BULLETIN OFFICIEL DES ARMÉES

Édition Chronologique n° 05 du 8 février 2018

PARTIE PERMANENTE
Administration Centrale

Texte 1

DIRECTIVE N° 34/DEF/DGSIC
relative aux articles contrôlés de la sécurité des systèmes d'information du ministère de la défense.

Du *10 mars 2015*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION : *sous-direction de la sécurité des systèmes d'information.*

DIRECTIVE N° 34/DEF/DGSIC relative aux articles contrôlés de la sécurité des systèmes d'information du ministère de la défense.

Du 10 mars 2015

NOR D E F E 1 5 5 2 6 4 5 X

Pièce(s) Jointe(s) :

Six annexes

Classement dans l'édition méthodique : BOEM 160.4

Référence de publication : BOC n° 05 du 8 février 2018, texte 1.

---

1. GÉNÉRALITÉS.

La présente directive centrale a pour objet de préciser, en complément de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, de l'instruction interministérielle n° 910 relative aux articles contrôlés de la sécurité des systèmres d'information (ACSSI) et de l'instruction ministérielle n° 900 relative à la protection du secret de la défense nationale au sein du ministère de la défense, les exigences de gestion et de mise en œuvre des ACSSI au niveau du ministère.

La présente directive ne traite pas des données liées au chiffre et à la gestion des réseaux de chiffrement qui relèvent de la responsabilité des autorités qualifiées et des autorités d'emploi. Il n'en reste pas moins que les articles contrôlés de la SSI participent, notamment, de l'exploitation du chiffre qui constitue l'une des composantes privilégiées de la sécurisation d'un système d'information (cf. [II n° 500bis]). Les ACSSI concourent, en particulier, à la mise en œuvre des réseaux de chiffrement.

La directive s'applique à toute personne physique ou morale du ministère de la défense détenant ou manipulant des ACSSI.

Les règles précédentes étaient adaptées à la protection de produits de chiffrement ou de clés cryptographiques sensibles, dépourvus de protections techniques et dont la perte pouvait compromettre la totalité d'un réseau de correspondants. Depuis cette date, les moyens et informations cryptographiques ont évolué et se sont diversifiés. Aux côtés de produits qui demeurent particulièrement sensibles, soit parce qu'ils reposent sur des technologies anciennes, soit parce que l'usage auquel ils sont destinés l'impose, certains moyens comportent aujourd'hui des dispositifs d'autoprotection (logiciels signés, paramètres secrets chiffrés, dispositifs anti-intrusion, par exemple), d'autres ont vocation à être largement déployés, à devenir des outils du quotidien quitte à être perdus - c'est le cas notamment des moyens de communication mobiles chiffrant.

Elle doit être déclinée au sein des armées, directions et services du ministère afin d'en préciser la mise en œuvre. Cependant, les règles, principes et définitions restent applicables *stricto sensu*.

1.1. **Définition et typologie des articles contrôlés de la sécurité des systèmes d'information.**

1.1.1. ***Définition.***

Les articles contrôlés de la sécurité des systèmes d'information (ACSSI) sont les moyens classifiés ou non, tels que les dispositifs de sécurité ou leurs composants, et certaines informations relatives à ces moyens

(spécifications algorithmiques, documents de conception, clés de chiffrement, rapports d'évaluation, etc.), qu'il est essentiel de pouvoir localiser à tout moment et en particulier en cas de compromission suspectée ou avérée.

1.1.2. ***Typologie.***

Tous les ACSSI sont soumis aux mêmes règles, notamment de traçabilité, qui peuvent néanmoins faire l'objet d'une granularité variable. Ils bénéficient en outre d'éventuelles mesures de protection, justifiées par les risques qui pèsent sur eux en fonction de leurs conditions d'emploi. Ces mesures se traduisent par une mention de protection.

Ainsi, les moyens et informations ACSSI peuvent, par leur conception, leurs conditions d'emploi, les risques couverts ou tout autre élément décrit dans l'agrément, être répartis en deux catégories :

- Les ACSSI classifiés, qui sont à la fois ACSSI et classifiés Confidentiel Défense, Secret Défense et Très Secret Défense. Ils seront désignés et marqués ACSSI CD, ACSSI SD, ou ACSSI TSD (suivi de la catégorie dans ce dernier cas).

- Les ACSSI non classifiés, qui sont à la fois ACSSI et non classifiés de défense (Diffusion Restreinte ou Non Protégé). Ils seront désignés et marqués ACSSI DR ou ACSSI NP.

Les deux mentions, accolées l'une à l'autre, sont à la fois distinctes et complémentaires :

- distinctes car la dénomination Non Protégé ne soustrait pas l'ACSSI aux contraintes de traçabilité, de contrôle et d'information en cas d'incident et pendant tout son cycle de vie ;

- complémentaires car la classification ou non de l'ACSSI pourra définir en partie les contraintes de traçabilité.

Sauf mention contraire, le terme ACSSI désignera indifféremment, dans la suite du document, les ACSSI classifiés et les ACSSI non classifiés. Le cas des équivalents étrangers (*controlled cryptographic items* ou CCI, …) est traité au point 8. (Organisation et responsabilités relatives aux moyens et informations étrangers).

1.2. **Attributions de la mention « articles contrôlés de la sécurité des systèmes ».**

La notion d'ACSSI est introduite au cours des démarches d'analyse de sécurité (agrément ou homologation). Elle contribue à protéger, tout au long de leur cycle de vie, les ressources essentielles qui ont de la valeur pour l'organisme et qui sont nécessaires à la réalisation de la mission (informations, fonctions, sous forme numérique ou matérielle) définies dans cette analyse.

Dans ce cadre pour le ministère, l'attribution de la mention ACSSI est de la responsabilité du comité de pilotage du programme pour les programmes d'armements et de la direction générale pour l'armement (DGA) pour le développement de tous les matériels chiffre et la conception des algorithmes de cryptologie dont elle a la responsabilité en coordination avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Pour les moyens faisant l'objet d'un agrément, l'attribution de la mention ACSSI est validée par l'ANSSI après avis de la commission d'agrément du dispositif de sécurité concerné.

D'autre part, dans le cadre des programmes d'armement, pour ce qui concerne les matériels importés (OTAN – US…) identifiés articles COMSEC (1) par leur autorité nationale de sécurité d'origine (ANS), la DGA définit, dans le respect des accords internationaux, l'identification du matériel en indiquant notamment les éventuelles mentions afférentes (CCI…) et les conditions d'emploi du matériel. Ces éléments sont communiqués aux autorités qualifiées utilisatrices. Elles sont chargées de les faire appliquer au sein de leur organisation.

Concernant les matériels importés en dehors du cadre d'un programme d'armement, l'autorité qualifiée faisant l'acquisition du matériel est chargée d'obtenir ou de définir, dans le respect des accords internationaux,

l'identification du matériel en indiquant notamment les éventuelles mentions afférentes (CCI…) et les conditions d'emploi du matériel.

Enfin, l'autorité d'homologation d'un système d'information peut, après avis de la commission d'homologation, décider de classer ACSSI un dispositif de sécurité non soumis à agrément ou ses composants ou les informations qui y sont liées. Dans ce cadre (afin de conserver une cohérence dans l'attribution de la mention ACSSI et le niveau de protection attribué au sein du ministère) cette décision sera transmise pour avis à la DGSIC. Cette décision s'applique à l'ensemble des dispositifs du même type présents au sein du ministère.

Les risques pesant sur ces moyens et informations, les besoins de traçabilité, la chaîne de remontée d'alerte en cas d'incident, les mesures de protection, les mentions de classification sont inscrits dans l'agrément délivré par l'ANSSI, s'ils y sont soumis, ou la décision d'homologation dans le cas contraire. Une liste exhaustive des éléments qui doivent figurer dans un agrément relatif à un produit susceptible de recevoir la mention ACSSI figure en annexe IV.

1.3. **Gestion spécifique des articles contrôlés de la sécurité des systèmres d'information.**

Les ACSSI font l'objet d'une gestion spécifique tout au long de leur cycle de vie afin de garantir la sécurité (confidentialité, intégrité, disponibilité et authenticité) des ressources essentielles qu'ils protègent. Cette gestion spécifique, appelée gestion ACSSI, recouvre les fonctions suivantes :

- le suivi des ACSSI, c'est-à-dire la concrétisation des actes de prise en compte, de création, de modification ou de destruction liés à la « vie » des ACSSI et regroupés sous la terminologie : « comptabilité ACSSI » ;

- la validation (2) et la mise en œuvre des plans de déploiement des ACSSI, le besoin étant défini par les chaînes « emploi » ;

- la réalisation des inventaires et le contrôle de la manipulation et de la protection conformes des ACSSI (3);

- le traitement des incidents.

Cette gestion spécifique a pour but essentiel d'assurer, dans les meilleures conditions, la traçabilité des ACSSI et le traitement des incidents de sécurité (4) :

- perte de tout ou partie d'un moyen ou d'une information ;

- perte d'intégrité ou de confidentialité, avérée ou supposée, d'un moyen ou d'une information ;

- vulnérabilité sur un moyen ou une information, qui implique des mesures conservatoires.

Ces incidents de sécurité potentiels et leurs conséquences sont étudiés lors de l'analyse de risque qui précède l'agrément du dispositif de sécurité, ou la décision d'homologation concernant le système d'information auquel le dispositif de sécurité appartient. La décision de marquer ACSSI un moyen ou une information entraine l'obligation de respecter la présente directive.

L'agrément ou la décision d'homologation contiennent des obligations et/ou des recommandations qui auront des conséquences sur l'organisation de la gestion de l'ACSSI.

Ainsi, selon la portée de l'impact prévisible des incidents de sécurité potentiels, la gestion de l'ACSSI doit être assurée au bon niveau de gestion (cf. point1.4.). Celui-ci doit nécessairement :

- s'appuyer sur une organisation dont les principes sont définis au point 2 ;

- dépendre de l'incident de sécurité qui aurait l'impact le plus critique, tel qu'évalué lors de l'analyse de risque ;

- être précisé dans l'agrément (ou la décision d'homologation) ou, si l'agrément le permet ou ne le précise pas, le choix appartient à ou aux autorités qualifiées mettant en œuvre l'ACSSI considéré *;*

- être unifié au sein du ministère pour un type d'ACSSI donné, notamment pour les matériels.

1.4. **Les principes d'organisation du suivi des articles contrôlés de la sécurité des systèmres d'information.**

Le suivi en gestion des ACSSI se décline en suivi en gestion centralisée et suivi en gestion locale.

Le suivi en gestion locale n'est applicable qu'aux ACSSI non classifiés [diffusion restreinte (DR) et non protégé (NP)] sous réserve que l'agrément ou la décision d'homologation ne l'interdise pas.

1.4.1. ***LE SUIVI EN GESTION CENTRALISEE.***

Le suivi en gestion centralisée (ou encore suivi en gestion centrale, ou encore suivi central) s'appuie sur une organisation à plusieurs niveaux :

- un premier niveau central, en mesure de fournir une vision totale des ACSSI déployés au sein d'un organisme ;

- un ou plusieurs niveaux locaux, assurant le suivi spécifique et l'affectation à une entité des ACSSI mis à disposition par le premier niveau central.

