BULLETIN OFFICIEL DES ARMÉES

Édition Chronologique n° 63 du 12 décembre 2014

PARTIE PERMANENTE
Marine nationale

Texte 10

INSTRUCTION N° 0-15684-2014/DEF/EMM/BPPS
relative à l'organisation du secret dans la marine.

Du *21 octobre 2014*

ÉTAT-MAJOR DE LA MARINE : *bureau principal de protection du secret.*

INSTRUCTION N° 0-15684-2014/DEF/EMM/BPPS relative à l'organisation du secret dans la marine.

Du 21 octobre 2014

NOR D E F B 1 4 5 2 0 0 6 J

Références :

a) Code pénal (notamment ses articles 413-9 à 414-9).
b) Code de la défense (notamment ses articles R.* 1132-2., R.* 1132-3., D. 1132-5. et R. 2311-1. à R. 2312-2.).
c) Arrêté du 30 novembre 2011 (JO n° 279 du 2 décembre 2011, texte n° 1 ; signalé au BOC 39/2012 ; BOEM 120-0.1.4) modifié.
d) Arrêté du 21 mars 2012 (n.i. BO ; JO n° 82 du 5 avril 2012, texte n° 8).
e) Instruction interministérielle n° 2100/SGDSN/SSD du 1er décembre 1975 (n.i. BO).
f) Instruction n° 43/DEF/EMM/MG/SEC/SP/-- du 12 septembre 1996 modifiée (n.i. BO ; partie principale du BDR).
g) Instruction n° 1/DEF/EMM/MG/SEC/SP/-- du 9 février 2004 modifiée (n.i. BO ; partie principale du BDR).
h) Instruction n° 106/DEF/DPMM/SDG du 1er octobre 2004 (BOC, 2004, p. 5729 ; BOEM 321.4, 326.2.5).
i) Instruction ministérielle n° 900/DEF/CAB/-- du 26 janvier 2012 (n.i. BO).
j) Instruction générale interministérielle n° 2102/SGDSN/PSE/PSD du 12 juillet 2013 (n.i. BO).
l) Note n° 0-18867-2013/DEF/EMM/BPS-P/-- du 12 septembre 2013 (n.i. BO).
k) Guide n° 548/DEF/DPSD/DPEG/BEG/-- du 23 janvier 2013.

Pièce(s) Jointe(s) :

Quatre annexes.

Texte abrogé :

Note-circulaire n° 003/DEF/EMM/MG/SEC/SP/-- du 22 décembre 1995 modifiée (n.i. BO).

Classement dans l'édition méthodique : BOEM 120-0.1.4

Référence de publication : BOC n° 63 du 12 décembre 2014, texte 10.

Préambule.

L'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD (IGI 1300), annexe de l'arrêté du 30 novembre 2011 cité en référence c), rappelle que la protection du secret de la défense nationale fait l'objet de mesures de protection particulières en raison de la gravité des atteintes qui peuvent être portées à la défense et à la sécurité nationale par la divulgation de certaines informations et supports classifiés (ISC).

L'attention des commandants de formations administratives et d'unités ainsi que celle de leurs officiers de sécurité (OS) est attirée sur les risques pénaux qu'ils encourent en cas de compromission d'information au sein de leur organisme. La responsabilité de l'ensemble de la chaîne de protection du secret peut être recherchée si les règles n'ont pas été appliquées correctement et respectées à tous les échelons, en particulier sur les domaines de délégation accordée par le commandement, de moyens consacrés à la mission et de

formation reçue et dispensée par l'OS.

La présente instruction définit l'organisation de la marine dans le domaine de la protection du secret. Elle ne se substitue pas à la connaissance et au respect des textes cités en référence.

1. CADRE GÉNÉRAL.

1.1. **Rappel des textes.**

La réglementation sur la protection du secret est fixée par l'IGI 1300.

Au sein du ministère de la défense, cette réglementation est déclinée à travers l'instruction ministérielle n° 900/DEF/CAB/-- du 26 janvier 2012 (1) (IM 900). Afin d'aider les acteurs du domaine à exercer leur fonction, le guide pratique à l'attention des OS [référence k)] a été édité par la direction de la protection et de la sécurité de la défense (DPSD). Constitué de fiches pratiques relatives aux différents domaines de la protection du secret, ce guide permet de faciliter leur action.

L'ensemble du corpus documentaire concernant la protection du secret est disponible en ligne sur intramar sur le site DOC OPS (lien : http://centdoc-opl.emm.marine.defense.gouv.fr - domaine protection du secret).

1.2. **Principes de base.**

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

- le « besoin d'en connaître » fondé sur le principe selon lequel une personne ne peut avoir connaissance d'informations classifiées que dans l'exercice de ses fonctions ou si l'accomplissement de la mission l'exige ;

- la délivrance, par décision, de l'habilitation correspondant au degré de classification de l'information considérée. La décision d'habilitation est assortie d'un engagement à respecter, après en avoir dûment pris connaissance, les obligations et responsabilités liées à la protection des informations ou supports classifiés.

1.3. **Rappel de l'organisation.**

Au même titre que la protection-défense, la cyber-protection, la sécurité nucléaire et le contrôle gouvernemental de l'intégrité des moyens (CGIM), la protection du secret est identifiée comme l'un des cinq piliers du secteur d'activités d'importance vitale (SAIV) de l'opérateur d'importance vitale (OIV) marine nationale.

L'organisation de la protection du secret comprend trois niveaux - central, régional et local - et se décline en deux chaînes fonctionnelles, l'une relative à la protection du secret et la seconde à la protection des personnes.

2. ORGANISATION DE LA PROTECTION DU SECRET DANS LA MARINE.

2.1. **Principe.**

Le chef d'état-major de la marine (CEMM) est le responsable de la protection du secret de la défense nationale au sein de la marine. Il désigne un officier de sécurité de 1er niveau (OS1) chargé d'organiser et de superviser la protection du secret de la marine.

Par délégation du CEMM, l'état-major de la marine (EMM), la direction du personnel militaire de la marine (DPMM), la direction centrale du service de soutien de la flotte (DCSSF), les autorités organiques (AO), les commandants d'arrondissements maritimes (CAM), les commandants interarmées (COMIA) et le commandant de la marine à Paris (COMAR Paris), font appliquer les directives de l'échelon central et ont

autorité, dans ce domaine, sur les formations administratives qui leurs sont rattachées. Elles désignent, dans ce cadre, un officier de sécurité de 2e niveau (OS2).

Enfin, chaque commandant de formation ou d'unité subordonnée à l'une des autorités hiérarchiques précitées, est responsable de l'exécution des règles de la protection du secret au sein de son organisme. Pour l'assister dans cette responsabilité, il désigne un officier de sécurité de 3e niveau (OS3).

2.2. **Les chaînes de la protection du secret dans la marine.**

La protection du secret de la marine est composée de deux chaînes :

- la chaîne des OS qui présente l'organisation des OS et leur place dans l'organisation marine ;

- la chaîne des autorités d'habilitation qui s'appuie sur l'arrêté du 21 mars 2012 (A) portant délégation des pouvoirs du ministre de la défense en matière de décisions d'habilitation à connaître des informations et supports couverts par le secret de la défense nationale [référence d) (1)].

