Protection des infrastructures critiques : approches physique et cyber

Matinée d'information Horizon 2020
6 novembre 2018

Laurent DUCAMIN
Direction de la protection et de la sécurité de l'Etat
Et
Julien PAYET
Agence nationale de la sécurité des systèmes d'information

Sommaire

1. Principes et bilan de la SAIV
2. La SSI dans la SAIV
3. La dimension européenne

SGDSN

Qu'est-ce qu'une activité d'importance vitale ?

Une activité « *dont l'indisponibilité risquerait de diminuer d'une façon importante le* ***potentiel de guerre ou économique, la sécurité ou la capacité de survie*** *de la nation* »

(extrait de l'article L. 1332-1 du code de la défense)

Les établissements « *dont la destruction ou l'avarie […] peut présenter un* ***danger grave pour la population.*** »

(extrait de l'article L. 1332-2 du code de la défense)

SGDSN

Quelles sont les obligations ?

« Les opérateurs publics ou privés [d'importance vitale] sont tenus de ***coopérer à leurs frais*** *[…] à la protection [des sites qu'ils exploitent] contre toute menace, notamment à caractère terroriste. »*

(extrait de l'article L. 1332-1 du code de la défense)

SGDSN

Quels sont les risques et menaces ?

« […] un acte de malveillance, de sabotage ou de terrorisme »

(extrait de l'article R. 1332-1 du code de la défense)

Depuis 2013, tous les risques auxquels sont potentiellement exposés les opérateurs (risques naturels, technologiques, sanitaires *etc.*).

SGDSN

L'approche « tous risques »

Impact

Pandémie

Accidents de transport, dans une usine

NRBC

Explosifs et IED dans les transports et les ERP

Cyber (SSI)

Inondation

Tempêtes

Feux de forêts

Malveillance Humaine (contamination, tirs d'armes, etc.)

SGDSN

Probabilité et/ou vraisemblance

Définition des secteurs

Arrêté du 2 juin 2006
fixant la liste des SAIV et les ministres coordonnateurs

Douze secteurs d'activités d'importance vitale

Dominante régalienne	Dominante humaine	Dominante économique	Dominante technologique
			
■ Activités civiles de l'Etat	■ Alimentation	■ Energie	■ Industrie
			
■ Activités judicaires	■ Gestion de l'eau	■ Transports	■ Communications électroniques et audiovisuel
			
