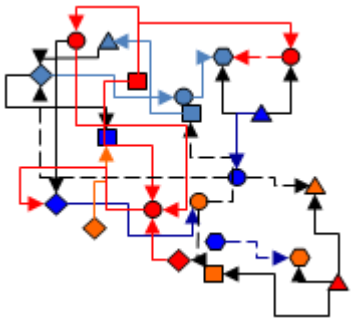
# SECURITE DES ACTIVITES D'IMPORTANCE VITALE



# GUIDE
# POUR L'ELABORATION D'UN PLAN DE SECURITE D'OPERATEUR

VIGIPIRATE

**Edition juillet 2018**

SGDSN

En contribuant aux besoins essentiels des populations, à leur sécurité ou au fonctionnement de l'économie, de nombreux opérateurs publics et privés revêtent un caractère indispensable pour la Nation.

Ces opérateurs d'importance vitale (OIV) sont ainsi des acteurs majeurs du dispositif de sécurité des activités d'importance vitale (SAIV) dont l'objectif est de les protéger plus efficacement contre une menace terroriste élevée et multiforme, des aléas climatiques, des risques technologiques ou des attaques de plus en plus fréquentes et agressives contre les systèmes d'information.

Le dispositif SAIV doit ainsi permettre aux opérateurs d'analyser leurs risques et d'appliquer les mesures en cohérence avec les décisions des pouvoirs publics.

Le présent guide propose des conseils aux opérateurs d'importance vitale en vue de l'élaboration et de la mise en œuvre de leur plan de sécurité d'opérateur. Il fournit les éléments généraux facilitant l'élaboration du plan et cerne les points à considérer. Il n'a pas de valeur contraignante pour les opérateurs.

Il complète et précise les éléments fournis par la réglementation et par l'instruction générale interministérielle N° 6600/SGDSN/PSE/PSN du 7 janvier 2014.

# Table des matières

# INTRODUCTION : QU'EST-CE QU'UN PSO ?

Le plan de sécurité d'opérateur définit la politique et l'organisation de la sécurité de l'opérateur. Il précise, de façon générique, les mesures à mettre en œuvre pour chaque point d'importance vitale (PIV) tant sur le plan organisationnel (organiser l'alerte et gérer la crise), qu'en matière de prévention (réduire les vulnérabilités) et de protection (réduire les conséquences).

Il est fondé sur une analyse de risque prenant en compte notamment les scénarios de la ou les directives nationales de sécurité (DNS).

Il s'appuie sur le dispositif de sécurité existant et sur l'expérience acquise par l'opérateur dans la gestion de la sécurité et de la sûreté.

*Quelle commission rend un avis sur le PSO ?*

- Le périmètre du PSO dépasse celui de la zone de défense : la commission interministérielle de défense de sécurité (CIDS).
- Le périmètre du PSO ne dépasse pas le ressort de la zone de défense : la commission zonale de défense et de sécurité (CZDS).
- Les PSO relevant du ministère de la défense ne font pas l'objet d'un avis de la CIDS ou de la CZDS.

Il est rédigé par l'opérateur et fait l'objet d'un avis de la commission interministérielle ou zonale de défense et de sécurité (CIDS ou CZDS) selon le cas, après instruction par le ministre coordonnateur du secteur. L'avis rendu porte aussi bien sur les mesures de sécurité proposées par l'opérateur que sur la liste des PIV.

Pour chaque PIV, l'opérateur est tenu de rédiger un plan particulier de protection (PPP) qui adapte, aux conditions locales de chaque site, les principes du PSO. Le préfet de département approuve le PPP et élabore pour chaque PIV un plan de protection externe (PPE) comportant les mesures de surveillance et d'intervention de la force publique.

Document structurant pour la sécurité de l'OIV, le PSO doit être pensé comme un instrument stratégique qui assiste l'opérateur dans la gestion de sa sécurité. Il doit permettre à l'opérateur de s'interroger sur des scénarios majeurs et, le cas échéant, de repenser certains dispositifs opérationnels. Il doit également amener à une connaissance partagée de ces enjeux avec les pouvoirs publics.

Le PSO, ainsi que tous les documents qui s'y rattachent, sont protégés par le secret de la défense nationale. Ils ne sont communiqués qu'aux personnes ayant à en connaître (SGDSN, ministère coordonnateur, préfets de la zone de défense et de sécurité et du département concerné).

