Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 22 octobre 2013

INSTRUCTION INTERMINISTÉRIELLE

RELATIVE AUX ARTICLES CONTRÔLÉS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ACSSI)

n°910/SGDSN/ANSSI

NOR :

PRM	**D**	**1**	**3**	**2**	**8**	**1**	**1**	**7**	**J**

SOMMAIRE

INTRODUCTION

L'instruction générale interministérielle 1300 (IGI 1300) établit que :

« Certains moyens, 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.) peuvent nécessiter la mise en œuvre d'une gestion spécifique visant à assurer leur traçabilité tout au long de leur cycle de vie ainsi que la connaissance de la version logicielle et matérielle. Il s'agit des moyens et des informations, qu'ils soient eux-mêmes classifiés ou non, qu'il est essentiel de pouvoir localiser à tout moment et en particulier en cas de compromission suspectée ou avérée.

Ces moyens et informations sont appelés « articles contrôlés de la sécurité des systèmes d'information » (ACSSI). Ils portent un marquage spécifique les identifiant, en plus, le cas échéant, de leur mention de classification.

La décision de classer ACSSI un moyen ou une information est prise par l'ANSSI après avis de la commission d'agrément du dispositif de sécurité concerné. Dans le cas où le dispositif de sécurité n'est pas soumis à agrément, l'autorité d'homologation d'un système d'information qui met en œuvre un tel dispositif de sécurité peut décider après avis de la commission d'homologation de classer ACSSI ce dispositif ou ses composants ou les informations qui y sont liées.

Les principes de gestion des ACSSI ont pour objectif :

- *de former, de sensibiliser et de responsabiliser les détenteurs de tels moyens et informations ;*
- *d'assurer la comptabilité[1] de ces moyens et informations, et d'en établir l'inventaire à un niveau central ou local, selon les besoins, de façon qu'ils puissent être localisés à tout moment ;*
- *de gérer leur diffusion ;*
- *de contrôler périodiquement leur localisation et leur état ;*
- *d'informer la chaîne fonctionnelle[2] de toute compromission suspectée ou avérée à la suite d'événements tels que la perte, le vol ou la disparition, même temporaire ;*
- *de s'assurer de leur destruction. »*

La présente instruction interministérielle a pour objet de préciser, en complément de l'instruction générale interministérielle 1300 sur la protection du secret de la défense nationale, les exigences de gestion et de mise en œuvre des *« articles contrôlés de la sécurité des systèmes d'information » (ACSSI).*

Elle s'applique à toute personne physique ou morale détenant ou manipulant des ACSSI.

Les règles établies en 1994 étaient adaptées à protection de produits de chiffrement ou de clés cryptographiques sensibles, dépourvus de protections techniques et dont la perte pouvait

1 Au sens suivi et traçabilité.

2 Chaîne fonctionnelle de la sécurité des systèmes d'information dédiée aux ACSSI.

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-intrusions, 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 chiffrants. Par ailleurs, il est apparu pertinent de gérer selon les règles applicables aux ACSSI des produits ou logiciels non-cryptographiques.

La multiplication de ces nouveaux types d'ACSSI a rendu nécessaire une refonte de la réglementation de 1994 afin d'assouplir dans certains cas les règles de gestion, de manipulation, de stockage, de maintenance et de transport. La nouvelle réglementation conserve cependant la possibilité de soumettre certains ACSSI aux mêmes règles que celles de 1994 lorsque la situation le justifie. Le principal aménagement porte sur la granularité de la gestion (traçabilité centrale ou locale) en fonction de la sensibilité de l'ACSSI.

Chapitre 1 :
Chaîne fonctionnelle et responsabilités

Art. 1 : L'autorité responsable de la gestion des ACSSI

Dans les ministères, l'*autorité responsable* de la gestion des ACSSI est le haut fonctionnaire de défense et de sécurité (HFDS)[3]. Désigné par le ministre et relevant directement de lui, le HFDS veille au déploiement dans son ministère des moyens sécurisés de communication électronique gouvernementale et s'assure de leur bon fonctionnement[4]. A ce titre, il a la responsabilité d'organiser la chaîne fonctionnelle ACSSI à travers la directive centrale ministérielle de suivi des ACSSI.