2.2.1. ***La chaîne des officiers de sécurité.***

Le principe d'une organisation par rattachement organique prévaut. Toutefois, des rapprochements territoriaux sont opérés pour tenir compte des réalités géographiques et fonctionnelles.

Cela est particulièrement le cas pour les bâtiments de la force d'action navale (FAN) affectés outre-mer qui sont placés sous l'autorité du commandement interarmées ou certaines écoles dépendant de la DPMM rattachées aux CAM.

La chaîne est présentée en annexe I. La désignation des OS est un acte de commandement. Les OS doivent avoir fait l'objet d'une décision d'admission au secret défense (SD) et sont nommés après agrément de la DPSD (cette désignation se prépare au moins trois mois avant la mutation de l'OS en poste). Les rôles et responsabilités des OS sont décrits ci-après. Dans certaines formations, les fonctions d'OS2 et OS3 peuvent être cumulées.

2.2.1.1. L'officier de sécurité de 1er niveau.

Officier supérieur désigné par le CEMM, l'OS1 est responsable de la déclinaison correcte et de la mise en œuvre des textes de référence au sein de la marine et notamment :

- il le conseille et propose l'organisation de la protection du secret de la marine ;

- il exerce une autorité fonctionnelle sur l'ensemble des OS de la marine ;

- il oriente et contrôle l'action des OS2 ;

- il contribue à la formation des OS et leur fait bénéficier de son expertise dans le traitement des cas complexes auxquels ils peuvent être confrontés, particulièrement dans le domaine des compromissions ;

- il dirige le bureau principal de protection du secret (BPPS) de la marine ainsi que le sous réseau COSMIC de la marine ;

- il est le correspondant privilégié de la DPSD (échelon central) et du secrétariat général de la défense et de la sécurité nationale (SGDSN) pour la marine ;

- il est le coordonnateur central du système informatique de gestion numérique des procédures d'habilitation SOPHIA (Synergie pour l'optimisation des procédures d'habilitation des industries et de l'administration) ;

- il est la tête de chaîne du pilier « protection du secret » du SAIV de l'OIV marine nationale. Dans ce domaine de compétence il est l'interlocuteur privilégié du délégué à la défense et la sécurité (DDS) ; fonction exercée par le sous-chef d'état-major opérations aéronavales.

2.2.1.2. L'officier de sécurité de 2e niveau.

Officier désigné par son autorité hiérarchique (cf. point 2.1.) et fonctionnellement subordonné à l'OS1, l'officier de sécurité de 2e niveau (OS2) est responsable des bonnes déclinaisons et mise en œuvre des textes de référence et des directives de l'OS1 dans les formations ou unités subordonnées. Pour ce faire :

- il conseille son commandement et prolonge l'action de l'OS1 dont il diffuse et fait appliquer les directives auprès des OS3. Il en contrôle également la bonne application ;

- il contribue à la formation des OS3 ;

- il est le correspondant de la DPSD (échelon régional) ;

- il dirige un bureau secondaire de protection du secret (BSPS) ;

- il est le coordonnateur de l'outil SOPHIA des formations ou unités qui lui sont rattachées.

2.2.1.3. L'officier de sécurité de 3e niveau.

Désigné par son commandant de formation et fonctionnellement subordonné à l'OS2, il est responsable des bonnes déclinaisons et mise en œuvre des textes de référence et des directives de l'OS1 et de l'OS2 au sein de sa formation. Pour ce faire l'officier de sécurité de 3e niveau (OS3) :

- conseille son commandement et propose l'organisation de la protection du secret en accord avec les directives émises par l'OS2 et l'OS1 ;

- dirige un bureau rattaché de protection du secret (BRPS) s'il détient des ISC de niveau SD, ou, un bureau de sécurité s'il détient des ISC de niveau confidentiel défense (CD) ;

- est le correspondant de la DPSD (échelon local) ;

- est chargé de la sensibilisation, de l'information et de la formation de son personnel en matière de protection du secret ;

- contrôle la mise en œuvre des mesures relatives à la protection du secret au sein de sa formation ;

- contrôle et surveille le personnel présentant ou pouvant présenter, du fait de sa vulnérabilité, un risque pour la protection du secret ;

- s'assure du traitement des informations et des matériels classifiés conformément aux règles en vigueur ;

- s'assure des changements et de la conservation des combinaisons de coffres et armoires fortes [tous les six mois, à chaque mouvement de personnel (mutation, changement de détenteur) ou en cas de compromission] ;

- procède à la passation de suite avec son remplaçant qui donne lieu à l'établissement d'un « procès-verbal de passation de consignes » dont un exemplaire est transmis à l'officier de sécurité de niveau 2 ;

- établit, contrôle et expédie les dossiers d'habilitation, les demandes d'avis d'opportunité ou de contrôle élémentaire. De fait, il est le correspondant direct du centre national des habilitations de la défense (CNHD) pour le suivi des dossiers émanant de son domaine fonctionnel ;

- tient à jour les catalogues d'emplois de son périmètre [2e et 3e niveau et, le cas échéant, réseaux divers de 1er niveau (très secret)] et communique à son autorité d'habilitation les versions actualisées ;

- établit (au débarquement ou pour une mission) le certificat de sécurité des administrés ;

- est le responsable SOPHIA de sa formation ou unité.

2.2.1.4. L'officier de sécurité adjoint d'unité.

Quand la taille ou l'organisation de la formation l'exige, un commandant de formation peut désigner un ou plusieurs officiers de sécurité adjoint d'unité (OSAU) subordonnés fonctionnellement à l'OS et qui prolongeront son action.

Le commandement, après accord de la DPSD, désigne et fixe les attributions du ou des OSAU dans un ordre particulier. Dans ce cadre, l'OSAU assure la gestion de la protection du secret de son périmètre fonctionnel (à ce titre, il est l'auxiliaire de l'officier de sécurité).

2.3. **Les bureaux de protection du secret et les secrétariats de sécurité.**

Pour les soutenir dans leur action, les OS disposent de bureaux de protection du secret (BPS) et les OSAU de secrétariats de sécurité.

2.3.1. ***Rôle des bureaux de protection du secret.***

2.3.1.1. Le bureau principal de protection du secret.

Placé sous l'autorité de l'OS1, le BPPS :

- prépare les textes d'organisation de la chaîne de protection du secret de la marine ;

- est le référent des BPS des formations, il leur communique les consignes de l'OS1 ;

- assure le récolement des éléments permettant d'établir le rapport annuel d'évaluation du secret de la défense nationale.

2.3.1.2. Le bureau secondaire de protection du secret.

Placé sous l'autorité d'un OS2, le bureau secondaire de protection du secret (BSPS) :

- est responsable de l'enregistrement, de l'expédition, de la réception et de la circulation des supports classifiés au niveau SD, qui ne peuvent transiter que par son intermédiaire, à l'exclusion de ceux comportant la mention « ACSSI » (2), dont la gestion est définie au titre V. de l'IGI n° 1300/SGDSN/PSE/PSD et déclinée pour les armées dans la DIAGA (3) ;

- effectue ou fait effectuer les inventaires d'ISC des détenteurs de sa formation ou de son périmètre ;

- gère les dossiers habilitation du personnel de sa formation ou de son périmètre ;

- s'assure du respect des règles de protection du secret ;

- prépare et participe aux séances d'instruction et sensibilisation du personnel ;

- fait appliquer les textes de référence, les directives de son commandement et de l'OS1 aux BRPS de son périmètre et contrôle leur action.