# 1. DESCRIPTION DE L'ATTENDU

## 1.1. Principes généraux

Les articles R. 1332-19 et suivants du code de la défense prévoient que l'opérateur élabore un plan de sécurité d'opérateur à partir d'une ou plusieurs directives nationales de sécurité qui lui ont été notifiées.

Le PSO décrit l'organisation et la politique de sécurité de l'opérateur. Il lui permet, en outre, de s'assurer d'une cohérence dans l'organisation de la sécurité de ses différents points d'importance vitale. Ainsi, le plan particulier de protection de chaque PIV se conforme à la politique globale de sécurité définie préalablement dans le PSO. Par ailleurs, le PSO étant

établi sur un plan-type, il assure un niveau d'exigence commun entre les opérateurs d'un même secteur d'activités.

Le PSO permet également de constituer un référentiel pour la sécurité des sites qui n'ont pas été retenus comme point d'importance vitale.

## 1.2. Cadre d'élaboration

Le plan du PSO doit respecter le modèle type annexé à l'arrêté du Premier ministre du 2 juillet 2018. Ce plan-type doit permettre à l'opérateur de ne rien omettre dans la rédaction du PSO et assure, pour les pouvoirs publics, un canevas commun pour l'ensemble des OIV.

L'opérateur prend en compte la ou les DNS qui lui ont été notifiées. Il définit sa politique de sécurité en intégrant, d'une part, les objectifs généraux de sécurité énoncés dans la DNS et, d'autre part, en déclinant les scénarios de menace listés dans celles-ci.

Il mentionne les autres obligations juridiques éventuelles ou conventions de service public pouvant exister.

*Cas d'un opérateur intéressant plusieurs DNS*

- Les ministères concernés et la CIDS se concertent pour définir un correspondant privilégié pour l'OIV.
- Le correspondant privilégié transmet à l'opérateur les DNS nécessaires à l'élaboration du PSO.
- L'opérateur rédige son PSO à partir des DNS qui lui ont été notifiées et le transmet au ministère retenu comme « correspondant privilégié ».

L'OIV peut, s'il le souhaite, solliciter son ministère coordonnateur pour l'aider dans la rédaction du PSO.

La rédaction du PSO se fera sur un poste informatique sécurisé.

## 1.3. Base documentaire

Pour l'accompagner dans la rédaction de son PSO, l'opérateur dispose des documents suivants :

- articles L. 1332-1 à L. 1332-7 du code de la défense ;
- articles R. 1332-1 à R. 1332-45 du code de la défense ;
- le plan VIGIPIRATE du 1er décembre 2016 (parties publique et confidentielle) ;
- l'instruction générale interministérielle relative à la sécurité des activités d'importance vitale n° 6600/SGDSN/PSE/PSN du 7 janvier 2014 ;
- l'instruction méthodologique d'analyse de risque fixée par arrêté du Premier ministre du 2 juillet 2018 ;
- le plan-type du PSO annexé à l'arrêté du Premier ministre du 2 juillet 2018 ;
- la ou les directives nationales de sécurité qui lui ont été notifiées ;
- le présent guide d'élaboration du plan de sécurité d'opérateur.

## 1.4. Articulation avec les plans et règlementations existants

### *1.4.1. Le plan VIGIPIRATE*

L'opérateur décline et adapte dans son PSO les mesures sectorielles et les mesures des domaines transverses du plan VIGIPIRATE qui lui sont applicables et qu'il est susceptible de mettre en œuvre pour atteindre les objectifs de sécurité fixés par la DNS.

Le PSO permet une forte collaboration entre l'État et l'ensemble des opérateurs désignés d'importance vitale afin de prendre des dispositions cohérentes avec celles que le Gouvernement aura arrêtées ou recommandées au niveau national.

### *1.4.2. Le plan de continuité d'activité (PCA)*

Le PCA décrit la stratégie adoptée par une organisation pour rétablir et reprendre son activité à la suite d'une perturbation importante. En listant et hiérarchisant l'ensemble des scénarios de risque et de menace pour un secteur donné, la directive nationale de sécurité constitue un référentiel pour le PCA et le PSO. Si ce dernier insiste sur les actes de malveillance (terrorisme, sabotage etc.), le PCA doit tenir compte de l'ensemble des scénarios.