Il peut déléguer cette responsabilité.

Tout organisme dépendant d'un ministère de tutelle, ou ayant des liens contractuels l'amenant à traiter des ACSSI, a pour *autorité responsable* le HFDS du ministère de tutelle.

Les organismes privés, notamment les opérateurs d'importance vitale (OIV), qui échappent au cas précédent, doivent s'adresser à l'agence nationale de la sécurité des systèmes d'information (ANSSI) afin d'être orientés vers un ministère coordonnateur. Au sein des organismes publics placés dans la même situation, la responsabilité est confiée à la plus haute autorité de l'organisme.

Art. 2 : La directive centrale ministérielle de suivi des ACSSI

L'organisation de la chaîne fonctionnelle ACSSI est précisée par la directive centrale ministérielle de suivi des ACSSI, qui décrit et encadre les responsabilités des différents acteurs, formalise les délégations de responsabilité éventuelles et définit certains processus de traitement des ACSSI[5].

---

[3] Désigné haut fonctionnaire de défense et de sécurité, haut fonctionnaire de défense ou haut fonctionnaire correspondant de défense et de sécurité, selon le ministère auquel il appartient.

[4] Article R1143-5 du code de la défense.

[5] L'annexe 4 récapitule les informations devant figurer *a minima* dans la directive.

Cette directive est signée par l'*autorité responsable*. L'ANSSI peut demander à en être destinataire.

La structure administrative ou fonctionnelle dont l'*autorité responsable* est chargée au sens du présent article sera par la suite dénommée « organisme ».

1) Responsabilités

La directive centrale ministérielle de suivi des ACSSI doit préciser, dans l'organisation de la chaîne fonctionnelle ACSSI, quels sont les acteurs chargés de tenir chacun des rôles suivants :

- *chargé du suivi des ACSSI* : assure la traçabilité des ACSSI, remonte les incidents au travers de la chaîne fonctionnelle ;
- *autorité d'attribution des ACSSI* : valide le plan de déploiement des ACSSI et traite des conséquences des incidents, notamment la qualification des compromissions ;
- *inspecteur des ACSSI du ministère* : réalise les audits réguliers (cf. chapitre 8) ;
- *officier de sécurité des ACSSI* : s'assure de la formation requise pour les ACSSI manipulés et délivre les attestations de formation correspondantes. Il assure la délivrance des DACSSI et vérifie les conditions le permettant ;
- *détenteur* : détient un ou plusieurs ACSSI. Il a été formé à leur manipulation et en est responsable ;
- *convoyeur* : il doit connaître la conduite à tenir en cas d'incident pour les ACSSI dont il assure le transport. Il peut être extérieur à l'organisme.

Eu égard à la sensibilité particulière des ACSSI, il appartient aux autorités citées de rappeler les sanctions administratives encourues par les détenteurs en cas de perte, d'incident non déclaré ou de toute négligence menaçant la sécurité des moyens et informations mis à disposition. Ces sanctions n'excluent pas les conséquences pénales qui pourraient résulter de la compromission des données classifiées protégées par les ACSSI.

2) Processus

La directive centrale ministérielle de suivi des ACSSI doit *a minima* définir les processus suivants :

- affectation et suivi des ACSSI (cf. chapitre 4 et 6) ;
- délivrance et traitement des DACSSI (cf. chapitre 5) ;
- traitement des incidents (cf. chapitre 7) ;
- inspections (cf. chapitre 8).

Chapitre 2 :
Typologie des ACSSI

Art. 3 : Dispositions communes

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 « biens » essentiels définis dans cette analyse[6].

Des moyens ou des informations ayant un fort besoin de traçabilité peuvent également recevoir la mention ACSSI à l'initiative du développeur ou de l'industriel, avant d'être agréés par l'ANSSI ou homologués par une autorité.

Tous les ACSSI sont soumis aux mêmes règles, notamment de traçabilité, qui peuvent néanmoins faire l'objet d'une granularité variable (gestion locale ou centrale). 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 classification ou de protection.

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 2.

Art. 4 : Typologie

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* ou *Secret Défense*. Ils seront désignés et marqués ACSSI CD ou ACSSI SD
- Les ACSSI non classifiés, qui sont à la fois ACSSI et non classifiés (*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.

