Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

SECRETARIAT GENERAL DE LA DEFENSE
ET DE LA SECURITE NATIONALE

Direction Protection et Sécurité de l'Etat

INSTRUCTION GENERALE INTERMINISTERIELLE RELATIVE A LA SECURITE DES ACTIVITES D'IMPORTANCE VITALE

N°6600/SGDSN/PSE/PSN du 7 janvier 2014

N° NOR : PRMD1400503J

Annule et remplace l'instruction générale interministérielle n°6600/SGDSN/PSE/PPS du 26 septembre 2008

SOMMAIRE

ANNEXES 4

ILLUSTRATIONS 4

INTRODUCTION 6

1. PRINCIPES GENERAUX 7

1.1. ARCHITECTURE GENERALE DU DISPOSITIF SAIV ET PLAN VIGIPIRATE 7
1.2. SECTEURS D'ACTIVITES D'IMPORTANCE VITALE 8
1.3. LE DIALOGUE ETAT-OPERATEUR POUR LA PLANIFICATION DE SECURITE 9

2. LES ACTEURS DE LA SAIV 10

2.1. LES INSTANCES NATIONALES 10
2.1.1. Le Premier ministre 10
2.1.2. Le Secrétariat général de la défense et de la sécurité nationale (SGDSN) 10
2.1.3. La commission interministérielle de défense et de sécurité (CIDS) 10
2.2. LE MINISTRE COORDONNATEUR 10
2.2.1. Rôle du ministre coordonnateur 10
2.2.2. Rôle particulier du ministre de l'intérieur 11
2.3. LES INSTANCES TERRITORIALES 11
2.3.1. Le préfet de zone de défense et de sécurité 11
2.3.2. La commission zonale de défense et de sécurité (CZDS) 11
2.3.3. Le préfet de département 12
2.4. L'OPERATEUR D'IMPORTANCE VITALE (OIV) 13
2.4.1. Processus de désignation d'un OIV 13
2.4.2. Critères de désignation d'un OIV 15
2.4.3. Le délégué pour la défense et la sécurité (DDS) 17

3. LE DISPOSITIF DE SAIV 18

3.1. LA DIRECTIVE NATIONALE DE SECURITE (DNS) 18
3.1.1. Définition et objectifs 18
3.1.2. Modalités d'élaboration 18
3.1.3. Transmission des DNS aux OIV 18
3.1.4. Modalités de révision 19
3.2. LE PLAN DE SECURITE D'OPERATEUR (PSO) 19
3.2.1. Contenu du PSO 19
3.2.2. Outils et méthodologie 19
3.2.3. Elaboration 20
3.2.4. Mise en œuvre du PSO 20
3.2.5. Révision du PSO 20
3.3. LE POINT D'IMPORTANCE VITALE (PIV) 21
3.3.1. Définition d'un PIV 21
3.3.2. Périmètre d'un PIV et notion de composant névralgique 22
3.3.3. Processus de désignation d'un PIV 22
3.3.4. Modalités de contrôle des personnes accédant à un PIV 24
3.3.5. Modification des conditions d'exploitation ou cession d'un PIV 28
3.4. LA ZONE D'IMPORTANCE VITALE (ZIV) 28
3.5. LE PLAN PARTICULIER DE PROTECTION (PPP) 30
3.5.1. Approbation du PPP 31
3.5.2. Mise en œuvre du PPP 31
3.5.3. Révision du PPP 31
3.5.4. Modification du PPP par le préfet de département 32
3.5.5. Diffusion du PPP 32
3.5.6. Mise en œuvre d'équivalences 32
3.5.7. Le PPP de zone d'importance vitale 33

3.6. PLAN DE PROTECTION EXTERNE (PPE) 34
3.7. GESTION DE LA CONFIDENTIALITE ET PROTECTION DU SECRET DE LA DEFENSE NATIONALE 34
3.7.1. Elaboration, conservation et transmission des documents classifiés 34
3.7.2. Destruction des documents classifiés 35
3.7.3. Cas d'un opérateur ne souhaitant pas mentionner certaines informations jugées très sensibles dans le PSO ou les PPP 35

4. AUDIT ET CONTROLE 35

4.1. AUDIT INTERNE MENE PAR L'OIV 35
4.2. CONTROLES PAR LES PREFETS 35
4.3. CONTROLES PAR LES COMMISSIONS DE DEFENSE ET DE SECURITE 36
4.3.1. Objectifs du contrôle 36
4.3.2. Préparation du contrôle sur place 37
4.3.3. Déroulement du contrôle 38
4.3.4. Rapport de contrôle 40

5. PARTICULARITES DU SECTEUR D'ACTIVITES D'IMPORTANCE VITALE « ACTIVITES MILITAIRES DE L'ETAT » 41

5.1. LE PROCESSUS DE SECURITE DES ACTIVITES D'IMPORTANCE VITALE APPLIQUE AU SECTEUR « ACTIVITES MILITAIRES DE L'ETAT » 41
5.2. LE PLAN DE SECURITE D'OPERATEUR 43
5.3. LE PLAN PARTICULIER DE PROTECTION 43
5.3.1. Approbation du PPP 43
5.3.2. Modification du PPP par l'autorité militaire. 43
5.4. PLAN DE PROTECTION EXTERNE 43
5.5. MODALITES DE CONTROLE 43

6. ARTICULATION AVEC D'AUTRES PLANS ET DISPOSITIONS REGLEMENTAIRES 44

6.1. LIEN AVEC LES PLANS D'INTERVENTION : PLANS PIRATE ET DISPOSITIF ORSEC 44
6.2. AUTRES DISPOSITIFS 45
6.2.1. Lien avec les installations prioritaires de défense 45
6.2.2. Lien avec les zones protégées 45
6.2.3. Lien avec les lieux abritant des éléments couverts par le secret de la défense nationale ..45
6.2.4. Lien avec les zones interdites à la prise de vue aérienne et les zones interdites de survol .45
6.2.5. Lien avec les zones maritimes réglementées 46
6.2.6. Lien avec la défense opérationnelle du territoire 46
6.2.7. Lien avec les régimes d'application exceptionnelle 46
6.2.8. Lien avec les plans de continuité d'activité et les plans d'urgence 47
6.3. CAS PARTICULIER DU SECTEUR NUCLEAIRE 47
6.3.1. Installations nucléaires civiles 47
6.3.2. Installations nucléaires intéressant la dissuasion (INID) 48

7. LES INFRASTRUCTURES CRITIQUES EUROPEENNES 49

7.1. DIRECTIVE DU CONSEIL SUR LE RECENSEMENT DES INFRASTRUCTURES CRITIQUES EUROPEENNES 49
7.2. OBLIGATIONS POUR L'ETAT ET LES OPERATEURS 50
7.3. IDENTIFICATION D'UNE INFRASTRUCTURE CRITIQUE EUROPEENNE 50
7.4. DESIGNATION D'UNE INFRASTRUCTURE CRITIQUE EUROPEENNE EN FRANCE 51

8. CONTESTATION DES ACTES PRIS PAR L'AUTORITE ADMINISTRATIVE (ART. R. 1332-33 DU CODE DE LA DEFENSE) 51

8.1. PRINCIPE 51
8.2. EXCEPTION 51

9. BASE DE DONNEES « DIVA » 52

9.1. ATTRIBUTION DU NUMERO D'IDENTIFICATION (TRIPLET) DES PIV ET DES ZIV 52
9.2. INFORMATIONS CONCERNANT LES OIV 52
9.3. INFORMATIONS CONCERNANT LES PIV ET LES ZIV 52

ANNEXES

1. Glossaire
2. Répertoire des acronymes
3. Architecture de la planification anti-terroriste
4. Synoptique des actions à mener selon le niveau de responsabilité
5. Repères chronologiques pour la mise en œuvre du dispositif de sécurité des activités d'importance vitale
6. Transmission des documents
7. Modèle de rapport de contrôle d'un PIV par une commission interministérielle ou zonale de défense et de sécurité des secteurs d'activités d'importance vitale
8. Informations à transmettre pour la mise à jour de la base de données DIVA
9. Modèle de formulaire de demande d'avis adressée à l'autorité administrative avant l'accès d'une personne à un PIV
10. Modèle de formulaire d'information à la personne concernée qu'elle est susceptible de faire l'objet d'une enquête administrative
11. Modèle de formulaire de rejet de demande d'accès à un PIV en cas de demande non recevable
12. Modèle de formulaire de réponse de la préfecture à l'OIV

ILLUSTRATIONS

Figure 1 : Acteurs et documents de sécurité....7
Figure 2 : Relations entre les pouvoirs publics et les opérateurs....9
Figure 3 : Désignation d'un OIV – processus initié par un ministre coordonnateur....14
Figure 4 : Cas particulier de désignation d'un OIV – processus initié par un préfet de département 14
Figure 5 : Processus d'instruction du plan de sécurité d'un opérateur....21
Figure 6 : Processus de désignation d'un PIV....23
Figure 7 : Types de ZIV....29
Figure 8 : Processus de désignation d'une ZIV....30
Figure 9 : Présentation du PPP de zone à l'autorité administrative....33
Figure 10 : Processus SAIV du secteur AME....42

REFERENCES

- Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection
- Articles L. 1332-1 à L. 1332-7 du code de la défense
- Articles R. 1311-39 à R. 1311-43, R. 1332-1 à R.1332-42, et R. 1421-1 du code de la défense
- Décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »
- Décret n° 2012-491 relatif à l'accès aux points d'importance vitale (dit décret « criblage »)
- Arrêté du Premier ministre du 2 juin 2006 modifié fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs, modifié par l'arrêté du 3 juillet 2008
- Arrêté du Premier ministre du 12 mars 2007 pris pour l'application du 1° et du 2° de l'article 12 du décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale
- Arrêté du Premier ministre n° 10166/SGDSN/PSE/CD du 27 avril 2007 portant approbation du plan-type de plan de sécurité d'OIV
- Arrêté du Premier ministre du 27 septembre 2007 portant approbation du plan-type de PPP (PRMD0766738A)
- Arrêté du Premier ministre du 27 septembre 2007 portant approbation du plan-type de plan de protection externe (PRMD0766625A)
- Instruction générale interministérielle n°1300 du 30 novembre 2011 sur la protection du secret de la défense nationale

INTRODUCTION

– POINT-CLE –

Cette instruction constitue le mode d'emploi de la mise en œuvre du dispositif de sécurité des activités d'importance vitale. Elle comporte un rappel des textes législatifs et réglementaires fondateurs auxquels il convient de se référer prioritairement.

Le dispositif de sécurité des activités d'importance vitale (SAIV) est inséré dans le code de la défense (notamment ses articles R. 1332-1 à 1332-42, pris sur le fondement de ses articles L. 1332-1 à 1332-7). Il constitue le cadre législatif et réglementaire permettant d'associer les opérateurs d'importance vitale (OIV), publics ou privés, au système national de protection contre le terrorisme, le sabotage et les actes de malveillance et d'analyser les risques et d'appliquer les mesures de leur niveau en cohérence avec les décisions des pouvoirs publics.

Il réforme en profondeur, en les unifiant, les dispositifs antérieurs applicables aux installations d'importance vitale[1] et aux points et réseaux sensibles[2]. Ce dispositif juridique fait disparaître les anciennes réglementations.

