) et à condition que le candidat :

- ait fait l'objet d'une enquête administrative[18] au moment du recrutement, de la nomination ou de l'affectation ;

- ait rempli la notice individuelle de sécurité ;

- 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 en est informé, selon les modalités qu'il a définies.

[18] Cf. articles L. 114-1 et L. 114-2 du code de la sécurité intérieure.

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.

3.3. L'enquête administrative et l'avis de sécurité

Le candidat à l'habilitation fait l'objet d'une enquête administrative[19] dont le résultat se matérialise par un avis de sécurité. Celui-ci 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 préalable à une habilitation est du ressort :

- de la Direction générale de la sécurité intérieure (DGSI) pour le personnel civil relevant des SPM ainsi que pour les entreprises contractantes avec les SPM et leur personnel effectuant les travaux prévus par ces contrats ;

- de la Direction du renseignement et de la sécurité de la défense (DRSD), pour le personnel militaire (et anciens militaires radiés des contrôles depuis moins de cinq ans) relevant des SPM.

La durée maximale de l'enquête administrative 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 sont de trois types :

- **un avis sans objection**, lorsque l'instruction n'a révélé aucune vulnérabilité de nature à constituer un risque pour la sécurité des ISC ni pour celle de l'intéressé ;

- **un avis restrictif**, lorsque le candidat présente certaines vulnérabilités constituant des risques directs ou indirects pour la sécurité des ISC auxquels il aurait accès, mais que des mesures de sécurité spécifiques prises par l'OS, 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 ;

- **un 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.

[19] Cf. article R. 114-2 du code de la sécurité intérieure.

Un avis restrictif ou défavorable comporte des éléments communicables ou non communicables. Les éléments non communicables peuvent être classifiés.

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 (sens 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).

Le service enquêteur (DGSI ou DRSD) fait parvenir à l'autorité d'habilitation deux exemplaires de l'avis de sécurité « restrictif » ou « défavorable » *via* l'un de ses agents, accompagnés d'une fiche confidentielle 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 façon strictement nécessaire, à l'autorité compétente.

Ne pouvant être reproduite, la fiche confidentielle est retournée après communication et sans délai au service enquêteur.

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.

3.4. La mise en éveil et la mise en garde

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 garde de l'autorité compétente ou de l'OS de l'organisme dont relève le candidat à l'habilitation ;

- la mise en éveil de l'intéressé.

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

3.4.1. La procédure de mise en garde de l'employeur

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'OS 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.

3.4.2. La 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'enquête.

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'habilitation, 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'autorité d'habilitation en informe le service enquêteur.

3.5. La décision d'habilitation et le refus d'habilitation

Sur la base des conclusions de l'avis de sécurité (qui cependant ne le lient pas), le HFDSa/PM prend la décision d'habiliter, ou non le demandeur.

Plusieurs cas de figure sont possibles.

L'avis de sécurité est « sans objection » : le HFDSa/PM peut établir une décision d'habilitation (cf. IGI 1300 - annexe 8), qu'il adresse *via* l'OS concerné au chef d'organisme employeur.
L'avis de sécurité est restrictif ou défavorable : Le HFDSa/PM peut décider de prononcer ou de refuser l'habilitation :

- **il prononce l'habilitation :** l'habilitation intervient le plus souvent après une mise en garde de l'employeur et/ou une mise en éveil de l'intéressé. Dans ce cas, le HFDSa/PM réceptionne l'attestation de bon déroulement de cette ou ces procédures (IGI 1300 - annexes 9 et 10), donne son accord aux mesures de sécurité envisagées localement et établit une décision d'habilitation puis l'adresse au chef d'organisme employeur ;

- **il prononce un refus d'habilitation :** dans ce cas, le HFDSa/PM 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 administratif et contentieux, ainsi que des délais qui lui sont ouverts pour contester cette décision. A cette fin, l'OS lui remet un récépissé de notification de décision de refus d'habilitation (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 sont adressées à l'autorité d'habilitation. Le service enquêteur en est informé.

Si le HFDSa/PM décide ultérieurement d'accorder l'habilitation, après l'avoir refusée dans un premier temps, il en informe le service enquêteur. Cette décision est dispensée de motivation.

Le HFDSa/PM 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.

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 ou compte tenu de la mission ;

- en cas de procédure d'urgence (cf. 3.2.2).

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.

La décision prise par le HFDSa/PM 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.

Lors de la notification de la décision d'habilitation, l'OS fait signer à l'intéressé le premier volet de l'engagement de responsabilité (cf. IGI 1300 - annexe 11). Cette notification doit être assortie d'une sensibilisation aux obligations particulières imposées pour l'accès à des ISC.

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, de l'accomplissement de sa mission ou d'une candidature à un poste nécessitant une habilitation.

3.6. La gestion et la fin de l'habilitation

3.6.1. La validité de l'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.

3.6.2. La conservation des décisions et des refus d'habilitation

Les décisions d'habilitation et les refus d'habilitation sont conservés par l'OS pendant leur durée de validité, à l'exception de ceux rendus 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.

Dès lors que la décision d'habilitation a cessé d'être valide, l'OS retourne celle-ci, accompagnée de l'engagement de responsabilité, dont les volets 1 et 2 ont été préalablement signés, au service du HFDS/PM.

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

3.6.3. Le certificat de sécurité

Chaque fois qu'il est nécessaire, pour l'accomplissement d'une mission ou d'une activité, 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 le HFDSa/PM ou le cas échéant, par l'officier de sécurité, au vu de la décision d'habilitation effectivement détenue.

La durée de validité de ce document, limitée à un an au maximum, est précisée et, en tout état de cause, ne peut dépasser celle de l'habilitation correspondante. Avant la fin de validité du certificat (1 an maximum) et au terme de la mission, l'intéressé procède ou fait procéder à sa destruction.

3.6.4. Le 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.

3.6.5. Le changement de situation de l'habilité et révision de l'habilitation

La personne habilitée a l'obligation d'informer le chef d'organisme employeur, *via* son OS, de tout changement affectant sa vie personnelle et professionnelle. Elle l'informe notamment 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 (NIS) et la transmet à l'autorité d'habilitation, qui la communique 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 :

- 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 ;

- 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.

3.6.6. La 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.

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 d'habilitation. Il est conservé un an après la fin de validité de l'avis de sécurité par le service du HFDS/PM.

3.6.7. La portabilité de l'avis de sécurité en cas de changement de fonction

Lorsqu'une personne habilitée change d'emploi au sein des SPM ou lorsqu'elle les quitte définitivement, son habilitation pour le poste initial prend fin. 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, afin d'identifier d'éventuelles vulnérabilités liées au nouveau poste. La notice individuelle de sécurité est conservée dans le dossier d'habilitation.

