GOUVERNEMENT
Liberté
Égalité
Fraternité

Secrétariat général du ministère de l'Économie, des Finances et de la Relance

Service du Haut fonctionnaire de défense et de sécurité

Paris, le 23 décembre 2020

Directive centrale ministérielle de suivi des articles contrôlés de la sécurité des systèmes d'information (ACSSI).

NOR ECOP2036731C

Résumé :

Le 1er juillet 2020, l'Etat a créé un nouvel Opérateur des Systèmes d'Information Interministériels Classifiés (OSIIC) rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN)**. Conformément aux instructions générales interministérielles n° 910 et n° 1300, la présente directive centrale ministérielle précise l'organisation de la chaîne de gestion des articles contrôlés de la sécurité des systèmes d'information (ACSSI) au sein du ministère l'économie des finances et de la relance (MEFR) et du ministère de la transformation et de la fonction publiques (MTFP). Elle décrit et encadre les responsabilités des différents acteurs, formalise les délégations de responsabilité éventuelles et définit certains processus de traitement des articles contrôlés de la sécurité des systèmes d'information (ACSSI) qui passent, pour l'essentiel par des échanges avec la mission des moyens sécurisés de communication (MMSC) du service du** Haut fonctionnaire de défense et de sécurité **(SHFDS).**

1. Responsabilités, délégations, organisation de la chaîne fonctionnelle ACSSI et les processus liés

1.1. Autorité responsable de la gestion des ACSSI

L'autorité responsable de la gestion des articles contrôlés de la sécurité des systèmes d'information (ACSSI) est le Haut fonctionnaire de défense et de sécurité (HFDS). Désigné par le ministre et relevant directement de lui, le HFDS veille au déploiement des moyens sécurisés de communication électronique gouvernementale et s'assure de leur bon fonctionnement. Il organise la chaîne fonctionnelle ACSSI à travers cette directive centrale ministérielle de suivi des ACSSI. Des ACSSI sont des moyens tels que les dispositifs de sécurité, leurs composants ou certaines informations relatives à ces moyens peuvent nécessiter la mise en œuvre d'une gestion spécifique, visant à assurer leur traçabilité tout au long de leur cycle de vie. La décision de classer ACSSI un moyen ou une information est prise par l'agence nationale de sécurité des systèmes d'information (ANSSI)

Au sein du service du Haut fonctionnaire de défense et de sécurité (SHFDS), cette responsabilité est déléguée au chef du département sécurité des systèmes d'information (DSSI) qui pilote la mission des moyens sécurisés de communication (MMSC).
Toute entité sous l'autorité ou la tutelle du MEFR et du MTFP (services, opérateurs d'importance vitale (OIV)), ou ayant des liens contractuels avec le MEFR et le MTFP l'amenant à utiliser des ACSSI, a pour autorité responsable le HFDS du MEFR et du MTFP.
La structure administrative ou fonctionnelle dont l'autorité responsable est chargée au sens de la présente directive centrale ministérielle est par la suite dénommée « **l'entité** ».

1.2. Acteurs opérationnels et responsabilités

Les différents acteurs de la chaîne fonctionnelle ACSSI du MEFR et du MTFP sont les suivants :
- la mission des moyens sécurisée de communication (MMSC) du SHFDS, chargée de la gestion opérationnelle des ACSSI (perception, transport, mise en œuvre, comptabilité et réintégration) et de la délivrance des décisions d'accès aux ACSSI (DACSSI) et de la tenue des inventaires ;

- les officiers de sécurité (OS) des entités détentrices réalisent les demandes d'ACSSI auprès de la MMSC et s'assurent de la formation requise des détenteurs pour la manipulation des ACSSI ;
- les détenteurs utilisateurs d'un ou plusieurs ACSSI qui sont formés à la manipulation et responsable des ACSSI attribués.

Il appartient aux OS des entités 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 systèmes information mis à disposition. Ces sanctions n'excluent pas les conséquences pénales qui pourraient être prononcées au titre de la protection du secret de la défense nationale.