1.4.2. ***LE SUIVI EN GESTION LOCALE.***

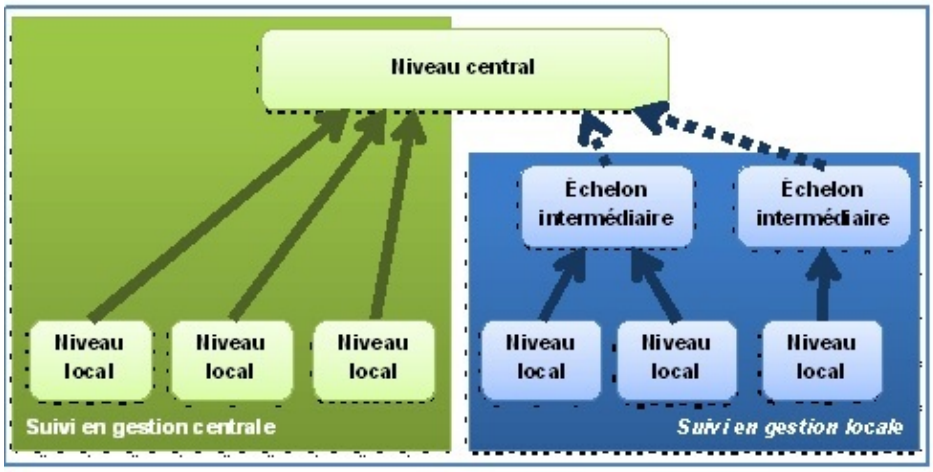
Le suivi en gestion locale (ou encore suivi local) repose sur des structures (appelées échelons intermédiaires dans l'[II910]) ayant reçu délégation des autorités qualifiées. Les ACSSI peuvent alors être gérés directement par ces structures selon leur organisation, sans que l'échelon central de gestion des ACSSI n'ait à approuver les mouvements réalisés.

Cependant, même si ces structures ne dépendent pas directement de l'autorité qualifiée leur ayant délégué le suivi d'un type d'ACSSI, l'échelon central de cette dernière doit pouvoir accéder à leurs informations de suivi pour permettre de fournir, autant que de besoins, une vision globale à son autorité qualifiée, voire au niveau ministériel.

Il convient de noter que la gestion locale :

- n'est en principe pas de nature géographique,

- peut être transverse à plusieurs autorités qualifiées (contrairement à la gestion centralisée), les échelons intermédiaire pouvant avoir un périmètre de responsabilité transverse à plusieurs autorités qualifiées (cf. par exemple le périmètre de responsabilité de la SIMMAD)



2. CHAÎNE FONCTIONNELLE ET RESPONSABILITÉS.

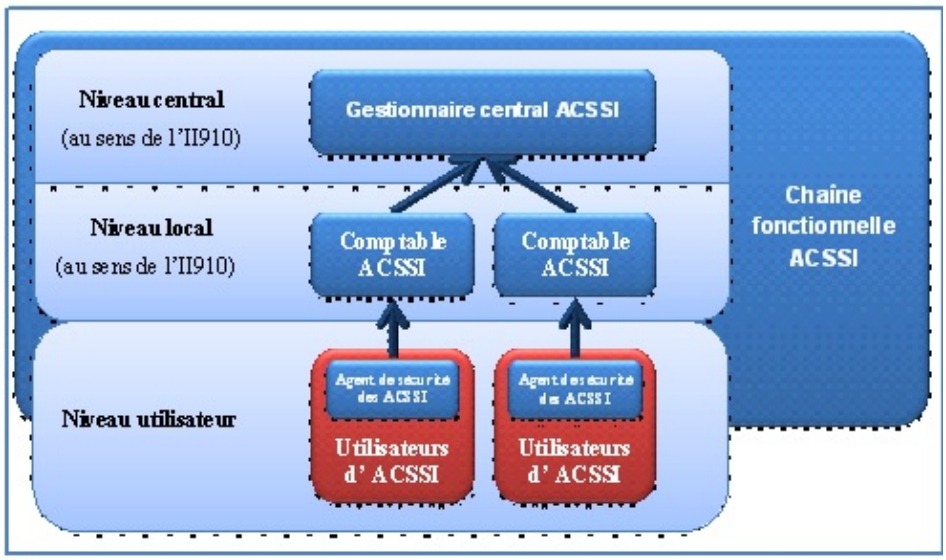
2.1. **LA CHAINE FONCTIONNELLE DES ARTICLES CONTRÔLÉS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.**

Sous-ensemble de la chaîne fonctionnelle de sécurité des systèmes d'information, la chaîne fonctionnelle ACSSI est chargée de prescrire, d'appliquer pour ce qui la concerne, de contrôler l'application des mesures de sécurité des ACSSI, et de traiter les incidents sur ces derniers.

Elle est composée majoritairement des spécialistes SSI ou le cas échéant SIC ayant suivi une instruction idoine et détenteurs d'une décision d'accès aux ACSSI (cf. point 4.).

L'arborescence fonctionnelle de la chaîne identifie les autorités qualifiées en SSI, les gestionnaires centraux ACSSI, les comptables ACSSI et les agents de sécurité des ACSSI.

Les utilisateurs (i.e. les chefs d'entités) et les exploitants d'ACSSI n'en font pas partie. Les échelons intermédiaires et la chaîne mise en place par ces derniers pour gérer les ACSSI dont la gestion leur a été déléguée ne sont pas intégrés aux chaînes fonctionnelles ACSSI.



2.2. **LES RESPONSABILITES POUR LA GESTION CENTRAL DES ARTICLES CONTRÔLÉS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.**

2.2.1. ***L'autorité responsable de la gestion des articles contrôlés de la sécurité des systèmres d'information.***

L'autorité responsable de la gestion des ACSSI est le haut fonctionnaire correspondant de défense et de sécurité (HFCDS). Désigné par le ministre et relevant directement de lui, le HFCDS veille au déploiement au sein du ministère de la défense des moyens sécurisés de communication électronique gouvernementale et s'assure de leur bon fonctionnement (5). À ce titre, il a la responsabilité d'organiser la chaîne fonctionnelle ACSSI à travers la directive centrale de suivi des ACSSI.

Cette responsabilité est déléguée au directeur général des systèmes d'information et de communication (DGSIC).

Tous les organismes sous tutelle du ministère de la défense traitant des ACSSI, ou ayant des liens contractuels les amenant à traiter des ACSSI, ont pour autorité responsable de la gestion des ACSSI le HFCDS.

2.2.2. ***Les autoritées qualifiées.***

Conformément à l'[IGI1300], les autorités qualifiées sont responsables de la mise en œuvre des procédures réglementaires prescrites pour la gestion des ACSSI, y compris dans les échelons intermédiaires de leur périmètre.

Chaque autorité qualifiée du ministère de la défense met en place une chaîne fonctionnelle ACSSI chargée d'assurer la gestion centralisée des ACSSI.

Le suivi en gestion centralisée est placé sous la responsabilité d'un gestionnaire central ACSSI unique pour chaque autorité qualifiée.

2.2.3. ***Niveau central : le gestionnaire central des articles contrôlés de la sécurité des systèmres d'information.***

Situé au niveau haut de la chaîne fonctionnelle ACSSI, le gestionnaire central ACSSI unique :

- Dirige la gestion centralisée des moyens le justifiant.
    - cela concerne :
        - les moyens et les informations ACSSI classifiés (obligatoire) ;
        - les informations ACSSI non classifiées (sauf cas particuliers à formaliser) ;
    - cela ne concerne pas les moyens ACSSI non classifiés lorsque leur gestion a été déléguée à un ou plusieurs échelons intermédiaires.
- Est l'organe de synthèse de circonstance concernant les ACSSI (moyens ou informations) relevant d'une gestion locale sur le périmètre de son autorité qualifiée (en propre ou au titre d'une tutelle).

Il est responsable de fournir à l'autorité qualifiée, et par voie de conséquence au HFCDS, l'état des ACSSI de son organisme. À ce titre il entretient des liens privilégiés avec les structures qui se sont vu déléguer la gestion d'ACSSI non classifiés. Il est notamment chargé de leur conseil en matière d'application de la réglementation ACSSI au sein de leur chaîne et est rendu destinataire des rapports (ou extraits) d'inspection et de contrôle pour ce qui le concerne.

Il est à noter que si le niveau central peut se scinder en plusieurs entités distinctes spécialisées par domaine suivant l'importance de l'organisation, le principe d'unicité de la fonction doit demeurer.

Ainsi, au titre de la gestion des ACSSI, les missions du niveau central sont les suivantes :

- Mission « suivi et traçabilité des ACSSI » :

  - assurer le suivi et la traçabilité des ACSSI placés sous leur responsabilité et dont la gestion n'a pas été déléguée ;

  - déterminer le niveau de gestion des ACSSI placés sous leur responsabilité lorsque les conditions le permettent.

- Mission « contrôle » :

  - contrôler les entités possédant des ACSSI, qu'elles les mettent en œuvre ou non.

- Mission « incidents » :

  - traiter les incidents remontant jusqu'à leur niveau, et prononcer les compromissions.

*2.2.4. **Niveau local : les comptables des articles contrôlés de la sécurité des systèmres d'information.***

Le terme niveau local est uniquement employé par opposition à niveau central. Ainsi suivant l'importance de l'organisme des niveaux médians pourront être créés.

Ils exécutent les actes de gestion décidés par le gestionnaire central ACSSI et sont responsables de la conservation des ACSSI non attribués à un utilisateur.

Ils traitent les incidents sur leur périmètre de responsabilité.

*2.2.5. **Niveau utilisateur : le chef d'entité et l'agent de sécurité des articles contrôlés de la sécurité des systèmres d'information .***

Les utilisateurs d'ACSSI exploitent les ACSSI qui leur sont confiés en exécution d'un acte de gestion. Ils sont responsables de la conservation et du bon usage de ces derniers.

Le cas échéant, et lorsque l'utilisateur d'ACSSI est le commandant d'unité, il fait prendre en compte les ACSSI par son personnel afin d'assurer la traçabilité jusqu'à la personne qui détient effectivement un ACSSI (on parle alors d'exploitant d'ACSSI). Bien qu'ils restent responsables de la gestion des ACSSI au niveau de leur entité, ils s'appuient sur un de leur personnel, sous réserve qu'il soit formé, pour remplir tout ou partie des missions qui leur sont dévolues vis-à-vis des ACSSI. Ce personnel assure alors la fonction d'**agent de sécurité des ACSSI** et fait partie de la chaîne fonctionnelle ACSSI.

2.3. **RÔLES PARTICULIERS.**

*2.3.1. **Responsabilités vis-à-vis de l'Organisation du traiter de l'Atlantique nord, de l'Union Européenne et des alliés.***

La *National Distribution Agency* (NDA) est responsable de la gestion centralisée (limitée à la traçabilité) du matériel et des informations cryptographiques mis à disposition par l'OTAN pour les armées. Son périmètre est élargi aux matériels équivalents de l'Union Européenne et des autres partenaires étrangers.

Pour des systèmes particuliers, le périmètre (par exemple hors du ministère) de la NDA peut faire l'objet de directives spécifiques et l'octroi de ressources complémentaires.

En revanche, les moyens agréés par les organisations précitées mais acquis par l'administration française ou produits par elle, ne rentrent pas dans le cadre de cette gestion mais sont du ressort de la gestion « classique » des biens (exemple : gestionnaires de biens pour les biens non classifiés) et des informations en fonction de

leur classification et des délégations consenties.

L'action de la NDA s'inscrit uniquement vis-à-vis de l'acheminement et de la prise en compte des moyens et ne couvre pas leur emploi. Ainsi les demandes vers les autorités de contrôle ne lui incombent pas, cependant elle peut, grâce à son réseau, apporter son concours pour faciliter les échanges.

La NDA s'assure que des procédures appropriées sont appliquées et des filières établies pour que l'ensemble de ces matériels fasse l'objet d'une comptabilisation complète et soit manipulé, conservé, et distribué dans les conditions de sécurité (6) prévues.

Conformément au [SDIP293/1] pour l'OTAN et au [TECH-I01] pour l'Union Européenne, la NDA doit notamment, sur le périmètre élargi des équivalents ACSSI de l'OTAN, de l'UE et des autres partenaires étrangers :

- assurer la comptabilité des matériels et informations cryptographiques pris en compte ;

- s'assurer des contrôles réglementaires des matériels et informations cryptographiques détenus ;

- pouvoir accéder aux informations relatives à la position géographique et à l'état pour chacun des matériels et informations cryptographiques ;

- inspecter ou contrôler les chaînes fonctionnelles ACSSI concernées tous les ans.

Le rôle de NDA est assuré par la DIRISI. Le commandement des réseaux particuliers de l'armement (CRPA) peut se voir confier une partie des responsabilités, notamment au profit des industriels.