2.3.1.3. Le bureau rattaché de protection du secret.

Placé sous l'autorité d'un OS3, le bureau rattaché de protection du secret (BRPS) :

- est responsable de l'enregistrement, de l'expédition, de la réception et de la circulation des supports classifiés au niveau SD, qui ne peuvent transiter que par son intermédiaire, à l'exclusion de ceux comportant la mention « ACSSI », dont la gestion est définie au titre V. de l'IGI 1300 et déclinée pour les armées dans la DIAGA ;

- effectue ou fait effectuer les inventaires d'ISC des détenteurs de son périmètre ;

- gère les dossiers habilitation de son personnel ;

- s'assure du respect des règles de protection du secret ;

- prépare et participe aux séances d'instruction et sensibilisation du personnel ;

- fait appliquer les textes de référence, les directives de son commandement, de l'OS2 et de l'OS1 aux secrétariats de sécurité de son périmètre.

2.3.2. ***Le secrétariat de sécurité.***

Sous l'autorité d'un OSAU et selon le périmètre fonctionnel défini par l'OS, le secrétariat de sécurité :

- assure la continuité de l'action du BSPS (ou du BRPS) au sein de la formation ou unité ;

- est responsable de l'enregistrement, de l'expédition, de la réception et de la circulation des supports classifiés au niveau SD, qui ne peuvent transiter que par son intermédiaire, à l'exclusion de ceux comportant la mention « ACSSI », dont la gestion est définie au titre V. de l'IGI 1300 et déclinée pour les armées dans la DIAGA ;

- s'assure que l'élaboration et la conservation des ISC (à partir du niveau SD) s'effectue dans le respect de la réglementation ;

- effectue ou fait effectuer les inventaires d'ISC des détenteurs de son périmètre ;

- gère les dossiers habilitation de son personnel ;

- s'assure du respect des règles de protection du secret ;

- prépare et participe aux séances d'instruction et sensibilisation du personnel.

2.4. **Organisation de la formation du personnel.**

2.4.1. ***La formation des officiers de sécurité.***

L'OS doit obligatoirement suivre un stage de formation avant ou au début de sa prise de fonction. La formation de l'OS est de la responsabilité de celui qui l'a désigné et de son OS de niveau supérieur.

Il revient à chaque commandant de formation d'inscrire son OS au stage annuel organisé par les bureaux de protection du secret de l'état major des armées (EMA) et des trois armées, avec la participation de la DPSD.

À défaut, ils doivent participer aux stages de formation que les OS2 doivent organiser régulièrement au profit des formations ou unités qui leurs sont subordonnées.

2.4.2. ***L'instruction du personnel à la sécurité.***

Chaque OS et officier de sécurité des systèmes d'information/correspondant en sécurité des systèmes d'information (OSSI/CSSI) de formation doit veiller à l'instruction et à la sensibilisation du personnel en matière de protection du secret. Il peut se faire assister par la DPSD ou par des experts du domaine de la sécurité.

L'instruction de sécurité est essentielle, en matière de prévention, pour faire face aux différentes menaces telles que l'espionnage, le sabotage et les menées subversives.

Le personnel militaire ou civil détenant ou ayant accès à des ISC doit être régulièrement sensibilisé sur ces menaces en insistant sur les règles de discrétion et de prudence à adopter.

Cette instruction a également pour objectif de responsabiliser les personnes ayant accès aux secrets de la défense nationale et de les informer des peines encourues en cas de négligence ou d'insouciance de leur part, pouvant déboucher sur des compromissions lourdes de conséquence (articles 410-1 à 414-9 du code pénal).

2.5. **Organisation des inspections.**

Les OS de chaque niveau sont chargés du suivi de la mise en œuvre des mesures relatives à la protection du secret au sein des formations en sous ordre.

Dans ce cadre, ils doivent régulièrement mener (ou faire mener) des inspections visant à s'assurer de l'application des dispositions relatives à la détention des ISC, à la protection des installations et des personnes au regard de la réglementation.

À cette occasion, des recommandations pour améliorer le dispositif sont notifiées à l'OS de la formation.

Parallèlement, des inspections sont régulièrement conduites par d'autres organismes tels que la DPSD/GSTAD, l'inspection des armées (IdA) ou l'inspection de la marine nationale (IMN).

2.6. **Le rapport annuel.**

Tous les ans, selon les prescriptions qui sont communiquées (au plus tard début décembre de l'année précédente) par le BPPS aux OS2, les formations établissent un rapport annuel d'évaluation de la protection du secret. Ce document résume l'activité « protection du secret » de l'année écoulée (recensement des habilitations du personnel, des inspections et contrôles effectués, etc.).

Les éléments recueillis au niveau élémentaire (OS3) sont synthétisés par chaque OS2 puis transmis à l'OS1 début février pour rédaction du rapport final remis au haut fonctionnaire correspondant de défense et de sécurité [HFCDS - cabinet du ministre de la défense (MINDEF)].

Le format du rapport annuel est défini par le HFCDS. Un exemple type est fourni en annexe IV.

3. LA PROTECTION DES PERSONNES.

3.1. **Le « besoin d'en connaître » et le catalogue des emplois.**

L'appréciation du « besoin d'en connaître » est fondée sur le principe selon lequel une personne ne peut avoir connaissance d'informations classifiées que dans la mesure où l'exercice de sa fonction ou l'accomplissement de sa mission l'exige.

Ce besoin est matérialisé au sein d'un catalogue des emplois établi par l'OS et validé par l'autorité d'habilitation. Il fixe la liste des postes de la formation nécessitant une habilitation pour chaque niveau [CD, SD, très secret défense (TSD)]. Les catalogues doivent être mis à jour au moins une fois par an et lors de chaque réorganisation de service.

3.2. **Procédure d'habilitation.**

La procédure d'habilitation est destinée à vérifier 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. Elle comprend une enquête de sécurité permettant à l'autorité d'habilitation de prendre sa décision en toute connaissance de cause.

La procédure [fixée au titre II. de l'IGI 1300 et de l'IM 900 (1)] est initiée par le personnel du BPS ou du secrétariat de sécurité au regard du catalogue des emplois puis validée par l'officier de sécurité. Elle donne lieu à l'édition, par les services enquêteurs, d'un avis de sécurité qui permettra à l'autorité d'habilitation (liste définie en annexe II.) d'émettre une décision d'admission ou de refus.

L'ensemble des procédures relatives à la protection des personnes sont dorénavant exécutées depuis le système d'information SOPHIA (déployé dans la marine en 2014).

3.3. **Protection de l'anonymat.**

En vertu de l'arrêté du 7 avril 2011 relatif au respect de l'anonymat de militaires et de personnels civils du ministère de la défense, il est rappelé que, pour des raisons de sécurité, l'anonymat du personnel qui est affecté dans certaines unités du domaine du renseignement, des opérations spéciales ou de la force océanique stratégique (FOST) notamment, doit être respecté.

Tout message ou courrier faisant référence à l'identité et l'affectation de ce personnel doit a minima porter la mention de protection « diffusion restreinte ».

4. LA PROTECTION DES INFORMATIONS.

4.1. **Généralités.**

La classification d'une ISC relevant du secret de la défense nationale répond à un besoin de protection de cette information ou de ce support. Ainsi, l'autorité qui décide de la classification place ceux-ci sous la protection du code pénal (article 413-9 et suivants) tout en autorisant leur traitement par des personnes habilitées.