A l'exception des ACSSI NP, les ACSSI bénéficient des mesures de protection liées à la mention de protection ou la classification associée, conformément aux exigences définies dans l'IGI 1300 et dans l'instruction interministérielle relative aux mesures de protection des systèmes d'information traitant d'informations sensibles non classifiées de défense de niveau *Diffusion Restreinte*.

Sauf mention contraire, le terme ACSSI désignera indifféremment, dans la suite du document, les ACSSI classifiés et les ACSSI non classifiés.

---

[6] On entend par « bien » toute ressource qui a de la valeur pour l'organisme et qui est nécessaire à la réalisation de sa mission.

Chapitre 3 :
Marquage des ACSSI

Art. 5 : Marquage

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 placé à proximité de la mention de classification (CD ou SD) ou de protection (DR). Les ACSSI non protégés sont uniquement marqués ACSSI. 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[7] ;
- 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.

Chapitre 4 :
Suivi spécifique des ACSSI

Art. 6 : Justification du suivi des ACSSI

Les ACSSI font l'objet d'un suivi spécifique tout au long de leur cycle de vie afin de garantir la sécurité (confidentialité, intégrité, disponibilité et authenticité) des « biens » qu'ils protègent.

Ce suivi spécifique a pour but essentiel d'assurer, dans les meilleures conditions, la traçabilité des ACSSI et le traitement des incidents de sécurité[8] :

- 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 potentiels de sécurité 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 instruction.

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.

---

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

8 La gestion des incidents de sécurité est décrite au chapitre 7.

Ainsi, selon la portée de l'impact prévisible des incidents de sécurité potentiels, la gestion de l'ACSSI est assurée au *bon* niveau de gestion. Celui-ci doit nécessairement :

- s'appuyer sur l'organisation définie au chapitre 1 ;
- être local ou central pour un ACSSI déterminé ;
- 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) ; si l'agrément le permet, le choix appartient à l'*autorité responsable* ;
- être unifié au sein de chaque organisme pour un type d'ACSSI donné.

Art. 7 : Gestion centrale et gestion locale

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

- un premier niveau central qui est en mesure de fournir une vision totale des parcs de matériels ACSSI déployés au sein de l'organisme ;
- un ou plusieurs niveaux locaux qui permettent le suivi spécifique et l'affectation à une entité des ACSSI mis à disposition par le premier niveau central.

Le suivi en gestion locale (ou suivi local) s'appuie sur une organisation décidée par l'*autorité responsable* et définie dans la directive centrale ministérielle de suivi des ACSSI. Elle repose sur des échelons intermédiaires ayant reçu délégation de l'autorité. Les ACSSI peuvent alors être gérés par ces autorités sans que l'échelon central n'ait connaissance de l'ensemble des mouvements.

Art. 8 : Détermination du niveau de gestion

Selon les risques pesant sur un ACSSI, l'*autorité responsable* décide d'en assurer le suivi de façon centrale ou de façon locale, si l'agrément ou la décision d'homologation lui en laisse la latitude.

Les ACSSI DR et les ACSSI NP peuvent être gérés localement par défaut, sous réserve que l'agrément ou la décision d'homologation l'autorise.

En revanche, les ACSSI CD et les ACSSI SD doivent être gérés de manière centralisée, sans dérogation possible.

Tout ACSSI déployé en dehors de la chaîne fonctionnelle ACSSI d'un organisme doit être géré de manière centralisée (notamment lors du prêt entre ministères d'un équipement de chiffrement pour des besoins opérationnels temporaires).

Art. 9 : Modalités de suivi

Le suivi spécifique des moyens et informations ACSSI peut se faire individuellement ou par lot constitué (par exemple, lot de plusieurs ACSSI identiques conditionnés de manière à garantir globalement leur intégrité). Lorsque le lot est éclaté, le suivi devient individuel.

Dans le cas des composants intégrés, l'agrément ou la décision d'homologation précise si le suivi spécifique d'un composant est lié au suivi de l'équipement hôte. Ce type de suivi, qui lie un composant à un équipement et, inversement, un équipement à un ou plusieurs composants,

offre une redondance en matière de traçabilité. Le suivi spécifique doit également être en mesure d'indiquer les configurations successives du composant.