*2.3.2. **Rôle particulier du commandement des réseaux particuliers de l'armement.***

Le commandement des réseaux particuliers de l'armement (CRPA) de la DGA est le gestionnaire central des ACSSI mis à disposition de la DGA et des industriels de l'armement. Vis-à-vis des industriels, il faut distinguer les principaux cas suivants :

a) mise à disposition auprès d'industriels d'ACSSI de propriété DGA dans le cadre d'un contrat DGA (7):

Les termes de la mise à disposition (responsabilités, transport, restitution …) doivent être prévus dans le contrat et son annexe de sécurité (ou au travers du CAC armement).

Le CRPA assure la gestion centralisée des ACSSI. La gestion logistique des biens mis à disposition est assurée par le gestionnaire de biens DGA qui contrôle ces biens.

b) mise à disposition auprès d'industriels d'ACSSI de propriété non DGA dans le cadre d'un contrat DGA (7) :

Les clauses de mise à disposition applicables sont celles du contrat et de son annexe de sécurité (et du CAC armement), elles sont étudiées en amont de la notification du contrat avec le service propriétaire des ACSSI.

Le gestionnaire central ACSSI reste celui d'origine. Le CRPA est responsable devant ce dernier de la traçabilité des ACSSI mis en place chez les industriels. Dans ce cadre il rendra destinataire le gestionnaire central ACSSI d'origine des contrôles qu'il effectue en application des directives du gestionnaire central ACSSI d'origine. Vis-à-vis de ce dernier, le CRPA assure alors le rôle de gestionnaire local pour remise au Gestionnaire central ACSSI de l'entreprise dénommé ACC (Agent Chiffre Central). La gestion logistique des biens reste de la responsabilité du gestionnaire de biens d'origine.

c) acquisition d'ACSSI par l'industriel dans le cadre de ses activités au profit de la défense :

L'industriel doit faire une demande d'acquisition et d'exploitation auprès du CRPA. Le CRPA, après vérification du bien-fondé validera la demande et assurera la traçabilité de mise à disposition auprès de l'industriel détenteur de ces ACSSI. L'industriel est responsable d'assurer leur traçabilité au sein de son entreprise.

2.3.3. ***Rôle particulier du centre de transmissions gouvernemental.***

Le centre de transmission gouvernemental assure nominalement le transport des ACSSI (ou équivalent étrangers) vers les postes permanents à l'étranger, hormis ceux de la DPSD.

2.4. SYNTHESE SUR LA CHAÎNE FONCTIONNELLE DES ARTICLES CONTRÔLÉS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.

La chaîne fonctionnelle ACSSI du ministère est constituée par la réunion des chaînes fonctionnelles ACSSI globalement indépendantes, spécifiques, mises en place par chaque autorité qualifiée afin d'assurer le suivi en gestion des ACSSI mis en œuvre par les entités subordonnées.

Elle est complétée d'un échelon circonstanciel de coordination central qui dispose au besoin d'une vision ministérielle sur l'ensemble des ACSSI. Cet échelon n'est activé et désigné que dans la gestion des incidents concernant plusieurs autorités qualifiées, et éventuellement sur saisine du HFCDS pour d'autres sujets.

Une autorité qualifiée peut décider de déléguer la gestion de ses ACSSI à une autre autorité qualifiée du ministère de la défense. L'autorité qualifiée délégataire doit tenir à jour la liste des délégations réalisées.

3. SUIVI EN GESTION DES DES ARTICLES CONTRÔLÉS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.

La fonction de suivi et de traçabilité des ACSSI est réalisée pour chaque autorité qualifiée au sein de la chaîne fonctionnelle ACSSI au niveau central à partir des informations remontées par :

- le ou les niveaux locaux de la chaîne fonctionnelle ACSSI, *a minima* pour les ACSSI classifiés ;

- la ou les structures qui se sont vues déléguer la gestion d'ACSSI non classifiés.

Les utilisateurs d'ACSSI sont responsables du suivi au niveau de leur entité. Par exemple, lorsqu'ils décident de faire prendre en compte un ACSSI à un personnel de leur entité, ils informent leur agent de sécurité des ACSSI qui assure alors le suivi au niveau de l'entité.

3.1. Définition du suivi.

Le suivi d'un ACSSI consiste à :

- pouvoir déterminer la position géographique d'un ACSSI à tout instant ;

- pouvoir déterminer l'exploitant, l'utilisateur, le comptable ou le gestionnaire central d'un ACSSI à tout instant (à partir des actes de comptabilité ACSSI) ;

- pouvoir déterminer précisément la version matérielle et logicielle d'un ACSSI ;

- pouvoir déterminer le statut d'un ACSSI, notamment pour un bien matériel (bien en exploitation, bien disponible, bien non disponible et ses sous-statuts, conformément à [ARRGESTLOG]), l'applicabilité de ce statut étant étendu aux informations ACSSI pour lesquelles cela est pertinent.

La traçabilité est l'historisation du suivi pendant toute la vie d'un ACSSI. Elle doit être assurée (cf. point 3.4.).

3.2. **Principes généraux.**

Il convient de distinguer le suivi en gestion des moyens et informations ACSSI classifiés de défense de celui des moyens et informations ACSSI non classifiées de défense.

1. Les moyens ou informations ACSSI classifiés de défense sont suivis en gestion centralisée, sans dérogation possible au travers du système d'information de gestion des ACSSI. Tout mouvement d'un ACSSI classifié est soumis à accord préalable du gestionnaire central ACSSI de l'autorité qualifiée concernée.

2. Les moyens ACSSI non classifiés de défense peuvent, sur délégation d'une autorité qualifiée, être suivis en gestion locale (au sens du suivi ACSSI) par les gestionnaires logistiques de biens du ministère de la défense qui assurent, conformément à [ARRGESTLOG], la gestion patrimoniale et logistique de ces biens. S'il y a délégation, la gestion logistique se substitue à la gestion ACSSI. Les autorités qualifiées doivent tenir à jour la liste des délégations qu'elles réalisent et les communiquer à leur gestionnaire central.

3. Les informations ACSSI non classifiées de défense sont, par principe, suivies en gestion centralisées à l'exception de celles utilisées pour les réseaux de chiffrement tactiques qui peuvent être suivies en gestion locale sur décision de l'autorité qualifiée responsable de ces informations ACSSI.

Les biens classés ACSSI s'inscrivent dans le périmètre des biens matériels des différents gestionnaires de biens. Ils sont clairement identifiés par un marquant spécifique dans les systèmes d'information logistique et permettent tout échange d'information entre le gestionnaire de bien et la chaîne ACSSI.

3.3. **Prêts ou mise à disposition d'articles contrôlés de la sécurité des systèmres d'information .**

Le suivi des ACSSI mis à disposition ou prêtés au sein du ministère suit les principes ci-après :

- Pour un ACSSI classifié ou un l'ACSSI dont la gestion n'a pas été déléguée à un échelon intermédiaire, le suivi est réalisé par le gestionnaire central ACSSI unique de l'autorité qualifiée d'origine (autorité qui prête le bien) ;

- Pour un moyen ACSSI dont la gestion est déléguée, conformément à [INSGESTLOG], le gestionnaire de biens d'origine continue d'en assurer la gestion et donc le suivi ;

- Pour une information ACSSI dont la gestion est déléguée, si le destinataire a lui-même reçu délégation de son autorité qualifiée pour gérer des ACSSI, le suivi est réalisé par le destinataire. En revanche, si le destinataire n'a pas reçu délégation de son autorité qualifiée pour gérer des ACSSI, l'ACSSI passe en gestion centrale.

Quoi qu'il en soit, tout ACSSI déployé en dehors du ministère fera l'objet d'un suivi centralisé (notamment lors du prêt entre ministères d'un équipement de chiffrement pour des besoins opérationnels temporaires). Ce suivi sera réalisé par le gestionnaire central ACSSI de l'autorité qualifiée d'origine.

Le cas particulier des prêts d'ACSSI aux industriels dans le cadre d'un développement au profit d'un projet ou d'un programme d'armement est traité au point 2.3.2.

3.4. **Modalités de suivi.**

3.4.1. ***Systèmes d'information de suivi des articles contrôlés de la sécurité des systèmres d'information.***

Si leur suivi a été délégué, les moyens ACSSI non classifiés sont suivis dans les systèmes d'information logistique des gestionnaires de biens.

Afin d'assurer le suivi de l'ensemble des ACSSI sous la responsabilité de son autorité qualifiée, le gestionnaire central ACSSI dispose d'un accès aux systèmes d'information logistiques des gestionnaires de biens pour les biens ACSSI ou peut *a minima* solliciter les échelons intermédiaires pour obtenir les informations de suivi qui lui sont nécessaires, et ce jusqu'au niveau utilisateur (au sens de l'[ARRGESTLOG]).

Pour chaque autorité qualifiée, les ACSSI dont la gestion n'a pas été déléguée sont suivis dans un système d'information de gestion des ACSSI dédié, sous la responsabilité du gestionnaire central ACSSI unique. L'exploitation de ce système d'information est réalisée par la chaîne fonctionnelle ACSSI de l'autorité qualifiée (8). La base de données de ce système d'information est classifiée au minimum CONFIDENTIEL DÉFENSE (9).

Les données de traçabilité doivent être disponibles à tout moment.

Même dans le cas d'une gestion locale, le gestionnaire central ACSSI d'autorité qualifiée doit être en mesure de connaître directement au travers des systèmes d'information *ad hoc* :

- les ACSSI présents sur un site particulier ;

- l'affectation d'un ACSSI particulier, son utilisateur (au sens de l'[ARRGESTLOG]) ;

- les utilisateurs successifs d'un ACSSI particulier (au sens gestion logistique des biens) ;

- pour les informations ACSSI, la distribution réalisée.

3.4.2. ***Lots.***

Le suivi des ACSSI peut se faire individuellement ou par lot constitué (par exemple, un lot de plusieurs ACSSI identiques conditionnés de manière à garantir globalement leur intégrité ou une unité collective composée de plusieurs ACSSI comme les dispositifs de transfert de clés dont l'unité collective comprend un DTC (10) associé à un ou plusieurs CIK (11) qui sont ACSSI). Lorsque le lot est éclaté, le suivi devient individuel. Il faut donc s'assurer que les composants puissent être suivis dans les systèmes d'information logistiques des gestionnaires de biens.

3.4.3. ***Composants cryptographiques.***

Les composants (12) cryptographiques intégrés par des équipementiers français font l'objet d'un suivi particulier indépendant de la gestion centralisée ou locale des ACSSI. La gestion de ces composants est centralisée et est assurée par la DGA.

Le suivi spécifique doit également être en mesure d'indiquer la configuration actuelle (les composants étant de plus en plus programmables leur interchangeabilité nécessite de bien maitriser leur configuration) mais aussi les configurations successives du composant. Lorsqu'un composant est changé, la DGA en est informée *via* les gestionnaires centraux des autorités qualifiées.

3.4.4. ***Identifiant unique.***

Tout ACSSI est suivi de manière unitaire dans les systèmes d'information assurant la fonction de suivi. En conséquence, l'identification d'un bien ACSSI matériel est réalisée à partir de son NNO (13) ou du couple référence constructeur/code article lorsque le NNO n'existe pas, suivi de son numéro de série.

3.4.5. ***L'entrée en suivi des articles contrôlés de la sécurité des systèmres d'information.***

L'entrée en suivi des ACSSI résulte de :

- sa prise en compte par un des gestionnaires centraux (ou par un échelon intermédiaire si la délégation le prévoit) lors de l'acquisition d'un matériel ACSSI auprès d'un constructeur, la prise en compte d'un ACSSI relevant d'une autre chaîne fonctionnelle ACSSI ou d'un partenaire étranger, *etc.* ;

- de sa création (création d'un document ACSSI, gravure d'un CD-ROM contenant un logiciel/fichier ACSSI…) ;

- de sa génération (génération d'une clé (14) par un centre d'élaboration des clés…).