En cas de changement de fonctions au sein des SPM, lorsque l'avis de sécurité ayant fondé la précédente habilitation est toujours en cours de validité et qu'aucun changement de situation justifiant sa révision n'est survenu, une nouvelle décision d'habilitation peut être délivrée sur la base de l'avis de sécurité (n'excédant pas la durée de validité de ce dernier) ;

Lorsque la personne quitte les SPM et que ses nouvelles fonctions nécessitent une habilitation, la nouvelle autorité d'habilitation prend contact avec le service du HFDS/PM. Si l'avis de sécurité est toujours en cours de validité, le service du HFDS/PM lui transmet une « attestation d'avis de sécurité » (cf. IGI 1300 - annexe 15) mentionnant la fin de validité de l'avis de sécurité[20]. 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 justifiée.

En cas de changement d'autorité d'habilitation, l'OS de l'entité quittée renvoie la décision d'habilitation et l'engagement de responsabilité au HFDSa/PM.

3.6.8. L'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

[20] De la même manière, le HFDSa/PM demande une attestation d'avis de sécurité à la précédente autorité d'habilitation, pour instruire la demande d'habilitation d'un agent intégrant les services du Premier ministre et habilité dans ses précédentes fonctions.

délivrance. Cela peut être le cas lorsque des éléments de vulnérabilités apparaissent, signalés notamment par le service enquêteur, l'autorité compétente ou l'OS 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). Le HFDSa/PM informe le service enquêteur 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.

3.7. L'habilitation des personnes morales dans le cadre des contrats

L'habilitation d'une personne morale [21] répond à la nécessité d'apprécier les garanties présentées avant d'attribuer un marché avec accès ou détention d'ISC ou de passer une convention avec une personne morale de droit privé associée à la protection des intérêts fondamentaux de la Nation.

La décision d'habilitation permet :

- à l'administration d'attribuer des marchés comportant l'accès ou la détention d'ISC à une personne morale : l'autorité contractante ne peut signer aucun contrat avant la réception de l'attestation d'habilitation de la personne morale ;

- à cette personne morale d'exécuter de tels contrats.

L'habilitation d'une personne morale est au préalable justifiée par un besoin avéré d'avoir accès et/ou de détenir des ISC et s'accompagne, pour celle-ci, de la mise en place d'une structure de sécurité adaptée aux travaux classifiés qu'elle doit exécuter (dont la désignation d'OS). Par ailleurs, la détention d'ISC impose aux personnes morales de disposer, en plus de l'habilitation, de locaux conformes et le cas échéant, de systèmes d'information homologués. Le futur contrat comporte un plan contractuel de sécurité (PCS) précisant, pour les ISC concernés, les mesures de protection requises.

L'habilitation de la personne morale [22] et de son responsable légal sont un préalable indispensable à l'habilitation de son personnel, à l'exception des phases précontractuelles nécessitant l'accès à des ISC pour l'établissement du contrat, pour lesquelles une ou des personnes physiques spécifiquement désignées peuvent faire l'objet d'une décision d'habilitation. La composition du dossier d'habilitation est précisée dans l'annexe 20 de l'IGI 1300.

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 délais fixés

[21] Les dispositions détaillées relatives à l'habilitation des personnes morales figurent au § 4.4 de l'IGI 1300.

[22] Comme de ses sous-traitants, le cas échéant.

par l'autorité contractante, par exemple), le candidat est réputé avoir renoncé à sa demande. Il ne peut donc plus prétendre à l'attribution du contrat.

L'habilitation d'une personne morale peut faire l'objet d'un réexamen, à l'initiative du service enquêteur ou de l'autorité d'habilitation ou de la personne morale concernée. C'est le cas en particulier lorsque les caractéristiques de la personne morale ont subi des modifications (par exemple : les fusions, acquisitions, rachat ou cession d'activité). Elle peut également être abrogée par décision de l'autorité d'habilitation, après avis du service enquêteur si la personne morale ne remplit plus les conditions nécessaires à sa délivrance.

4. LA SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES TOUT AU LONG DE LEUR CYCLE DE VIE

4.1. La décision de classifier

Pour les SPM, le Premier 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.

Sous le contrôle de l'autorité émettrice, « ***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* (IGI 1300, § 7.1). Il procède à l'analyse de l'importance de l'information (ou de la donnée numérique ou du fichier) au regard de son contexte, de sa nature et des directives de classification applicables. Il détermine ainsi le niveau de classification (*Secret* ou *Très Secret*).

Il est ainsi impérativement tenu compte de ce que :

- utilisée de façon abusive, la classification nuit à la fluidité des échanges par les mesures de protection qu'elle impose et dévalue le secret ;

- sous-employée, elle facilite l'accès à des informations et supports dont la divulgation est de nature à nuire aux intérêts fondamentaux de la Nation.

Lors de la classification, l'auteur choisit avec soin la date de déclassification.

4.2. L'élaboration de l'ISC

Elaborer des ISC consiste à apposer un timbre de classification lisible. Cette classification a pour conséquence de placer l'information ou le support sous la protection des articles 413-9 et suivants du code pénal.

L'élaboration d'un document classifié est toujours effectuée dans un lieu abritant (cf. paragraphe 5) par une personne détenant une habilitation de niveau au moins équivalent à celui de l'information ou du document considéré et, le cas échéant, à partir d'un système d'information homologué au minimum au niveau de classification de l'information concernée.

L'élaboration d'ISC de niveau *Très Secret* se fait impérativement dans une zone réservée.

NB :

- par principe, l'objet d'un document classifié est lui-même classifié ;

- un ensemble d'informations ou supports, dit « agrégat », est classifié si le regroupement des informations ou supports qui le composent le justifie, alors même qu'aucun de ces éléments n'est classifié ;

- les documents préparatoires ayant servi à l'élaboration du document classifié (brouillons, impressions sur papier, matériels informatiques de type clé USD ou CD-ROM) portent la mention du niveau de classification adapté. Ils sont détruits ou effacés, dès qu'ils sont devenus sans objet et au plus tard lorsque le document classifié est émis ;

- pour les informations dématérialisées, la décision d'homologation du système vaut décision de classification. Un support informatique conserve le niveau de classification le plus élevé du ou des documents qu'il contient ou aura contenus. Il ne peut être déclassifié que si toutes les informations qu'il contient l'ont été au préalable.

4.3. Le marquage

Les ISC doivent être identifiés comme étant classifiés avant leur consultation. Un timbre de classification visible est apposé sur le document ou le support :

- le timbre est apposé à l'encre rouge. Il est définitif et toujours visible. 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,

- sur chaque document, figurent pour l'identifier :
    - o le timbre du niveau de classification,
    - o l'échéance de la classification,
    - o les références de l'autorité émettrice et de l'auteur de l'ISC,
    - o la date d'émission,
    - o le numéro d'enregistrement,
    - o le niveau de protection ou de classification de l'objet.

- chaque page du document est numérotée.

4.4. L'enregistrement

Le but de l'enregistrement est d'établir sans ambiguïté l'attribution des 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 est alors régulièrement sauvegardé notamment sur un support externe), dont l'accès est restreint aux personnes habilitées et ayant le besoin d'en connaître.