Il s'inscrit plus largement dans une démarche d'ensemble visant à adapter les conditions dans lesquelles la Nation se prémunit contre toute menace, notamment la menace terroriste, explicitement prise en compte dans les articles précités du code de la défense, en améliorant l'articulation des dispositions que mettent en œuvre respectivement les pouvoirs publics et les opérateurs, en particulier dans le cadre du plan Vigipirate.

Le *Livre blanc sur la défense et la sécurité nationale* consacre cette politique comme un élément du renforcement de la résilience de la Nation.

Les objectifs généraux de la réforme visent à faciliter l'application du plan Vigipirate, à associer pleinement les opérateurs à l'effort de vigilance, de prévention et de protection, et à sélectionner rigoureusement les points devant faire l'objet d'une protection efficace adaptée au niveau de la menace.

Le dispositif formalise le dialogue permanent entre l'Etat et les opérateurs afin de mieux assurer leur propre sécurité. Il trouve un prolongement dans le Programme européen de protection des infrastructures critiques. Par ailleurs, selon l'article L2151-4 du code de la défense relatif au service de sécurité nationale, les opérateurs d'importance vitale doivent mettre en place des plans de continuité et de rétablissement d'activité.

La présente version de l'instruction, au bénéfice des avancées et des questions résultant du commencement de la mise en œuvre de la réglementation du SAIV, explicite et développe les conditions d'application de ce régime de protection, notamment dans ses interactions avec d'autres dispositifs concourant à la politique de défense et de résilience de la Nation.

[1] Ordonnance n° 58-1371 du 29 décembre 1958.
[2] Instruction générale interministérielle n° 4600 du 8 février 1993.

1. PRINCIPES GENERAUX

1.1. ARCHITECTURE GENERALE DU DISPOSITIF SAIV ET PLAN VIGIPIRATE

Le dispositif SAIV vise à fournir un cadre adapté pour, d'une part, définir et appliquer des mesures de sécurité pour la protection prioritaire des points d'importance vitale (PIV) contre la menace terroriste, et d'autre part, faciliter les relations entre les opérateurs et les pouvoirs publics, afin de permettre l'application optimale (par les autorités publiques et par les opérateurs) des mesures de vigilance, de prévention et de protection inscrites dans la planification gouvernementale VIGIPIRATE.

Les directives nationales de sécurité (DNS), documents sectoriels, comportent ainsi en annexe la liste des mesures du plan VIGIPIRATE applicables au secteur d'importance vitale concerné.

Parallèlement, les plans de sécurité d'opérateur (PSO) et les plans particuliers de protection des points d'importance vitale (PPP) transposent de manière concrète les mesures du plan VIGIPIRATE, de sorte que toute adaptation de la posture de sécurité décidée par le Premier ministre fasse l'objet d'une application effective par les opérateurs et connue des pouvoirs publics. Il en va de même pour les plans de protection externe (PPE).

Les différents documents de sécurité, émanant soit de l'Etat, soit de l'opérateur, sont ainsi élaborés en cohérence les uns avec les autres.

Par ailleurs, indépendamment des mesures permanentes ou graduées qui figurent dans le PSO et/ou les PPP, les services de l'Etat informent l'opérateur de toute menace spécifique pouvant affecter un ou plusieurs PIV et, dans ce cadre, une discussion peut s'instaurer pour vérifier la pertinence des mesures prévues tant par l'opérateur que les pouvoirs publics.

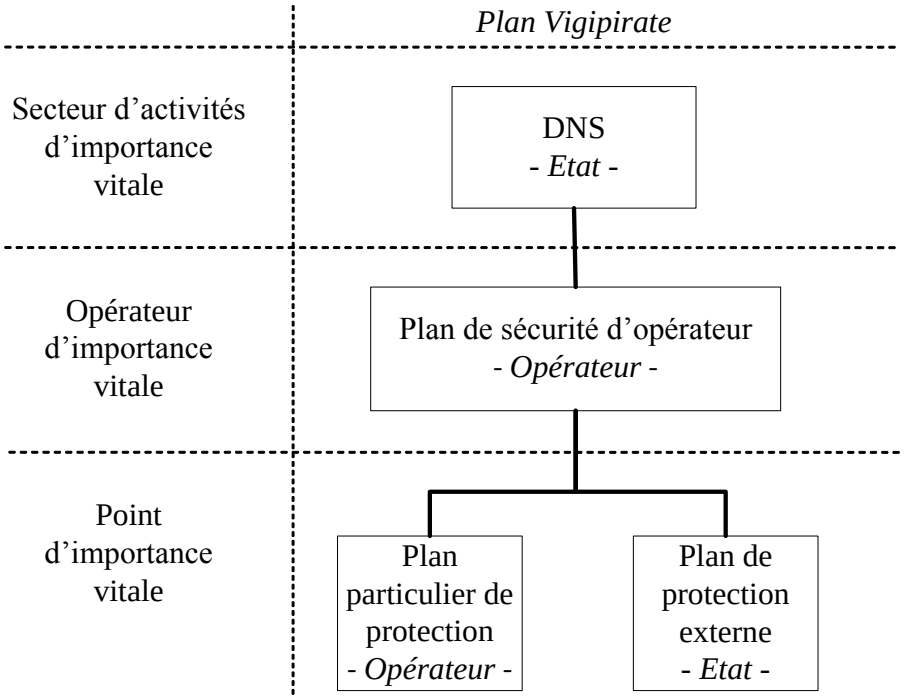


Figure 1 : Acteurs et documents de sécurité

1.2. SECTEURS D'ACTIVITES D'IMPORTANCE VITALE

Les secteurs d'activités d'importance vitale, ainsi que toutes les dispositions qui s'y rapportent, sont définies dans les articles R. 1332-2 et suivants du code de la défense.

Un secteur d'activités d'importance vitale est constitué d'activités concourant à un même objectif.

Ces activités soit ont trait, de manière difficilement substituable ou remplaçable, à la production et la distribution de biens ou de services indispensables, soit peuvent présenter un danger grave pour la population.

Ces biens ou services doivent être indispensables :

- à la satisfaction des besoins essentiels pour la vie des populations ;
- ou à l'exercice de l'autorité de l'Etat ;
- ou au fonctionnement de l'économie ;
- ou au maintien du potentiel de défense ;
- ou à la sécurité de la Nation.

L'arrêté du Premier ministre du 2 juin 2006, modifié par l'arrêté du 3 juillet 2008, fixe la liste des douze secteurs d'activités d'importance vitale et désigne les ministres coordonnateurs desdits secteurs. La liste des secteurs d'importance vitale peut être modifiée par arrêté du Premier ministre, après avis de la commission interministérielle de défense et de sécurité des secteurs d'activités d'importance vitale (CIDS). Le périmètre d'un secteur d'activités est défini dans l'analyse de risque conduite pour élaborer la ou les DNS du secteur.

SECTEUR	MINISTRE COORDONNATEUR
Activités civiles de l'Etat (ACE)	Ministre de l'intérieur
Activités judiciaires	Ministre de la justice
Activités militaires de l'Etat (AME)	Ministre de la défense
Alimentation	Ministre chargé de l'agriculture
Communications électroniques, audiovisuel et information	Ministre chargé des communications électroniques
Energie	Ministre chargé de l'énergie
Espace et recherche	Ministre chargé de la recherche
Finances	Ministre chargé de l'économie et des finances
Gestion de l'eau	Ministre chargé de l'écologie
Industrie	Ministre chargé de l'industrie
Santé	Ministre chargé de la santé
Transports	Ministre chargé des transports

1.3. LE DIALOGUE ETAT-OPERATEUR POUR LA PLANIFICATION DE SECURITE

La résilience se définit comme la volonté et la capacité d'un pays, de la société et des pouvoirs publics à résister aux conséquences d'une agression ou d'une catastrophe majeures, puis à rétablir rapidement leur capacité de fonctionner normalement, ou à tout le moins dans un mode socialement acceptable. Elle concerne non seulement les pouvoirs publics, mais encore les acteurs économiques et la société civile tout entière[3].

L'appropriation collective de la stratégie de défense et de sécurité nationale est la condition *sine qua non* de la résilience de la Nation. Au-delà des ministères concernés, l'Etat doit associer à la mise en œuvre de cette stratégie d'autres acteurs sans lesquels la gestion de crise ne peut être envisagée.[4]

A tous les échelons du dispositif, les autorités étatiques et les OIV sont donc amenés à coopérer pour l'analyse des risques, les mesures de prévention, de vigilance et de protection, et les procédures à mettre en place pour le temps de crise.

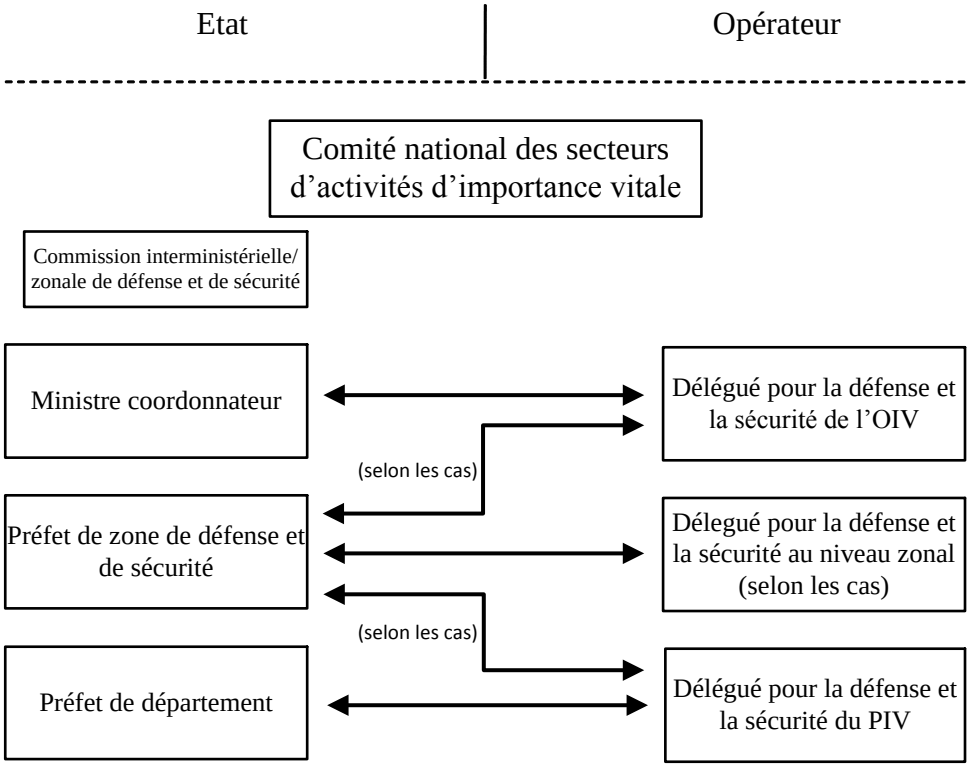


Figure 2 : Relations entre les pouvoirs publics et les opérateurs

[3] Livre Blanc sur la défense et la sécurité nationale, 2008.
[4] Livre Blanc sur la défense et la sécurité nationale, 2013.

2. LES ACTEURS DE LA SAIV

Ce chapitre rappelle les responsabilités de chacune des autorités impliquées dans la mise en place et l'animation du dispositif de sécurité des activités d'importance vitale.