3.4.6. ***Le suivi des articles contrôlés de la sécurité des systèmres d'information.***

Les transactions suivantes doivent être tracées :

- entrée en suivi ;

- transfert d'un comptable ACSSI vers un autre (appartenant ou non à la même chaîne fonctionnelle ACSSI), ou d'un comptable ACSSI vers un gestionnaire central ACSSI ;

- inventaire ;

- réception d'un ACSSI délivré par un comptable ACSSI à un utilisateur, ou reversé par un utilisateur à un comptable ACSSI ;

- maintenance (incluant les mises à jour) ;

- sortie du suivi (destruction, …).

Ces informations doivent *a minima* se retrouver dans les modèles mis en place par chaque chaîne fonctionnelle ACSSI.

Une fois remplies, ces pièces sont les éléments constitutifs de la comptabilité ACSSI.

3.4.7. ***La sortie du suivi des articles contrôlés de la sécurité des systèmres d'information.***

La sortie du suivi d'un ACSSI résulte de sa réforme, de sa destruction selon les procédures réglementaires, de sa disparition (suite à une perte, un vol, …) une fois cet incident traité, du retrait de la mention ACSSI dans le cas particulier des documents, ou de son archivage.

La sortie du suivi ne signifie pas que les données du suivi sont supprimées. En effet, les données de traçabilité doivent être conservées selon les modalités suivantes :

- ACSSI TSD : minimum 10 ans après la sortie de suivi ;

- ACSSI SD : minimum 5 ans après la sortie de suivi ;

- ACSSI CD et non classifiés : minimum 3 ans après la sortie de suivi.

Les durées de conservation effectives et les dérogations à cette règle sont instruites par les autorités qualifiées.

Dans le cas d'une disparition la date du constat de la disparition sera identifiée dans le suivi ainsi que la date de son éventuelle « récupération ».

La sortie du suivi d'un ACSSI est prononcée par les gestionnaires centraux ACSSI ou par l'échelon intermédiaire en cas de délégation.

Dans les cas de déficits constatés après recensement, de pertes/vols, de destructions et de certaines détériorations, les gestionnaires centraux ACSSI prononcent la sortie de l'ACSSI du suivi. La sortie du suivi peut être prononcée par l'échelon intermédiaire sur délégation.

Dans le cas des ACSSI détruits volontairement suite à l'emploi du système les embarquant (missile notamment), seule une sortie du suivi est réalisée en précisant une mention permettant de déterminer facilement la raison du retrait (« missile tiré » par exemple). Aucun autre document n'est exigé (compte-rendu de perte par exemple).

4. LA GESTION DE L'ACCÈS AUX DES ARTICLES CONTRÔLÉS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.

4.1. **Principes.**

La sensibilité particulière d'un moyen ou d'une information, qui a conduit à le déclarer ACSSI, doit être portée à la connaissance de son utilisateur et du personnel chargé de la mise à jour de la base de données des systèmes d'information logistiques ou des systèmes d'information gérant les ACSSI. Pour les utilisateurs d'ACSSI classifiés, ceci est réalisé au travers d'une procédure de décision d'accès aux ACSSI. Celle-ci doit lui permettre d'engager sa responsabilité concernant ce moyen ou cette information.

En principe, tous les acteurs amenés à développer, manipuler, gérer les ACSSI ou interagir avec eux doivent avoir fait l'objet d'une décision d'accès aux ACSSI, notamment :

- les concepteurs (développeurs, chargés d'étude, évaluateurs …) ;

- les techniciens (techniciens de maintenance, opérateurs d'assemblage, opérateurs d'injection, administrateurs de fonctions de sécurité, …) ;

- les responsables du suivi local ou central des ACSSI ;

- les manutentionnaires manipulant des ACSSI classifiés et non colisés ;

- les utilisateurs ou exploitants d'ACSSI classifiés.

Ces derniers bénéficient d'une attestation de formation à la manipulation des ACSSI. Le contenu de la formation, délivrée par l'agent de sécurité des ACSSI de son entité, doit intégrer :

- la manipulation de l'ACSSI ;

- une présentation des procédures d'urgence ;

- un rappel des sanctions administratives encourues par l'utilisateur ou l'exploitant en cas de perte ou d'incident non déclaré ou de toute négligence menaçant la sécurité des moyens et informations mis à disposition.

L'attestation de formation à l'utilisation des ACSSI comporte une reconnaissance de sensibilisation signée par l'utilisateur ou l'exploitant et délivrée lors de la prise en compte de l'ACSSI.

Des exceptions peuvent figurer dans l'agrément ou la décision d'homologation.

4.2. **Conditions de délivrance de la décision d'accès aux articles contrôlés de la sécurité des systèmres d'information.**

La délivrance d'une décision d'accès aux ACSSI n'est possible que si son bénéficiaire :

- est titulaire d'une décision d'habilitation aux informations classifiées de défense au bon niveau dans le cas où ces actions concernent des ACSSI classifiés ou dont les informations manipulées sont classifiées ;

- a besoin, en raison de son emploi ou de sa fonction, de manipuler ou de détenir des informations concernant les ACSSI (« besoin d'en connaître ») ou des ACSSI (« besoin d'usage ») ;

- a reçu une formation à l'usage (15) des ACSSI détenus dans le cadre de son emploi, qui inclut nécessairement un socle commun composé de :

  - la conduite à tenir en cas d'incident de sécurité (importance du compte rendu immédiat et des opérations préventives pour limiter l'impact),

  - la destruction des moyens ou l'effacement d'urgence des informations confiées.

La formation doit être adaptée aux risques auxquels l'ACSSI est exposé, ainsi qu'à son contexte d'emploi. L'attestation de formation à la manipulation des ACSSI est délivrée sur ce même socle.

4.3. **Modalités de délivrance de la décision d'accès aux articles contrôlés de la sécurité des systèmres d'information.**

Sous réserve de satisfaire aux trois conditions visées au point précédent, une décision d'accès aux ACSSI (16) est délivrée pour une période maximale de cinq ans renouvelable selon les besoins, attestant d'un niveau minimum de connaissances pour l'emploi tenu ou l'usage envisagé. Dès lors que le titulaire ne remplit plus les conditions de sécurité requises, la décision d'accès aux ACSSI doit lui être immédiatement retirée.

À l'occasion de certaines missions spécifiques (inspections, convoyages, *etc.*), une décision d'accès temporaire aux ACSSI peut être délivrée au demandeur. La durée de validité est précisée sur la décision.

Les décisions d'accès aux ACSSI ne sont pas protégées. Chaque entité tient à jour un état des décisions en vigueur concernant son personnel.

La délivrance et le retrait des décisions d'accès aux ACSSI sont de la responsabilité de chaque autorité qualifiée du ministère. Elle peut déléguer ces fonctions au chef de l'entité d'appartenance du personnel concerné. L'agent de sécurité des ACSSI est responsable du suivi des décisions d'accès aux ACSSI du personnel de son entité.

Concernant les opérateurs d'importance vitale du secteur privé relevant du ministère de la défense et les entreprises sous contrat avec le ministère, la formation à l'usage des ACSSI et la délivrance des décisions d'accès aux ACSSI est de la responsabilité de chaque autorité qualifiée avec délégation possible à leur gestionnaire central d'ACSSI.

5. MANIPULATION DES DES ARTICLES CONTRÔLÉS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.

5.1. **Marquage des articles contrôlés de la sécurité des systèmres d'information matériels.**

Sauf dérogation éventuelle, explicitement précisée dans l'agrément de sécurité du dispositif ou dans la décision d'homologation du système mettant en œuvre le dispositif, les ACSSI font l'objet d'un marquage indélébile placé à proximité de la mention de classification (CD, SD ou TSD) ou de protection (DR). Les ACSSI non protégés sont uniquement marqués ACSSI NP. La mention ACSSI est apposée définitivement et s'applique tout au long du cycle de vie des moyens et informations, depuis leur conception jusqu'à leur destruction.

L'apposition du marquage doit prendre en compte la nature des équipements et des supports d'information. Elle doit toutefois, sauf dérogation, respecter les principes suivants :

- le timbre ACSSI de couleur rouge doit être gravé, imprimé ou apposé par étiquette indécollable sur les équipements ;

- les supports électroniques ACSSI doivent être identifiés ;

- les documents ACSSI doivent être paginés et identifiés (17) ;

- le marquage doit être adapté à l'emploi opérationnel des matériels. Il peut être invisible de l'extérieur si les conditions d'utilisation du matériel le justifient.

5.2. **Protection des articles contrôlés de la sécurité des systèmres d'information tout au long de leur cycle de vie.**

5.2.1. ***Conception et production industrielle.***

Certains moyens et informations peuvent recevoir la mention ACSSI à l'initiative de la maîtrise d'ouvrage, de la maîtrise d'œuvre, de l'autorité d'homologation ou du donneur d'ordre si ces derniers estiment que les risques lors du développement ou de tout autre phase du projet seront mieux couverts à l'aide de cette mention.

Chaque décision fera l'objet d'une transmission vers l'ANSSI *via* le FSSI.

Cette initiative ne remplace pas les processus d'agrément ou d'homologation qui doivent être conduits par ailleurs. Le cycle de vie antérieur à l'agrément pourra être examiné pour la délivrance de celui-ci.

Tout contrat d'étude et de développement d'un moyen :

- déclaré ACSSI ;

- susceptible d'être ACSSI ou intégrant des ACSSI ;

et susceptible de protéger des informations classifiées, doit comporter une annexe de sécurité. Les informations qui doivent y figurer sont énumérées à l'annexe 3.

En outre, le contrat doit comporter des clauses interdisant les possibilités de réutilisation des ACSSI ou des composants, fonctions et technologies spécifiques de l'ACSSI, sans accord de l'autorité contractante. Un avis d'opportunité peut être demandé à l'ANSSI par l'autorité contractante avant de donner un tel accord.

5.2.2. ***L'acheminement des articles contrôlés de la sécurité des systèmres d'information.***

Le terme « transmission » désignera par la suite un transfert d'informations sous forme électronique. Le terme « transport » désignera par la suite un transfert physique. Le terme « acheminement » désignera par la suite une transmission ou un transport.

L'acheminement induisant un risque supplémentaire, il convient de prendre connaissance des agréments de sécurité, des accords de sécurité (dans le cas d'un transport vers l'étranger), des annexes de sécurité et des instructions d'emploi des ACSSI concernés, avant d'arrêter toute forme de transport ou de transmission.

Sauf contrainte opérationnelle, un plan de transport sera rédigé préalablement à tout acheminement hors métropole (il est facultatif pour les acheminements en métropole). Il formalise, entre l'expéditeur et le destinataire, l'itinéraire, les conditions de transport et prend ainsi en compte les risques spécifiques à chaque envoi. Dans le cadre de contrats avec les industriels (cf. 2.3.2), les annexes de sécurité doivent inclure les

plans de transport envisagés.

Les mesures à mettre en œuvre pour l'acheminement des ACSSI doivent permettre de contrôler, à chaque étape, la bonne réception (préavis d'envoi, justificatif de délivrance, accusé de réception) et l'intégrité du contenu.

5.2.2.1. Le transport des articles contrôlés de la sécurité des systèmres d'information matériels.

Le transport (18) d'un ACSSI est un changement de localisation géographique impliquant un changement d'utilisateur ACSSI, de comptable ACSSI ou de gestionnaire central ACSSI au profit d'un autre utilisateur ACSSI, comptable ACSSI ou gestionnaire central ACSSI.

Il est consécutif à un acte de gestion formalisé.

Pour tout transport, que les ACSSI soient classifiés ou non, les mesures suivantes doivent être appliquées :

- Les clés et dispositifs de sécurité amovibles nécessaires au fonctionnement d'un moyen ACSSI doivent être retirés, être conditionnés séparément et si possible faire l'objet d'un envoi séparé ;

- S'il apparaît qu'un colis a été ouvert ou manipulé anormalement, un incident de sécurité doit être déclaré et l'émetteur du colis doit en être informé dans les plus brefs délais. Le colis est écarté et mis sous scellés. Le FSSI doit être informé. Il peut décider de renvoyer le moyen ACSSI vers DGA-MI pour expertise.