Si l'objet des documents est classifié *Secret* et est mentionné dans le système d'enregistrement (manuel ou informatisé), celui-ci est classifié au même niveau que les documents qu'il référence. Pour les ISC au niveau *Très secret*, le système d'enregistrement est *a minima* classifié *Secret*, même si les objets ne sont pas mentionnés.

Si le système d'enregistrement est classifié, les personnes qui le manipulent sont 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'est 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.

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.

4.5. L'inventaire obligatoire des ISC

Par principe, les ISC sont conservés dans un coffre-fort homologué attribué à une personne physique dûment habilitée qui en est responsable et identifiée comme étant le « détenteur » au sens de la présente instruction.

L'inventaire du contenu d'un coffre 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. Le cas échéant, au moment de l'inventaire, il procède à la destruction (cf. paragraphe 4.7) ou à la déclassification (cf. paragraphe 4.9) des ISC qu'il détient.

Un document de travail (ex : brouillon, courriel…) est identifié, protégé et suivi mais ne nécessite pas d'être inventorié.

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, selon le modèle figurant en annexe VII :

- lors du changement de titulaire d'un emploi figurant au catalogue des emplois, il est procédé à un inventaire détaillé contradictoire entre les détenteurs *prenant* et *quittant*, signé des deux personnes. Cet inventaire est enregistré et conservé au niveau de l'organisme et permet de connaître le responsable actuel de l'ISC. Si cet inventaire contradictoire entre les détenteurs quittant et prenant n'est pas possible, l'inventaire du coffre est réalisé par le détenteur quittant en présence de l'officier de sécurité ;

- un inventaire des ISC matériels (support et documents papiers) est réalisé chaque année et arrêté au 31 décembre de l'année en cours. Les dates d'expiration de validité sont vérifiées aux fins de déclassement ou de déclassification (cf. paragraphe 4.9) : la réévaluation du niveau de protection des ISC est réalisée et, le cas échéant, leur destruction ou leur versement aux archives sont étudiés.

Pour le niveau *Secret*, l'inventaire annuel est effectué par chaque détenteur sous la supervision de l'OS ou du bureau de protection du secret s'il existe.

Pour le 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 ;

- une fiche de suivi du support (IGI 1300 – 7.3.2.1) ;

- un procès-verbal de versement à un dépôt d'archives.

4.6. La diffusion physique des ISC

Lorsqu'une information classifiée ne peut être diffusée *via* un système informatique homologué, une transmission physique n'est possible qu'à certaines conditions.

Les autorités d'expédition sont :

- au niveau *Secret*, les personnes en charge de la gestion des ISC à ce niveau ;

- au niveau *Très Secret*, le bureau de protection du secret (BPS).

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. 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 émargée 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 :

- 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, accompagné d'un bordereau « recommandé avec accusé de réception », si l'envoi est assuré par le service postal ;

- l'enveloppe extérieure, renforcée et si possible plastifiée, porte l'indication du service expéditeur, l'adresse du destinataire (sans mention trop explicite de nature à attirer l'attention sur le caractère classifié du contenu) et la mention du suivi. Elle ne porte en aucun cas la mention du niveau de classification de l'information ou du support qu'elle contient ;

- l'enveloppe intérieure de sécurité 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 nom et la fonction du destinataire ainsi que l'indication de l'entité dans laquelle il est affecté.

Ces règles sont également applicables aux informations classifiées stockées sur un support amovible sont, lorsqu'elles sont transportées en dehors d'une zone protégée.

L'expéditeur reste responsable des ISC transportés jusqu'à leur 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 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 et B 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' est conservé par l'expéditeur jusqu'à réception du feuillet B qui lui est alors substitué.

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 dument habilité, 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 *Très Secret*), ou par le service en charge de la gestion des ISC à ce niveau ou le destinataire du courrier (*Secret)* ;

- 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. Dans le cas d'une information classifiée dématérialisée, la réception est assurée par les obligations de traçabilité des SI.

4.7. La destruction des ISC

Lorsque des ISC sont périmés ou devenus inutiles, il est procédé à leur destruction. Cependant, afin d'établir la distinction entre les documents à détruire et ceux nécessitant une conservation, il est nécessaire de prendre contact avec la mission des archives des services du Premier ministre.

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.

La destruction des ISC est effectuée de façon à rendre impossible toute reconstitution, même partielle, des informations contenues sur les supports, à l'aide de moyens homologués (broyeurs ou incinération).

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 des ISC à détruire sollicite officiellement le service auteur et lui rend compte, sauf avis contraire de sa part, qu'il procédera à la destruction du support. 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-verbal. 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. 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.

4.8. L'impression et la reproduction d'informations classifiées

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. Ils ne sont en aucun cas reliés au réseau informatique de l'entité.

Si ces matériels sont connectés à un SI, ils sont intégrés dans le périmètre d'homologation de ce SI et sont 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 d'ISC au strict besoin d'en connaître.

Pour le niveau *Secret*, *l*a 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.

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.

Pour le niveau *Très Secret*, *l*a 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), 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.

4.9. La déclassification

La déclassification consiste à supprimer toute mention de classification. La déclassification d'un document peut résulter d'une initiative de l'autorité émettrice ou du service auteur, d'une demande d'un destinataire (lors d'une révision annuelle de l'inventaire ou lors du versement aux archives), être provoquée par une requête en déclassification judiciaire, par une demande de communication d'archives ou intervenir à l'issue du délai mentionné lors de la classification du document.

L'IGI 1300 prévoit l'obligation pour l'auteur d'un ISC d'apposer sur celui-ci au moment de sa création une date de déclassification (ou exceptionnellement, une date de réévaluation de la classification). La date d'échéance vaut timbre de déclassification.

La date de déclassification est déterminée par l'auteur, selon les directives reçues du responsable d'organisme et répond aux critères suivants, développés au paragraphe 7.6 de l'IGI 1300 :

- n'excède pas 50 ans ; pour autant, l'autorité émettrice conserve la possibilité de prolonger à tout moment le délai fixé ;

- répond à une logique opérationnelle (quelle est la durée utile de la classification ?) ;

- lorsqu'à titre exceptionnel aucune date ne peut être déterminée, l'auteur de l'information classifiée indique la date ou le délai au terme duquel, le niveau de classification doit impérativement être réévalué. Cette date ou ce délai n'excède pas 20 ans à compter de la date de production du support.

La décision de déclassifier des ISC, émise par une entité relevant du périmètre de compétence du HFDS/PM, appartient au Premier ministre, autorité émettrice. Le Premier ministre peut également prendre toutes les mesures justifiées visant à déclasser ou reclasser[23] les ISC.