2.1. LES INSTANCES NATIONALES

2.1.1. Le Premier ministre

Le Premier ministre, s'appuyant sur le SGDSN, met en place le cadre général du dispositif de la SAIV en fixant la liste des secteurs, en désignant les ministres coordonnateurs desdits secteurs, en déterminant la méthode d'analyse et de gestion du risque ainsi que la méthode à suivre pour déterminer, par secteur d'activités d'importance vitale, les scénarios de menace et leur hiérarchisation selon le type ou le niveau de menace envisagé, et en élaborant les plans types des PSO, des PPP et des PPE.

Il supervise la mise en place du dispositif et oriente la stratégie de sécurité des activités d'importance vitale.

2.1.2. Le Secrétariat général de la défense et de la sécurité nationale (SGDSN)

Le SGDSN coordonne le dispositif SAIV au niveau national. Il assure la présidence et le secrétariat de la commission interministérielle de défense et de sécurité (CIDS). Il administre la base de données d'importance vitale (DIVA – cf. chapitre 9). Il est l'entité de synthèse nationale en ce qui concerne la progression de la réalisation des PSO et des PPP. Il tient à jour des tableaux de bord qu'il diffuse aux autorités nationales.

2.1.3. La commission interministérielle de défense et de sécurité (CIDS)

La commission est présidée par le secrétaire général de la défense et de la sécurité nationale ou son représentant. Sa composition est définie à l'article R-1332-10 du code de la défense. Elle a un rôle consultatif. Son avis est notamment sollicité sur :

- la désignation des OIV, sur proposition des ministères coordonnateurs ;
- les DNS (sauf celles relevant du ministre de la défense) ;
- les PSO (sauf ceux relevant du ministre de la défense) dont le périmètre dépasse celui d'une zone de défense ;
- la liste des PIV annexée aux PSO, avec la possibilité de proposer des ajouts et des suppressions. Lorsqu'il est fait usage de cette faculté, les motifs en sont portés au compte-rendu.

Elle peut être saisie d'autres sujets tels que mentionnés à l'article R-1332-12.

2.2. LE MINISTRE COORDONNATEUR

2.2.1. Rôle du ministre coordonnateur

Chaque ministre coordonnateur veille à l'application du dispositif SAIV dans les secteurs d'activités dont il a la charge et au sein desquels il :

- élabore la ou les DNS correspondantes ;
- sélectionne et prend les décisions de désignation des OIV après avis de la CIDS ;
- instruit les PSO de ses OIV ;

- transmet les PSO à la CIDS ou à la CZDS suivant le cas de figure (à l'exception du ministre de la défense) ;
- prend les décisions de désignation des PIV.

Il s'assure du respect de la réglementation dans les secteurs d'activités dont il a la charge.

En raison de la nécessité de protection du secret de la défense, le ministre de la défense, ministre coordonnateur du secteur d'activité AME, bénéficie de dispositions dérogatoires au schéma général de mise en œuvre du dispositif SAIV. Ces dérogations sont décrites au chapitre V de la présente instruction.

2.2.2. Rôle particulier du ministre de l'intérieur

Outre son rôle de ministre coordonnateur du secteur d'activités « activités civiles de l'Etat », et sans préjudice des compétences nationales, générales et interministérielles dévolues au SGDSN et des compétences de coordination nationale des ministres dans le secteur d'activité dont ils sont coordonnateurs, l'animation de la mise en œuvre territoriale est assuré par le ministère de l'intérieur, au travers des services du haut fonctionnaire de défense (SHFD).

2.3. LES INSTANCES TERRITORIALES

2.3.1. Le préfet de zone de défense et de sécurité

Le préfet de zone qui, selon l'article R*1311-4 du code de la défense, dirige l'action des préfets de département et des délégués de zone en ce qui concerne les mesures de défense non militaires est l'acteur territorial en charge de la coordination du dispositif SAIV. Il préside la CZDS (cf. paragraphe suivant).

Sous son autorité, l'état-major interministériel de la zone de défense et de sécurité (EMIZDS) reçoit une mission générale d'animation, d'appui aux préfectures, et de relais d'information entre l'échelon central et les échelons départementaux. Celui-ci dirige l'action des délégués de zone de défense et de sécurité et coordonne l'action des correspondants de zone de défense et de sécurité désignés dans les conditions définies aux articles R. 1312-1 à R. 1312-6, afin qu'ils apportent leur concours à l'exercice des missions attribuées au préfet de zone de défense et de sécurité, et notamment celles relatives à la SAIV.

Dans les cinq zones de défense et de sécurité d'outre-mer, cette mission est assurée par les hauts fonctionnaires de zone de défense et de sécurité d'outre-mer définis par l'article R. 1681-2 du code de la défense.

2.3.2. La commission zonale de défense et de sécurité (CZDS)

La CZDS est présidée par le préfet de zone de défense et de sécurité ou son représentant. Sa composition est définie à l'article R. 1332-13 du code de la défense. Elle est chargée d'une mission générale de coordination, d'assistance, et de contrôle de la mise en œuvre des PPP (à l'exception de ceux dépendant d'OIV relevant du ministre de la défense). Elle peut bénéficier de l'expertise et du concours des services déconcentrés de l'Etat, grâce au réseau des délégués de zone des ministères. Elle peut s'adjoindre l'expertise de toute personne qu'elle juge utile.

La commission a un rôle consultatif. Son avis est sollicité sur :

- les PSO des OIV dont le périmètre d'activité ne dépasse pas le ressort de la zone défense. Les PSO sont transmis à la CZDS par l'autorité administrative ayant désigné l'opérateur ;
- la liste des PIV annexée au PSO des OIV de son périmètre avec la capacité de proposer des ajouts ou suppressions ;

- la désignation et le périmètre exact d'une zone d'importance vitale ainsi que sur le PPP de zone d'importance vitale qui lui est transmis par le préfet de département ayant créé ladite zone ;
- la désignation, par un préfet de département, d'un OIV qui gère exclusivement un établissement mentionné à l'article L. 511-1 du code de l'environnement ou comprenant une installation nucléaire de base, quand la destruction ou l'avarie de certaines installations de cet établissement peut présenter un danger grave pour la population, et la désignation du PIV correspondant. Une demande d'avis motivée est préalablement adressée à la commission par le préfet de département concerné.

Sur demande de son président ou du préfet de département concerné, la commission peut être amenée à donner un avis sur les plans de protection externe. Cette démarche permet d'évaluer l'adéquation du plan au regard des moyens zonaux qui pourraient être sollicités.

L'examen des PSO et des PPP suppose des contacts en amont avec les opérateurs afin de les orienter, si nécessaire, dans leurs travaux d'élaboration.

La CZDS peut contrôler sur place les mesures prises pour la sécurité des PIV. Ce contrôle porte sur le PPP et sur le PPE du PIV (ou de la ZIV) (cf. partie 3.4).

Pour le département de Saint-Pierre-et-Miquelon, le rôle de la CZDS est assuré par la CIDS. Sans préjudice du rôle d'animation territoriale qui incombe au ministère de l'intérieur, cette dernière peut conseiller et appuyer le préfet de Saint Pierre et Miquelon dans la mise en œuvre de la présente instruction.

2.3.3. Le préfet de département

Pour l'outre-mer, l'autorité préfectorale est le représentant de l'Etat dans le territoire (préfet, haut-commissaire, administrateur supérieur).

Le préfet de département est chargé de la mise en œuvre du dispositif SAIV en application de la compétence générale qui lui est attribuée de conduite interministérielle des actions de l'Etat, notamment en ce qui concerne la protection des personnes, la sauvegarde des installations et ressources d'intérêt général, ainsi que la production et l'utilisation des diverses catégories de ressources (Art R* 133-33 du code de la défense).

Cette responsabilité s'exerce notamment pour la protection externe des PIV, via le PPE (cf. § 3.6). Il veille à la réalisation effective des mesures de sécurité prévues dans les PPP. Il peut saisir la CZDS de toute question qu'il juge utile. Sur convocation du préfet de zone, il participe à la CZDS.

Ses responsabilités particulières sont les suivantes :

- approbation du PPP des PIV des opérateurs ne relevant pas du ministre de la défense, et du PPP des zones d'importance vitale ;
- décision d'équivalence entre un plan de protection réalisé au titre d'une autre réglementation, et le PPP (voir § 3.5.6) ;
- élaboration du PPE de chaque PIV ou ZIV, en liaison avec le DDS de ce point ou de cette zone ;
- désignation des zones d'importance vitale (ZIV) après avis de l'OGZDS lorsque celle-ci inclut un PIV relevant du ministère de la défense ;
- désignation des OIV qui gèrent exclusivement un établissement mentionné à l'article L. 511-1 du code de l'environnement ou comprenant une installation nucléaire de base, quand la destruction ou l'avarie de certaines installations de cet établissement peut présenter un danger grave pour la population, et désignation du PIV correspondant ;

- mise en demeure de l'opérateur d'établir un PPP ;
- mise en demeure de l'opérateur d'exécuter une mesure de son PPP ;
- injonction à l'opérateur de modifier son PPP.

2.4. L'OPERATEUR D'IMPORTANCE VITALE (OIV)

– POINT-CLE –

L'OIV :
- est désigné par le ministre coordonnateur du secteur concerné ;
- nomme un délégué pour la défense et la sécurité d'opérateur et transmet sa demande d'habilitation ;
- élabore son PSO et le transmet accompagné de la liste des PIV proposés ;
- transmet les demandes d'habilitation des délégués pour la défense et la sécurité des PIV désignés ;
- élabore les PPP et les transmet au préfet pour approbation à l'exception de ceux relevant du ministère de la défense (article R. 1332-23 du code de la défense) ;
- met en œuvre les PPP approuvés ;
est en liaison avec l'autorité administrative en charge de la rédaction du PPE.

2.4.1. Processus de désignation d'un OIV

– POINT-CLE –

L'OIV est désigné par le ministre coordonnateur.

Exception : l'OIV gère seul un établissement mentionné à l'article L. 511-1 du code de l'environnement ou comprenant une installation nucléaire de base, il peut être désigné par le préfet de département.

a - Cas général

L'article R.1332-3 du code de la défense prévoit qu'un OIV est désigné comme tel par le ministre coordonnateur de son secteur d'activités d'importance vitale, en concertation avec le ou les ministres intéressés et après avis de la CIDS ou de la CZDS.

La notification à l'opérateur de l'intention de le désigner OIV est l'occasion d'une concertation entre l'autorité administrative (ministre coordonnateur ou préfet de département selon le cas) et l'opérateur. Dans les deux mois dont il dispose pour faire ses remarques, l'opérateur peut faire connaître à l'autorité administrative ayant émis la notification, la liste et la nature des infrastructures qu'il pourrait par la suite proposer en annexe de son PSO. Le nombre et la nature de ces infrastructures orientent le choix du processus de désignation à mettre en œuvre (voir schémas ci-dessous).