5.2.2.1.1. Transport des articles contrôlés de la sécurité des systèmres d'information classifiés.

Ils sont transportés conformément à l'[IM900] (19).

Par exception, si le colis contenant les moyens et informations est acheminé dans un conteneur agréé, le convoyeur n'est pas tenu de le conserver sous sa surveillance permanente et directe, notamment lors des passages en douane.

Le convoyeur dispose d'une lettre de courrier dans le cas d'un acheminement vers l'étranger.

5.2.2.1.2. Transport des articles contrôlés de la sécurité des systèmres d'information non classifiés.

Ces ACSSI sont transportés en métropole conformément aux annexes de l'[IM900] traitant du diffusion restreinte, y compris pour les ACSSI non protégés.

En métropole, l'emploi de conteneurs sécurisés est recommandé sous réserve de respecter la procédure [DT404329]. Il est obligatoire pour les ACSSI acheminés hors métropole en raison des contraintes spécifiques liées au transit à l'étranger. Les opérations suivantes sont tracées lors de ces transports :

- prise en compte du colis (dépôt du colis auprès de l'organisme transporteur) ;

- passage aux douanes (le cas échéant) ;

- remise du colis au destinataire ;

- message à l'expéditeur attestant de la bonne réception du colis et de son intégrité.

Le transport en conteneur sécurisé homologué par une autorité qualifiée ne nécessite pas de convoyeur.

5.2.2.1.3. Transport simultanés des clés et des équipements.

Il est possible de transporter ensemble l'équipement et les clés qui lui seront associées (ou un équipement à la clé) à condition que la révocation des clés puisse être effectuée sans impact sur d'autres équipements en service.

5.2.2.2. La transmission des articles contrôlés de la sécurité des systèmres d'information immatériels.

La transmission des ACSSI immatériels comprend toutes les opérations de distribution d'un paramètre de pré-personnalisation ACSSI ou d'un ES (20) vers les différents abonnés d'un réseau de chiffrement, jusqu'à l'injection dans l'équipement, et l'émission d'un document informatique ACSSI vers un ou plusieurs destinataires.

La transmission des ACSSI immatériels est assurée par les gestionnaires centraux ACSSI, les comptables ACSSI et les utilisateurs ACSSI.

Les opérations suivantes sont tracées lors des transmissions :

- prise en compte des données électroniques ;

- message à l'expéditeur attestant de la bonne réception du message ou de la pièce-jointe.

Le suivi de ces opérations peut être assuré soit directement au sein du système d'information, soit de manière décorrélée, par exemple au moyen d'un autre système.

La transmission des informations ACSSI s'appuie sur des systèmes homologués à cette fin.

5.3. **Utilisation et circulation.**

Lors de leur utilisation, les ACSSI doivent être manipulés conformément à leur classification et/ou à la classification des informations qu'ils protègent. Des mesures particulières, liées notamment aux conditions d'emploi, peuvent figurer dans les décisions d'agrément ou d'homologation. Elles sont alors déclinées dans les instructions techniques d'emploi, les procédures d'exploitation de la sécurité et les manuels d'utilisation ou d'administration.

Certains ACSSI (chiffreur isolé, équipements portables dont sont dotés les utilisateurs : téléphone chiffrant, document, notamment) peuvent être transportés par l'opérateur ou l'utilisateur lui-même (21). Dans ce cas, les conditions précises sont définies dans les instructions d'emploi des équipements et sont communiquées aux utilisateurs.

5.4. **Stockage des moyens des articles contrôlés de la sécurité des systèmres d'information.**

Pour les ACSSI classifiés, la protection lors des phases de stockage est conforme aux dispositions de l'[IM900] (22) et aux décisions d'agrément ou d'homologation.

Pour les ACSSI non classifiés, l'intégrité du matériel doit être garantie pendant les phases de stockage (armoires et locaux fermés à clé). Si cela est possible et raisonnable, les sous-ensembles permettant la désensibilisation sont retirés de l'équipement et conservés au plus près de l'utilisateur ou de l'exploitant ou dans des armoires ou locaux fermés à clé, conformément aux décisions d'agrément ou d'homologation.

5.5. **Maintenance.**

Les opérations de maintenance d'un moyen ACSSI doivent être soigneusement tracées. Elles font partie intégrante de l'historique de l'ACSSI.

Dans ce cadre les organismes habilités à réaliser des opérations de maintenance doivent être connus du gestionnaire central ACSSI unique ainsi que la liste des opérations autorisées par matériel (qui doivent figurer dans le plan de maintenance).

Durant ces opérations, la traçabilité doit porter sur :

- l'acheminement ;

- la gestion de l'équipement et de ses composants (réparation ou remplacement avec précision de leur configuration) ;

- la mise à jour d'éventuels composants ACSSI (reprogrammation ou remplacement) dans le suivi de l'équipement ;

- la mise à jour d'un composant logiciel ;

- le retour de l'équipement ou son stockage.

Les opérations de maintenance doivent être maîtrisées. Lors d'une opération de maintenance nécessitant l'ouverture d'un ACSSI, les éléments et données sensibles doivent être préalablement effacés ou retirés avant l'envoi vers le centre chargé de réaliser cette opération, conformément aux procédures décrites dans l'agrément ou l'homologation. Si l'effacement ou le retrait des éléments et données sensibles ne sont pas possible (par nature ou en raison d'une défaillance), l'ACSSI est manipulé et conservé au niveau de classification des éléments secrets injectés et des données qu'il a traitées avant sa mise en maintenance.

5.6. **Fin de vie.**

5.6.1. ***Destruction.***

Un moyen ou une information reste catégorisé ACSSI de sa conception jusqu'à sa destruction, sauf cas particuliers énoncés au point 3.4.7.

Lorsque cela est possible, les composants les plus sensibles doivent être séparés du reste de l'équipement en vue de leur destruction (23).

Les composants cryptologiques doivent être retirés des équipements et envoyés à la DGA qui se chargera de leur élimination.

Les règles de destruction diffèrent selon le type d'ACSSI : ACSSI classifié, ACSSI non classifié dont au moins un composant interne est classifié ou ACSSI non classifié dont aucun composant interne n'est classifié.

Préalablement à toute élimination physique, les biens ACSSI doivent respecter le processus administratif d'élimination décrit dans les instructions traitant de la gestion logistique des biens.

Les ACSSI classifiés sont détruits selon les procédures décrites dans l'[IM900].

Les ACSSI non classifiés dont au moins un composant interne est classifié sont détruits avec les mêmes exigences techniques que les moyens et informations Confidentiel Défense.

Dans ces deux cas, les conditions suivantes doivent être réunies :

- la personne présente pour la destruction détient une habilitation du niveau des ACSSI détruits ainsi qu'une décision d'accès aux ACSSI ;

- la personne en charge de la destruction est soit un agent de l'état dûment mandaté, soit issue d'un organisme titulaire d'un contrat classifié ou sensible pour détruire des informations ou supports

classifiés.

Les ACSSI non classifiés dont aucun composant interne n'est classifié sont détruits sous le contrôle visuel d'un agent de l'état dûment mandaté.

Le procès-verbal de destruction doit être cosigné par les deux personnes présentes au moment de la destruction. Dans le cas d'un moyen, le procès-verbal mentionne également les éventuels composants ou sous-ensembles eux-mêmes ACSSI.

Une procédure de destruction d'urgence de chaque type d'ACSSI est établie lors de la phase de conception du système d'information en fonction des menaces potentielles liées aux contextes d'emploi ou qui pèsent sur les ACSSI eux-mêmes. Validée par l'autorité d'homologation, sa connaissance est une condition nécessaire à la délivrance de l'attestation de formation et de la décision d'accès aux ACSSI si l'exploitant n'en dispose pas (cf. point 4.).

5.6.2. ***Autres cas.***

Certains ACSSI peuvent être amenés à être volontairement abandonnés (par exemple un chiffreur embarqué dans un missile ou un capteur abandonné sur le terrain) ou non maîtrisés en permanence avec parfois de fortes probabilités de perte (par exemple un chiffreur dans un satellite). L'agrément ou l'homologation doit décrire les procédures permettant de gérer ces événements sans entrainer nécessairement d'incident de sécurité.

La mention ACSSI peut ne plus être pertinente sur certains documents. Il est alors possible, après autorisation de l'autorité ayant décidé de l'attribution initiale de cette mention, de ne plus considérer un document comme ACSSI. Il est alors sorti du suivi, les données de traçabilité étant conservées. Le document doit faire l'objet d'un marquage précisant que la mention a été retirée et faisant référence à la décision de retrait sur sa première page.

6. CONTROLES ET INSPECTIONS.

6.1. **Inspections.**

Des inspections programmées ou inopinées doivent être menées à l'initiative de chaque autorité qualifiée. Elles sont réalisées par du personnel n'appartenant pas à la chaîne fonctionnelle ACSSI de l'autorité qualifiée concernée. Elles témoignent de la bonne tenue et de l'efficacité du suivi spécifique et du respect des mesures de protection, d'installation et d'exploitation de ces ACSSI. Les modalités de ces inspections sont précisées dans la directive de gestion des ACSSI de chaque autorité qualifiée.

L'inspection doit se limiter à des constats visuels, sans porter atteinte à l'intégrité ou aux fonctions de sécurité des ACSSI. Il s'agit en effet d'une inspection relative à la gestion des ACSSI et non au chiffre.

En complément, les inspections des ministères réalisées par l'ANSSI peuvent intégrer un volet relatif aux ACSSI. À cette occasion, l'ANSSI peut demander à se faire remettre la directive de gestion des ACSSI de l'autorité concernée ainsi que tout document de mise en œuvre des ACSSI inspectés (24).

La liste des processus qui doivent être analysés est la suivante :

- la conservation, la manipulation et le transport des ACSSI ;

- les ordres de mises en place, les annexes de sécurité ;

- la vérification de la présence effective d'un échantillonnage (25) d'ACSSI en compte au sein de l'entité ;

- la protection des locaux et la sécurité des installations ;

- les habilitations, décisions d'accès aux ACSSI ainsi que les attestations de formation et reconnaissance de sensibilisation des personnels manipulant des ACSSI ;

- la rédaction de la documentation afférente à la gestion et à l'utilisation des ACSSI ;

- le soutien, la maintenance et le suivi des évolutions de configuration des ACSSI ;

- la vérification des procès-verbaux des inventaires réalisés au titre du contrôle interne de l'entité ;

- la traçabilité des composants cryptographiques ;

- la destruction des ACSSI.

Certains objectifs propres à chaque autorité qualifiée peuvent être ajoutés aux motifs de l'inspection, mais l'inspection doit avant tout être menée pour s'assurer que le suivi est fait conformément aux directives (centrale et d'autorité qualifiée) et qu'il n'existe pas de risque particulier de compromission lié à la manière dont les ACSSI sont mis en œuvre dans leur contexte d'emploi particulier.

L'inspection peut porter sur l'organisation de la gestion des ACSSI en local, sur le lien entre le niveau local et le niveau central, sur l'organisation mise en place par les échelons intermédiaires pour gérer les ACSSI en cas de délégation ainsi que sur la manière dont les ACSSI sont suivis et mis en œuvre.

La fréquence des inspections est laissée à l'appréciation des autorités qualifiées. Elles doivent néanmoins leur permettre de disposer d'une bonne appréciation de la sécurité entourant les ACSSI sous leur responsabilité.

6.2. **Le contrôle des articles contrôlés de la sécurité des systèmres d'information.**

La gestion des ACSSI d'une entité doit faire l'objet d'un contrôle régulier. Ces opérations doivent permettre de :

- s'assurer de la bonne tenue et de l'efficacité du suivi spécifique des ACSSI ;

- du respect des mesures d'utilisation et de protection de ces derniers ;

- de la présence effective des ACSSI détenus par l'entité, y compris des composants cryptographiques de rechange le cas échéant (non intégrés dans un matériel).