Les OIV sont désormais tenus de rédiger un plan de continuité d'activité (article L. 2151-1 du code de la défense). Ils ont la possibilité de le décliner pour chacun de leur PIV.

Il est recommandé pour l'élaboration de ce plan de continuité d'activité, d'utiliser le guide méthodologique proposé par le secrétariat général de la défense et de la sécurité nationale (SGDSN) intitulé *Guide pour réaliser un plan de continuité d'activité.* Il est disponible sur le site internet www.sgdsn.gouv.fr/.

### *1.4.3. La sécurité des systèmes d'information, l'application des articles L. 1332-6-1 à L. 1332-6-6 du code de la défense*

Les dispositions réglementaires issues de l'article 22 de la loi de programmation militaire du 18 décembre 2013 imposent de nouvelles obligations aux opérateurs d'importance vitale en matière de sécurité de leurs systèmes d'information. Elles comprennent la désignation des systèmes d'information d'importance vitale (SIIV), la déclaration d'incidents et la mise en œuvre de règles fixées par l'ANSSI. Les mesures SSI décrites dans le PSO doivent être cohérentes avec les arrêtés sectoriels pris en application de l'article L. 1332-6-1 du code de la défense.

L'identification des SIIV s'appuie sur les missions et activités essentielles définies dans la DNS.

Bien que n'étant pas soumis à l'avis de la CIDS ou CZDS, la liste des systèmes d'information d'importance vitale peut figurer dans le PSO.

### *1.4.4. La révision des directives nationales de sécurité (DNS)*

Le processus de révision des DNS lancé en 2013 à trois objectifs principaux : prendre en compte le nouveau plan VIGIPIRATE, renforcer la sécurité des systèmes d'information et adopter une approche tous risques afin d'inciter les opérateurs à se préparer à faire face à toutes sortes de crises affectant leurs ressources (humaines, immobilières, réseaux...), en élaborant des plans de continuité d'activité (PCA).

*Quand réviser son PSO ?*

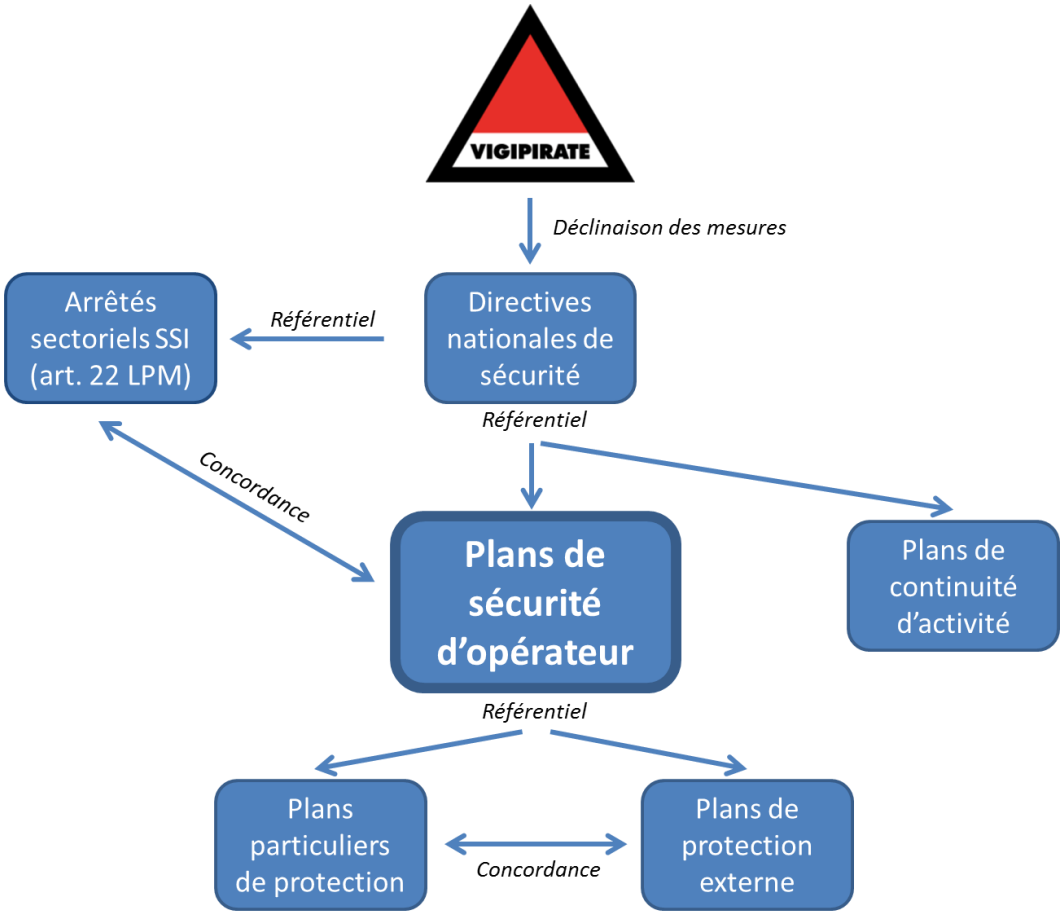
- En cas de notification d'une DNS révisée.
- Sur initiative de l'opérateur, en cas de modification majeure de son organisation ou de sa politique de sécurité.