Le suivi spécifique doit être pertinent et défini au moment de l'agrément ou de la décision d'homologation (exemples : par numéro de série, par dépositaire, par lieu de détention, par date de prise en compte, par numéro chrono et numéro d'exemplaire pour un document, par désignation, par contrat, par nomenclature, présence de commentaires, etc.)

Le suivi peut s'appuyer sur un système d'information simple et évolutif. Ce système d'information, associé à des acteurs formés et responsabilisés et à des procédures détaillées, contribue dans une large mesure à une résolution rapide des incidents.

La base de données ainsi créée est sensible. La granularité des informations qu'elle contient détermine son niveau de classification. Tout extrait de la base de données doit faire l'objet de la même attention.

Les données de traçabilité des ACSSI doivent être disponibles à tout moment.

Même dans le cas d'une gestion locale, l'échelon central d'un organisme doit être en mesure de connaître, soit directement, soit en s'adressant aux échelons locaux désignés :

- les ACSSI présents sur un site particulier ;
- l'affectation d'un ACSSI particulier et son détenteur ;
- les détenteurs successifs d'un ACSSI particulier ;
- les réseaux de chiffrement concernés[9].

Le nombre de sites où des ACSSI peuvent être présents doit être maîtrisé. L'échelon central peut s'adresser à n'importe quel échelon local afin qu'il lui adresse un inventaire précis de son parc.

Chapitre 5 :
Accès aux ACSSI

Art. 10 : Bénéficiaires de l'accès

La sensibilité particulière d'un moyen ou une information, qui a conduit à le déclarer ACSSI, doit être portée à la connaissance de son détenteur au travers d'une procédure de décision d'accès aux ACSSI (DACSSI). 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 (DACSSI), 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 non colisés ;
- les détenteurs utilisateurs.

[9] Les réseaux de chiffrement sont des réseaux de communication reposant sur des ACSSI, créés afin d'assurer la protection des informations traitées.

Toutefois, cette obligation ne concerne pas les détenteurs utilisateurs d'ACSSI non classifiés. Ces derniers bénéficient d'une attestation de formation à la manipulation des ACSSI dont les modalités de délivrance sont décrites dans la directive centrale ministérielle de suivi des ACSSI. Ces modalités doivent notamment prévoir une formation à la manipulation et aux procédures d'urgence. L'attestation de formation à l'utilisation des ACSSI comporte une reconnaissance de sensibilisation signée par le détenteur, délivrée lors de la prise en compte de l'ACSSI.

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

Art. 11 : Conditions de délivrance de la DACSSI

La délivrance d'une DACSSI 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[10] 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 ou l'effacement d'urgence des moyens ou informations confiés.

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.

Art. 12 : Modalités de délivrance de la DACSSI

La directive centrale ministérielle de suivi des ACSSI définit les modalités de délivrance des DACSSI. Les opérateurs d'importance vitale (OIV) doivent appliquer les dispositions de la directive de leur ministère coordonnateur. La formation à l'usage des ACSSI et la délivrance des DACSSI peuvent être déléguées aux OIV pour leur usage propre par le ministère coordonnateur.

Les autres cas doivent être soumis à l'ANSSI.

Sous réserve de satisfaire aux trois conditions visées à l'art. 11, une DACSSI[11] est délivrée pour une période maximale de cinq ans renouvelable, 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 DACSSI doit lui être immédiatement retirée par l'autorité qui a pris cette décision.

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

[10] Manipulation, détention, administration, etc.

[11] Le modèle de décision figure en annexe 1.

Les décisions d'accès aux ACSSI ne sont pas protégées, sauf si l'*autorité responsable* en décide autrement. Chaque organisme tient à jour un état des décisions en vigueur concernant son personnel.

Chapitre 6 :
Protection des ACSSI tout au long de leur cycle de vie

Art. 13 : 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 la chaîne fonctionnelle.

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.

Art. 14 : Acheminement

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

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. La rédaction d'un plan de transport est recommandée préalablement à tout acheminement, et plus particulièrement hors métropole. Celui-ci permet de formaliser, entre l'expéditeur et le destinataire, l'itinéraire, les conditions de transport et de prendre ainsi en compte les risques spécifiques à chaque envoi. Le plan de transport peut être un document générique, court et synthétique, décrit par l'*autorité responsable* dans un document de plus haut niveau.