Le contrôle de la gestion des ACSSI d'une entité est réalisé par :

- la chaîne commandement au titre du contrôle interne ;

- la chaîne fonctionnelle ACSSI.

Les contrôles réalisés par ces deux chaînes sont complémentaires et, dans la mesure du possible, ne se recouvrent pas.

Les opérations de contrôle interne logistique se substituent au contrôle ACSSI dans le cas de matériels ACSSI dont la gestion a été déléguée. Pour les informations ACSSI dont la gestion a été déléguée, le contrôle est de la responsabilité de l'échelon intermédiaire.

6.2.1. ***Contrôle des articles contrôlés de la sécurité des systèmres d'information exercé par la chaîne commandement.***

Le commandement, par nature, a des responsabilités en matière de contrôle. Celui-ci, réalisé au titre du contrôle interne, porte sur :

- la protection des locaux et la sécurité des installations abritant des ACSSI ;

- l'application des règles et instructions d'emploi des ACSSI ;

- les habilitations, décisions d'accès aux ACSSI ainsi que les attestations de formation et de reconnaissance de sensibilisation des personnels manipulant des ACSSI ;

- l'observation des règles relatives à la conservation, la manipulation et au transport des ACSSI, notamment ceux qui sont protégés ;

- la vérification de la présence effective des ACSSI en compte au sein de l'entité au titre d'un inventaire périodique.

Les contrôles internes sont réalisés au moins une fois par an.

Le contrôle interne de deuxième niveau contrôle le dispositif de contrôle interne de premier niveau. Il est assuré par les autorités fonctionnelles des entités et porte plus spécifiquement, au titre des ACSSI, sur la vérification de l'existence des opérations de contrôles citée dans ce point.

6.2.2. ***Contrôle exerce par la chaîne fonctionnelle des articles contrôlés de la sécurité des systèmres d'information.***

La chaîne fonctionnelle ACSSI contrôle les entités mettant en œuvre ou possédant des ACSSI. Le contrôle porte sur :

- la documentation afférente à la gestion et à l'utilisation des ACSSI rédigée par la formation ;

- le soutien et la maintenance des ACSSI ;

- la présence physique d'un échantillonnage (26) d'ACSSI de l'entité et la vérification de leur état ;

- la vérification des procès-verbaux des inventaires réalisés au sein de l'entité ;

- la traçabilité des composants cryptographiques ;

- la destruction des ACSSI.

Ce contrôle est réalisé sous mandat du gestionnaire central ACSSI. Il porte sur tout type d'ACSSI (moyens ou informations).

Dans un souci de rationalisation, les contrôles réalisés au titre de la gestion des ACSSI par la chaîne fonctionnelle ACSSI peuvent être combinés aux contrôles portant sur le chiffre (contrôle des réseaux de chiffrement).

7. LA GESTION DES INCIDENTS.

7.1. **Définitions.**

Selon l'[II910], un incident de sécurité est un événement indésirable ou inattendu présentant une probabilité forte de porter atteinte à la confidentialité, l'intégrité ou la disponibilité des informations ou des systèmes protégés par les ACSSI.

Un incident de sécurité peut ou non conduire à une compromission. En revanche, une compromission est nécessairement tracée sous la forme d'un incident de sécurité.

Dans la suite ne sont considérés que les incidents affectant un ACSSI.

7.2. **Principes.**

La gestion des incidents est réalisée selon trois aspects :

- un aspect technique, traité par la chaîne fonctionnelle ACSSI ;

- un aspect opérationnel, traité directement par le niveau central de la chaîne fonctionnelle ACSSI (27) et, le cas échéant, par les autorités d'emploi des réseaux de chiffrement concernés par l'incident ;

- un aspect commandement, traité par la chaîne commandement.

Le périmètre de la présente directive ne recouvre que l'aspect technique des incidents et ne traite pas des fautes de chiffrement, ces dernières devant être essentiellement traitées sous les aspects opérationnels et commandement.

Les incidents de sécurité peuvent être divisés en 3 types :

- les fautes de chiffrement (dont certaines peuvent entraîner une compromission) ;

- les incidents de conservation (dont certains peuvent entraîner une compromission) ;

- les incidents de gestion (la mauvaise tenue des documents de comptabilité, les corrections non effectuées ou mal effectuées, la copie non autorisée d'une information ACSSI, *etc.*). Les incidents de gestion n'entraînent pas de compromission.

7.3. **Incidents de sécurité.**

La liste des événements qui doivent obligatoirement être considérés comme des incidents de sécurité est précisée en annexe VI.

Toute personne constatant un incident de conservation ou de gestion doit faire un compte-rendu oral immédiat à son agent de sécurité des ACSSI. Ce dernier rend alors compte sous couvert de son autorité responsable, après confirmation de l'incident :

- pour un incident de gestion : au comptable ACSSI (ou à l'échelon immédiatement supérieur dans la chaîne fonctionnelle ACSSI) qui peut, selon le type d'incident de gestion, décider de le faire traiter au niveau central [28] ;

- pour un incident de conservation : au comptable ACSSI (ou à l'échelon immédiatement supérieur dans la chaîne fonctionnelle ACSSI) et au gestionnaire central ACSSI (29) ;

Le traitement des incidents est réalisé par le comptable ACSSI (ou l'échelon immédiatement supérieur dans la chaîne fonctionnelle ACSSI) ou par le gestionnaire central ACSSI. La remontée d'incident est assurée par la chaîne fonctionnelle ACSSI qui a la responsabilité de l'ACSSI considéré.

La procédure de remontée d'incident est précisée dans la directive de gestion des ACSSI de chaque autorité qualifiée.

Un inventaire des incidents sera adressé annuellement au FSSI par chaque chaîne fonctionnelle ACSSI, même en cas d'état néant. L'inventaire ministériel sera adressé à l'ANSSI.

Pour les ACSSI dont la gestion a été déléguée, tout incident de conservation est remonté *via* une chaîne mise en place par l'échelon intermédiaire. L'échelon intermédiaire rend compte au niveau central lui ayant délégué la gestion de l'ACSSI. La remontée d'un incident de gestion au gestionnaire central ACSSI concerné est laissée à la libre appréciation de l'échelon intermédiaire, sauf consigne contraire lors de la délégation de la gestion de l'ACSSI considéré.

7.4. **Mesures conservatoires.**

L'autorité d'emploi du réseau de chiffrement concernée le cas échéant ou le gestionnaire central des ACSSI concerné sinon, sont avertis sans délai. Ils décident des mesures conservatoires à prendre au plus tôt selon l'incident rapporté : révocation de l'équipement du réseau de chiffrement, changement de clé cryptographique ou toute autre mesure qu'ils jugent nécessaire pour limiter les conséquences de l'incident. Ils qualifient l'importance de l'incident en liaison avec l'autorité d'agrément ou d'homologation de l'ACSSI concerné.

7.5. **Compromissions des articles contrôlés de la sécurité des systèmres d'information.**

Une compromission d'ACSSI est un incident de sécurité concernant un ACSSI dont l'issue possible ou avérée est la divulgation d'un bien protégé par cet ACSSI à une personne non légitime, de manière fortuite ou délibérée.

Il en existe deux sortes : les compromissions directes et les compromissions indirectes

7.5.1. ***Les compromissions directes.***

C'est la connaissance directe d'un système, d'un document ou d'une information ACSSI (clé, code, logiciel…) par un tiers n'ayant ni droit, ni besoin d'en connaître. Elle résulte généralement d'un incident de conservation.

7.5.2. ***Les compromissions indirectes.***

Elles résultent de la connaissance indirecte d'un système ou d'un document ou d'une information ACSSI (clé, code, logiciel…) suite à des travaux (cryptanalyse, …) menés par un attaquant. Ces travaux sont favorisés par les fautes d'exploitation ou par l'inobservation des règles de sécurité, ainsi que par l'indiscrétion éventuelle des personnes ayant accès aux ACSSI. Elles peuvent également résulter du piégeage, d'un mauvais fonctionnement ou de la défaillance d'un matériel ACSSI.

La compromission indirecte n'est pas toujours perçue par l'utilisateur lorsqu'elle se produit. Aussi, de façon à l'éviter, il importe que le personnel fasse preuve d'une grande vigilance lors de la manipulation ou le traitement d'ACSSl. Elle peut résulter de :

- l'utilisation d'une clé de chiffrement inappropriée (défectueuse, périmée, etc.) ;

- l'introduction de parties claires dans un message chiffré ;

- le chiffrement d'un message avec un équipement dont l'algorithme est défectueux ;

- la copie ou duplication non autorisée d'information ACSSI.

7.5.3. ***Traitements des conséquences d'une compromission des articles contrôlés de la sécurité des systèmres d'information.***

Les conséquences d'une compromission d'ACSSI peuvent comporter deux aspects : la compromission de l'ACSSI lui-même, et éventuellement la divulgation possible ou avérée de biens protégés par l'ACSSI.

Concernant le premier aspect, le FSSI, qui doit être informé de toute compromission d'ACSSI, en avertit l'ANSSI.

L'ANSSI peut unilatéralement déclarer une compromission d'ACSSI concernant un matériel, un composant, un document ou un réseau. Elle s'adresse alors au FSSI afin que celui-ci lui transmette dans les plus brefs délais les éléments relatifs :

- aux utilisateurs ou exploitants dont les ACSSI sont potentiellement compromis (volume, géographie, contexte opérationnel,…) ;

- aux localisations des dispositifs déclarés compromis ;

- à la quantité des moyens ou informations déclarés compromis par site ;

- à toute autre information pertinente.

Pour les ACSSI dont la gestion aurait été déléguée, toute compromission est remontée *via* une chaîne mise en place par l'échelon intermédiaire dans les délais les plus courts. L'échelon intermédiaire rend immédiatement compte au niveau central lui ayant délégué la gestion de l'ACSSI.

Pour le second aspect, au regard de la déclaration de l'incident de sécurité, l'autorité d'emploi du réseau de chiffrement concerné le cas échéant ou le niveau central de la chaîne fonctionnelle ACSSI concernée sinon, évalue l'impact de l'incident et prononce ou non une compromission. Elle précise les actions à mener par les acteurs responsables qui, au besoin, les relaient au niveau local.

En fonction de la décision de l'autorité d'emploi du réseau de chiffrement concerné le cas échéant ou du niveau central de la chaîne fonctionnelle ACSSI concernée sinon, la DPSD est saisie conformément à l'[IM900].

7.6. **Délais de traitement des incidents.**

Les délais de traitement sont conditionnés par :

- la gravité de l'impact sur le système intégrant l'ACSSI compromis ou sur le réseau de chiffrement dont l'ACSSI est un élément ;

- les obligations vis-à-vis d'institutions internationales.

Ces délais sont fixés en annexe VI. de la présente directive.

7.7. **Retour d'expérience.**

Conformément à la [DIR_RETEX], les incidents feront l'objet d'une analyse systématique identifiant clairement les causes et les mesures correctrices associées, y compris en cas de fausses alertes.

8. ORGANISATION ET RESPONSABILITÉS RELATIVES AUX MOYENS ET INFORMATIONS ÉTRANGERS.

8.1. **Définitions.**

Les moyens et informations cryptographiques étrangers équivalents aux ACSSI sont appelés par la suite articles COMSEC (30). Leur traçabilité doit être assurée.

Les accords de sécurité relatifs à l'usage en France d'articles COMSEC requérant une gestion spécifique visant à assurer leur traçabilité, doivent mentionner que ces derniers sont gérés de la même façon que les ACSSI. Dès lors qu'ils arrivent sur le territoire national, ou dans toute zone où la réglementation nationale s'applique,

ils sont pris en compte par un personnel appartenant à la chaîne fonctionnelle ACSSI à laquelle est rattachée l'unité d'emploi du matériel.