L'instruction des dossiers de déclassification[24] est effectuée par le cabinet militaire du Premier ministre. Celui-ci est chargé d'évaluer la sensibilité des informations classifiées et donne un avis sur leur déclassification.
La procédure de déclassification varie selon que l'ISC comporte ou non une date d'échéance de classification (cf. paragraphe 7.6.3 de l'IGI 1300).

Pour les ISC qui comportent une date d'échéance de classification, la déclassification intervient automatiquement à cette date, sans qu'une décision formelle de déclassificaion (matérialisée par l'apposition d'un timbre de déclassification) ne soit nécessaire.

En revanche, 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

[23] La déclassification se distingue du déclassement et du reclassement. 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,* y compris ceux faisant l'objet d'une classification spéciale). Le reclassement consiste à apposer sur un document le niveau de classification supérieur.

[24] Ou de déclassement ou reclassement.

comportant la date et les références de la décision. Le document déclassé ou reclassé fait lui aussi l'objet d'un marquage analogue comportant la date et les références de la décision.

La décision de déclassification pour les ISC sans mention d'échéance (c'est-à-dire antérieurs au 1er juillet 2021) continue d'être prise ponctuellement et matérialisée par un tampon spécifique, selon les prescriptions détaillées dans l'IGI 1300 au paragraphe 7.6.3.4.

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.

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 s'assure qu'aucun autre motif d'incommunicabilité ne trouve à s'appliquer en vertu des articles L. 213-2 et suivants du code du patrimoine.

4.10. L'accès des magistrats aux ISC des SPM

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 Premier ministre, autorité émettrice. La demande de déclassification est instruite par le cabinet militaire du Premier ministre.

Une perquisition envisagée dans un lieu identifié comme abritant des éléments couverts par le secret de la défense nationale, ne peut être effectuée que par un magistrat, accompagné par le président (ou son représentant) de la commission du secret de la défense nationale (CSDN). L'autorité responsable du lieu et son OS sont présents pendant la perquisition. Seul le président de la CSDN (ou son représentant) peut prendre connaissance d'éléments classifiés, papier ou numérique, découverts sur les lieux.

Si la perquisition s'effectue dans un lieu n'étant pas identifié comme un lieu abritant des éléments couverts par le secret de la défense nationale, le magistrat ou l'OPJ ne peuvent pas prendre connaissance d'éléments classifiés découverts de manière fortuite. Les opérations de perquisition sont suspendues jusqu'à l'arrivée du présent de la CSDN (ou de son représentant) qui prendra en charge les éléments classifiés. S'il ne peut se déplacer, les documents sont placés sont sous scellés et conservés dans un lieu abritant.

5. LA PROTECTION DES LIEUX ABRITANT DES ISC

5.1. La justification et l'étendue de la protection

Les lieux abritant des ISC ou dans lesquels sont déployés des systèmes d'information classifiés font l'objet de mesures de protection particulières qui ont pour objet d'éviter toute perte, dégradation ou compromission. Ces mesures comprennent des moyens organisationnels, humains, techniques et logiques dissociés ou combinés en fonction du niveau de classification et des menaces identifiées. Elles sont détaillées dans l'annexe 30 de l'IGI 1300.

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 procèdent d'une analyse précise des risques, effectuée par l'autorité responsable du site concerné (ou l'AQSSI pour les mesures informatiques), et suivre l'avis du service enquêteur compétent.

La liste des lieux des SPM identifiés comme abritant des éléments couverts par le secret de la défense nationale est tenue par le HFDSa/PM et mise à jour au moins annuellement, au plus tard pour le 15 novembre. Sans attendre la mise à jour annuelle, les OS informent le HFDSa/PM de toute modification intervenant dans leurs entités.

La protection des ISC implique également de manière complémentaire de :

- sécuriser l'accès à des locaux non abritant mais qui hébergent des moyens techniques concourant à la protection (énergie, moyens de communication par exemple) ;

- contrer 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) ;

- éliminer les signaux parasites compromettants, y compris en matière de câblage[25], lorsque ces lieux abritent des SI classifiés ;

- prendre toutes mesures organisationnelles locales permettant le déroulement d'éventuelles perquisitions dans le respect des modalités arrêtées au § 1.2.2.2 de l'IGI 1300.

5.2. L'évaluation de la protection

La capacité physique de lieux propres au stockage et au traitement au niveau requis est appréciée par :

- l'OS pour tous les lieux abritant des ISC de niveau *Secret* ;

- le service enquêteur (la DGSI) dans les autres cas (organisme sous contrat avec les SPM ou lieux abritant des ISC de niveau *Très Secret*).

5.3. La sécurité des lieux abritant temporaires

Lorsque des ISC sont manipulés en dehors du lieu les abritant en temps normal (dans le cas, par exemple, d'une réunion ou d'une conférence classifiées), l'autorité organisatrice applique les recommandations suivantes avant, durant et après la communication des ISC :

[25] Pour le détail, se référer à l'instruction interministérielle n° 300/SGDSN/ANSSI du 23 juin 2014.

- le lieu dans lequel se déroule l'activité doit être sécurisé et son accès contrôlé ;

- un contrôle des lieux est effectué sous la responsabilité de l'autorité organisatrice avant, éventuellement pendant, et après l'activité ;

- L'organisateur s'assure :
    - avant la réunion que les participants sont habilités au niveau requis et ont besoin d'en connaître ;
    - 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…) ;
    - en application stricte du cloisonnement de l'information classifiée, que la communication, en particulier pour le niveau *Très Secret*, dont les classifications spéciales, demeure limitée à l'objet de l'activité ;
    - après la réunion, de la récupération et de la mise en sécurité des informations ou supports classifiés éventuellement mis à la disposition des auditeurs ;
    - de la destruction des supports provisoires et préparatoires ;
    - de la sensibilisation des participants sur leurs obligations en matière de protection du secret de défense.

5.4. Les zones protégées et les zones réservées

En matière organisationnelle, la protection des lieux abritant peut également se traduire par la mise en œuvre de zones protégée ou réservée.

Les demandes de création de ces zones sont adressées, pour instruction, au HFDSa/PM. Celui-ci s'assure de l'existence du besoin et prescrit les aménagements nécessaires dans les locaux concernés. Il rédige le projet d'arrêté de création présenté à la signature du HFDS et veille à sa publication.

Une **zone protégée** (ZP) est un local, un ensemble de locaux, un bâtiment, un établissement ou un terrain clos, rattaché à un service de l'Etat, à un établissement public ou à toute personne physique ou morale, publique ou privée, intéressant la défense nationale auquel l'accès est soumis à autorisation et dont l'ensemble des accès est contrôlé en permanence afin d'éviter toute pénétration par inadvertance. Il s'agit de conférer à la zone choisie une protection juridique renforcée (notamment pénale) contre les intrusions, afin de protéger son contenu et notamment les ISC.

La création d'une ZP est conseillée pour les lieux abritant des ISC au niveau *Secret* et obligatoire au niveau *Très Secret* (voir ci-dessous la zone réservée).