■ Activités militaires de l'Etat	■ Santé	■ Finances	■ Espace et recherche

SGDSN

La directive nationale de sécurité

CONFIDENTIEL DÉFENSE

Ministère de l'Environnement, de l'Énergie et de la Mer

Sécurité des activités d'importance vitale

DIRECTIVE NATIONALE DE SECURITE

SECTEUR DES TRANSPORTS

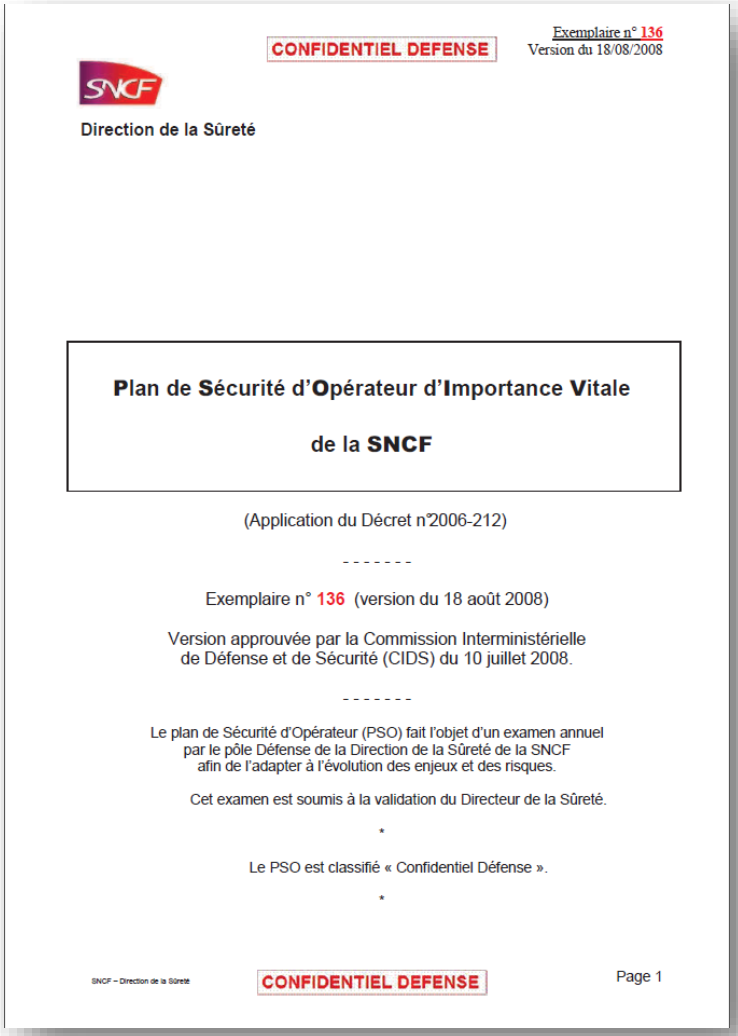
Sous-secteur des transports terrestres

Édition janvier 2016

CONFIDENTIEL DÉFENSE

SGDSN

Le plan de sécurité d'opérateur



CONFIDENTIEL DEFENSE

Exemplaire n° 136
Version du 18/08/2008

SNCF

Direction de la Sûreté

Plan de Sécurité d'Opérateur d'Importance Vitale

de la SNCF

(Application du Décret n°2006-212)

- - - - - - -

Exemplaire n° 136 (version du 18 août 2008)

Version approuvée par la Commission Interministérielle
de Défense et de Sécurité (CIDS) du 10 juillet 2008.

- - - - - - -

Le plan de Sécurité d'Opérateur (PSO) fait l'objet d'un examen annuel
par le pôle Défense de la Direction de la Sûreté de la SNCF
afin de l'adapter à l'évolution des enjeux et des risques.

Cet examen est soumis à la validation du Directeur de la Sûreté.

*

Le PSO est classifié « Confidentiel Défense ».

*

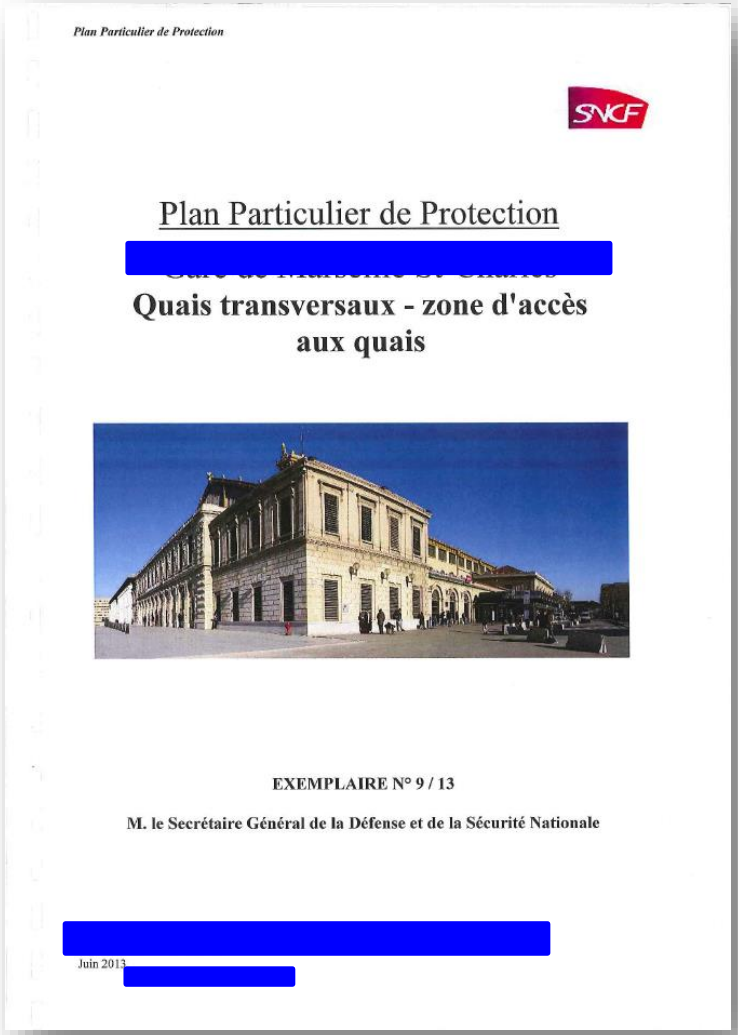
SNCF – Direction de la Sûreté

CONFIDENTIEL DEFENSE

Page 1

SGDSN

Le plan particulier de protection



Plan Particulier de Protection

SNCF

Plan Particulier de Protection

[redacted]

Quais transversaux - zone d'accès aux quais

EXEMPLAIRE N° 9 / 13

M. le Secrétaire Général de la Défense et de la Sécurité Nationale

[redacted]