Sur le territoire national, les articles COMSEC peuvent être sous deux positions :

- la position amont désigne la situation dans laquelle un moyen ou une information est utilisé à des fins de conception, de développement, de production, de qualification ou de maintenance industrielle (avant la mise en service opérationnelle de ce moyen) ;

- la position opérationnelle désigne la situation dans laquelle un moyen est homologué, agréé ou qualifié et exploité à des fins opérationnelles ainsi que toute situation où une information est utilisée pour servir ce moyen. Le maintien des articles COMSEC en conditions opérationnelles et le maintien en conditions de sécurité relèvent de la position opérationnelle.

Un moyen passe d'une position à l'autre lors de la mise en service opérationnel ou, exceptionnellement, lors de sa qualification.

8.2. **Organisations.**

8.2.1. ***Position amont.***

Tout article COMSEC utilisé dans le cadre d'un programme franco-étranger doit faire l'objet d'un accord précisant notamment les procédures de stockage, d'échange transfrontalier, de manipulation et d'accès à ces moyens et informations. Cet accord, compatible avec les accords ou les règlements de sécurité établis entre la France et ses partenaires, doit être approuvé par l'ensemble des nations participantes. La contribution nationale à cet accord s'appuiera sur la présente directive ainsi que sur l'[IM900].

Dans la position amont, l'ANSSI désigne, sur proposition du ministère, une ou plusieurs autorités à qui elle délègue :

- l'application des réglementations et procédures relatives au suivi et à la protection des moyens et informations du programme ou du projet ;

- le suivi des moyens et informations mis en œuvre au sein du programme ou du projet ;

- la protection et la distribution conformément aux annexes de sécurité des contrats ou conventions.

Le cas échéant, ces points viennent s'ajouter aux éléments contractuels conclus entre les nations participantes.

8.2.2. ***Position opérationnelle.***

8.2.2.1. Cas de l'Organisation du traiter de l'Atlantique nord et de l'Union Européenne.

Marquage : les articles COMSEC utilisés dans le cadre de l'OTAN et de l'UE, portent la mention CCI (Controlled Cryptographic Item ou Controlled COMSEC Item) ou CRYPTO. Le marquage CRYPTO concerne notamment des clés de chiffrement, des documents et certains matériels de sécurité particulièrement sensibles. Ainsi, ces équipements ne doivent pas être marqués ACSSI mais conformément aux directives de la DGA qui veillera à une appellation conforme à celle des alliées.

Le marquage CCI regroupe la grande majorité des matériels concourant à la sécurité des systèmes d'information.

Les moyens CRYPTO sont en général classifiés. Les moyens CCI sont, par spécification, non classifiés. Ces moyens se conforment à des réglementations communes en matière de manipulation et de transport appliquées par la France (31).

Fonctions : l'ANSSI est garante de la conformité aux réglementations et aux procédures de l'OTAN et de l'UE. Elle est le correspondant officiel vis-à-vis de l'étranger pour l'application des réglementations concernant la gestion nationale des COMSEC, ainsi que pour les décisions techniques.

Dans la position opérationnelle, l'ANSSI désigne, sur proposition du ministère, une ou plusieurs autorités à qui elle délègue :

- l'application des réglementations et des procédures relatives au suivi et à la protection des moyens et informations de l'OTAN et de l'UE ;

- le suivi des moyens et informations provenant de l'OTAN ou de l'UE ;

- la protection et la distribution conformément à la présente instruction ;

- la surveillance et la transmission des incidents relatifs à ces moyens et informations ;

- l'assistance aux utilisateurs finaux au plus près du besoin opérationnel.

8.2.2.2. Autres cas interalliés.

Les règles applicables à la gestion des COMSEC s'appuient sur les accords généraux de sécurité, dont le garant est le Secrétariat général de la défense et de la sécurité nationale (SGDSN) et sur des accords passés à l'initiative des ministères. Des délégations peuvent être accordées par le SGDSN à des autorités qu'il désigne.

8.2.3. ***Cohérence des mentions de classification.***

Pour le suivi des moyens interalliés, la correspondance suivante doit être adoptée :

Réglemtation interalliée	Réglementation française
CRYPTO	ACSSI Classifié
CCI	ACSSI Non Classifié

Il n'y a pas de double marquage : le marquage d'origine est conservé.

Bien que présentant la majorité des cas, ce tableau n'est pas l'exhaustif. Il est nécessaire pour les cas non listés de se référer aux accords internationaux et aux annexes de sécurité.

9. MESURES TRANSITOIRES.

9.1. **Admissions et agrément de la sécurité des systèmes d'information.**

L'instruction interministérielle 910/DISSI/SCSSI/DR du 19 décembre 1994 et la directive 911/DISSI/SCSSI/DR du 20 juin 1995 distinguaient admission et agrément de la sécurité des systèmes d'information (SSI).

À titre transitoire, toutes les décisions en cours de validité à la date de la présente instruction peuvent, jusqu'à leur expiration, être considérées comme des décisions d'accès aux ACSSI.

À compter du 1er janvier 2016, la décision d'accès aux ACSSI sera le seul document valable pour développer, manipuler, interagir ou gérer des ACSSI.

9.2. **Agréments antérieurs à la présente instruction.**

Les ACSSI dont l'agrément est antérieur à la date de publication de la présente instruction doivent faire l'objet d'une attention particulière. Si les correspondances indiquées *infra* ne sont pas jugées suffisantes par les

autorités qualifiées, elles doivent s'adresser au FSSI qui se retournera vers l'ANSSI. Cette dernière peut décider d'adapter les mesures de protection, dans le sens d'un renforcement ou d'un allègement, ou encore d'entamer une nouvelle procédure d'agrément. Dans le cas des produits qui ont reçu la mention ACSSI à l'issue d'une décision d'homologation, il appartient à l'autorité d'homologation de se prononcer sur les dispositions transitoires. Ces ACSSI doivent être gérés de manière centralisée, sauf si une décision relative à la possibilité d'une gestion locale est prise par l'ANSSI.

9.3. **Correspondances.**

ANCIENNE DENOMINATION		NOUVELLE DENOMINATION
ACSSI (ancienne génération)	Diffusion Restreinte	ACSSI DR
	Confidentiel Défense	ACSSI CD (ou supérieur)
ACSSI - S	Confidentiel Défense	ACSSI CD (ou supérieur)
	Secret Défense	ACSSI SD
ASGLI	Non Protégé	ACSSI NP

Pour le ministre de la défense et par délégation :

L'ingénieur général hors classe de l'armement,
directeur général des systèmes d'information et de communication,

Marc LECLÈRE.

---

(1) COMmunication SECurity

(2) Il s'agit ici de la validation technique de la faisabilité du besoin exprimé par l'autorité d'emploi.

(3) Qui se traduit par l'émission ou la révocation des décisions d'accès ACSSI ou par la délivrance d'attestation de sensibilisation.

(4) La gestion des incidents de sécurité est décrite au point 7.

(5) Article R1143-5 du code de la défense.

(6) Conformément au C-M(2002)49.

(7) Dans le cas d'une mise à disposition d'ACSSI hors contrat DGA, un ordre de service est établi pour se retrouver dans le cas du point 2.3.2.a) ou dans le cas du point 2.3.2.b) du présent document.

(8) Ce qui n'empêche pas que le suivi logistique de biens ACSSI classifiés soit aussi réalisé dans les systèmes d'information logistiques sous réserve que la classification des informations relatives aux mouvements de ces derniers soit compatible du système d'information logistique et du besoin d'en connaître.

(9) Toutefois la mention de protection des fichiers ou impressions générées doit être ajustée aux informations effectivement exportées. Par exemple, il n'est pas utile de classifier un bordereau de prise en compte d'un ACSSI généré par le système d'information, sauf consignes explicites.

(10) DTC : dispositif de transfert de clés.

(11) CIK : crypto ignition key.

(12) Un composant est une ressource matérielle dont le changement nécessite un niveau de soutien industriel (étatique ou privé).

(13) NNO : numéro de nomenclature OTAN.

(14) Papier et/ou électronique

(15) Manipulation, détention, administration, etc.

(16) Le modèle de décision figure en annexe 1.

(17) Au sens des dispositions de l'IGI 1300 relatives au marquage d'un support papier.

(18) Le transport ne couvre pas la circulation d'un ACSSI (transport par l'utilisateur lui-même). La circulation d'un ACSSI est traitée au point 5.2.3.

(19) Comme indiqué précédemment dans la directive, les mesures complémentaires de protection à apporter aux équipements ACSSI classifiés sont identiques à celles des équipements non ACSSI de même classification. Par exemple, les règles à appliquer pour le transport d'un équipement ACSSI CD sont celles du Confidentiel Défense.

(20) Elément Secret

(21) Sous réserve que rien ne s'y oppose dans les agréments, les décisions d'homologation ou les instructions techniques d'emploi.

(22) Comme indiqué précédemment dans la directive, les mesures complémentaires de protection à apporter aux équipements ACSSI classifiés sont identiques à celles des équipements non ACSSI de même classification. Par exemple, les règles à appliquer pour le transport d'un équipement ACSSI CD sont celles du Confidentiel Défense.

(23) En gestion logistique des biens, il s'agit d'un démantèlement : le bien X est sorti de la gestion pour donner naissance à des biens A et B (composants).

(24) Instruction technique d'emploi, procédures d'exploitation de la sécurité, notamment.

(25) Dans la liste des ACSSI à inspecter, l'inspecteur n'est obligé de contrôler l'ensemble de la liste mais peut choisir de n'en contrôler que certains. Il est seul apte à choisir les ACSSI qui doivent lui être présentés.

(26) Dans la liste des ACSSI à contrôler, le contrôleur n'est obligé de vérifier l'ensemble de la liste mais peut choisir de n'en contrôler que certains. Il est seul apte à choisir les ACSSI qui doivent lui être présentés.

(27) L'aspect opérationnel peut être traité par les échelons intermédiaires si la délégation le prévoit.

(28) Par exemple au cas où un incident de gestion apporterait un risque de compromission (correction non effectuée entraînant par exemple une ouverture/utilisation prématurée d'une clé).

(29) Ou à l'échelon intermédiaire si la délégation le prévoit.

(30) COMmunication SECurity, désignation empruntée à la réglementation OTAN et communément utilisée au-delà.

(31) Respectivement [SDIP293/1] (OTAN) et [TECH-I01] (UE).

ANNEXE I

RÉGLEMENTATION APPLICABLE.

1. RÉGLEMENTATION NATIONALE.

[IGI1300]	Arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle no 1300 sur la protection du secret de la défense nationale
[II910]	Instruction interministérielle n°910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)
[II500bis]	Instruction interministérielle n°500bis/SGDN/TTS/SSI/DR du 18 octobre 1996 relative au chiffre dans la sécurité des systèmes d'information
[IM900]	Instruction ministérielle n°900/DEF/CAB/DR du 26 janvier 2012 relative à la protection du secret de la défense nationale au sein du ministère de la défense
[ARRGESTLOG]	Arrêté du 21 février 2012 relatif à la gestion logistique des biens mobiliers affectés au ministère de la défense et des anciens combattants
[INSGESTLOG]	Instruction n° 12-001262 du 21 février 2012 relative aux modalités d'application de certains articles de l'arrêté du 21 février 2012 relatif à la gestion logistique des biens mobiliers affectés au ministère de la défense et des anciens combattants
[DT404329]	Directive technique n°404329/DEF/DIRISI/SDSSI/DRSF du 23 aout 2013 (n.i. BO)relative à l'emploi des conteneurs sécurisés pour le transport d'ACSSI
[DIR_RETEX]	Directive DGSIC n°33/DEF/DGSIC/NP du 5 février 2015 portant sur le retour d'expérience en cybersécurité au sein du ministère de la défense

2. RÉGLEMENTATION INTERNATIONALE.

[SDIP293/1]	SDIP-293/1 (OTAN) March 2011 – Instructions for the control and safeguarding of NATO cryptomaterial
[TECH-I01]	TECH-I-01 (UE) version 1.0 15 January 2007 – Instruction manual: CRYPTO and COMSEC material management.