Les OIV relevant du ministère de la défense ne peuvent être désignés que par le ministre de la défense (voir chapitre 5).

b - Cas particulier

Ce principe de désignation comporte toutefois une exception mentionnée au deuxième alinéa de l'article R. 1332-3 du code de la défense. Elle concerne les OIV qui gèrent exclusivement un établissement mentionné à l'article L. 511-1 du code de l'environnement ou comprenant une installation nucléaire de base visée à l'article L. 593-2 du code de l'environnement. Le préfet de département peut s'appuyer sur les DNS pour identifier les opérateurs qui pourraient répondre aux critères permettant de les nommer. Dans ce cas, l'OIV est désigné par le préfet du département dans

le ressort duquel se trouve cet établissement, après avis de la CZDS des secteurs d'activités d'importance vitale, et information du ou des ministres coordonnateurs concernés.

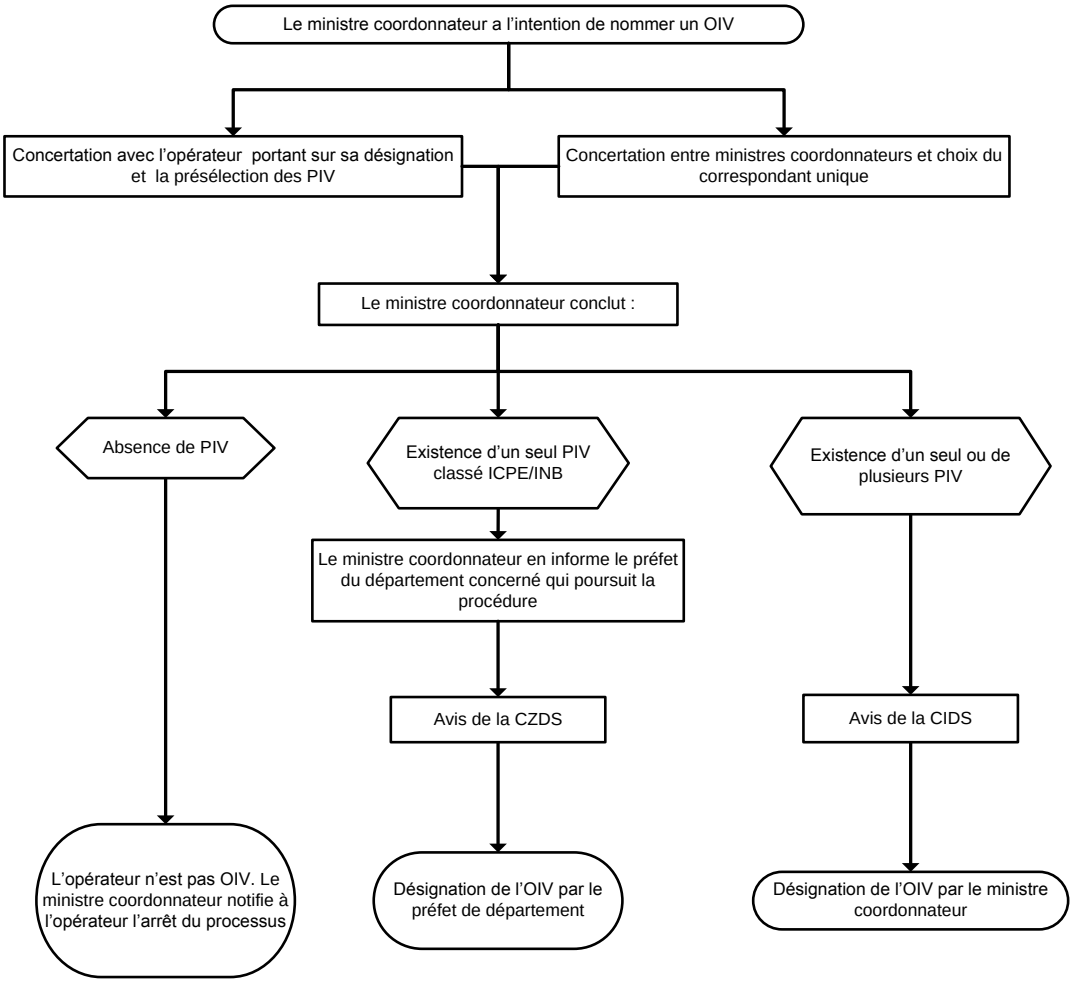


Figure 3 : Désignation d'un OIV – processus initié par un ministre coordonnateur

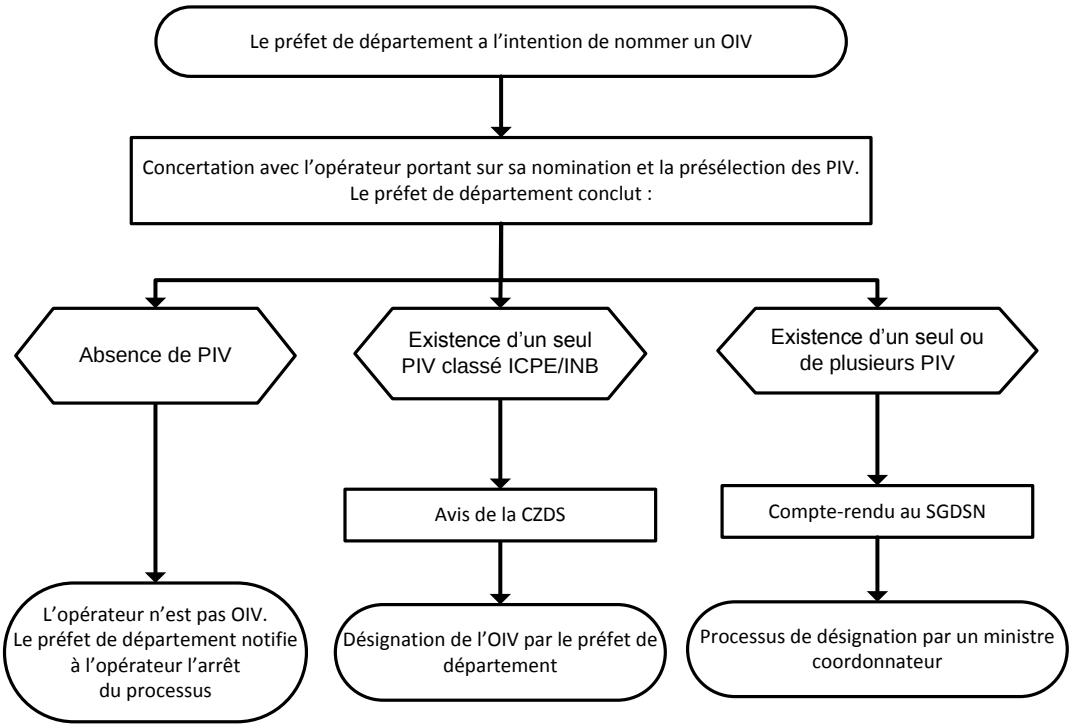


Figure 4 : Cas particulier de désignation d'un OIV – processus initié par un préfet de département

2.4.2. Critères de désignation d'un OIV

– POINT-CLE –

L'existence et la nature d'installations ou d'ouvrages susceptibles d'être désignés PIV conditionnent le processus de désignation de l'OIV.

a - Cas général

Le statut d'OIV repose sur deux conditions :

- que son activité s'exerce en tout ou en partie dans un secteur d'activités d'importance vitale ;
- qu'il gère ou utilise au moins un établissement, un ouvrage ou une installation dont le dommage, l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait de quelque manière que ce soit d'avoir des conséquences majeures sur les capacités de survie de la Nation ou sur la santé ou la vie de la population *(telles que définies par l'article R. 1332-1 du code de la défense*).

☞ Il est, par conséquent, nécessaire de s'attacher à définir l'existence et la nature d'éventuels PIV en amont du processus de désignation d'un OIV.

☞ L'appréciation du caractère d'importance vitale, lié aux conséquences graves d'une menace plausible, quelle que soit la vulnérabilité du point, se fonde sur les critères définis par les différentes DNS, ou, en complément, par le ministre coordonnateur du secteur d'activités (*cf. § 3.3.1*).

▪ Définition des entités susceptibles d'être désignées OIV

De manière générale et sans préjudice des précisions sectorielles apportées par les DNS, un OIV peut être :

- une société ;
- une association, une fondation ou une organisation internationale ;
- un service de l'Etat, une collectivité territoriale, un groupement de collectivités, un établissement public, une autorité administrative indépendante.

S'agissant d'une entreprise, ce peut être une société-mère ou une filiale. Le choix de l'entité *ad hoc* se fait après concertation avec l'opérateur concerné, en prenant en compte :

- son organisation de la sûreté-sécurité et ce pour répondre au mieux aux objectifs de sécurité du dispositif SAIV ;
- le lien entre l'entité retenue et les installations, établissements ou ouvrages susceptibles d'être désignés PIV.

Ainsi, plusieurs filiales d'un même groupe peuvent, le cas échéant, être désignées.

▪ Choix du secteur de rattachement

Lorsque la désignation d'un opérateur est envisagée par un seul ministre coordonnateur, le secteur de rattachement retenu correspond à l'un des secteurs dont ce ministre a la charge. Le cas particulier d'un opérateur relevant de secteurs rattachés à des ministres coordonnateurs différents est traité au paragraphe 'b' ci-dessous.

Lorsqu'un préfet a l'intention de nommer un OIV, le secteur de rattachement correspond à l'activité dans le périmètre duquel se situe l'établissement pressenti comme PIV.

- Notification de la désignation à l'OIV

L'autorité administrative désigne l'OIV par arrêté. L'arrêté doit préciser le ou les secteurs de rattachement ainsi que la ou les DNS applicables (cf. § b).

Dès qu'il a connaissance de sa désignation, l'OIV adresse à l'autorité administrative l'ayant désigné la demande d'habilitation du délégué pour la défense et la sécurité envisagé.

b - Cas particuliers

- Interdépendances d'un opérateur avec des sous-traitants

Dans le cadre de son activité normale, un OIV peut avoir sous-traité ou externalisé une ou plusieurs fonctions concourant à la réalisation de l'activité d'importance vitale. Dans ce cas, il appartient à l'OIV de prendre les dispositions nécessaires vis-à-vis de son sous-traitant ou de son fournisseur, notamment dans les spécifications du contrat les liant, pour que celui-ci concoure à la réalisation des objectifs de sécurité de l'opérateur.

- Délégations et contrats d'exploitation

La question des délégations de service et des contrats d'exploitation se pose notamment dans les secteurs de la gestion de l'eau et des transports collectifs. Dans la mesure où la désignation d'un OIV repose sur l'existence d'au moins un PIV, l'OIV sera le plus souvent le gestionnaire ou l'exploitant. Pour les activités faisant l'objet de telles délégations ou concessions de service public, il est indispensable, d'associer la collectivité responsable au processus de désignation, en application du principe de libre administration des collectivités territoriales édicté au deuxième alinéa de l'article 72 de la Constitution . A cet égard, les éventuels investissements nécessaires à la mise en place d'un dispositif de protection doivent recueillir l'aval de la collectivité, dans le cadre des processus contractuels la liant à leur concessionnaire ou délégataire. Dès lors, la collectivité peut avoir besoin de connaître de documents classifiés, notamment d'une ou de plusieurs DNS. Elle devra alors demander à faire habiliter les personnes ayant besoin d'en connaitre.