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

1) Transport

- *Acheminement des ACSSI classifiés (*Confidentiel Défense *et* Secret Défense*)*

Ils sont transportés conformément à l'IGI 1300.

Par exception, si le colis contenant les moyens et informations est acheminé dans un conteneur agréé[12], 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.

- *Acheminement des ACSSI non classifiés (Non protégé et Diffusion Restreinte)*

Ces ACSSI sont transportés en métropole conformément aux annexes de l'IGI 1300 traitant du DR, y compris pour les ACSSI non protégés.

Selon les destinations et le type d'ACSSI, l'emploi de conteneurs approuvés par la directive centrale ministérielle de suivi des ACSSI est recommandé. 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.

Les convoyeurs n'ont pas l'obligation de détenir une DACSSI[13], sous réserve que leur emploi ne nécessite pas de manutention d'ACSSI non colisés.

Pour l'ensemble de ces transports (ACSSI classifiés ou non) :
- Les clés et dispositifs de sécurité amovibles nécessaires au fonctionnement d'un ACSSI doivent être retirés, faire l'objet de mesures différentiées et si possible l'objet d'un envoi séparé ;
- S'il apparaît manifeste qu'un colis a été ouvert ou manipulé frauduleusement, un incident de sécurité doit être déclaré et l'expéditeur du colis doit en être informé dans les plus brefs délais. Le colis est écarté et mis en sécurité.

- *Cas particulier des ACSSI transportés individuellement par un porteur*

Ces 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[14]. Dans ce cas, les conditions précises sont définies dans les instructions d'emploi des équipements et sont communiquées au transporteur.

- *Transports simultané des clés et des équipements*

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

12 Les conditions d'agrément d'un tel matériel sont en cours de spécification.

13 Sauf mention contraire dans la directive centrale ministérielle de suivi des ACSSI.

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

2) Transmission

L'emploi d'un système explicitement homologué pour la transmission d'ACSSI est obligatoire.

- *Transmission des ACSSI classifiés*

La transmission des informations s'appuie sur des systèmes homologués au niveau de classification requis.

- *Transmission des ACSSI non classifiés (Non protégé et Diffusion Restreinte)*

La transmission des informations s'appuie sur un système homologué Diffusion Restreinte.

Les opérations suivantes sont tracées lors de ces transmissions :

- prise en compte des données électroniques ;
- message à l'expéditeur attestant de la bonne réception du message ou de la pièce-jointe.

Ces opérations peuvent être assurées soit directement au sein du système d'information, soit de manière décorrélée, par exemple au moyen d'un autre système.

Art. 15 : Utilisation et stockage

Lors de leur utilisation, les ACSSI doivent être manipulés conformément 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.

Pour les ACSSI classifiés, la protection lors des phases de stockage est conforme aux dispositions de l'IGI 1300 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 du détenteur ou dans des armoires ou locaux fermés à clé, conformément aux décisions d'agrément ou d'homologation.

Indépendamment de la classification de l'ACSSI, chaque échelon de détention doit effectuer un recensement au minimum annuel et lors de chaque changement de détenteur. L'inventaire est mené à date fixe, précisée dans la directive centrale ministérielle de suivi des ACSSI.

Art. 16 : Maintenance

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

Durant ces opérations, la traçabilité doit porter sur :

- l'acheminement ;
- la gestion de l'équipement et de ses composants (réparation ou remplacement) ;
- la mise à jour comptable d'éventuels composants ACSSI (reprogrammation ou remplacement) dans le suivi de l'équipement ;
- 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, conformément aux procédures décrites dans l'agrément ou l'homologation. Si cette opération n'est pas possible (par nature ou en raison d'une défaillance), l'ACSSI est manipulé et conservé au niveau de classification des données qu'il a traitées avant sa mise en maintenance et des éléments secrets injectés.

Art. 17 : Fin de vie

1) Destruction

Un moyen ou une information reste catégorisé ACSSI de sa conception jusqu'à sa destruction.

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

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 classifiés dont aucun composant interne n'est classifié.