Quant à elle, une **zone réservée** (ZR) est un local ou un emplacement qui fait l'objet de mesures de protection matérielle particulières et dont l'accès est réglementé et subordonné à des conditions spéciales, l'ensemble visant à apporter une protection complémentaire aux ISC. Sa protection juridique provient de son inclusion dans une ZP.

Une 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).

5.5. Le contrôle des accès aux sites relevant du Premier ministre

Toute demande d'accès au point d'importance vitale (PIV) de Matignon, à ses sites annexes des 56 et 58 rue de Varenne, aux ZP du site de Ségur-Fontenoy peut donner lieu à une enquête administrative préalable (EA) réalisée par le commandant militaire (COMILI), dans les conditions fixées par le code de sécurité intérieure (cf. articles L. 114-1).

L'enquête administrative s'applique au personnel de l'organisme à qui appartient la zone sensible comme au personnel extérieur à l'organisme susceptible de pénétrer pour son travail dans cette même zone (prestation de service ou visite d'une délégation, par exemple).

Dans le cadre particulier d'un contrat sensible[26], le personnel de la société prestataire effectuant la mission fait l'objet d'une enquête administrative.

Pour l'accès aux ZP du site de Ségur-Fontenoy, les conclusions techniques résultant de l'enquête administrative effectuée par le COMILI se traduit par des avis écrits adressés au demandeur ou à son OS. À partir de cet avis, la décision d'autoriser ou pas l'accès à la zone ou à l'installation incombe au responsable du site (le DSAF - Directeur des services administratifs et financiers des SPM).

Comme pour toute enquête administrative, il est à noter que :

- l'individu soumis à l'enquête administrative en a été informé au préalable ;
- les refus sont notifiés par écrit à la personne en lui précisant les voies et délais de recours[27] ;
- le résultat d'une enquête administrative, qui est la « photographie » d'un individu à un instant donné en fonction des informations consultables, offre une garantie relative. Il ne se substitue pas à la vigilance qu'exerce le personnel affecté à une zone vis-à-vis des occupants temporaires (prestataires, stagiaires, etc…).

Le détail des mesures relatives aux enquêtes administratives pour les accès en ZP (et en ZR) est à consulter au § 5.3.1.1 de l'IGI 1300.

La Haute fonctionnaire
de défense et de sécurité

Claire LANDAIS

Original signé

[26] Ce type de contrat s'exerce dans un lieu abritant des ISC.

[27] Dans le cas d'un refus d'accès à un PIV, un recours administratif préalable obligatoire est nécessaire avant tout contentieux.

ANNEXES

ANNEXE I : GLOSSAIRE

Définition des principales notions

Archivage : opération consistant à verser à un service d'archives des supports d'information lorsqu'ils ne sont plus d'utilisation habituelle. Les supports faisant encore l'objet d'une classification ne peuvent être archivés que dans certaines conditions et dans des services habilités à les recevoir.

Auteur d'une information ou d'un support classifié : personne qui, sous le contrôle de l'autorité émettrice, prend la décision d'apposer le timbre de classification sur une information ou un support au niveau requis par son contenu. Il procède à l'analyse de l'importance de l'information au regard de son contexte et eu égard aux directives de classification reçues de l'autorité émettrice. C'est aussi lui qui fixe la date de déclassification.

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

Autorité émettrice : Etat français, Etat étranger, organisation internationale ou institution, organisation ou organisme de l'Union européenne sous la responsabilité de laquelle ou duquel un timbre de classification national ou étranger est apposé sur une information ou un support, afin de lui conférer une protection au titre du secret de la défense nationale.

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

Autorité nationale de sécurité (ANS) ; autorité de sécurité déléguée (ASD) : l'ANS est l'autorité nationale chargée d'assurer la protection des informations classifiées étrangères confiées aux organismes relevant de la juridiction de son Etat et d'assurer la liaison avec les autorités nationales de sécurité étrangères sur tout sujet relatif à la protection des ISC. En France, l'autorité nationale de sécurité est le secrétaire général de la défense et de la sécurité nationale. L'ANS peut déléguer sa mission à une autorité de sécurité déléguée (ASD) dans un domaine spécifique et selon des modalités précisées dans une décision de délégation.

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

Avis de sécurité : conclusion émise par un service enquêteur à l'issue d'investigations se rapportant à une personne, physique ou morale, et visant à détecter et à évaluer les vulnérabilités de cette personne. L'avis de sécurité est une aide à la décision d'habilitation, il ne lie pas l'autorité d'habilitation.

Avis technique d'aptitude physique (ATAP) : appréciation rendue par le service enquêteur portant sur la capacité physique des locaux à conserver et traiter des ISC au niveau requis selon

les modalités définies par la présente instruction. Cet avis prend en compte la conformité aux exigences de sécurité du système d'information chargé du contrôle d'accès.

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

Catalogue des emplois : dans un organisme, liste des emplois qui nécessitent l'accès aux ISC. Le catalogue des emplois est dressé sur le seul critère du besoin d'en connaître. Il est établi et tenu à jour par l'OS pour un niveau de classification donné. Un organisme peut ainsi détenir plusieurs catalogues des emplois.

Certificat de sécurité : document attestant de l'habilitation d'une personne à accéder à des ISC à un niveau donné.

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

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

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

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

Déclassification : suppression de la classification d'une information ou d'un support classifié. Selon les cas (cf. paragraphe 7.5.5 de l'IGI 1300), la déclassification peut être automatique ou être effective après l'adoption d'une décision formelle de déclassification par l'autorité émettrice compétente matérialisée sur le support classifié par un timbre de déclassification. A ne pas confondre avec le **déclassement** qui est la modification, par abaissement, du niveau de classification d'une information ou d'un support classifié.

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

Dossier d'habilitation d'une personne morale : dossier permettant d'apprécier les garanties offertes par la personne morale et d'évaluer l'intérêt porté par ses dirigeants à la protection du secret de la défense nationale et aux aspects liés à la sécurité des ISC.

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

cas échéant, en cas d'abrogation explicite de la décision d'habilitation, lors de la notification de la décision d'abrogation.

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

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

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

Haut fonctionnaire de défense et de sécurité (HFDS) : autorité chargée d'assister le ministre dans l'exercice de ses attributions de sécurité, de défense et de protection du secret.

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

Information et support classifié (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 à ce type d'information, il faut être habilité et avoir le besoin d'en connaître.

Lieu abritant des éléments couverts par le secret de la défense nationale : pièce dans laquelle sont conservés des ISC, quel qu'en soit le niveau.

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

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

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

Notice individuelle de sécurité : formulaire destiné à recueillir les renseignements nécessaires à l'habilitation d'une personne. Elle est renseignée par le candidat à l'habilitation et l'autorité sollicitant l'habilitation. Elle constitue un élément majeur du dossier d'habilitation et est exploitée par l'autorité d'habilitation et le service enquêteur compétent. Appelée parfois « NIS » ou improprement « 94A » nom de l'ancien formulaire.