- Cas d'un opérateur intéressant plusieurs secteurs d'activités d'importance vitale

Lorsque la désignation d'un opérateur est envisagée simultanément par plusieurs ministres coordonnateurs, une concertation menée d'abord par les services des ministres concernés puis en CIDS permet d'arrêter le choix du correspondant privilégié. Autant que possible le correspondant privilégié est le ministre coordonnateur responsable du secteur d'importance vitale dans lequel l'opérateur exerce son activité principale. A défaut, il est le ministre coordonnateur responsable du secteur d'activités d'importance vitale motivant en priorité la désignation de cet opérateur comme OIV.

Le correspondant privilégié de l'opérateur coordonne l'action des ministres coordonnateurs vis-à-vis de l'opérateur et transmet à ce dernier les DNS et les autres documents nécessaires. Il informe les ministres coordonnateurs de tout événement important concernant l'OIV et pouvant intéresser ces ministres. Il les consulte avant toute décision importante n'ayant pas un caractère d'urgence absolue.

L'arrêté de désignation de l'OIV est pris par le correspondant privilégié de l'opérateur, conjointement avec les autres ministres coordonnateurs intéressés. Cet arrêté précise les secteurs de rattachement.

Le ministre coordonnateur ou le préfet de département ayant désigné l'opérateur lui communique la ou les DNS qui lui sont nécessaires pour l'élaboration du PSO. Le choix de la ou des DNS à communiquer est arrêté au regard des activités de l'opérateur lors de la notification de l'intention de le nommer OIV.

2.4.3. Le délégué pour la défense et la sécurité (DDS)

a - Nomination et rôle du délégué

– POINT-CLE –

Il revient à l'opérateur d'importance vitale de communiquer à l'autorité administrative le nom de la personne chargée d'exercer la fonction de délégué pour la défense et la sécurité.

Le délégué pour la défense et la sécurité de l'opérateur représente celui-ci auprès de l'autorité administrative pour toutes les questions relatives à la sécurité des installations et aux plans de sécurité (PSO, PPP et PPE).

Pour garantir l'efficacité de la relation avec l'autorité administrative et comme le prévoit les articles R. 1332-5 et R. 1332-6 du code de la défense, l'opérateur désigne :

- Au niveau central : un délégué pour la défense et la sécurité de l'opérateur, interlocuteur principal du ministre coordonnateur ou du correspondant privilégié ;
- Au niveau local :
    - Cas d'un PIV : un délégué pour la défense et la sécurité du point d'importance vitale, interlocuteur principal du préfet de département ;
    - Cas d'une ZIV : un délégué pour la défense et la sécurité de la zone d'importance vitale, représentant les opérateurs qui la constituent auprès du préfet de département ou du préfet de département coordonnateur.

Pour faciliter la relation avec le préfet de zone de défense et de sécurité, notamment en cas de crise, l'opérateur peut désigner au niveau zonal un délégué pour la défense et la sécurité, interlocuteur principal du préfet de zone de défense et de sécurité qui peut par ailleurs exercer simultanément les fonctions de délégué pour la défense et la sécurité d'opérateur et/ou de points d'importance vitale ou zone d'importance vitale.

Un DDS peut exercer simultanément et indistinctement ses fonctions au niveau central, zonal et local (pour un ou plusieurs points d'importance vitale et/ou zone d'importance vitale).

Le DDS d'un OIV à PIV unique cumule naturellement les fonctions de DDS du PIV et de l'opérateur.

b - Habilitation

– POINT-CLE –

L'habilitation des délégués pour la défense et la sécurité respecte les modalités définies par l'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

Les délégués pour la défense et la sécurité doivent être habilités au niveau confidentiel défense.

Les décisions d'habilitation sont prises par le ministre coordonnateur du secteur d'activités d'importance vitale dont relève l'opérateur ou par l'autorité ayant reçu délégation à cet effet.

L'opérateur adresse la demande d'habilitation de son délégué pour la défense et la sécurité à l'autorité administrative. A l'issue de l'instruction de la demande, le ministre coordonnateur concerné ou son délégataire informe l'opérateur et, le cas échéant, le préfet de département ayant désigné l'opérateur d'importance vitale de la décision prise quant à l'habilitation dudit délégué.

La décision d'habilitation d'un délégué est conservée par l'autorité qui l'a prise. Celle-ci peut délivrer, en cas de nécessité, un certificat de sécurité.

L'habilitation d'un ressortissant étranger comme délégué pour la défense et la sécurité est instruite selon les modalités définies par l'article 37 de l'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

La demande d'habilitation du délégué pour la défense et la sécurité d'un point d'importance vitale doit, si ce dernier n'est pas habilité, s'effectuer avant l'envoi du plan de sécurité d'opérateur, lui-même accompagné de la liste des points d'importance vitale.

3. LE DISPOSITIF DE SAIV

3.1. LA DIRECTIVE NATIONALE DE SECURITE (DNS)

3.1.1. Définition et objectifs

Une DNS s'applique à tout ou partie d'un secteur d'activités d'importance vitale. Elle décrit le périmètre du secteur ou du sous-secteur, elle en identifie les responsables, les processus et les enjeux et en définit le besoin de sécurité des fonctions essentielles. A la suite d'une analyse de risque dans laquelle sont énoncés et hiérarchisés les scénarios de menace, elle précise les objectifs et les politiques de sécurité du secteur ou du sous-secteur concerné. A cette fin, la DNS peut notamment définir la nature des opérateurs et des infrastructures susceptibles d'être désignés d'importance vitale au titre dudit secteur et préciser les critères de leur désignation.

La DNS définit des mesures planifiées et graduées de vigilance, de prévention, de protection et de réaction contre toute menace, notamment à caractère terroriste. Elle **rappelle les mesures du plan VIGIPIRATE applicables aux opérateurs dudit secteur**. Elle constitue un document-cadre pour l'élaboration des plans de sécurité des OIV auxquels elle s'applique.

3.1.2. Modalités d'élaboration

Les DNS sont approuvées par arrêté du Premier ministre, après avis de la CIDS[5]. Elles sont notifiées selon un processus tel qu'il est décrit ci-après.

3.1.3. Transmission des DNS aux OIV

Après approbation, la DNS est adressée par le SGDSN au ministre coordonnateur concerné qui en assure la diffusion aux autres ministres coordonnateurs.

Chaque ministre coordonnateur, à l'exception du ministre de la défense, diffuse sa ou ses DNS aux préfectures de zone et aux services déconcentrés de son ministère. Les préfets de zone les transmettent aux préfets de département qui ont à en connaître[6].

Le ministre de la défense diffuse les DNS de son secteur aux officiers généraux de zone de défense et de sécurité[7].

L'OIV ne peut se voir transmettre la ou les DNS dont il a à connaître qu'après habilitation de l'un de ses employés (cf. § 2.4.3.b). Celui-ci peut être différent du délégué pour la défense et la sécurité afin de permettre éventuellement la transmission des documents classifiés nécessaires à la concertation préalable à la désignation de l'OIV.

Un opérateur qui, dans le cadre de son développement économique, pressent qu'il pourrait être désigné OIV, peut demander à ce qu'une ou plusieurs DNS lui soient communiquées. Pour cela, il adresse une demande motivée au ministre coordonnateur du secteur concerné, accompagnée de la

[5] Sauf les DNS des secteurs d'activité d'importance vitale relevant du ministère de la défense.

[6] Ceux-ci sont autorisés à en communiquer tout ou partie aux personnes habilités qui contribuent à la rédaction des documents avec le préfet (service de police, de gendarmerie, experts déconcentrés, …).

[7] Les services préfectoraux peuvent en avoir communication dans le cadre de la rédaction des PPE des PIV relevant du ministère de la défense.

demande d'habilitation (à défaut d'un certificat de sécurité) de la personne à qui lesdites directives seront adressées.

Une collectivité territoriale responsable d'un service public délégué ou soumis à contrat d'exploitation peut demander à ce qu'une ou plusieurs DNS lui soient communiquées. Elle adresse alors une demande motivée au préfet de département concerné, accompagnée de la demande d'habilitation (à défaut d'un certificat de sécurité) de la personne à qui lesdites directives seront adressées.

3.1.4. Modalités de révision

Toute modification du contexte réglementaire national ou international, de l'analyse de la menace ou de l'environnement économique peut justifier la révision d'une DNS. Cette révision est menée par le ministre coordonnateur du secteur concerné, à son initiative ou à la demande du Premier ministre, après avis de la CIDS[8] et en concertation interministérielle. Le Premier ministre approuve ces modifications par un arrêté qui peut compléter la DNS en vigueur ou la remplacer.

L'article R. 1332-31 du code de la défense indique que la révision d'une DNS entraine la révision, dans les délais prévus pour leur élaboration, du PSO ainsi que des PPP concernés. Néanmoins, les modalités exactes de la révision du PSO et des PPP sont définies par le ministre coordonnateur en concertation avec l'OIV.

3.2. LE PLAN DE SECURITE D'OPERATEUR (PSO)

– POINT-CLE –

L'opérateur doit élaborer :
- un PSO (non obligatoire s'il n'a qu'un seul PIV) ;
- un PPP par PIV (contenant une analyse du risque si pas de PSO) ;
- éventuellement un PPP de zone d'importance vitale.
NOTA : L'élaboration du plan de protection externe, en liaison avec le DDS du PIV, est de la responsabilité de l'autorité préfectorale.

Le PSO est le fondement d'une politique générale de sécurité, indissociable d'une politique globale de qualité et de gestion des risques.

3.2.1. Contenu du PSO

Le PSO décrit l'organisation et la politique de sécurité de l'opérateur. Cette politique peut s'appuyer sur le dispositif de sécurité existant et sur l'expérience acquise dans la gestion de la qualité. Le PSO doit permettre à l'opérateur de s'approprier la DNS à travers la rédaction d'une analyse de risque propre à l'OIV et retranscrite dans le PSO. Il prévoit des mesures permanentes et graduées transposant tant les mesures spécifiques de la DNS que les mesures VIGIPIRATE applicables. Le PSO prévoit, s'il y a lieu, les délais de réalisation des mesures de protection permanentes et des mesures temporaires et graduées qu'il prescrit.

3.2.2. Outils et méthodologie

L'autorité administrative ayant désigné un OIV lui communique le guide d'élaboration et le plan-type du PSO à l'occasion de la notification de la ou des DNS. L'opérateur doit se conformer au plan type défini par arrêté du Premier ministre.

L'autorité administrative ayant désigné le ou les PIV d'un opérateur lui communique le plan-type de PPP d'un PIV à l'occasion de la notification de désignation des PIV.

[8] Sauf en ce qui concerne les DNS du secteur « *Activités militaires de l'Etat* ».

Le préfet de département ou le préfet coordonnateur ayant notifié la création d'une zone d'importance vitale communique au délégué pour la défense et la sécurité de ladite zone le plan-type de PPP ainsi que les DNS nécessaires si ce délégué est désigné et habilité et si ces documents ne lui ont pas déjà été transmis du fait du cumul de plusieurs fonctions (cf. § 2.3.3).

3.2.3. Elaboration

L'opérateur élabore un PSO qui doit répondre aux prescriptions de la ou des DNS qui lui ont été communiquées.

La sélection des PIV proposés par l'opérateur est issue de l'analyse de risque qui explicite les raisons pour lesquelles chaque point est proposé. La liste des PIV précise succinctement la nature de l'activité qui s'exerce pour chacun des points. Dans le cas où le PSO est élaboré à partir de plusieurs directives, la liste des PIV qui lui est annexée précise pour chaque PIV la ou les directive(s) qui s'y applique(nt).