- Les ACSSI classifiés sont détruits selon les procédures décrites dans l'IGI 1300[15].
- 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 les deux cas précédents, les conditions suivantes doivent être réunies :

  - la personne présente pour la destruction détient une habilitation du niveau des ACSSI détruits ainsi qu'une DACSSI ;
  - la personne en charge de la destruction est issue soit de l'organisme détenteur des ACSSI mis pour destruction, soit 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 titulaire d'une DACSSI.

Dans tous les cas, un procès-verbal de destruction doit être cosigné par deux personnes habilitées au niveau des ACSSI détruits, dont une au moins doit détenir une DACSSI. Dans le cas d'un équipement, le procès-verbal intègre également les éventuels composants ou sous-ensembles eux-mêmes ACSSI.

Une procédure de destruction d'urgence est établie par chaque ministère en fonction des menaces potentielles qui pèsent sur l'organisme ou les ACSSI eux-mêmes, en tenant compte de la variété des conditions d'emploi. Validée par l'*autorité responsable*, sa connaissance est une condition nécessaire à la délivrance de la DACSSI ou de l'attestation (cf. chapitre 5).

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.

[15] A défaut vers le guide 972/SCSSI/SI du 9 avril 1998 relatif à la protection des supports classifiés de défense.

La mention ACSSI peut ne plus être pertinente sur certains documents. Il est alors possible, après autorisation de l'autorité d'origine, de ne plus considérer un document comme ACSSI.

Chapitre 7 :
Gestion des incidents de sécurité et des compromissions

Art. 18 : Définitions

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 issue d'un incident de sécurité.

Art. 19 : Incidents de sécurité

La liste des événements qui doivent obligatoirement être considérés comme des incidents de sécurité est précisée dans la directive centrale ministérielle de suivi des ACSSI. Des exemples figurent à l'annexe 5.

Tout incident de sécurité concernant un ACSSI doit être immédiatement, et par tout moyen, déclaré par le détenteur ou par celui qui constate l'incident. Cette remontée d'incident vers le HFDS 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 centrale ministérielle de suivi des ACSSI.

Un inventaire des incidents sera adressé annuellement à l'ANSSI, même en cas d'état néant.

Art. 20 : Compromissions

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

Au regard de la déclaration de l'incident de sécurité, l'*autorité d'attribution des ACSSI*[16], désignée par l'*autorité responsable*, 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'attribution des ACSSI*, les services enquêteurs sont saisis.

L'*autorité responsable* avertit l'ANSSI de toute compromission.

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

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

[16] Cf. article 2.

- aux localisations des dispositifs déclarés compromis ;
- à la quantité des moyens ou informations déclarés compromis par site ;
- à toute autre information pertinente.

Art. 21 : Mesures conservatoires

L'*autorité d'attribution des ACSSI* est avertie sans délai. Elle décide des mesures conservatoires à prendre au plus tôt selon l'incident rapporté : révocation de l'équipement du réseau de chiffrement, passage sur une clé de secours, ou toute autre mesure qu'elle juge nécessaire pour limiter les conséquences de l'incident. Elle qualifie l'importance de l'incident en liaison avec l'autorité d'agrément ou d'homologation de l'ACSSI concerné.

Art. 22 : 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 par la directive centrale ministérielle de suivi des ACSSI. Des recommandations figurent à l'annexe 5.

Chapitre 8 : Inspections

Art. 23 : Inspections

Des inspections programmées ou inopinées doivent être menées à l'initiative de l'*autorité responsable*. Elles témoignent de la bonne tenue et de l'efficacité du suivi spécifique et du respect des mesures de protection. Les modalités de ces inspections sont précisées dans la directive centrale ministérielle de suivi des ACSSI.

L'inspection doit se limiter à des constats visuels, sans porter atteinte à l'intégrité ou aux fonctions de sécurité des ACSSI.

En complément, les inspections des ministères réalisées par l'ANSSI peuvent intégrer un volet relatif aux ACSSI. A cette occasion, l'ANSSI peut demander à se faire remettre la directive centrale ministérielle de suivi des ACSSI ainsi que tout document de mise en œuvre des ACSSI inspectés[17].

L'annexe 6 dresse une liste des processus qui doivent être analysés.