2. Mise à disposition des ACSSI

2.1. Cartes destinée à l'intranet sécurisé interministériel pour la synergie-gouvernemental (ISIS)

2.1.1. Demande

La demande de carte ISIS est adressée par le futur détenteur, sous couvert de la voie hiérarchique, à l'OS de l'entité à laquelle il appartient. L'OS s'assure que l'agent à l'origine de la demande est détenteur d'une habilitation à la protection du secret et en cours de validité. L'OS transmet la demande à la MMSC au moyen de la boite fonctionnelle mmsc.shfds@finances.gouv.fr. La MMSC transfère la demande à l'opérateur des systèmes d'informations interministériels classifiés (OSIIC).

2.1.2. Remise de la carte

L'OSIIC produit la carte ISIS et la fournit à la MMSC, qui la remet à l'OS de l'entité demandeuse avec son code d'activation sous double enveloppe ainsi qu'un bordereau comptable en deux volets. L'OS remet ensuite en main propre au détenteur la double enveloppe contenant la carte ISIS et son code porteur, et retourne à la MMSC le feuillet B du bordereau comptable signé par le détenteur. L'OS remet également au détenteur d'une carte ISIS pour la première fois, une « procédure d'exploitation de sécurité ISIS – Déclinaison pour les utilisateurs d'ISIS ».

2.1.3. Restitution de la carte

Lors de la cessation de fonctions nécessitant une habilitation, il appartient à l'OS de solliciter auprès du détenteur la restitution de sa carte ISIS. En cas d'absence, il appartient à l'OS de faire un compte-rendu de perte. L'OS informe la MMSC sans délai de cette restitution au moyen de la boite fonctionnelle mmsc.shfds@finances.gouv.fr pour convenir avec la MMSC d'un rendez-vous de remise de la carte ISIS ou de son envoi par lettre recommandée avec accusé de réception. Une carte ISIS est renouvelée automatiquement à l'échéance du certificat.

2.2. Cartes ARIANE

La procédure de gestion des cartes ARIANE est globalement la même que pour les cartes ISIS, mais dans ce cas, MMSC gère en direct les demandes des usagers et délivrent la carte sans passer par l'OS auquel l'usager est rattaché.

2.3. Postes ISIS

Bien qu'ils ne constituent pas des ACSII au sens strict, les postes ISIS sont des équipements sensibles qui sont transportés, installés, maintenus et retirés par des agents habilités de l'OSIIC. A la demande expresse de l'OSIIC, les agents de la MMSC peuvent être autorisés, au cas par cas, pour procéder à des opérations liées à la maintenance, déplacement ou au remplacement de postes ISIS.

2.4. Chiffreurs

Les chiffreurs nécessaires au fonctionnement des réseaux classifiés sont transportés, installés, maintenus et retirés exclusivement par des agents habilités de l'OSIIC.

2.5. Postes téléphoniques TEOREM

Les postes téléphoniques TEOREM (constitués d'un combiné, d'une base, d'une carte SD et d'une carte SIM dans le cadre d'une fonction GSM, d'un code administrateur et d'un code utilisateur) sont fournis à la MMSC par l'OSIIC. Tout mouvement physique d'un poste TEOREM, doit donner lieu préalablement à un échange formalisé entre la MMSC et l'entité détentrice concernée. Lorsque l'entité détentrice est située sur la plaque parisienne (Paris et petite couronne), la MMSC peut se déplacer sur place pour les opérations le nécessitant. De même, l'entité peut désigner un agent pour se rendre directement au SHFDS (Bâtiment Bercy Necker) afin de procéder à des remises ou échanges, à condition que le transport soit réalisé dans des conditions de sécurité adaptées. Lorsque l'entité détentrice est située hors plaque parisienne, les opérations d'envoi, de retour ou d'échange de poste TEOREM sont réalisées exclusivement via un service postal sécurisé adéquat en deux colis comprenant le code utilisateur et la carte micro SD et un second, le combiné et la base.