Il existe trois niveaux de classification qui obéissent chacun à des règles de protection propres : TSD, SD et CD. Il convient, dans ce cadre, de se référer à l'annexe 3A de l'IM 900 (1) qui donne une délimitation indicative des domaines SD et CD.

Contrairement à certaines réglementations étrangères, la mention diffusion restreinte (DR) ainsi que les autres mentions particulières de confidentialité (confidentiel personnel, etc.) ne sont pas des niveaux de classification visant à la protection des secrets de la défense nationale mais des mentions de protection d'informations et de supports pour lesquels l'émetteur entend restreindre la diffusion. À ce titre, ils ne bénéficient pas de la protection juridique accordée par les articles 413-9 et suivants du code pénal.

Les modalités de traitement des ISC de niveau CD, SD et TSD sont clairement détaillées dans l'IM 900 (1), toutefois, quelques points saillants sont rappelés ci-après pour le traitement CD et SD.

4.2. **Responsabilités du détenteur d'une information ou d'un support classifié.**

La traçabilité de l'information est primordiale dans la gestion des ISC, c'est pourquoi la position d'un document classifié doit être connue en permanence dès son arrivée dans la formation. Le suivi de l'ISC débute dès sa prise en charge par le bureau courrier de l'unité qui doit procéder à son enregistrement et la remise à

son attributaire.

Pour chaque ISC, un détenteur, habilité au minimum au niveau de la classification de l'ISC, est obligatoire. Il est responsable de son traitement, depuis son enregistrement jusqu'à sa destruction, son versement au service historique de la défense (SHD) ou la prise en compte par un nouveau détenteur.

En cas de compromission, sa responsabilité pénale est engagée (article 413-10 du code pénal).

Nota. Pour être exploités, les ISC sont parfois confiés à plusieurs personnes (successivement). Aussi, dès qu'un document classifié doit être utilisé par une autre personne que le détenteur habituel, une fiche de position est signée par le nouveau détenteur même si la communication est temporaire et de brève durée. Cette fiche est conservée par le détenteur en titre. Lors de la réintégration, le document est replacé dans l'armoire forte ou coffre [correspondant au niveau de classification de l'ISC - point 4.3.3.2. de l'IM 900 (1)]. La fiche de position est conservée par le détenteur-responsable.

4.3. **Gestion des informations et supports classifiés de niveau confidentiel défense.**

4.3.1. ***L'élaboration, la diffusion et la reproduction.***

L'élaboration d'une ISC est obligatoirement effectuée par un personnel détenant une habilitation de niveau au moins équivalent. Elle est réalisée au sein d'une zone protégée, sur du matériel de niveau de protection similaire et conformément à la réglementation en vigueur.

La diffusion s'effectue selon les préceptes de l'IGI 1300 et de l'IM 900 (1).

La reproduction, totale ou partielle, ne peut être réalisée que sur du matériel dédié et doit faire l'objet d'un enregistrement réglementaire.

4.3.2. ***L'enregistrement.***

Après remise au détenteur contre émargement, l'enregistrement d'une ISC CD s'effectue sur un registre exclusivement réservé à cet usage. Ce registre permet de déterminer l'emplacement, l'état de l'ISC (papier, numérique) et d'en identifier le détenteur.

Il doit *a minima* comporter la date et la référence du document, le grade, nom, prénom, date de réception et émargement du détenteur. La position physique du document doit être connue par le détenteur et le cas échéant indiquée sur le registre.

Il est recommandé l'utilisation de registres papier reliés, cependant, un fichier informatique (tableur excel) peut se substituer à l'enregistrement manuel d'une ISC, sous réserve qu'il soit conforme à l'article 45. de l'IGI 1300 approuvée par l'arrêté du 30 novembre 2011 cité en référence c).

4.3.3. ***La conservation.***

Les ISC de niveau CD doivent être stockés dans une armoire forte ou dans une zone sécurisée répondant aux caractéristiques fixées par les annexes V. et VI. de l'IGI 1300.

Dans le cas d'un archivage mutualisé, des notes d'organisation définissant l'accès à la documentation classifiée doivent être établies pour chaque intervenant. Elles permettent de déterminer la responsabilité précise de chacun dans la détention de cette documentation sensible. Cette démarche vise à identifier le détenteur responsable en cas de compromission.

4.3.4. ***La réalisation des inventaires.***

Il est conseillé de procéder à un inventaire annuel. S'il y est procédé, un procès-verbal en est dressé et conservé au sein du bureau.

À défaut, un récolement annuel doit être effectué afin de vérifier la présence physique des documents.

Nota. L'inventaire consiste en un contrôle physique, sous la responsabilité du détenteur et en présence d'un témoin. Il fait l'objet d'un procès-verbal. Le récolement peut être réalisé par un tiers (désigné et habilité). Il fait l'objet d'un compte rendu.

Tout mouvement de personnel détenteur-responsable doit obligatoirement donner lieu à procès-verbal d'inventaire contradictoire entre le prenant et le quittant.

4.3.5. ***La destruction, la déclassification et le versement aux archives.***

4.3.5.1. La destruction.

En conformité avec les instructions de l'émetteur et dès qu'il le juge nécessaire, le détenteur procède à la destruction de toute ISC CD qu'il a en compte.

Un procès-verbal de destruction est alors systématiquement édité. Il sert à mettre à jour le registre de suivi et peut être réclamé à tout moment lors des inspections ou contrôles.

Toute ISC sur laquelle l'émetteur a apposé la mention « destruction interdite sans autorisation de l'émetteur » doit faire l'objet d'une demande officielle vers l'autorité classificatrice du document.

4.3.5.2. La déclassification.

« La sensibilité d'une information ou d'un support classifié pouvant évoluer en fonction du temps ou des circonstances, il revient à l'autorité émettrice d'en apprécier la durée utile de classification. » [l'article 46. de l'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD approuvée par l'arrêté du 30 novembre 2011 cité en référence c)]. La mention de la durée de maintien de la classification d'une ISC doit être indiquée [IGI 1300 et IM 900 (1)] et la révision du niveau de classification (de la responsabilité de l'autorité émettrice) effectuée dès que nécessaire (*a minima*, à l'échéance des 10 ans). Généralement, elle s'effectue :

- à l'initiative de l'autorité émettrice ;

- à la demande d'un destinataire ;

- lors des inventaires annuels ;

- lors du versement des ISC aux archives.

Elle fait l'objet d'une décision formelle de l'autorité émettrice, diffusée à tous les destinataires et mention en est portée sur l'ISC et le registre.

Nota. Selon l'article L213-2 du code du patrimoine : « [...] Ne peuvent être consultées les archives publiques dont la communication est susceptible d'entraîner la diffusion d'informations permettant de concevoir, fabriquer, utiliser ou localiser des armes nucléaires, biologiques, chimiques ou toutes autres armes ayant des effets directs ou indirects de destruction d'un niveau analogue. », en conséquence la déclassification des informations traitant de ce sujet dans une ISC n'est pas envisageable.

4.3.5.3. L'archivage.

Les versements de documents classifiés aux services des archives s'effectuent conformément aux principes énoncés par le code du patrimoine et les articles 61. et 62. de l'IGI 1300 et selon les modalités des textes techniques d'application propre à chaque autorité d'administration centrale.