[17] Instruction technique d'emploi, politique d'exploitation de la sécurité, notamment.

Chapitre 9 :
Organisation et responsabilités relatives aux moyens et informations étrangers

Art. 24 : Définitions

Ces moyens et informations cryptographiques étrangers équivalents aux ACSSI sont appelés par la suite *articles COMSEC*[18]. Leur traçabilité doit être assurée.

Lorsque des accords de sécurité relatifs à l'usage en France d'*articles COMSEC* requièrent une gestion spécifique visant à assurer leur traçabilité, ces articles sont soumis aux mêmes principes de gestion 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 une personne désignée par l'*autorité responsable* au sein de la chaîne fonctionnelle ACSSI.

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) ;
- 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.

Art. 25 : Organisation

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. Il est par conséquent recommandé de s'appuyer sur la présente instruction ainsi que sur l'IGI 1300 pour la contribution nationale à cet accord.

Dans la position amont, l'ANSSI désigne, sur proposition des ministères concernés, 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 ;
- le suivi des moyens et informations mis en œuvre au sein du programme ;
- la protection et la distribution conformément aux annexes de sécurité des contrats.

[18] *COMmunication SECurity*, désignation empruntée à la réglementation OTAN et communément utilisée au-delà.

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

2) Position opérationnelle

- *Cas OTAN et UE*

Marquage : les *articles COMSEC* utilisés dans le cadre de l'OTAN et de l'Union européenne, 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.

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[19].

Fonctions : l'ANSSI est garante de la conformité aux réglementations et aux procédures de l'OTAN et de l'Union européenne. 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 des ministères concernés, 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.

- *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.

[19] Respectivement SDIP-293 (OTAN) et TECH-I-01 (UE).

Art. 26 : Cohérence des mentions de classification

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

Réglementation interalliée	Réglementation française
CRYPTO	ACSSI Classifié
CCI	ACSSI Non Classifié

Il n'y a pas de double marquage.

Chapitre 10 :
Abrogation et mesures transitoires

Art. 27 : Abrogation

La présente instruction abroge l'instruction interministérielle sur les articles contrôlés de la sécurité des systèmes d'information (910/DISSI/SCSSI/DR du 19 décembre 1994) et la directive relative aux articles contrôlés de la sécurité des systèmes d'information (911/DISSI/SCSSI/DR du 20 juin 1995).

Art. 28 : Admission et agrément SSI

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 SSI.

A 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 (DACSSI).

L'*autorité responsable* fera figurer dans la directive centrale ministérielle de suivi des ACSSI la date à laquelle la DACSSI sera le seul document valable pour développer, manipuler, interagir ou gérer des ACSSI.

Art. 29 : 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 l'*autorité responsable*, celle-ci doit s'adresser à 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.

Art. 30 : Correspondances indicatives

Le tableau suivant décrit, de manière indicative, les correspondances entre les anciennes et les nouvelles dénominations :

Ancienne dénomination		Nouvelle dénomination
ACSSI (ancienne génération)	Diffusion Restreinte	ACSSI Diffusion Restreinte
	Confidentiel Défense	Minimum ACSSI CD
ACSSI-S	Confidentiel Défense	Minimum ACSSI CD
	Secret Défense	ACSSI Secret Défense

Fait à Paris, le 22 octobre 2013

Patrick PAILLOUX
Directeur général
Agence nationale de la sécurité des systèmes d'information

ANNEXE 1
MODELE DE DÉCISION D'ACCES AUX ARTICLES CONTRÔLÉS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (DACSSI)

_____

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 DACSSI 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)*
(nom et signature du demandeur)

à *(lieu)*, le *(date)*
(nom et signature de l'autorité responsable de la délivrance de la présente décision)

[(1)] Rayer les mentions inutiles

ANNEXE 2
INFORMATIONS DEVANT FIGURER DANS L'AGREMENT D'UN ACSSI OU DANS LA DECISION D'HOMOLOGATION D'UN SYSTEME D'INFORMATION METTANT EN ŒUVRE UN ACSSI

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 3
CONTRATS VISANT OU COMPORTANT DES ACSSI :
CONTENU DES ANNEXES DE SECURITE

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 4
CONTENU DE LA DIRECTIVE CENTRALE MINISTÉRIELLE DE SUIVI DES ACSSI

Cette liste –non exhaustive– rappelle les informations qui doivent figurer *a minima* dans la directive centrale ministérielle de suivi des ACSSI.