Organisme : au titre de la présente instruction, tout service de l'Etat (services centraux, services déconcentrés, services à compétence nationale), personne physique ou morale ayant accès, même à titre provisoire, à des ISC.

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

Politique de protection du secret, PPS (ou politique des ISC) : document définissant l'ensemble des mesures de protection mises en œuvre par l'organisme pour protéger les ISC auquel il a accès. Ce document est élaboré par l'officier de sécurité de l'organisme, en lien avec l'officier de sécurité des systèmes d'information pour les organismes utilisant un système d'information classifié. Il est conforme à la présente instruction, ainsi qu'à l'IGI 1300 et le cas échéant aux directives techniques particulières applicables. Il prend en compte les obligations souscrites par l'organisme dans le cadre des plans contractuels de sécurité qui lui sont applicables.

Politique de sécurité des systèmes d'information (PSSI) : politique, applicable à l'ensemble des organismes relevant de l'autorité qualifiée en sécurité des systèmes d'information, définissant les mesures de sécurité des systèmes d'information dans leur ensemble. Les lignes directrices pour la sécurité des systèmes d'information constituent un sous-ensemble de cette politique générale. A distinguer de la politique de sécurité d'un système d'information classifié, qui est un document, versé au dossier d'homologation, déclinant pour un système d'information donné les exigences de sécurité relatives à la sécurité des systèmes d'information intégrées dans la politique de sécurité des ISC de l'organisme.

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

Renouvellement d'habilitation : procédure déclenchée à la fin de validité d'un avis de sécurité concernant une personne déjà habilitée en vue d'obtenir un avis actualisé. Ce nouvel avis permettra d'évaluer l'opportunité de renouveler l'habilitation de la personne.

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

Sécurité des systèmes d'information (SSI) : ensemble des mesures techniques et non techniques menées pour atteindre l'état de cybersécurité pour les systèmes d'information, leur permettant de résister à des événements issus du cyberespace, susceptibles de compromettre la disponibilité, l'intégrité, la confidentialité ou la traçabilité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

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

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

Spécial France (SF) : mention complémentaire de protection visant à restreindre la divulgation d'une information ou d'un support aux seuls ressortissants français qualifiés au regard du code pénal. Une information ou un support portant cette mention ne peut, en aucune circonstance, être communiqué, en tout ou partie, à un État étranger ou à l'un de ses ressortissants, organisation internationale ou personne morale de droit étranger, même s'il existe un accord de sécurité entre la France et l'État ou l'organisation internationale considéré.

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

Système d'information (SI) : ensemble organisé de ressources (matériels, logiciels, données, etc.) permettant de traiter, stocker ou transmettre des informations sous forme dématérialisée ; Système d'information d'administration : système d'information comprenant les ressources nécessaires pour administrer un système d'information considéré ; système d'information classifié : système d'information homologué pour traiter, stocker ou transmettre des ISC.

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

Vulnérabilité : en matière de protection au sens large, la vulnérabilité est une faiblesse organique, fonctionnelle ou structurelle, permanente ou temporaire, dont l'exploitation pourrait favoriser la concrétisation d'une menace. Rapportée à la protection du secret, la vulnérabilité est aussi définie par le SGDSN comme un élément relatif à la situation d'une personne, d'un système d'information ou d'un local et qui amoindrit les garanties qu'il présente pour la protection des ISC.

Zone protégée (ZP) : zone créée par arrêté du ministre déterminant le besoin de protection et faisant l'objet d'une interdiction d'accès sans autorisation, sanctionnée pénalement en cas d'infraction.

Zone réservée (ZR) : local ou emplacement créé par le responsable d'organisme, au sein d'une zone protégée, qui fait l'objet de mesures de protection matérielle particulières et dont l'accès est réglementé et subordonné à des conditions spéciales.

Liste des acronymes

ACSSI	articles contrôlés de la sécurité des systèmes d'information
ANS	autorité nationale de sécurité
ANSSI	agence nationale de la sécurité des systèmes d'information
AQSSI	autorité qualifiée en sécurité des systèmes d'information
BPS	bureau de protection du secret
DR	diffusion restreinte
FSD	fonctionnaire de sécurité de défense
FSSI	fonctionnaire de sécurité des systèmes d'information
HFDS	haut fonctionnaire de défense et de sécurité
HFDSa	haut fonctionnaire de défense et de sécurité adjoint
IM	instruction ministérielle
ISC	Information et support classifiés
OIV	opérateur d'importance vitale
OS	officier de sécurité
OSIIC	opérateur des systèmes d'information interministériel classifié
OSSI	Officier de sécurité des systèmes d'information
PCS	plan contractuel de sécurité
PIV	point d'importance vitale
PPS	politique de protection du secret
PSSI	politique de sécurité des systèmes d'information
RGPD	règlement général sur la protection des données
RSSI	responsables de la sécurité du système d'information
S	Secret
SGDSN	secrétariat général de la défense et de la sécurité nationale
S-HFDS	service du haut fonctionnaire de défense et de sécurité
SIIV	système d'information d'importance vitale
TS	Très Secret
ZP	zone protégée
ZR	zone réservée

ANNEXE II : ATTRIBUTION DU FONCTIONNAIRE DE SECURITE DE DEFENSE (FSD)

En tant que tête de la chaîne fonctionnelle ministérielle « sécurité des ISC », le fonctionnaire de sécurité de défense des SPM (FSD/PM) est chargé d'accompagner les responsables d'organisme dépendant du champ d'attribution du HFDS/PM dans l'animation de leur chaîne fonctionnelle de sécurité des ISC.

A ce titre, il est chargé de :

- représenter le HFDSa/PM dans tous types de travaux relatifs à la protection des informations ;
- porter la réglementation relative à la protection du secret, des informations DR et sensibles à la connaissance des différents organismes et la faire mettre en œuvre dans le pôle ministériel ;
- gérer les dossiers d'habilitation relevant du périmètre des SPM ;
- tenir le catalogue des emplois relevant du périmètre des SPM ;
- définir les mesures concernant la sécurité relative aux personnes physiques et morales ;
- définir la politique de déploiement des moyens de communication sécurisés ;
- veiller à la gestion et à la protection physique des ISC et au bon fonctionnement des organismes qui les manipulent ;
- définir les règles relatives à la classification et à la manipulation des informations sensibles et en contrôle l'application ;
- faire assurer le suivi des lieux abritant des éléments couverts par le secret de la défense nationale relevant du périmètre des SPM ;
- organiser sur le périmètre des SPM les processus des contrôles et la sensibilisation du personnel ;
- proposer au HFDS et HFDS-adjoint toutes dispositions destinées à renforcer l'efficacité des mesures de protection mises en place ;
- établir un bilan d'activité annuel de la protection du secret et contribuer au rapport annuel sur la protection du secret.