Concrètement, avant leur versement aux archives du SHD, les ISC doivent être correctement marqués et répertoriés. En outre, l'autorité émettrice vérifie le niveau et la durée de vie de leur classification et décide le cas échéant de les déclassifier, de les déclasser ou de les reclasser » [point 3.1.6.6. de l'IM 900 (1) et article L213-2 du code du patrimoine].

4.4. **Gestion des informations et supports classifiés de niveau secret défense.**

4.4.1. ***L'élaboration, la diffusion et la reproduction.***

L'élaboration d'un document SD est obligatoirement effectuée par un personnel détenant une habilitation de niveau au moins équivalent. Elle est réalisé au sein d'une zone réservée, sur du matériel de niveau de protection similaire et conformément à la réglementation en vigueur.

La diffusion s'effectue selon les préceptes de l'IGI 1300 et de l'IM 900 (1).

La reproduction, totale ou partielle, ne peut se faire sans l'accord de l'émetteur et ne peut être réalisée que sur du matériel dédié. Elle doit faire l'objet d'un enregistrement.

4.4.2. ***L'enregistrement.***

Tout document SD est obligatoirement répertorié sur un registre réservé à cet usage et remis au détenteur impérativement contre émargement.

4.4.3. ***La réalisation des inventaires.***

Un inventaire, daté et signé par l'officier de sécurité, est obligatoirement établi :

- une fois par an (arrêté à la date du 31 décembre) ;

- à la suite de tout mouvement de personnel détenteur-responsable.

Lors de tout mouvement de personnel, il est obligatoirement procédé à un inventaire des ISC conservés. Un procès-verbal d'inventaire occasionnel signé conjointement entre le détenteur sortant et le détenteur entrant, ou une personne désignée en cas d'intérim (officier de sécurité, chef de bureau) est alors établi. Ce document est conservé par les détenteurs (quittant et prenant). Une copie est adressée au bureau de protection du secret.

4.4.4. ***La destruction, le déclassement et la déclassification, le versement aux archives.***

4.4.4.1. La destruction.

En conformité avec les instructions de l'émetteur et dès qu'il le juge nécessaire, le détenteur procède, après accord officiel de l'autorité classificatrice [conformément aux dispositions de l'article 59. de l'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD approuvé par l'arrêté du 30 novembre 2011 cité en référence c)], à la destruction de toute ISC SD qu'il a en compte.

Un procès-verbal de destruction est alors systématiquement édité. Il sert à mettre à jour le registre de suivi et peut être réclamé à tout moment lors des inspections ou contrôles.

4.4.4.2. Le déclassement et la déclassification.

« La sensibilité d'une information ou d'un support classifié pouvant évoluer en fonction du temps ou des circonstances, il revient à l'autorité émettrice d'en apprécier la durée utile de classification. [...] » [l'article 46. de l'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD approuvé par l'arrêté du 30 novembre 2011 cité en référence c)]. La mention de la durée de maintien de la classification d'une ISC doit être indiquée [IGI 1300 et IM 900 (1)] et la révision du niveau de classification (de la responsabilité de l'autorité émettrice) effectuée dès que nécessaire (*a minima*, à l'échéance des 10 ans).

Le déclassement d'une ISC SD consiste à maintenir la classification mais à en descendre le niveau à CD.

Généralement, le déclassement et la déclassification s'effectuent :

- à l'initiative de l'autorité émettrice ;

- à la demande d'un destinataire ;

- lors des inventaires annuels ;

- lors du versement des ISC aux archives.

Elle fait l'objet d'une décision formelle de l'autorité émettrice, diffusée à tous les destinataires et mention en est portée sur l'ISC et le registre.

Nota. Selon l'article L213-2 du code du patrimoine : « [...] Ne peuvent être consultées les archives publiques dont la communication est susceptible d'entraîner la diffusion d'informations permettant de concevoir, fabriquer, utiliser ou localiser des armes nucléaires, biologiques, chimiques ou toutes autres armes ayant des effets directs ou indirects de destruction d'un niveau analogue. », en conséquence la déclassification des informations traitant de ce sujet dans une ISC n'est pas envisageable.

4.4.4.3. L'archivage.

Les versements de documents classifiés au service des archives s'effectuent conformément aux principes énoncés par le code du patrimoine et les articles 61. et 62. de l'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD approuvé par l'arrêté du 30 novembre 2011 cité en référence c) et selon les modalités des textes techniques d'application propre à chaque autorité d'administration centrale.

Concrètement, avant leur versement aux archives du SHD, les ISC doivent être correctement marqués et répertoriés. En outre, l'autorité émettrice vérifie le niveau et la durée de vie de leur classification et décide le cas échéant de les déclassifier, de les déclasser ou de les reclasser » [point 3.1.6.6. de l'IM 900 (1) et article L213-2 du code du patrimoine].

4.5. **Transmission officielle de documents classifiés dématérialisés.**

Dans l'attente de directives ministérielles clairement définies, les formations de la marine appliqueront les dispositions suivantes :

- la transmission officielle de documents classifiés par voie informatique doit se faire sur un vecteur de niveau de classification équivalent à celui de l'information transmise (CD sur SIC 21, SD sur TEOREM, etc.) puis les documents doivent être conservés, en tout temps, sur un vecteur de niveau *ad hoc* ;

- à la réception du document, une réponse d'« accusé/réception » est obligatoire pour attester de la prise en charge du document auprès de l'expéditeur ;

- lors de sa reproduction sur support numérique (CD-ROM ou clef USB ou disque dur au bon niveau) ou son impression (pour transmission ou copie), un enregistrement est effectué sur le registre cité au point 4.3.2. (CD) ou au point 4.4.2. (SD).

4.6. **La compromission.**

Une ISC est compromise lorsqu'une personne non habilitée ou n'ayant pas le besoin d'en connaître est susceptible d'en avoir pris connaissance.

La compromission est possible dès que l'ISC a échappé au contrôle continu de la personne qui en a la charge. Cette compromission peut découler autant d'un vol, d'une consultation illicite, d'une perte, d'une erreur de traitement ou de protection que de l'exploitation de moyens électroniques, informatiques, audio et techniques. Ces ISC seront présumés compromis jusqu'à ce qu'une enquête prouve le contraire.

Les dispositions relatives aux compromissions sont traitées dans la note citée en référence (1). Cette note établit les moyens à mettre en œuvre pour prévenir les compromissions ainsi que la procédure à mettre en place en cas de compromission.

5. LES AUTRES RÉSEAUX DE LA PROTECTION DU SECRET.

5.1. **Généralités.**

Dans le cadre de ses relations avec des États étrangers ou des organisations internationales et interalliées, la France peut être amenée à échanger des informations classifiées. Ces échanges s'effectuent par des mesures de protection du secret définies selon des règles prévues par des accords de sécurité conclus entre la France et l'État ou l'organisation *ad hoc*.

D'une manière générale, ces règles sont identiques à celles utilisées pour la protection des informations nationales en s'attachant toutefois à respecter le principe de cloisonnement qui exige que les informations classifiées soient enregistrées sur des supports spécifiques et détenues séparément des informations nationales.

Par ailleurs, il est rappelé que les informations classifiées à mention « spécial France » ne peuvent être diffusées sur ces réseaux.