(Chaque information renvoie au chapitre ou à l'annexe dont elle est issue).

- responsabilités, délégations, organisation de la chaîne fonctionnelle ACSSI et des processus liés aux ACSSI [chapitre 1] ;
- conditions de délivrance de l'attestation permettant l'utilisation d'ACSSI non classifiés [chapitre 5] ;
- modalités de délivrance des DACSSI [chapitre 5] ;
- date à laquelle l'inventaire doit être mené [chapitre 6] ;
- liste des événements qui doivent obligatoirement être considérés comme des incidents de sécurité [chapitre 7] ;
- objectifs de l'inspection, contenu, conditions dans lesquelles elle est menée, fréquence et méthode utilisée [chapitre 8] ;
- date à laquelle la DACSSI remplacera définitivement les précédents procédés d'autorisation d'accès aux ACSSI (admission et agrément) [chapitre 10] ;
- contenu, délai et voie de transmission d'un compte rendu d'incident [annexe 5].

ANNEXE 5
RECOMMANDATIONS RELATIVES A LA GESTION DES INCIDENTS DE SECURITE

Exemples d'incidents

Liste indicative d'incidents de sécurité à faire remonter par la chaîne de gestion des ACSSI :

- disparition ou perte de documents ou de pages de documents ACSSI ;
- vol, disparition, destruction involontaire ou accidentelle ou perte d'un moyen ACSSI ;
- reproduction constatée et non prévue de tout ou partie de documents, de logiciels, etc.) ;
- destruction accidentelle, prématurée ou non motivée, d'un document ;
- réception d'un document ou moyen ACSSI mal conditionné (altération d'emballage, trace d'effraction, modification de scellés…) ;
- atteinte à l'intégrité d'un moyen ou information ACSSI (traces ou indices d'effraction) ;
- reproduction interdite d'une information ACSSI ;
- suspicion de piégeage ;
- impossibilité de vérifier l'intégrité d'un ACSSI ;
- accès facilité à un moyen ou une information ACSSI due à une protection insuffisante ;
- destruction non accidentelle d'un moyen ou information ACSSI par une autre procédure que celle autorisée ;
- perte de traçabilité sur un moyen ou une information.

Compte rendu d'incident

Le contenu type d'un compte rendu d'incident doit être précisé dans la directive centrale ministérielle de suivi des ACSSI. 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 correspondants SSI : identité du rédacteur, identité de l'OSSI de l'unité 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 centrale ministérielle de suivi des ACSSI doit préciser la façon dont le compte rendu est transmis au travers de la chaîne fonctionnelle. Par exemple :

- le niveau local de la chaîne SSI 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 à l'*autorité responsable* ou à une autorité déléguée. Cette dernière, 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. En sa qualité d'autorité d'agrément, l'ANSSI est en copie du compte rendu initial.
- 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.

Délais de soumission du compte rendu d'incident

Les délais de soumission du compte rendu d'incident doivent être précisés dans la directive centrale ministérielle de suivi des ACSSI.

Il est toutefois recommandé que le compte rendu initial soit adressé à l'*autorité responsable* :

- dans les 24 heures qui suivent tout incident sur les clés de chiffrement opérationnelles et tout incident avéré (sabotage, vol, piégeage, copie non autorisée) ;
- 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.

ANNEXE 6
REDACTION DE LA DIRECTIVE CENTRALE MINISTÉRIELLE : RECOMMANDATIONS RELATIVES AUX INSPECTIONS

La directive centrale ministérielle de suivi des ACSSI détaille les objectifs et le contenu des inspections ainsi que les conditions dans lesquelles elles sont menées.

Certains objectifs propres à l'organisme 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 à la directive 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 l'échelon local et l'échelon central ainsi que sur la manière dont les ACSSI sont suivis et mis en œuvre.

Enfin, la directive précise qui peut mener cette inspection, la fréquence (trois ans sont recommandés), le périmètre et la méthode (par échantillonnage, exhaustif…) des inspections.