ANNEXE III : ATTRIBUTIONS DU FONCTIONNAIRE DE SECURITE DES SYSTEMES D'INFORMATION (FSSI)

En tant que tête de la chaîne fonctionnelle ministérielle « sécurité des systèmes d'information (SSI) et des articles contrôlés de la sécurité des systèmes d'information (ACSSI) », le fonctionnaire de sécurité des systèmes d'information (FSSI) assure pour le compte du HFDS et du HFDSa, le pilotage de la mise en œuvre de la politique de sécurité du numérique.

A ce titre, il est plus particulièrement chargé de :

- représenter le HFDS dans tout type de travaux relatifs à la sécurité des systèmes d'information (SSI) ;

- rendre compte au FSD de l'application de la politique de protection du secret dans les SI ;

- établir, en coordination avec le FSD et avec les services intervenant dans le champ du numérique, la déclinaison de la politique générale SSI de l'Etat ;

- coordonner avec le FSD les inspections et contrôles dans les organismes mettant en œuvre des SI classifiés ou protégés (DR) ;

- en tant que tête de chaîne fonctionnelle SSI, animer et conseiller sur les sujets relatifs à la sécurité du numérique le réseau des autorités qualifiées pour la sécurité des systèmes d'information (AQSSI) et des responsables de la sécurité des systèmes d'information (RSSI) ;

- analyser et diffuser les alertes SSI.

ANNEXE IV : ATTRIBUTIONS DE L'OFFICIER DE SECURITE

<table>
<tr><th>Prévention</th><th>Protection des ISC et matériels DR ou sensibles</th></tr>
<tr><td rowspan="2">
Engagement des procédures d'habilitation (dont vérification des NIS) et notification des décisions aux impétrants.
Gestion des dossiers d'habilitations de son entité.
Tenue à jour de(s) catalogue(s) des emplois (un par réseau et par niveau d'habilitation) de son entité.
Demande et suivi des enquêtes administratives en matière d'accès à une zone protégée.
Suivi et contrôle des ressortissants étrangers, notamment visiteurs et stagiaires.
Traitement des compromissions avérées ou supposées.
Sensibilisation des habilités à l'occasion des signatures des 1er et 2nd volets de l'engagement de responsabilité.
Organisation de séances de formation et de sensibilisation avec l'appui de l'OSSI ou du RSSI et du FSD.
Sensibilisation avant une mission ou un départ à l'étranger et suivi des séjours à l'étranger (stage, mission).
Respect du RGPD dans les traitements de données qu'il met en œuvre.
</td><td>
Rédaction de la politique de protection du secret sous l'autorité du responsable et veiller à son application.
Direction du bureau de protection du secret (BPS) s'il existe[28].
Surveillance, protection et contrôle des ISC et des matériels DR ou sensibles.
Contrôle du personnel ayant accès aux ISC.
Suivi de la sécurité des SI classifiés et DR (en étroite collaboration avec l'OSSI ou le RSSI).
Tenue à jour d'indicateurs permettant son suivi d'activités et la rédaction du rapport annuel d'évaluation de la protection du secret.
Vigilance à l'égard de toute compromission.
</td></tr>
<tr><td>Protection des lieux abritant
Suivi des arrêtés de ZP ; tenue à jour des documents constitutifs des ZR.
Suivi des Avis technique d'aptitude physique (ATAP) émis par le service enquêteur et portant sur la capacité physique des locaux à conserver et traiter des ISC.
Mise à jour de la liste des lieux abritant auprès du FSD.
Suivi des dossiers de consignes, des autorisations d'accès, des visites.
</td></tr>
<tr><th colspan="2">Mesures de sécurité applicables aux contrats</th></tr>
<tr><td colspan="2">
Conseil en matière de prise en compte de la sécurité de défense dans les contrats auprès des acheteurs de son organisme.
Mise à jour de la liste des contrats avec détention ou accès à des ISC.
Elaboration et application du plan contractuel de sécurité en liaison avec le donneur d'ordre (ou l'acheteur).
Contrôle de la protection du secret chez ses éventuels sous-contractants ou chez ses prestataires (contrats sensibles).
</td></tr>
</table>

[28] Le BPS est obligatoire pour la gestion des ISC de niveau *Très Secret*.

ANNEXE V : GUIDE DE CLASSIFICATION

Cette annexe a pour objet de préciser les prescriptions des paragraphes 4.1 et 4.2 de la présente instruction.

Compte-tenu de la grande diversité des sujets traités au sein des services du Premier ministre, les orientations pour la classification d'une information ou d'un support de cette annexe ne permettent pas directement à un rédacteur de proposer un niveau de classification et une date de déclassification adaptés à toutes les informations et à l'ensemble des documents qu'il est amené à produire. Elles n'abordent que certains sujets transverses.

L'objectif du tableau infra, qui n'est pas exhaustif, est d'offrir aux différents responsables d'organisme une aide à la classification. Chaque responsable d'organisme inclut en effet dans sa politique de protection du secret, sous le contrôle du HFDSa/PM, des directives en matière de classification des informations et supports qu'il est amené à traiter.

Le choix définitif du niveau de classification des ISC, proposé par son rédacteur, appartient au responsable d'organisme.

Légende :