Parmi tous ces réseaux, les réseaux de l'organisation du traité de l'Atlantique Nord (OTAN) (COSMIC) et, plus récemment, union européenne (UE), sont les plus importants.

5.2. **Le réseau organisation du traité de l'Atlantique Nord.**

L'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD approuvée par l'arrêté du 30 novembre 2011 [cité en référence c)] définit les règles relatives à la protection des informations classifiées de l'OTAN. Elle traduit de façon pragmatique les engagements de la France à protéger ces informations classifiées.

Contrairement à la France, l'OTAN compte 4 niveaux de classification d'information :

- très secret COSMIC (TSC, équivalent du niveau TSD) ;

- secret OTAN (SO, équivalent du niveau SD) ;

- confidentiel OTAN (CO équivalent du niveau CD) ;

- diffusion restreinte OTAN (DRO, correspond à DR qui, en France, est une mention de protection et non un niveau de classification).

Le réseau français est composé :

- du bureau COSMIC central (BCC) implanté au SGDSN ;

- des bureaux COSMIC principaux (BCP) d'armées, des bureaux COSMIC secondaires (BCS) et parfois des sous-bureaux COSMIC secondaires (S-BCS) ;

- des bureaux COSMIC isolés (BCI) ;

- des bureaux SECRET OTAN (BSO).

L'organisation du sous réseau COSMIC de la marine est présentée en annexe III.

Toutes les informations classifiées de l'OTAN doivent impérativement circuler au sein de ce réseau. Le bureau COSMIC principal de la marine (BCP Marine) reçoit régulièrement de la documentation OTAN, qu'il met dès lors à disposition à l'ensemble des unités de la marine sur le portail opérationnel de la marine (POM), accessible *via* les postes SIC 21.

Le chemin d'accès est le suivant : https://pom.marine.defensecdd.gouv.fr/POM (rubriques à sélectionner « documentation OPS marine », puis « OTAN »). Il appartient à chacun de consulter ce site afin de recueillir ses besoins en informations OTAN.

5.3. **Le réseau Union européenne.**

Les règles relatives à la protection en France des informations classifiées de l'Union européenne sont définies dans l'instruction générale interministérielle n° 2102/SGDSN/PSE/PSD du 12 juillet 2013 référence j) (1) . L'application de ces nouvelles mesures est en cours de mise en place au sein des armées.

Le réseau UE compte 4 niveaux de classification d'information :

- très secret UE (TS-UE, équivalent du niveau TSD) ;

- secret UE (S-UE, équivalent du niveau SD) ;

- confidentiel UE (C-UE, équivalent du niveau CD) ;

- restreint UE (R-UE correspond à DR qui, en France, est une mention de protection et non un niveau de classification).

Le réseau français dont l'architecture devrait être identique à celui du COSMIC, est composé :

- du bureau central UE (BCUE) situé au SGDSN ;

- des bureaux très secret UE principaux, isolés ou subordonnés chargés des informations TS-UE ;

- des bureaux de protection des informations classifiées UE (ICUE) de niveau S-UE et C-UE.

Toutes les informations classifiées de l'UE doivent impérativement circuler au sein de ce réseau.

6. LA FORCE OCÉANIQUE STRATÉGIQUE.

Tous les aspects spécifiques et sensibles relatifs à la protection du secret de la force océanique stratégique (FOST) : protection des informations, des personnes, des installations, sont repris dans l'instruction citée en référence f) (1).

6.1. **Mutation du personnel dans les forces sous-marines.**

Le personnel muté dans les forces sous-marines (FSM), dans les unités concourant au fonctionnement de la FOST ou implantées dans les points sensibles des forces nucléaires stratégiques (FNS) doit obligatoirement faire l'objet d'une demande d'avis d'opportunité FNS. Cette demande doit être initiée dès que la désignation du personnel pour cet environnement est connue conformément à l'instruction citée en référence h).

6.2. **L'accès dans les sites de la force océanique stratégique.**

Les procédures relatives à l'accès du personnel dans les zones réservées et protégées de la FOST sont fixées dans l'instruction citée en référence f) (1).

L'attention est attirée sur les délais de traitement des demandes d'accès, d'au moins 3 semaines pour le personnel de nationalité étrangère notamment. Ces demandes peuvent être refusées à tout moment pour des raisons de sécurité ou tout motif lié à l'activité opérationnelle.

7. TEXTE ABROGÉ.

La note-circulaire n° 003/DEF/EMM/MG/SEC/SP/-- du 22 décembre 1995 (1) modifiée, relative à la composition du dossier de sûreté est abrogée.

8. PUBLICATION.

La présente instruction est publiée au *Bulletin officiel des armées*.

Pour le ministre de la défense et par délégation :

Le vice-amiral d'escadre,
major général de la marine,

Arnaud DE TARLÉ.

---

(1) n.i. BO.

(A) n.i. BO ; JO n° 82 du 5 avril 2012, texte n° 8.

(2) Articles contrôlés de la sécurité des systèmes d'information, tels que définis par l'instruction interministérielle n° 910/SGDN/DISSI/SCSSI/SSD/-- du 22 octobre 2013.

(3) La DIAGA est la directive interarmées pour la gestion des ACSSI (référence : directive n° 404132/DEF/DIRISI /DIRCEN/SDSSI/-- du 19 juillet 2011).

ANNEXE I.

CARTOGRAPHIE DE LA PROTECTION DU SECRET DANS LA MARINE - CHAÎNE DES OFFICIERS DE SÉCURITÉ.