Juin 2013

SGDSN

Le plan de protection externe

CONFIDENTIEL DEFENSE

Plan de Protection Externe

SNCF
Version 1
13/09/2013

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREFET DE LA REGION PROVENCE ALPES COTE D'AZUR
PREFET DES BOUCHES-DU-RHONE

SNCF

Plan de Protection Externe

[redacted]

Quais transversaux - zone d'accès aux quais

EXEMPLAIRE N° 1 / 10

M. le Secrétaire Général de Défense et de Sécurité Nationale

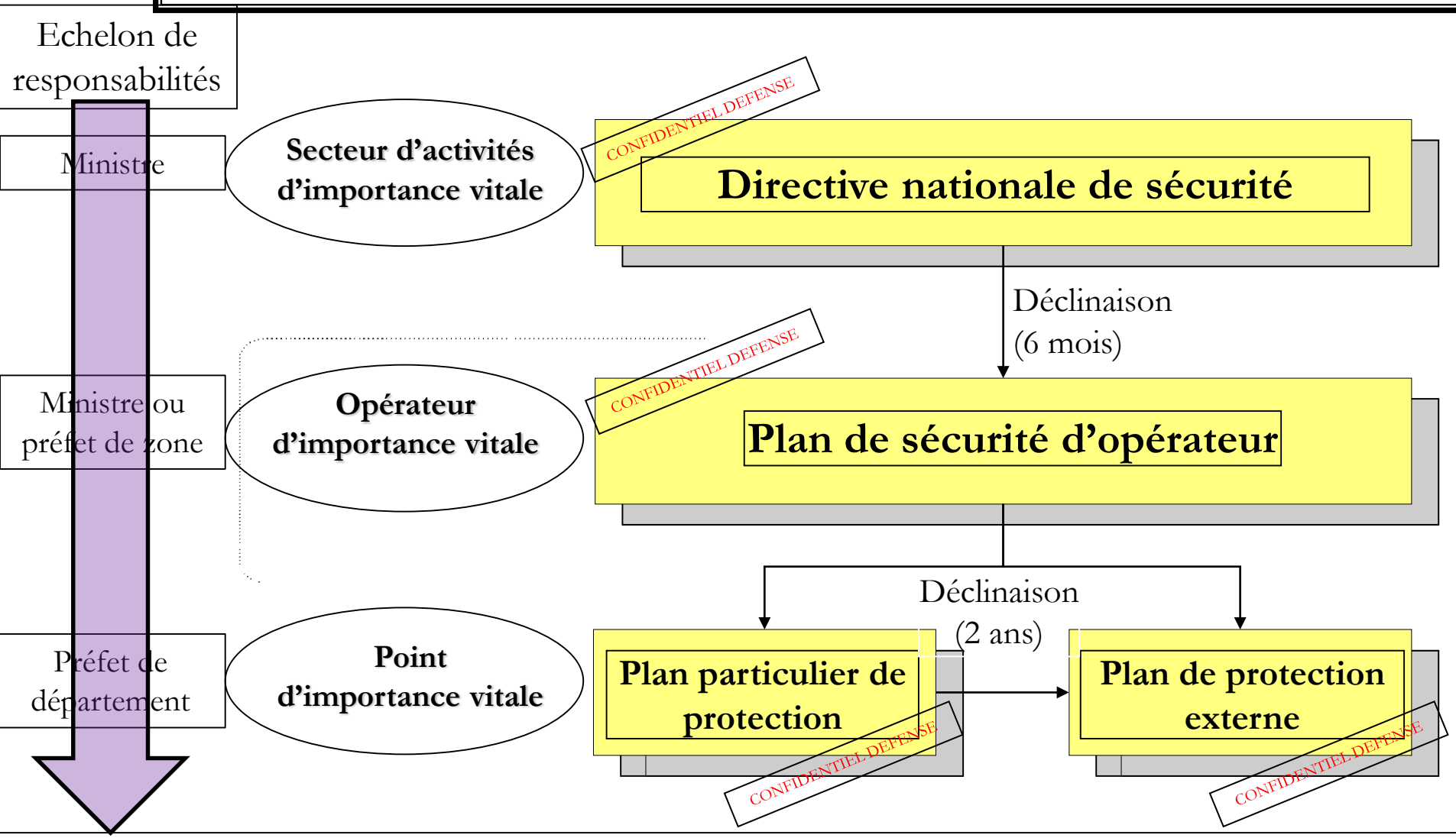
Plan de Protection Externe

Page 1 sur 42

CONFIDENTIEL DEFENSE

SGDSN

Niveaux et responsabilités



Mode d'emploi = instruction générale interministérielle 6600

Bilan quantitatif

- 12 secteurs
- 22 directives nationales de sécurité
- 250 opérateurs d'importance vitale
- < 1500 points d'importance vitale