Les DNS, qui constituaient déjà un référentiel pour les PSO, le seront dorénavant pour les PCA.

### *1.4.5. La révision des plans de sécurité d'opérateur (PSO)*

La révision du plan VIGIPIRATE en 2016, l'application des articles L. 1332-6-1 à L. 1332-6-6 du code de la défense et la révision des DNS induisent une nécessaire actualisation du PSO pour tenir compte de ces évolutions. Cette révision doit également permettre à l'opérateur de considérer de nouvelles menaces ou qui se sont accentuées depuis la précédente version du PSO (exemples : attaques cyber, survols de drones, radicalisation…).

### *1.4.6. Schéma de synthèse*



# 2. COMMENT ELABORER UN PSO ? PRINCIPES DIRECTEURS PAR CHAPITRE

Cette section présente des lignes directrices des étapes à réaliser en mettant l'accent sur la cohérence entre la politique de protection des points d'importance vitale, le dispositif VIGIPIRATE et les mesures de renforcement de la sécurité des systèmes d'information.

Elle suit les chapitres du plan-type du PSO assurant à l'opérateur la prise en compte des principaux enjeux de sécurité.

## 2.1. Préambule : rapport de présentation (non classifié)

Le préambule doit rappeler les principales dispositions du PSO : la méthodologie d'élaboration, les différents acteurs, les objectifs du plan, l'articulation avec les plans et réglementations en vigueur.

Le contenu du rapport de présentation doit être pensé pour pouvoir s'adresser à une population restreinte, interne à l'entreprise, mais pas nécessairement habilitée au niveau « confidentiel défense » (exemple : membres du conseil d'administration, instances représentatives du personnel, etc.).

## 2.2. Introduction. Champ d'application du plan de sécurité d'opérateur d'importance vitale

L'opérateur présente succinctement son activité, son organisation interne, les missions qu'il considère d'importance vitale au regard de la DNS.

Il peut préciser également les limites éventuelles de la démarche d'élaboration du plan de sécurité d'opérateur (interdépendances, implantations en dehors du territoire national).

## 2.3. Analyse de risque

Objectif

L'analyse de risque doit permettre à l'opérateur de définir les priorités de sa politique de sécurité en s'appropriant la DNS (notamment en reprenant les scénarios de menace qui y sont présentés). Il complète ces scénarios par ceux qu'il estime pertinents au regard de son activité.

L'analyse de risque doit également tenir compte de l'appréciation des impacts, de l'analyse des vulnérabilités propres à l'opérateur, de la probabilité d'occurrence (dans le cas d'aléas naturels) et de l'attractivité (dans le cas de malveillances).

L'appréciation de ces éléments (menace, impact, vulnérabilité, occurrence, attractivité) permet d'évaluer le risque pour chacun des points qu'il souhaite qualifier d'importance vitale. Ainsi, la hiérarchisation des scénarios peut varier en fonction des spécificités locales des PIV retenus.

**Exemple** : le risque cyclonique sera élevé dans une zone intertropicale comme la Polynésie et nul en métropole.

Méthode

Aucune méthode d'analyse de risque n'est imposée dans la rédaction du PSO. Le ministère coordonnateur en charge de l'instruction du dossier, ainsi que la commission interministérielle ou zonale de défense et de sécurité, jugeront de la pertinence et des résultats de la méthode.

Comme référence, l'opérateur peut utiliser l'instruction méthodologique d'analyse de risque fixée par arrêté du Premier ministre du 2 juillet 2018.