CHAINE DE PROTECTION DU SECRET DE LA MARINE
les Officiers de Sécurité

CHEF D'ETAT-MAJOR DE LA MARINE
OS 1

Formations administratives affectées étranger et outre-mer

CECLANT	CECMED	ALFAN	ALAVIA	ALFOST	ALFUSCO	COMAR MANCHE	COMAR PARIS	DPMM	DCSSF	EMM	COMSUP / COMIA
OS 2	OS 2	OS 2	OS 2	OS 2	OS 2	OS 2	OS 2	OS 2	OS 2	OS 2	OS 2
CRMAR OS 3	FOSIT TOULON OS 3	Bâtiments zone Méditerranée OS 3	BAN LDV OS 3	COMILO OS 3	BASEFUSCO OS 3	FOSIT CHERBOURG OS 3	CC MILLE OS 3	SPM OS 3	DSSF TOULON OS 3	SIRPA Marine OS 3	BN ABU DHABI OS 3
CEPPOL OS 3	BN TOULON EMP TOULON SLM TOULON CMP TOULON OS 3	GPD MED OS 3	11F OS 3	ESNA ESNA OS 3	CDO de MONFORT OS 3	BN CHERBOURG SLM CHERBOURG OS 3	CM PEPINIERE OS 3	CERH OS 3	DSSF BREST OS 3	CPSIM OS 3	BN DEGRAD DES CANNES OS 3
FOSIT BREST OS 3	COMAR CORSE OS 3	FLOPHEB OS 3	12F OS 3	ESNLE ESNLE CPSM BREST OS 3	CDO de PENFENTENYO OS 3	COMAR DUNKERQUE OS 3	CESM OS 3	SRM OS 3	Antennes SSF Locales OS 3	CEMM CAB OS 3	BN DJIBOUTI OS 3
BN ADOUR OS 3	COMAR MARSELLE OS 3	*REACH BACK SPE FREMM TOULON (1)* OS 3	17F OS 3	CIRA OS 3	CDO HUBERT OS 3	COMAR LE HAVRE OS 3	CPPE OS 3			EMO MARINE (2) OS 3	BN FORT DE France OS 3
MARINE BORDEAUX OS 3	CEPN CEPN GIUBF OS 3	***ALFAN BREST*** OS 3	57S OS 3	CTM France SUD OS 3	CDO JAUBERT OS 3	ECOFOU (3) OS 3	COMAR STRASBOURG OS 3				BN NOUMEA OS 3
COMAR NANTES OS 3	APER TOULON OS 3	ALFAN ANTENNE CHERBOURG OS 3	CENTEX GAE OS 3	CTM ROSNAY OS 3	CDO TREPEL OS 3	EAMEA EAMEA Jacques Cadenelle OS 3	IMN OS 3				BN PAPEETE OS 3
BN BREST EMP BREST SLM BREST CMP OS 3	ECOPLONGE OS 3	GPD ATLANT OS 3	BAN LBH OS 3	CTM STE ASSISE OS 3	CDO KEIFFER OS 3						BN PORT DES GALETS OS 3
CIN BREST OS 3	CENTRE "DPMM LAMALGUE" OS 3	GPD MANCHE OS 3	4F OS 3		GFM BREST OS 3						BN MAYOTTE OS 3
ENGEP ENGM OS 3	CIN ST MANDRIER OS 3	REACH BACK SPE FREMM BREST OS 3	21F OS 3		GFM TOULON OS 3						Bâtiments Outre mer OS 3
APER BREST OS 3	SLM CENTRAL OS 3	Bâtiments zone Atlantique - Manche Mer du Nord OS 3	23F OS 3		CIFUSIL (4) OS 3						antennes SSF outre mer OS 3
CEMF OS 3	BMP MARSEILLE OS 3		24F OS 3		ECOFUS LORIENT OS 3						
	EMP MARSEILLE OS 3		CENTEX PATSMAR OS 3								
			CELAE LBH OS 3								
			BAN LVC OS 3								
			22S OS 3								
			32F OS 3								
			33F OS 3								
			34F OS 3								
			50S ESP LVC OS 3								
			BAN HYE OS 3								
			31F OS 3								
			35F OS 3								
			36F OS 3								
			CCMAR MED OS 3								
			CENTEX HELICO OS 3								
			CEPA/105 OS 3								
			EAN COGNAC OS 3								

Legende

OS 1 : tête de chaine "marine"

OS 2 : responsable protection du secret (PDS) d'une chaine organique (ou assimilée)

OS 3 : responsable PDS de sa formation

ALFAN BREST: Une délégation de signature a été accordé par ALFAN à ALFAN BREST et aux COMIA pour toutes les formations de sa chaine identifiées en bleu,

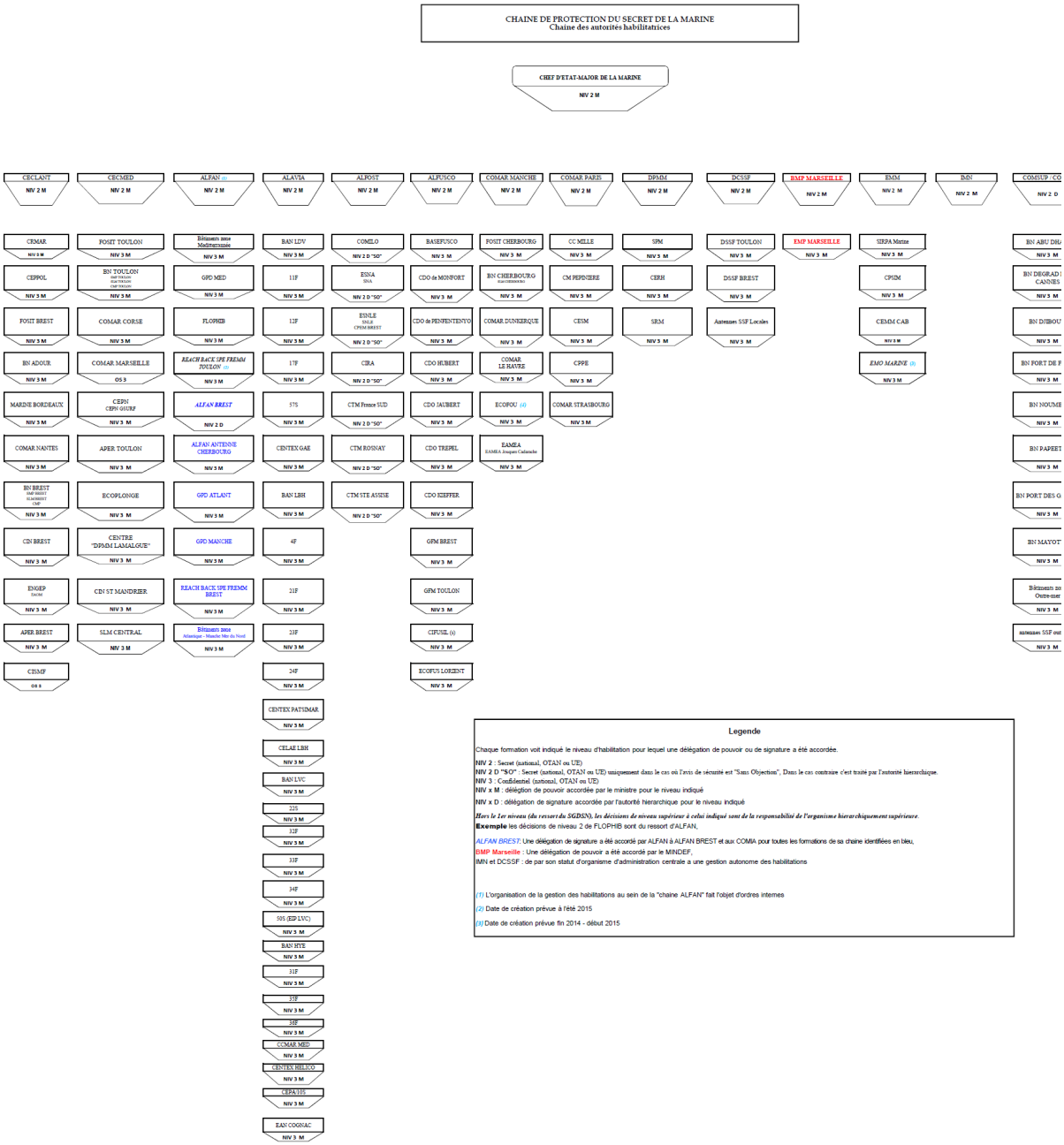
BMP Marseille : Hors la gestion des habilitations, est subordonné à CECMED dans le cadre de la PDS,

CIAM et CFSI dissous en septembre 2014
(1) Date de création prévue à l'été 2015
(2) Date de création previsionnelle : fin 2014-début 2015

ANNEXE II.