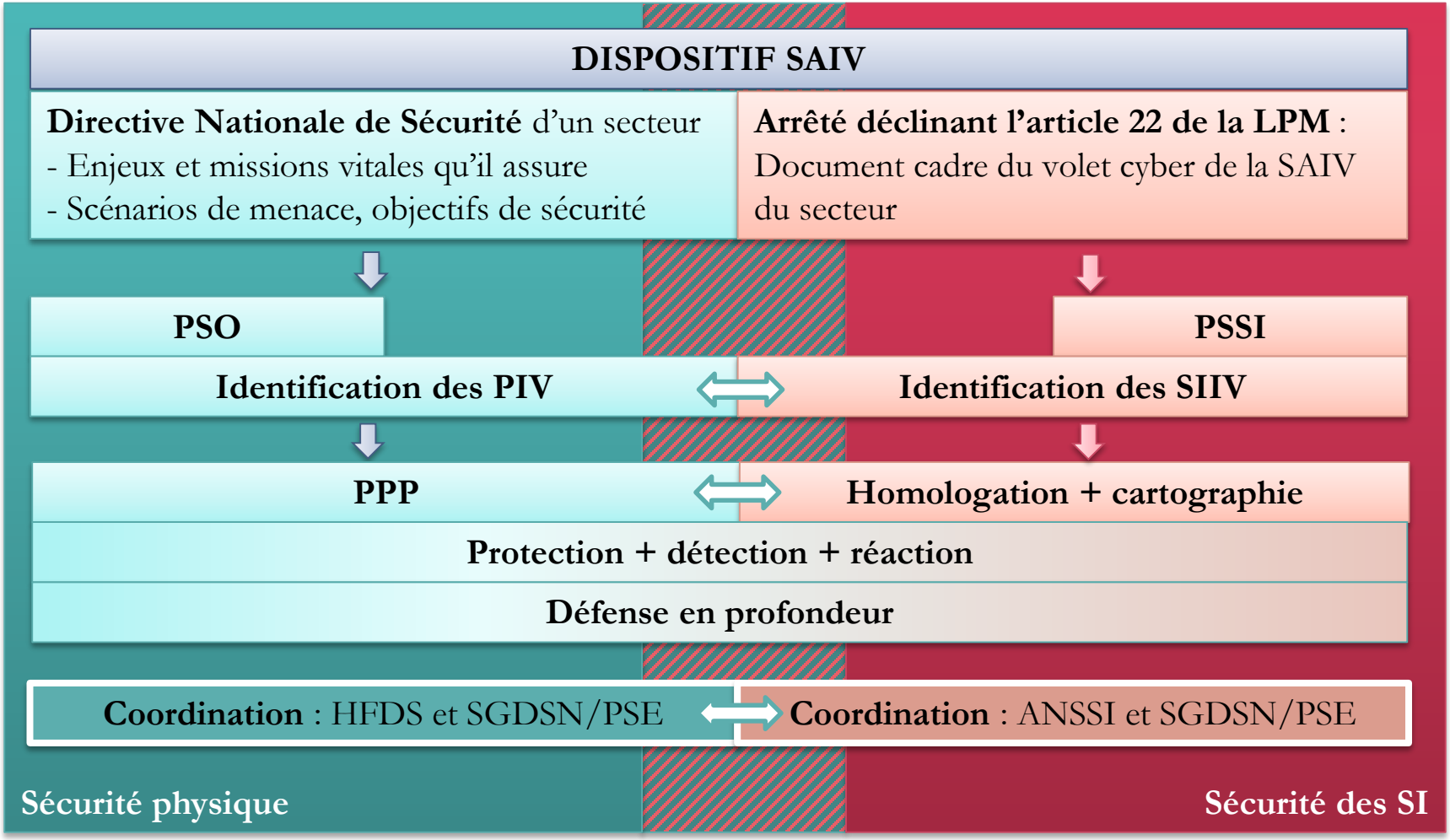
SGDSN

Bilan qualitatif :
une communauté d'intérêts, un cercle de confiance

- Forte implication des ministères coordonnateurs
- Adhésion des opérateurs
- Augmentation de la culture de sécurité
- Application territoriale plus lente