Dans le cas où l'opérateur envisage de proposer un seul établissement, un seul ouvrage ou une seule installation comme PIV, il accuse réception de la DNS qui lui a été transmise et soumet au ministre coordonnateur, dans un **délai de six mois à compter de la date de notification de la DNS** qui lui est applicable, une analyse de risque justifiant *in fine* la désignation d'un unique PIV. Il précise à cette occasion les caractéristiques géographiques et économiques du PIV.

Dans le cas où l'opérateur envisage de proposer la désignation de plusieurs PIV, l'opérateur dispose d'un **délai de six mois à compter de la date de notification de la dernière DNS** qui lui est applicable[9] pour soumettre une première version de son PSO au ministre coordonnateur.

Si l'OIV ressent le besoin de se voir communiquer, à titre d'information, une autre DNS, il en formule une demande motivée auprès de l'autorité l'ayant désigné OIV. Celle-ci transmet la demande au ministre coordonnateur en charge de cette directive avec son avis sur la suite à réserver à cette demande.

3.2.4. Mise en œuvre du PSO

Le PSO est mis en œuvre par une organisation de sécurité définie par l'opérateur et comprenant le délégué pour la défense et la sécurité.

Il est décliné pour chaque PIV de l'opérateur sous la forme du PPP. Pour les autres installations et réseaux de l'opérateur, il peut être décliné sous forme de directives, consignes particulières ou fiches réflexes, qui ne sont pas nécessairement classifiées.

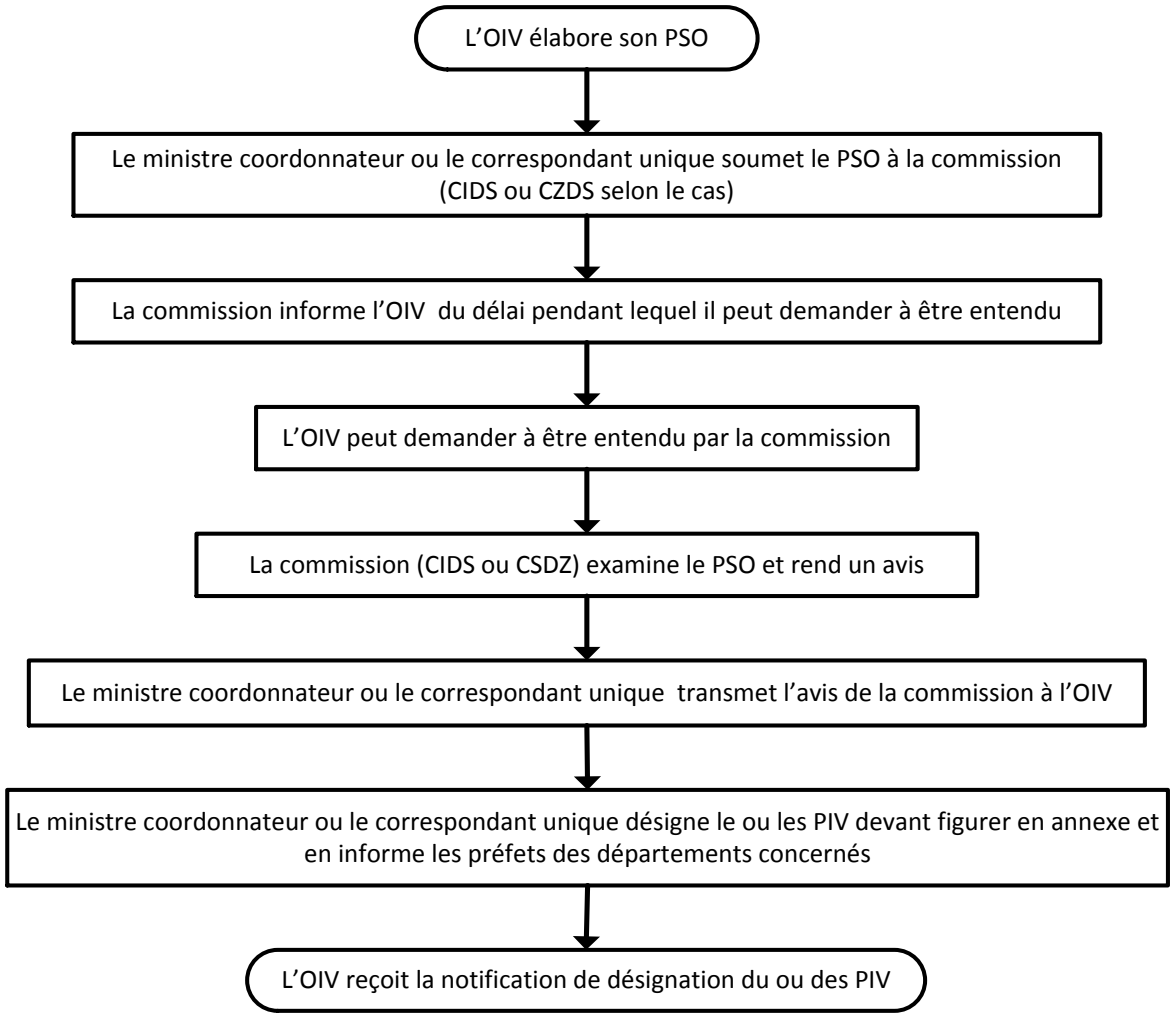
La politique d'exercices et d'audit concourt à l'évaluation du plan, en vue de son adaptation et de son amélioration.

3.2.5. Révision du PSO

Le PSO peut être révisé en cas de modification d'une DNS notifiée à l'opérateur (selon précisions du § 3.1.4). Il peut l'être également à l'initiative de l'opérateur. Pendant toute la durée du processus de révision, le plan en vigueur continue à s'appliquer. Le plan révisé remplace le plan préexistant dès réception de l'arrêté de désignation des PIV.

Dans l'éventualité où l'opérateur contesterait la décision de désignation des PIV, le PSO initial resterait en vigueur jusqu'à résolution du contentieux.

[9] La concertation préalable à la désignation de l'OIV aura permis d'identifier les DNS que l'opérateur a à connaître.



NB : Ce processus ne s'applique pas au PSO d'un opérateur relevant du ministre de la défense.

Figure 5 : Processus d'instruction du plan de sécurité d'un opérateur proposant la désignation de plusieurs PIV

3.3. LE POINT D'IMPORTANCE VITALE (PIV)

3.3.1. Définition d'un PIV

Un PIV est un établissement, une installation ou un ouvrage sis sur le territoire national dont le dommage, l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement :

- d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ;
- ou de mettre gravement en cause la santé ou la vie de la population.

Le premier critère, tiré des dispositions de l'article L. 1332-1 du code de la défense, permet de déterminer les PIV qui sont au cœur du dispositif, en ce qu'ils concourent directement aux activités d'importance vitale, à l'échelle d'un secteur ou à l'échelle du pays.

Il implique de prendre en compte :

- la notion de non-substituabilité des capacités du PIV par d'autres moyens ;

- le délai de remise en fonction.

Le deuxième critère, issu des dispositions de l'article L. 1332-2 du code de la défense, s'attache exclusivement aux conséquences humaines, c'est-à-dire aux conséquences sur la vie ou la santé de la population, de la destruction ou de l'avarie du PIV.

Ce critère ne doit pas conduire à désigner indifféremment tous les sites. Parmi les établissements classés SEVESO seuil haut, une analyse de risque portant sur les menaces, les vulnérabilités et les impacts pour la population permettra de désigner les OIV strictement nécessaires. Bien que l'on vise les installations classées pour l'environnement, un impact sur l'environnement sans conséquence directe pour la santé ou la vie de la population ne sera pas pris en compte.

Dans les deux cas, les critères s'appliquent pour toute menace perçue comme plausible, en prenant en compte tant les vulnérabilités du PIV que les conséquences résultant d'une attaque.

S'agissant de l'application de ces règles aux départements et collectivités d'outre-mer, l'éloignement de la métropole et l'éventuel caractère insulaire doivent être pris en compte dans la définition d'un PIV. Les notions de non-substituabilité des capacités du PIV par d'autres moyens et de délai de remplacement peuvent dans certains cas prendre une dimension accrue.

3.3.2. Périmètre d'un PIV et notion de composant névralgique

Dans un souci d'efficacité, il convient de calquer autant que possible la délimitation d'un PIV sur celle de l'entité géographique gérée ou utilisée par l'opérateur. La délimitation du PIV doit permettre la mise en œuvre la plus efficiente[10] du dispositif de sécurité des activités d'importance vitale par l'opérateur et le préfet de département pour ce qui concerne leurs responsabilités respectives.

Le composant névralgique est une installation ou un ouvrage de taille plus réduite que le PIV, à la fois indispensable au fonctionnement de ce dernier et vulnérable. Un PIV peut comprendre un ou plusieurs composants névralgiques.

Afin d'éviter la multiplication de PIV dans un établissement détenu par un même opérateur et les conséquences induites (*multiplication du nombre de PPP et de PPE*), le PIV peut être constitué d'un ou de plusieurs composants névralgiques dont la sécurité est assurée, à l'intérieur du PIV, par un dispositif de défense en profondeur[11].

3.3.3. Processus de désignation d'un PIV

L'identification initiale des PIV est une responsabilité de l'OIV. L'analyse de risque qu'il conduit pour élaborer son PSO (voir § 3.2.3) lui permet de proposer, en annexe à ce plan, la liste de ses installations, établissements ou ouvrages qu'il estime pertinent de faire désigner comme PIV.

Ce processus, qui ne s'applique pas aux PIV relevant du ministère de la défense, est illustré par le graphe qui suit.

[10] Efficience : notion qui exprime le fait d'atteindre les objectifs fixés tout en engageant le minimum de moyens ou en créant le minimum de contraintes.

[11] La défense en profondeur consiste en la superposition de plusieurs lignes de défense, composées d'un ensemble de mesures de sécurité, chaque ligne devant contribuer à affaiblir l'attaque et à permettre aux suivantes de se renforcer en vue soit d'empêcher la destruction ou la prise de contrôle des composants névralgiques du PIV, soit d'en limiter ou d'en retarder les effets.