## 2.4. Mesures destinées à réduire les risques – mise en œuvre du plan VIGIPIRATE

Objectifs

Les mesures décrites dans le PSO doivent permettre à chaque délégué pour la défense et la sécurité d'un point d'importance vitale de décliner localement, en fonction de son contexte spécifique, le dispositif de sécurité global et les mesures opérationnelles. L'ensemble étant regroupé dans le plan particulier de protection (PPP).

Les délais de réalisation des mesures de protection permanentes et des mesures temporaires et graduées sont indiqués.

Les mesures de sécurité du plan de sécurité d'opérateur s'appuient sur les dispositifs existants.

Mise en œuvre du plan VIGIPIRATE

Les mesures de sécurité prises par l'opérateur doivent être cohérentes avec les objectifs et les exigences de sécurité de la DNS. En effet, la DNS précise les mesures du plan VIGIPIRATE applicables au secteur ou sous-secteur. Le PSO décline ces mesures qui doivent être classées en :

- **mesures socles**, correspondant aux investissements indispensables et aux actions permanentes de vigilance ;
- **mesures additionnelles** activables en fonction des consignes transmises à l'opérateur dans le cadre de l'activation de mesures spécifiques du plan VIGIPIRATE. Ces mesures peuvent être techniques, organisationnelles ou comportementales.

Les mesures du plan VIGIPIRATE, volontairement larges, doivent être adaptées et déclinées au contexte de l'entreprise. C'est l'objet du PSO et des PPP.

**Exemple** : la mesure additionnelle BAT 31-01 « renforcer la surveillance interne et limiter les flux (dont interdiction de zone) » peut se décliner concrètement en contrôlant et limitant l'accès aux zones névralgiques des PIV (relevé des identités de chaque personne qui accède à la zone, interdire l'accès en dehors des heures d'ouverture du PIV, s'assurer que les personnes soient accompagnées…).

## 2.5. Dispositif d'alerte et de gestion de crise

Cette partie traite des procédures spécifiques à la gestion des situations d'urgence :

- prévention de crise (veille, gestion des signaux faibles) ;
- gestion de l'alerte (schéma d'alerte, gestion des astreintes, remontée d'incidents) ;

- organisation de la cellule de crise (fonctionnement de la cellule de crise, liaison avec les autres cellules de crise et les centres opérationnels des pouvoirs publics) ;
- continuité et reprise d'activité (description succincte de la stratégie de continuité d'activité, gestion du mode dégradé, liste des scénarios retenus dans le PCA) ;
- formations, entrainements, exercices (typologie, périodicité, retour d'expérience).

NB. Certaines procédures décrites dans cette partie peuvent être redondantes avec la description de mesures VIGIPIRATE du chapitre précédent (exemple : les objectifs de sécurité du domaine « alerte-intervention »). Aussi faut-il décrire les mesures qu'une seule fois et faire des références si besoin.

**Exemple** : les procédures d'alerte et de gestion de crise existent souvent dans les entreprises de manière formelle ou informelle. Il n'y a pas de format à privilégier, l'essentiel étant que ces procédures soit applicables et facilement assimilables par l'organisation. L'opérateur peut s'en assurer à travers des exercices réguliers.

## 2.6. Dispositions de sauvegarde des personnes et des biens - plans de secours

Les plans de secours déjà réalisés comme le plan de sauvegarde en cas de crue, le plan d'organisation interne (POI) peuvent être intégrés ou rappelés dans cette partie par l'opérateur. L'articulation avec le dispositif ORSEC est également à prévoir.

**Exemple** : une société concessionnaire d'autoroutes va rappeler les plans d'intervention et de sécurité (PIS) qui la concerne. Elle peut en expliquer les grands principes, les obligations auquel elle est assujettie (surveillance des installations, interventions…) et qui auraient un intérêt dans le cadre du PSO.

## 2.7. Mesures génériques de protection par type de point d'importance vitale

L'opérateur détaille, par type de PIV, les mesures de protection génériques (passives et actives, techniques et organisationnelles : types de clôtures, d'éclairage, de surveillance, de contrôles, de protection de son système d'information, etc.) qui seront effectivement retenues et déclinées de façon plus précise dans chaque plan particulier de protection de point d'importance vitale.