TS/CS : Très Secret « Classification spéciale »
TS : Très Secret
S : Secret

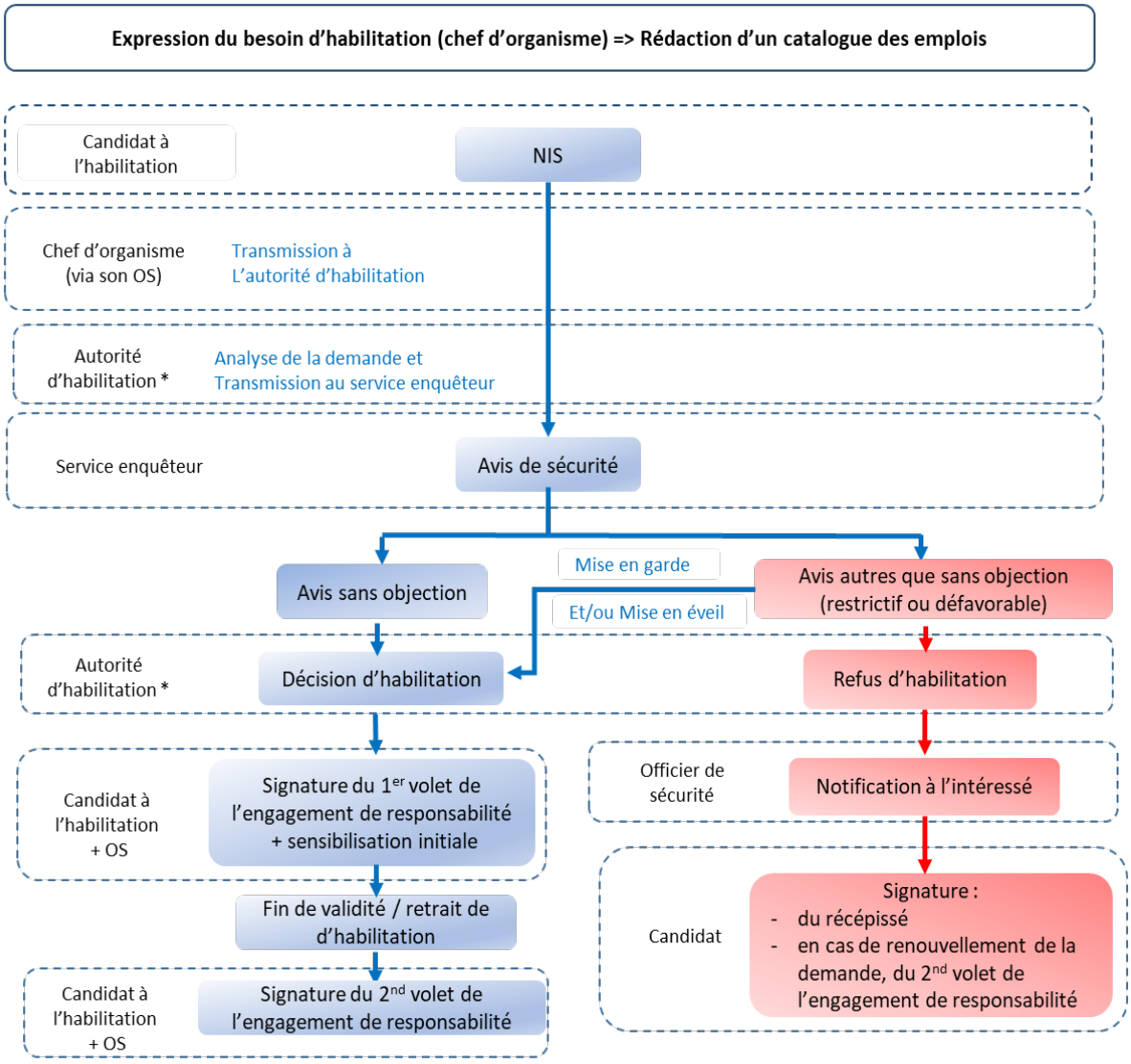
1. QUESTIONS D'ORDRE GENERAL		
Informations	**Niveau**	**Durée de classification proposée**
La plupart des documents liés aux réunions du Conseil de défense et de sécurité nationale	TS / CS	50 ans
Rapports particuliers ou occasionnels sur les sujets pouvant présenter une sensibilité particulière	TS	50 ans
Les études sur les sujets sensibles	S	50 ans
Certaines études dans les domaines militaires touchant aux forces et aux opérations	S	50 ans
La plupart des études et des plans à long terme	S	50 ans
Certains documents concernant les négociations internationales	S	50 ans
la plupart des études générales, synthèses, comptes rendus de renseignement	S	50 ans
Certaines études générales, synthèses, comptes rendus de renseignement	TS	50 ans
2. QUESTIONS RELATIVE A LA PROTECTION DES SITES		
Informations	**Niveau**	**Durée de classification proposée**
Plans de protection des sites relevant les SPM	S	20 ans
Certaines questions d'infrastructure liées à la sécurité des zones sensibles (ZP, ZR)	S	20 ans
Rapports d'inspection et comptes rendus d'évaluation ou d'exercices concernant la protection des sites relevant des SPM (dont le PIV)	S	20 ans

3. SUJETS RELATIFS AUX SYSTEMES D'INFORMATION		
Informations	**Niveau**	**Durée de classification proposée**
Les rapports d'audit ou d'analyse en matière de sécurité des systèmes d'information. Les éléments et comptes rendus d'incident SSI	S	20 ans
Les études sur des vulnérabilités des systèmes d'information	S	20 ans
Dossiers d'architecture technique des SIIV et de certains équipements de SSI.	S	20 ans
Documents de conception de nommage et d'adressage complets des réseaux informatiques.	S	20 ans
Certaines clés de chiffrement ou certains éléments secrets d'identification.	S	20 ans
4. CLASSIFICATION DES AGREGATS[29]		
Informations	**Niveau**	**Durée de classification proposée**
Le regroupement de trois informations (au moins) classifiées Secret permettant d'obtenir une information classifiée Très Secret.	TS	Identique à la durée la plus élevée des informations agrégées
Le regroupement de trois informations (au moins) protégées par la mention Diffusion Restreinte. *NB : La somme des informations DR stockées sur un système d'information homologué n'entraine pas nécessairement la classification de ce SI.*	S	A déterminer par l'auteur de l'information classifiée

[29] Pour le principe de classification de l'agrégat, se reporter au c) du § 7.1.1.2 de l'IGI 1300.

ANNEXE VI : PROCESSUS D'HABILITATION DES PERSONNES PHYSIQUES

Le processus d'habilitation suit un cheminement rigoureux décrit dans le schéma ci-dessous et précisé dans l'IGI 1300 au paragraphe 3.3.



* Pour les SPM, l'autorité d'habilitation (AH) est le HFDSa/PM, chef du S-HFDS.

ANNEXE VII : MODELE D'INVENTAIRE DES ISC

NB :

- *au regard des informations contenues dans le document ci-dessous, celui-ci peut être classifié au niveau requis ;*

- *l'inventaire est toujours classifié s'il comporte les intitulés des documents recensés.*

* Le cas échéant, apposer sur le document le timbre de classification *Secret*[30]

Fait à , le

N°

PROCES VERBAL D'INVENTAIRE OCCASIONNEL
DE DOCUMENTS CLASSIFIES DE NIVEAU *SECRET*

Date de l'inventaire :

Inventaire contradictoire réalisé à l'occasion du changement de titulaire ou Inventaire annuel

Nom et fonction du détenteur responsable (quittant) :

Nom et fonction du détenteur responsable (prenant) :

Nombre de documents classifiés :

Nombre de support numérique classifiés :

Détenteur responsable (quittant)	Détenteur responsable (prenant)
Nom prénom	**Nom prénom**

[30] L'inventaire est classifié *Secret*, si les intitulés des documents recensés sont indiqués.

* Le cas échéant, apposer sur le document le timbre de classifcation *Secret*

Documents classifiés

Référence	Distributeur[31]	Timbre	Date	N° d'exemplaire	Intitulé (facultatif)	Sortie d'inventaire[32]	Référence et date du procès-verbal[33]

[31] COMILI ou CABMIL ou Autre entité

[32] Préciser l'opération ayant conduit au retrait du document de l'inventaire : destruction, retour au distributeur, archivage, déclassification

[33] Les procès-verbaux de destruction ou de remise aux archives ou de déclassification des documents de niveau « Confidentiel Défense » ou « Secret » doivent être transmis au distributeur du document classifié.

Supports numériques classifiés

Type de support	Référence du support	Nombre de documents sur le support
Clef USB		