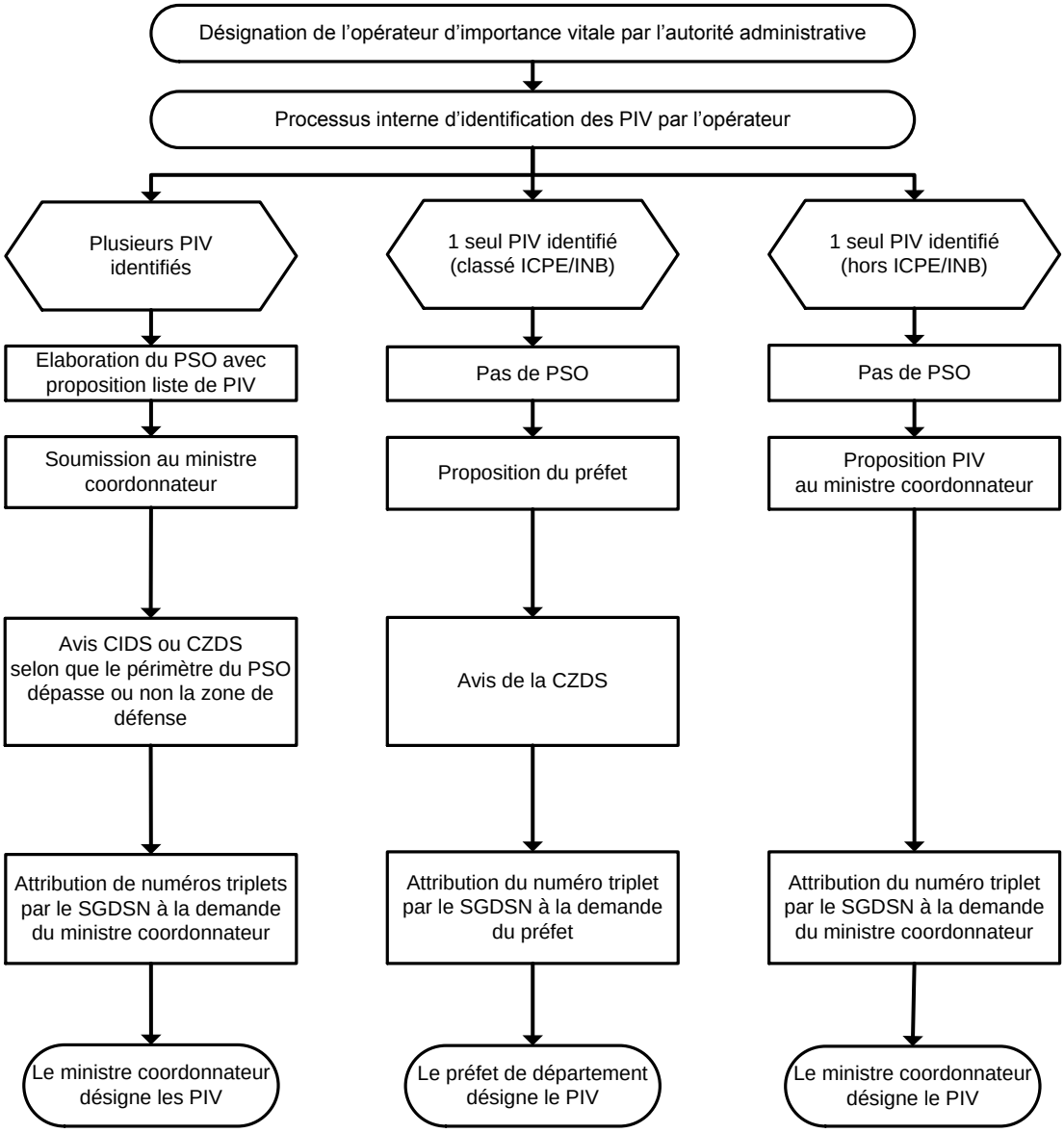


Figure 6 : Processus de désignation d'un PIV

Lors de l'examen du PSO, la commission interministérielle (ou zonale) de défense et de sécurité des secteurs d'activités d'importance vitale s'assure que la liste des PIV est pertinente. Elle peut proposer le retrait ou l'ajout de PIV. Son avis est transmis au ministre coordonnateur, ou au préfet dans le cas des opérateurs d'une seule installation classée pour la protection de l'environnement ou installation nucléaire de base proposée à la désignation par ce dernier. Dès réception de cet avis, cette autorité administrative désigne le ou les PIV.

Préalablement à la notification de désignation d'un ou plusieurs PIV, l'autorité administrative (*ministre coordonnateur, correspondant privilégié ou préfet de département par l'intermédiaire du préfet de zone de défense*) demande au SGDSN l'attribution d'un numéro d'identification (voir § 9.1) pour chaque PIV.

Les informations nécessaires à l'instruction de cette demande sont :

- la dénomination sociale de l'OIV ;
- la dénomination du PIV ;
- sa localisation.

3.3.4. Modalités de contrôle des personnes accédant à un PIV

– POINTS-CLES –

Afin de réduire les risques d'atteintes à un point d'importance vitale dont il a la charge, l'opérateur d'importance vitale peut, s'il le souhaite, requérir l'avis de l'autorité administrative ou militaire (selon les cas) avant d'autoriser l'accès de certaines personnes aux zones particulièrement sensibles d'un PIV dont il a la charge.

Pour ce faire, l'opérateur est tenu de solliciter par écrit l'avis du préfet de département (le préfet de police à Paris) dans le ressort duquel se situe le point d'importance vitale.

Au préalable, l'opérateur doit impérativement avoir envisagé le champ d'application du criblage dans son PPP, qui doit être approuvé.

Par ailleurs, l'opérateur est tenu d'informer par écrit la personne concernée qu'elle est susceptible de faire l'objet d'une enquête administrative.

L'autorité administrative ou militaire rend son avis après la réalisation d'une enquête administrative.

L'avis formulé par l'administration ne revêt aucun caractère contraignant pour l'opérateur qui, seul, choisit d'autoriser ou non l'accès au point d'importance vitale concerné.

NOTA :
Dans le cas d'un opérateur d'importance vitale relevant du ministère de la défense, il revient à l'autorité militaire désignée par le chef d'état-major des armées d'émettre un avis.

a - Demande d'avis à l'autorité administrative

La saisine pour avis du préfet ou de l'autorité militaire compétente, en ce qu'elle permet la réalisation d'une enquête administrative sur des personnes accédant à un PIV, participe au dispositif général de prévention de ces sites contre tout acte de malveillance. Elle contribue, en amont, à la protection des composants les plus névralgiques d'un point d'importance vitale. Si la décision d'autorisation d'accès d'une personne à un point d'importance vitale relève bien du seul opérateur, l'administration lui apporte son concours dans ce processus décisionnel. Les articles L. 1332-2-1 et R. 1332-22-1 à R. 1332-22-3 du code de la défense prévoient la procédure par laquelle, avant d'autoriser l'accès d'une personne à un point d'importance vitale qu'il gère, l'opérateur peut solliciter l'avis du préfet de département[12] dans lequel est situé le PIV. Pour les opérateurs d'importance vitale dont le ministre coordonnateur est le ministre de la défense, leur demande d'avis est adressée à l'autorité militaire désignée (service enquêteur du ministère de la défense).

De manière à faciliter les échanges et à réduire *a minima* les temps de traitement de l'enquête par les services territoriaux compétents, la demande devra, dans la mesure du possible, être émise par le délégué à la défense et à la sécurité (DDS) du PIV concerné[13]. La demande d'avis doit être signée par le DDS et adressée par écrit dématérialisé, selon le modèle joint en annexe n°9, au préfet du département (préfet de police, le cas échéant) ou à l'autorité militaire dans lequel se situe le PIV.

[12] Sauf cas particulier de la désignation d'un préfet coordonnateur désigné et détenant le pouvoir de police pour un PIV situé hors de son ressort départemental.

[13] Compte tenu de la relation étroite entre le criblage et le PPP et des relations privilégiées entre les préfectures et les DDS (seules personnalités de l'OIV connues des préfectures comme étant habilitées).

Elle doit impérativement comporter les informations suivantes, regroupées en trois rubriques :

- *Données relatives à l'opérateur et au PIV* :
    - année / numéro d'ordre de la demande pour le PIV concerné
    - numéro de triplet
- *Données relatives à la personne :*
    - nom et prénom(s) ;
    - date et lieu de naissance ;
    - domicile actuel ;
    - nom de l'employeur (si différent du demandeur) ;
    - profession.
- *Données relatives à l'accès au site :*
    - désignation, conformément au zonage codifié dans le PPP, de la partie ou des parties du PIV justifiant une demande d'avis en vue de l'accès ;
    - justification de la nécessité de l'accès à la partie du PIV concernée ;
    - justification de l'impossibilité de mettre en place des mesures de prévention autres ;
    - durée prévue de l'accès au site (date, durée, période et répétition éventuelle) ;
    - numéro d'immatriculation du véhicule (si l'accès en véhicule est sollicité).

Aucun élément d'identification du PIV ou de l'opérateur (charte graphique, logo, etc.) ne doit figurer sur le document transmis de manière à ce qu'il puisse être acheminé par voie dématérialisée.

Il revient à l'opérateur, dans son intérêt propre, d'effectuer la demande le plus en amont possible de la date prévue d'accès au point d'importance vitale. Dans la mesure du possible, et sauf exception précisée infra, l'opérateur sollicite les services préfectoraux au minimum 3 semaines avant la venue effective sur site de la personne concernée. De la même manière, et sauf exception, l'OIV dont le ministre coordonnateur est le ministre de la défense sollicite l'autorité militaire désignée au minimum 2 mois avant la venue effective sur site de la personne concernée.

En cas d'urgence dûment justifiée par l'OIV, ce délai de sollicitation peut être réduit à 72h. Les services préfectoraux instruisent alors la demande en priorité afin, dans la mesure du possible, de rendre un avis dans les délais compatibles avec la date prévue de l'accès au PIV par la personne concernée.

Cette procédure exceptionnelle ne doit aucunement venir palier un défaut d'organisation interne de l'opérateur. Le recours à cette procédure ne peut en aucun cas revêtir un caractère systématique. La demande devra être transmise à la préfecture ou à l'autorité militaire selon la procédure dématérialisée habituelle en utilisant le document prévu pour celle-ci.

Dans tous les cas, la production de l'avis par l'administration n'est pas un préalable obligatoire à l'accès d'une personne à un point d'importance vitale.

b - <u>Encadrement des possibilités de demandes d'avis</u>

Conformément aux dispositions légales et réglementaires, les demandes d'avis adressées à l'administration sont encadrées au regard, d'une part, des lieux compris dans le PIV auquel il est accédé (encadrement *ratione loci*) et, d'autre part, des personnes accédant à ces lieux (encadrement *ratione personae*) :

- Encadrement *ratione loci* de la demande d'avis :

La demande d'avis ne peut concerner que l'accès aux parties du PIV devant faire l'objet d'une surveillance particulière car présentant une vulnérabilité spécifique au regard des scenarii de menaces retenues.

Ces parties du PIV doivent être précisément identifiées dans le PPP (zonage codé). Elles peuvent correspondre, en tout ou en partie, aux composants névralgiques identifiés par le PPP. Les zones

dont l'accès sera soumis au dispositif de la présente circulaire seront explicitement mentionnées dans le PPP en référençant notamment l'article R-1332-22-1 du code de la défense.

Il faut exclure par exemple les zones recevant temporairement ou de façon permanente du public telles que les postes d'accueil, les salles de réunion ou les salles de conférence. De même, les PIV sans dispositif de filtrage et de contrôle des accès sont exclus du dispositif.

- Encadrement *ratione personae* de la demande d'avis :

Conformément à l'article R. 1332-22-2 du code de la défense, deux catégories de personnes ne peuvent faire l'objet d'une demande d'avis quant à leur accès aux PIV :

- les personnes mentionnées par le décret n° 2005-1124 du 6 septembre 2005 fixant la liste des enquêtes administratives donnant lieu à la consultation des traitements automatisés de données personnelles mentionnés à l'article 230-6 du code de procédure pénale.

En effet, du fait de leur emploi ou des fonctions qu'elles occupent lors de leur accès au PIV, ces personnes ont déjà fait l'objet d'une enquête administrative.