3. Conditions et modalités particulières

3.1. Rappel des types d'ACSSI détenus au sein du MEFR et du MTFP :

- cartes ISIS (avec code) ;
- cartes Ariane (avec code) ;
- chiffreurs d'artères (avec bouchon ou clé) ;
- téléphones OSIRIS (sans code) ;
- visioconférence HORUS (sans code) ;
- téléphones TEOREM (avec codes).

NB : Les postes ISIS ne sont pas des ACSSI au sens strict mais sont suivis dans un inventaire spécial et font l'objet d'une formation à l'utilisation spécifique lors de l'attribution à un nouvel utilisateur.

3.2. Bénéficiaire de l'accès à un ACSSI

Le détenteur d'un ACSSI fait l'objet d'une décision d'accès aux ACSSI (DACSSI) matérialisée à l'occasion du « Bordereau comptable de documents et de matériel ACSSI » par exemple dans la « Procédure d'exploitation de sécurité ISIS – Déclinaison pour les utilisateurs d'ISIS », éditée par l'OSIIC. Ce document comporte une reconnaissance de sensibilisation signée par le détenteur, délivrée lors de la prise en compte de l'ACSSI.

3.3. Spécificité des OIV

Les opérateurs d'importance vitale (OIV) qui sont dotés d'ACSII appliquent les dispositions de cette directive centrale ministérielle. Toutefois, la formation à l'usage des ACSSI et la délivrance des ACSSI peut leur être déléguée par le MEFR et le MTFP. L'attestation d'information à l'utilisation des ACSSI comporte une reconnaissance de sensibilisation et de responsabilité signée par le détenteur, délivrée lors de la prise en compte de l'ACSSI.

3.4. Inventaire

A la demande de l'OSIIC, le MEFR et le MTFP via la MMSC fournissent annuellement un inventaire des ACSSI qu'ils contrôlent. En lien avec le département en charge de la protection du secret du SHFDS, la MMSC effectue une revue annuelle des cartes ISIS à l'aide de l'annuaire informatique du MEFR et du MTFP. L'inventaire des postes ISIS est réalisé sous la responsabilité des OS des entités détentrices qui le communique à la MMSC.

3.5. Transport

Lorsqu'ils ne sont pas directement transportés par des agents de l'OSIIC, les ACSSI attribués au MEFR et au MTFP sont transportés (entre les locaux de l'OSIIC et ceux du SHFDS ou entre les locaux du SHFDS et ceux des entités détentrices) par les agents de la MMSC.
Une carte ISIS ou un poste téléphonique TEOREM peut être confié par la MMSC à un agent dûment désigné d'une entité détentrice située sur la plaque parisienne, à condition que le transport s'effectue dans des conditions strictes de sécurité (Cf point 2.5. supra).
Pour rappel, il est possible de transporter ensemble un équipement et la clé qui lui sera associée, à condition que la révocation de la clé puisse être effectuée sans impact sur d'autres équipements en service.

Tout traitement ou toute autre situation doit faire l'objet d'un accord préalable formel (écrit) de l'OSIIC.

3.6. Stockage temporaire

Les ACSSI en attente d'installation ou destinés à retourner à l'OSIIC ne peuvent être stockés au sein des locaux de la MMSC que durant une durée maximale d'un mois (31 jours).

3.7. Maintenance, fin de vie, destruction

Toute restitution d'un ACSSI doit être transmise à l'OSIIC qui, seul peut procéder à son retraitement ou à sa destruction. Un remplacement peut s'effectuer avant ou après le retour de l'ACSSI d'origine à partir du moment où tout mouvement est tracé et inventorié. Un bordereau comptable suit chaque ACSII, pour la mise à jour de l'inventaire et du suivi comptable.

4. Evénements et incidents de sécurité

4.1. Définitions

Un incident de sécurité est un événement indésirable et 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 du secret de la défense nationale. En revanche, une compromission est nécessairement le résultat d'un incident de sécurité.

4.2. Traitement des incidents de sécurité

Tout incident de sécurité concernant un ACSSI est immédiatement, et par tout moyen, déclaré au HFDS par le détenteur ou par celui qui constate l'incident. La MMSC adresse un inventaire annuel des incidents à l'OSIIC même en cas d'état néant.