Obligations en matière de SSI

Les mesures de sécurité du plan de sécurité d'opérateur répondent directement de la spécificité des fonctions concernées au regard de leurs vulnérabilités, des menaces particulières auxquelles elles sont exposées et des conséquences pouvant en résulter. Les mesures génériques de SSI doivent être cohérentes avec les obligations liées à l'application des articles L. 1332-6-1 à L. 1332-6-6 du code de la défense.

Les délais de réalisation des mesures de protection sont indiqués.

Bien que n'étant pas soumis à l'avis de la CIDS ou CZDS, la liste des systèmes d'information d'importance vitale peut figurer dans le PSO.

**Exemple** : selon la stratégie de sécurité de l'opérateur, les mesures génériques peuvent être très précises (« tous les PIV devront être équipés d'une clôture périmétrique de 3 mètres minimum et ils devront disposer d'un système de vidéosurveillance ») ou ne se limiter qu'à des mesures organisationnelles (« tous les PIV devront rendre le port du badge obligatoire »). Le degré de précision est défini par l'opérateur.

## 2.8. Relations avec les services de l'Etat - délégué pour la défense et la sécurité

L'opérateur décrit ses relations avec les pouvoirs publics, notamment dans le cadre du plan VIGIPIRATE (à l'échelle nationale, zonale ou locale).

Il porte une attention particulière aux mesures dont l'application relève d'actions conjointes de l'opérateur et des pouvoirs publics. En effet, l'opérateur reçoit directement de son ministère de tutelle des instructions classifiées qui doivent être transmises et déclinées pour ses PIV. Les préfets s'assurent ensuite, auprès des opérateurs de leur département, de la cohérence des mesures adoptées. La mise en œuvre concrète de ce circuit d'information doit être précisée.

Les coordonnées du DDS et éventuellement des correspondants locaux, habilités au niveau confidentiel défense, sont indiquées.

**Exemple** : pour un établissement de santé qui interagit à différents niveaux avec les services de l'Etat, un schéma peut illustrer le mécanisme de déclenchement des mesures du plan VIGIPIRATE. Il précisera ainsi les relations avec le centre de crise du ministère de la santé (CORRUS), avec le centre opérationnel zonal (COZ) et le centre opérationnel départemental (COD).

*Le rôle du DDS*

Le délégué pour la défense et la sécurité joue un rôle prépondérant au sein du dispositif SAIV. Interlocuteur privilégié des autorités publiques, il coordonne la rédaction du PSO et des PPP, il reçoit, adapte et diffuse les postures VIGIPIRATE. Il participe ainsi la planification de défense et de sécurité nationale.

## 2.9. Dépendances vis-à-vis d'autres secteurs d'activités d'importance vitale

Les dépendances amont envers d'autres systèmes (énergie, télécommunications…) doivent être prises en compte dans l'analyse globale de sécurité.

De la même manière, les dépendances aval (conséquences de l'arrêt de l'opérateur pour d'autres secteurs d'activités d'importance vitale) doivent être décrites.

Enfin, les aspects internationaux doivent également être considérés (dépendance envers d'autres pays).

La description des interdépendances doit permettre à l'opérateur de s'assurer que ces vulnérabilités sont correctement identifiées et, au besoin, redondées. De la même façon, cette information permet aux pouvoirs publics d'identifier d'éventuels opérateurs qui répondraient aux critères d'un OIV.

**Exemple** : un laboratoire pharmaceutique précisera, dans la mesure du possible, son niveau de dépendance en matières premières importées de l'étranger.

## 2.10. Annexe : liste des points d'importance vitale

Cette liste énumère les points d'importance vitale retenus par l'opérateur. Elle doit préciser succinctement la nature de l'activité de chacun des points. Un point d'importance vitale peut être constitué de composants essentiels appelés alors points névralgiques[1].

Le choix d'un PIV est fait à partir :

- des critères qui peuvent être définis dans la ou les DNS qui concernent l'opérateur ;
- de l'analyse de risque réalisée par l'opérateur ;
- des sites difficilement remplaçables ou substituables qui participent aux activités essentielles de l'opérateur ;
- des sites dont la destruction ou l'avarie peut présenter un danger grave pour la population.

Le fait qu'un site dispose de moyens de protection et prévention efficaces ne lui retire pas son caractère indispensable à l'échelle de la Nation. Il ne peut donc s'agir d'un critère pour écarter un site de la liste des PIV.

[1] Point névralgique : point à la fois vital et vulnérable, qui peut n'être qu'un composant d'un point d'importance vitale.