ANNEXE II.

DÉFINITIONS.

ACSSI	On appelle Article Contrôlé de la Sécurité des Systèmes d'Information (ACSSI) certains moyens classifiés ou non, tels que les dispositifs de sécurité ou leurs composants, et certaines informations relatives à ces moyens (spécifications algorithmiques, documents de conception, clés de chiffrement, rapports d'évaluation, *etc.*), qu'il est essentiel de pouvoir localiser à tout moment et en particulier en cas de compromission suspectée ou avérée.
Chaîne fonctionnelle ACSSI	Sous-ensemble de la chaîne fonctionnelle de sécurité des systèmes d'information, la chaîne fonctionnelle ACSSI est chargée de **prescrire**, d'**appliquer** pour ce qui la concerne, de **contrôler l'application des mesures de sécurité des ACSSI**, et de **traiter les incidents** sur ces derniers.
Comptabilité ACSSI	Ensemble des actes formels de prise en compte, de création, de modification et de destruction des ACSSI essentiels à leur suivi.
Éléments secrets	On appelle éléments secrets l'ensemble des clés de chiffrement et des informations d'identification ou de camouflage protégées (fréquences, certificats, *etc.*). Dans ce document la définition est étendue aux supports passifs permettant de stocker ces information ou clés (*canister*, cartes CAM, *etc.*). En revanche, les éléments secrets traités dans ce document sont ceux qui sont effectivement des ACSSI.
Gestion ACSSI	La gestion des ACSSI recouvre les fonctions suivantes : - le suivi des ACSSI, c'est-à-dire la concrétisation des actes de comptabilité liés à la vie des ACSSI ; - la validation et la mise en œuvre des plans de déploiement des ACSSI, le besoin étant défini par les chaînes « emploi » ; - la réalisation des inventaires et le contrôle de la manipulation et de la protection conformes des ACSSI ; - le traitement des incidents.
Gestion centralisée ACSSI	On appelle gestion centralisée ACSSI la gestion réalisée au niveau d'une autorité qualifiée. Elle est réalisée par le gestionnaire central ACSSI de l'autorité qualifiée.
Réseau de chiffrement	On appelle réseau de chiffrement l'ensemble des correspondants organisés pour échanger entre eux des informations chiffrées, c'est-à-dire qui disposent d'un moyen de cryptographie compatible, de conventions et d'éléments secrets ou d'une infrastructure de gestion de clés communs.

ANNEXE III.

MODÈLE DE DÉCISION D'ACCÈS AUX ARTICLES CONTRÔLÉS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.

Décision initiale(1) - provisoire(1) - de renouvellement(1) - de modification(1)

La présente décision de référence …… délivrée par ..... (nom et fonction de l'autorité de décision) est valable pour l'intéressé ci-dessous pour une durée de ……mois(1) ans(1) avec les limitations indiquées :

ÉTAT CIVIL ET EMPLOI :

Nom et Prénoms :

Date et lieu de naissance :

Grade ou emploi :

Service employeur :

DÉCISION D'ADMISSION AUX INFORMATIONS CLASSIFIÉES :

SECRET DEFENSE(1) - CONFIDENTIEL DEFENSE(1) - AUTRE(1)

Référence et date de validité :

_____

NATURE DE LA FONCTION JUSTIFIANT L'ACCES AUX ACSSI :

Étude, développement(1) - Évaluation(1) - Administration de fonctions de sécurité(1) Maintenance(1) - Élaboration ou manipulation de paramètres secrets accessibles(1) – Mise en œuvre(1) – Gestion(1) - Manutention(1) - Utilisation(1)

Autre(1) (à préciser) :

FORMATION DE L'INTÉRESSÉ EN SSI :

OBSERVATIONS : Précisions quant aux ACSSI concernés ou limitations éventuelles (dont programme ou système particulier), *etc.*

Je soussigné déclare :

- avoir été informé de la décision d'accès aux ACSSI prise à mon endroit ;

- avoir pris connaissance de la présente instruction interministérielle ainsi que la directive centrale ministérielle de suivi des ACSSI de mon organisme ;

- être pleinement conscient de mes responsabilités en ce qui concerne le traitement des ACSSI.

à (lieu), le (date)	à (lieu), le (date)
(nom et signature du	(nom et signature de l'autorité
demandeur)	responsable de la délivrance de la

présente décision)

(1) Rayer les mentions inutiles

ANNEXE IV.

INFORMATIONS DEVANT FIGURER DANS L'AGRÉMENT D'UN ARTICLE CONTRÔLÉ DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION OU DANS LA DÉCISION D'HOMOLOGATION D'UN SYSTÈME D'INFORMATION METTANT EN OEUVRE UN ARTICLE CONTRÔLÉ DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.

L'agrément d'un produit ou la décision d'homologation d'un ACSSI doit comporter les informations suivantes :

- niveau de classification ou mention de protection de l'équipement seul ;

- niveau de classification de l'équipement à la clé ;

- niveau maximum de classification des informations pouvant être traitées ;

- mesures de protection pour les ACSSI non classifiés ;

- possibilités de gestion locale ou centrale ;

- éléments sur lesquels va porter la traçabilité ;

- critères de suivi spécifique ;

- version du logiciel ou de l'équipement ;

- pour les équipements contenant plusieurs ACSSI, association de chaque ACSSI avec le profil (utilisateur ou maintenance) chargé d'en assurer la traçabilité (par exemple, le contenant seul pour les utilisateurs, tous les composants pour la maintenance) ;

- conditions de transport (notamment pour les ACSSI « individuels » non classifiés de défense) ;

- les procédures particulières de fin de vie (cf. art. 17).

Toute information non classifiée fera l'objet de la mention NP ou DR dans la marge de l'agrément, afin de permettre la diffusion de cette information à des personnes non habilitées.

ANNEXE V.

CONTRATS VISANT OU COMPORTANT DES ARTICLES CONTRÔLÉS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION : CONTENU DES ANNEXES DE SÉCURITÉ.

Lors de l'établissement d'un contrat visant ou comportant des ACSSI, l'annexe de sécurité du contrat devra préciser *a minima :*

- le contractant et les sous-traitants éventuels, précisant leurs droits et leurs obligations respectives ;

- un rappel de l'objet de la prestation ;

- les besoins en décision d'accès aux ACSSI, notamment pour le personnel qui est affecté à la spécification et à la conception des équipements ACSSI ; - la catégorisation ACSSI des documents d'étude et de conception (plans, dossiers descriptifs de version, dossier de fabrication,…) ainsi que les documents d'évaluation ;

- la description de la protection durant les phases de développement, de test, d'assemblage, d'intégration ;

- les éventuelles restrictions portant sur tout ou partie des ACSSI (limites géographiques, possibilité ou non d'acheminer sous forme électronique, conditions de stockage…)

- les équipements de production dont les mémoires ou les constituants doivent être intégrés et peuvent contenir des informations relevant d'un niveau de sensibilité en rapport avec les équipements conçus ;

- les mesures nécessaires au cloisonnement des informations sensibles ;

- la destination à donner, en fin d'étude ou de production, aux logiciels, prototypes, bancs de tests et outils de développement ;

- un plan de transport ;

- l'obligation, pour le titulaire, de comptabiliser l'ensemble des ACSSI produits y compris les rebuts qui sont détruits ;

- les modalités de destruction des composants, rebuts, etc ;

- le cycle de vie antérieur à l'émission de l'agrément (marquage, suivi, stockage, destruction…) ;

- les conditions de contrôle de l'application de la présente instruction par l'autorité contractante.

ANNEXE VI.

RECOMMANDATIONS RELATIVES À LA GESTION DES INCIDENTS DE SÉCURITÉ.

1. INCIDENTS DE SÉCURITÉ.

Les incidents de sécurité sont de trois types :

- les fautes de chiffrement (hors périmètre de la présente directive) ;
- les incidents de conservation ;
- les incidents de gestion.

1.1. **Incidents de conservation.**

Certains incidents de conservation peuvent entraîner une compromission. Les incidents de conservation ont pour origine (liste non exhaustive) :

- la disparition ou la perte de documents, de pages de documents ou de correction définitive à des documents (nota 1) ;
- le vol, la disparition, la destruction non justifiable ou la perte d'ACSSI (nota 1) ;
- une reproduction constatée de tout ou partie de documents, de programmes,... (nota 1 ou 2) ;
- la destruction accidentelle, prématurée ou non motivée d'un document permanent ou périodique (clé ou code, en dehors du calendrier fixé) ;
- l'emploi d'un équipement cryptographique en dehors des normes techniques prescrites dans la documentation de référence (nota 1) ;
- la réception d'un document ou matériel mal conditionné (altération d'emballage, trace d'effraction, modification de scellés...) (nota 1) ;
- l'atteinte à l'intégrité d'un matériel (traces ou indices d'effraction) (nota 1).

Nota 1 : risque de compromission.

Nota 2 : compromission.

1.2. **Incidents de gestion.**

Les incidents de gestion recouvrent :

- la mauvaise tenue des documents de comptabilité ;
- les corrections non effectuées ou mal effectuées.

Au cas où un incident de gestion apporterait un risque de compromission (correction non effectuée entrainant par exemple une ouverture/utilisation prématurée d'une clé), il serait alors traité comme un incident de conservation.

2. COMPTE RENDU D'INCIDENT.

Le contenu type d'un compte rendu d'incident doit être précisé dans la directive de gestion des ACSSI de chaque AQ. Il peut notamment contenir les informations suivantes :

- type d'incident : perte, destruction anticipée, altération,… ;

- type de moyen concerné : identification du document ou du matériel et de son contexte ;

- niveau de classification et mention ACSSI : ACSSI DR, ACSSI CD… ;

- identification du moyen concerné : code de gestion, désignation et numéro de l'équipement concerné… ;

- usage de l'ACSSI concerné : opérationnel, en stockage, en maintenance… ;

- circonstances et causes de l'incident : date, lieu, organisme et personne incriminés, contexte… ;

- identités et agent de sécurité des ACSSI : identité du rédacteur, identité de l'agent de sécurité des ACSSI de l'entité concernée… ;

- mesures de sauvegarde prises : changement des clés, révocation des équipements, suspension d'utilisation du matériel, invalidation d'une carte à mémoire… ;

- commentaires éventuels.

La directive de gestion des ACSSI de chaque AQ doit préciser la façon dont le compte rendu est transmis au travers de la chaîne fonctionnelle. Par exemple :

- le niveau local de la chaîne ACSSI doit donner dans son compte rendu tous les éléments disponibles, formellement ou non, afin que le niveau central puisse évaluer la portée de la compromission (avérée, probable, impossible).

- un compte rendu initial écrit, protégé en confidentialité, détaillant les circonstances de l'incident et les mesures prises doit être établi dans les plus brefs délais et adressé au gestionnaire central ACSSI ou à l'échelon intermédiaire dans le cas d'une délégation de gestion d'ACSSI de type informations. Ce dernier, à partir des éléments qui auront été fournis par le niveau local, et indépendamment de la portée de la compromission, décide du niveau de classification du compte rendu final.

- lorsqu'un incident est clos, par exemple dans le cas d'une compromission non avérée, un compte rendu similaire à la déclaration initiale d'incident de sécurité doit être immédiatement établi ;

- à la suite d'un incident, si l'intégrité de l'ACSSI ne peut plus être garantie, celui-ci doit être mis sous séquestre pour être expertisé par les services techniques compétents.

3. DÉLAIS DE SOUMISSION DU COMPTE RENDU D'INCIDENT.

Les délais de soumission d'un compte rendu d'incident sont les suivants :

- au maximum dans les 24 heures qui suivent tout incident sur les clés de chiffrement opérationnelles et tout incident avéré (sabotage, vol, piégeage, copie non autorisée) ; Il est toutefois recommandée de faire immédiatement un compte-rendu dès le constat de l'incident.

- dans les 72 heures qui suivent tout autre incident.

Des recommandations supplémentaires peuvent être données dans les agréments. Les délais les plus contraignants sont alors retenus.