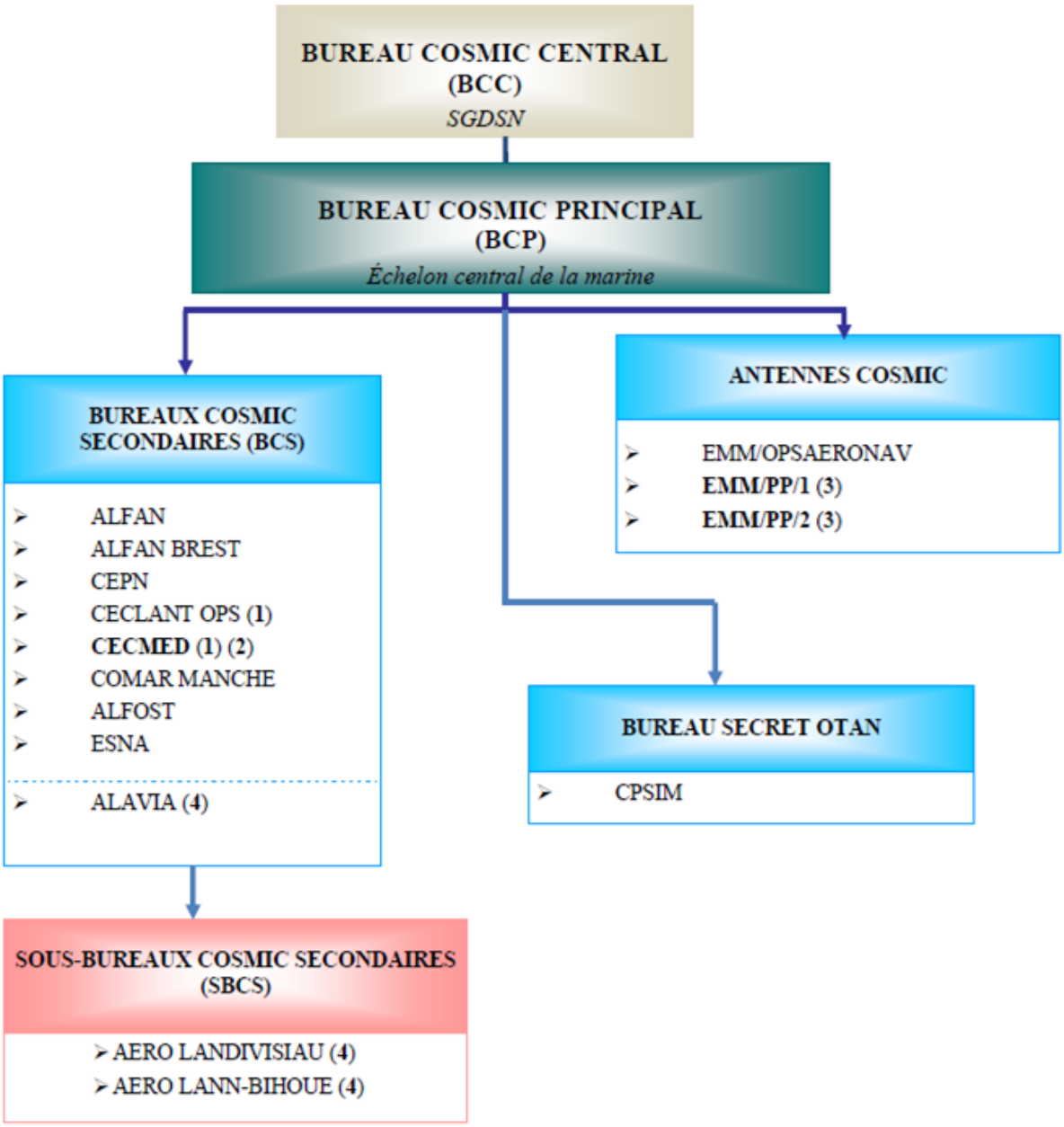
CHAÎNE PROTECTION DU SECRET - ORGANISATION DE LA GESTION DES HABILITATIONS.

CHAINE PROTECTION DU SECRET
ORGANISATION DE LA GESTION DES HABILITATIONS



ANNEXE III.

CARTOGRAPHIE DU SOUS RÉSEAU COSMIC DE LA MARINE.



(1) Section terminale, bureau d'enregistrement ayant délégation du BCC pour :
- recevoir directement les documents en provenance de l'étranger ;
- prendre en compte ces derniers au nom de la France ;
- adresser directement des documents à l'étranger.

(2) le BCS CECMED sera la nouvelle appellation du BCS COM TOULON avant fin 2014

(3) les antennes **EMM/BPROG/SURF/NAV/SURF1**, **EMM/BPROG/SURF/NAV/SURF2**, **EMM/EXPERT/AERO**, **EMM/OCEM**, **EMM/COE** deviendront les antennes **EMM/PP/1** et **EMM/PP/2** au plus tard, à l'échéance du déménagement Balard.

(4) BCS de rattachement.

ANNEXE IV.

RAPPORT ANNUEL D'ÉVALUATION SUR LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE.

Le format à utiliser obligatoirement pour la conception des rapports annuel d’évaluation sur la protection du secret de la défense nationale est présenté ci-après.

RAPPORT ANNUEL D'ÉVALUATION SUR LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE

ANNÉE 20*XX*

« *DESIGNATION ORGANISME* »

I. EFFECTIFS HABILITÉS

I.1- Nombre de personnes physiques habilitées au 31 décembre 20*XX* :

TRES SECRET DEFENSE	SECRET DEFENSE	CONFIDENTIEL DEFENSE

Commentaires :

I.2- Nombre d'habilitations délivrées au cours de l'année 20*XX* :

TRES SECRET DEFENSE	SECRET DEFENSE	CONFIDENTIEL DEFENSE

Commentaires :

I.3- Nombre de personnes morales habilitées :

TRES SECRET DEFENSE	SECRET DEFENSE	CONFIDENTIEL DEFENSE

II. NOMBRE DE LIEUX ABRITANT DES ÉLÉMENTS COUVERTS PAR LE SECRET DE LA DÉFENSE NATIONALE

III. INVENTAIRE DES INFORMATIONS CLASSIFIÉES AU NIVEAU SECRET DEFENSE	
AUTORITÉ ORGANIQUE ET ORGANISMES RATTACHÉS	**NOMBRE DE DOCUMENTS ET SUPPORTS CLASSIFIÉS DÉTENUS**
TOTAL « ***ORGANISME*** »	

IV. ETAT DES CATALOGUES DES EMPLOIS ET DES INVENTAIRES

IV.1 - Etat des catalogues des emplois :

IV.2 - Etat des inventaires :

V. NOMBRE D'INSPECTIONS OU DE CONTROLES EFFECTUÉS

V.1 - Nombre et type d'inspections effectuées :

V.2 - Nombre et type de contrôles effectués :

V.3 - Organismes concernés :

VI. DÉFICIENCES RELEVÉES DANS LE DISPOSITIF DE PROTECTION DU SECRET

VI.1 - Nombre de déficiences relevées, types de documents, suites (administratives, pénales) données :

VI.2 - Connaissance de la réglementation :

VI.3 - Sécurisation des locaux :

VI.4 - Gestion des habilitations / gestion des documents :

VII. ACTIONS CORRECTRICES ENGAGÉES

VII.1 - Sécurité des personnes :

VII.2 - Sécurité physique :

VII.3 - Autres actions correctrices :

VIII. COMPROMISSIONS CONSTATÉES ET ACTIONS DE FORMATION OU DE SENSIBILISATION MENÉES

VIII.1 - Nombre de compromissions constatées, types de documents, suites (administratives, pénales) données :

VIII.2 - Actions de formation menées :

VIII.3 - Actions de sensibilisation menées :