4.2.1. Liste d'événements obligatoirement considérés comme des incidents de sécurité

Il s'agit des cas suivants :
- vol, disparition, destruction involontaire ou accidentelle ou perte d'un moyen ACSSI ;
- intrusion physique dans un local contenant des ACSSI ;
- reproduction constatée et non prévue de tout ou partie d'ACSSI, de logiciels, etc. ;
- réception d'un ACSSI mal conditionné (altération d'emballage, trace d'effraction, modification de scellés) ;
- atteinte à l'intégrité d'un ACSSI (traces ou indices d'effraction) ;
- signalement d'anomalie par l'usager/réseau, suspicion de piégeage.

4.2.2. Compte rendu d'incident

Le compte rendu d'incident contient les informations suivantes :
- type d'incident : selon la typologie rappelée ci-avant (cf point 4.2.1.) ;
- type de moyen concerné : description du matériel et du contexte de son utilisation ;
- 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, identité et coordonnées des personnes incriminées, contexte… ;
- identité du (des) correspondant(s) SSI : identité du rédacteur, identité de l'OS de l'entité concernée… ;
- mesures de sauvegarde prises : changement de clés, révocation d'équipements, suspension d'utilisation du matériel …

Circuit de transmission du compte rendu d'incident :

- l'OS de l'entité concernée communique immédiatement à la MMSC les éléments disponibles, afin d'évaluer la portée de la compromission (avérée, probable, peu probable, impossible) ;
- parallèlement, un compte rendu initial écrit, classifié, détaillant les circonstances de l'incident et les mesures prises est établi et adressé à la MMSC qui, à partir des éléments fournis, décide du niveau de classification du compte rendu final. L'OSIIC est en copie du compte rendu initial ;
- lorsqu'un incident est clos, en cas d'une compromission non-avérée par exemple, un nouveau compte rendu, similaire à la déclaration initiale d'incident de sécurité est établi ;
- à la suite d'un incident, si l'intégrité de l'ACSSI ne peut plus être garantie, celui-ci est mis sous séquestre afin d'être remis et expertisé par les services techniques compétents de l'OSIIC.

4.3. Compromissions

Au regard de la déclaration de l'incident de sécurité, l'OS de l'entité concernée évalue l'impact de l'incident en vue de la prononciation éventuelle d'une compromission.
En fonction de la décision de l'autorité d'attribution des ACSSI, les services enquêteurs sont saisis.
Le HFDS avertit l'OSIIC de toute compromission.
L'OSIIC peut unilatéralement déclarer une compromission concernant un ACSSI. Il s'adresse alors à MMSC afin que celle-ci lui transmette dans les plus brefs délais les éléments relatifs :
- aux détenteurs 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.

4.4. Mesures conservatoires

MMSC est avertie sans délai et décide des mesures conservatoires à prendre au plus tôt selon l'incident : révocation de l'équipement du réseau de chiffrement 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'OSIIC.

4.5. 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. Le compte rendu d'incident initial est adressé à l'autorité responsable :
- dans les 24 heures pour tout incident portant sur les clés de chiffrement opérationnelles et tout incident avéré (sabotage, vol, piégeage, copie non autorisée) ;
- dans les 72 heures pour tout autre incident.

5. Inspections

Au-delà des inventaires annuels, le HFDS peut à son initiative, décider d'inspections programmées ou inopinées. Ces inspections visent à vérifier la bonne tenue et l'efficacité du suivi spécifique des ACSSI ainsi que le respect effectif des mesures de protection. L'inspection se limite à des constats visuels, sans porter atteinte à l'intégrité ou aux fonctions de sécurité des ACSSI.

Pour le ministre de l'Économie,
des Finances et de la Relance,

La secrétaire générale,
Haut fonctionnaire de défense et de sécurité,

Marie-Anne BARBAT –LAYANI

Pour la ministre de la Transformation
et de la Fonction Publique

La secrétaire générale,
Haut fonctionnaire de défense et de sécurité,

Marie-Anne BARBAT -LAYANI