SGDSN

Le volet cyber de la SAIV



Le volet cyber de la SAIV - Enjeux

- Articulation sécurité et SSI : l'un ne va pas sans l'autre !
- Articulation SSI et systèmes industriels (automaticiens)
- Identification des SIIV : exploration des processus métiers pour y déceler ce qui est vital – en lien avec les missions d'importance vitale
- Sensibilisation des sphères privée et public
- **Augmentation du niveau de cybersécurité des OIV, des prestataires et, par diffusion, des autres entités**

Le volet cyber de la SAIV – 4 piliers

- Préalable : identifier les systèmes d'information d'importance vitale (SIIV)

- 4 piliers :
  1. Règles s'appliquant sur les SIIV : organisationnelles, gouvernance, préventives et réactives
  2. Déclaration des incidents SSI à l'ANSSI
  3. Contrôles par l'ANSSI ou un prestataire d'audit SSI qualifié par l'ANSSI
  4. Le Premier ministre peut imposer sur proposition de l'ANSSI des mesures cyber aux OIV en cas de crise cyber majeure

Le volet cyber de la SAIV – L'action de l'ANSSI

- Rencontres, sensibilisation, assistance technique, aide à la réponse aux incidents

- CERT-FR : collecte d'incidents, veille sectorielle et multi-sectorielle, campagnes de marqueurs

- Actions génériques : notes techniques, guides (homologation, systèmes industriels), développement de l'offre technologique, labellisation de prestataires et de fournisseurs

Le volet cyber de la SAIV – Entrée en vigueur des arrêtés

- 1er juillet 2016 : Gestion de l'eau, Alimentation, Produits de santé
- 1er octobre 2016 : Energie (hors nucléaire) et transport
- 1er janvier 2017 : Industrie, Finances, Audiovisuel, Télécoms
- 1er avril 2017 : Nucléaire
- 1er octobre 2017 : Espace et Industrie de défense

- Secteurs restants : étatiques

- **Premier bilan : exercice bien lancé, qui enclenche des discussions et augmente le niveau de maturité des opérateurs. Le plus dur reste à faire : contrôle & suivi de la mise en œuvre!**

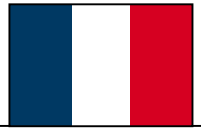
- **En perspective : aller plus loin avec la directive européenne NIS et les opérateurs de service essentiels…**

Le programme européen de protection des infrastructures critiques

- La directive du Conseil du 8 décembre 2008 : infrastructures critiques européennes
- Soutien de la Commission aux Etats membres
- Le réseau d'information CIWIN
- Le réseau européen de référence pour l'expérimentation de solutions de sécurité
- La politique envers les Etats tiers

Le programme européen de protection des infrastructures critiques

❑ Directive 2008/114/CE



❑ Code de la défense (SAIV)

2 secteurs : énergie, transports		12 secteurs
Infrastructure critique européenne	⇒	Point d'importance vitale
Plan de sécurité d'opérateur	⇒	PSO ou PPP
Correspondant pour la sécurité	⇒	Délégué pour la défense et la sécurité

- Equivalence des plans entre les deux dispositifs
- Pas d'autres référentiels que les DNS
- Pas de contrainte supplémentaire pour les opérateurs
- Identification des ICE françaises suite discussions bilatérales avec les Etats voisins

GENÈSE ET PLACE DANS LE PCRD

- Protection des infrastructures critiques : une des quatre missions principales identifiées dès 2006 dans les travaux de l'ESRAB.
- 7ème PCRD – Sécurité (2007-2013)
  - Périmètre CIP hors cyber
  - 55 projets financés pour 259 M€ de subventions
- Horizon 2020 – Défi société sûres
  - Position française pour une approche intégrée protection physique et digitale
  - depuis 2016, un call spécifique et commun entre la DG HOME et la DG CNECT

SGDSN

H2020 - WP 2016 - 2017

- CIP-01-2016-2017: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe.
- Projets financés en 2016 (22 M€ de subventions).
  - SAURON – ports – FR : THALES /MORPHO
  - STOP-IT – water supply
  - DEFENDER – energy – FR : THALES / INEO
- 25 propositions soumises pour 2017 (évaluation en cours)
  - Communication Infrastructure
  - Health Services,
  - Financial Services

SGDSN

Coordonnées

Laurent DUCAMIN
Chef du bureau planification
laurent.ducamin@sgdsn.gouv.fr
Secrétariat général de la défense et de la sécurité nationale
Direction de la protection et de la sécurité de l'Etat
www.sgdsn.gouv.fr

Julien PAYET
julien.payet@ssi.gouv.fr
Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Sous-direction stratégie
www.sss.gouv.fr