- les personnes dont l'accès au PIV fait l'objet de mesures de prévention et de sécurité suffisantes.

Il s'agit là des personnes qui, du fait notamment de la nature et de la durée de leur accès au site, peuvent faire l'objet d'un contrôle suffisant rendant inutile la réalisation d'une enquête administrative, et donc la formulation d'une demande d'avis auprès de l'administration. Il peut, par exemple, s'agir de personnes effectuant une courte visite du PIV et pouvant être accompagnées durant cette visite ou de personnes (stagiaires…) ne pouvant accéder aux parties les plus sensibles du PIV du fait de dispositifs d'accès restreint aux différentes parties du PIV.

Par ailleurs, il convient d'exclure du dispositif l'ensemble des personnes ayant à accéder à un PIV à l'occasion d'une ouverture au public et ce quel qu'en soit la forme (conférences, journées portes ouvertes, etc.).

Le PPP doit préciser les mesures de prévention et de sécurité mises en place pour contrôler l'accès aux différentes parties du PIV selon la raison pour laquelle cet accès s'effectue.

Avant de réaliser une enquête administrative, les services préfectoraux s'assurent que la demande d'avis formulée par l'OIV ne contrevient pas à ces critères *ratione loci* et *ratione personae*. Toute demande d'avis doit donc être justifiée au regard de ces critères. A défaut, elle sera rejetée par utilisation du formulaire de rejet précisé en annexe n°11.

c - Information de la personne accédant au PIV par l'opérateur d'importance vitale

L'opérateur doit obligatoirement notifier par écrit à la personne concernée qu'il a sollicité l'avis de l'administration quant à son accès au site et que, dans, ce cadre, conformément aux dispositions législatives et réglementaires en vigueur, elle fait l'objet d'une enquête administrative.

Il doit pour cela s'appuyer sur la formulation proposée :

« *Dans le cadre de …*(1)*, vous allez être amené à accéder à un/des site(s) relevant de la responsabilité de notre société. Afin de sécuriser l'accès à ce(s) site(s), et conformément aux dispositions législatives et réglementaires en vigueur, nous avons sollicité préalablement l'avis de l'autorité administrative. Dans ce cadre, une enquête administrative destinée à vérifier qu'aucun fait vous concernant n'est incompatible avec l'accès envisagé est susceptible d'être réalisée par l'autorité administrative.* »

(1) à compléter selon la raison de l'accès au site : activités professionnelles, stage de longue durée, visite sollicitée par la personne…

Cette notification ne devra pas faire apparaitre les raisons exactes qui prévalent au déclenchement d'une enquête. En particulier, le caractère très sensible de telle ou telle partie du point d'importance vitale ne sera pas porté à la connaissance de la personne visée par l'enquête.

d - Sens de l'avis et durée de validité

Si la demande de l'opérateur est jugé recevable, le préfet émet un avis sur la compatibilité des caractéristiques de la personne avec l'accès au PIV envisagé. Afin d'émettre cet avis, une enquête administrative est diligentée.

- Sens de l'avis :

A la suite de l'enquête administrative, le préfet transmet à l'opérateur d'importance vitale un avis précisant si les caractéristiques de la personne concernée sont « *compatibles* » ou « *incompatibles* » avec l'accès aux zones désignées du PIV.

Cet avis, qui n'est pas une décision administrative, n'est pas motivé. Il n'est pas contraignant pour l'OIV qui reste le seul responsable de l'accès d'une personne au site dont il a la charge.

- Durée de validité de l'avis :

L'avis formulé par l'administration est valable pour une durée de trois ans. Ce délai doit être entendu comme le terme avant lequel l'OIV ne sollicitera pas à nouveau l'administration pour l'accès de la même personne au même PIV. Néanmoins, si les conditions nécessaires à la délivrance de l'avis évoluent, c'est-à-dire que des changements radicaux de situation ou de comportement sont notés par le délégué à la défense et à la sécurité du site concerné, l'opérateur peut solliciter un nouvel avis de l'administration qui jugera de l'opportunité de conduire à nouveau une enquête.

e - Principes et cadre de l'enquête administrative

Conformément aux dispositions des articles L. 1332-2-1 et R. 1332-22-1 du code de la défense, l'enquête administrative peut donner lieu à la consultation du bulletin n° 2 du casier judiciaire ainsi que des traitements automatisés de données à caractère personnel relevant de l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Les fichiers d'identification[14] ne peuvent cependant pas être consultés.

Les services, civils ou militaires, en charge de l'enquête administrative doivent pouvoir s'appuyer sur l'ensemble des traitements automatisés de données visés au paragraphe précédent quel que soit l'organisme de gestion. Une collaboration efficace doit donc être mise en place entre les services du ministère de l'intérieur et ceux du ministère de la défense afin de s'assurer que tous les traitements automatisés de données opportuns soient consultés, sans qu'il en résulte pour autant une obligation de communication compte tenu de la nature de certaines informations. Ainsi, en tant que de besoin, les services du ministère de l'intérieur peuvent solliciter le concours des services du ministère de la défense dans le cadre des demandes d'avis émanant d'opérateurs ne relevant pas du ministère de la défense et, réciproquement, les services du ministères de la défense peuvent solliciter le concours de ceux du ministère de l'intérieur pour les demandes d'avis émanant d'opérateur relevant du ministère de la défense.

Le dispositif de contrôle d'accès aux points d'importance vitale ne se substitue pas aux dispositifs déjà existants fondés sur d'autres bases légales et permettant le contrôle de l'accès à des zones spécifiques.

f - Dispositions transitoires

Le dispositif de contrôle de l'accès aux PIV a été créé par la loi n° 2011-267 du 14 mars 2011 et par le décret n° 2012-491 du 16 avril 2012, désormais codifié.

[14] Il s'agit du fichier national automatisé des empreintes génétiques et du fichier automatisé des empreintes digitales.

Les employés travaillant déjà sur le site d'un PIV à la date du 16 avril 2012 ne peuvent faire l'objet d'une demande d'avis sauf cas exceptionnel qui devra être dûment justifié. Seuls les nouveaux employés pourront faire l'objet d'une demande d'avis, s'ils sont concernés par l'accès aux zones envisagées par le PPP et s'ils ne font pas partie des catégories de personnes exclues dans l'application du dispositif d'enquête.

3.3.5. Modification des conditions d'exploitation ou cession d'un PIV

– POINT-CLE –

L'OIV informe les autorités administratives des modifications des conditions d'exploitation. Le dispositif de sécurité des activités d'importance vitale appliqué à l'opérateur reste en vigueur jusqu'à décision de l'autorité administrative.

En cas de modification des conditions d'exploitation du PIV telles qu'elles remettraient en cause la désignation de l'établissement, de l'installation ou de l'ouvrage, l'OIV doit formuler une demande motivée d'abrogation de la décision de désignation auprès de l'autorité administrative l'ayant désigné OIV et en informer le préfet du département concerné.

L'autorité administrative instruit la demande et, après avis de la CIDS ou de la CZDS[15], selon le cas, statue sur la requête de l'OIV.

Dans l'éventualité où l'OIV ne dispose que d'un PIV, le déclassement de ce dernier implique l'abrogation de la décision de désignation de l'OIV. La décision d'abrogation intervient après avis de la CIDS ou de la CZDS, selon le cas.

En cas de transfert de propriété d'un PIV, l'OIV « vendeur » doit en avertir le préfet du département concerné et le ministre coordonnateur. L'autorité administrative ayant désigné l'OIV étudiera l'opportunité de maintenir l'établissement, l'installation ou l'ouvrage comme PIV.

Elle peut abroger la décision de désignation de cette installation comme PIV. Cette abrogation entraîne la révision de la liste des PIV annexée au PSO.

A défaut, les mesures du plan particulier de protection du point d'importance vitale restent applicables et ceci dans l'attente de :

- la désignation de l'acquéreur comme OIV,
- la désignation des délégués pour la défense et la sécurité,
- l'approbation des nouveaux plans.

3.4. LA ZONE D'IMPORTANCE VITALE (ZIV)

– POINT-CLE –

La constitution d'une zone d'importance vitale doit apporter une plus-value opérationnelle.

Une zone d'importance vitale est une aire dans laquelle sont implantés plusieurs PIV relevant d'OIV différents, pour lesquels une prise en compte commune de la sécurité présente une plus-value.

Il y a ainsi interdépendance en terme de sécurité entre les PIV dès lors que :

- l'exécution d'une menace sur l'un d'eux aurait des conséquences sur l'intégrité ou l'activité des autres ;

[15] sauf dans le cas d'OIV relevant du ministre de la défense.

- ou les mesures de sécurité mises en œuvre pour l'un des points ou sur une partie commune ont une incidence sur la sécurité d'un ou de plusieurs autres PIV.

Trois types de zone géographique peuvent être rencontrés :

- cas 1 : une zone constituée de PIV voisins. Les PIV sont contigus ou situés à une distance relativement réduite les uns des autres ;
- cas 2 : une zone constituée de PIV enclavés. Un PIV « 2 » se situe à l'intérieur d'un PIV « 1 » ;
- cas 3 : une zone combinant les caractéristiques des deux premières.

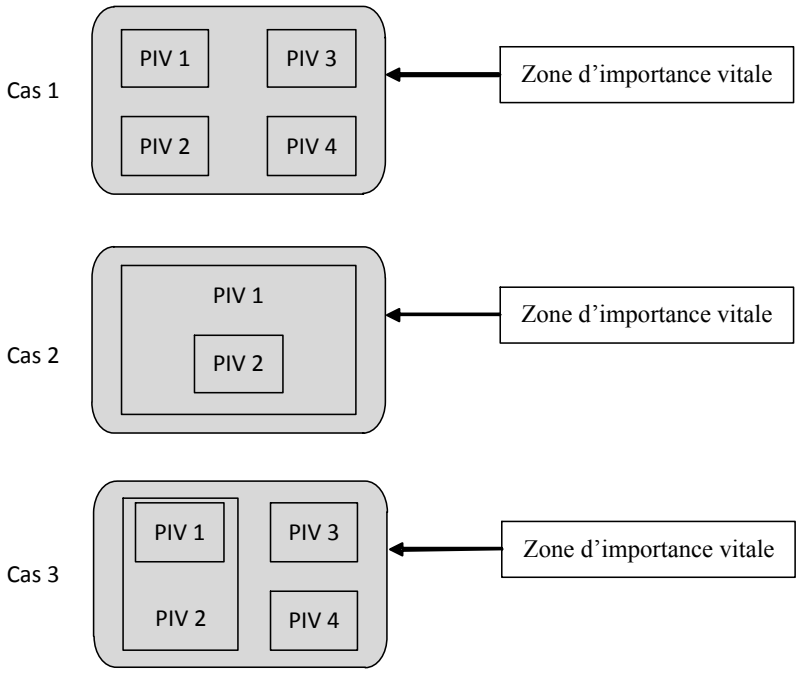


Figure 7 : Types de ZIV

Dans tous les cas, la création d'une zone d'importance vitale doit répondre à un besoin opérationnel et contribuer à améliorer la protection des PIV par la mise en commun et la rationalisation des moyens engagés. L'aire concernée doit s'entendre comme une zone présentant des caractéristiques homogènes, telles qu'il est possible d'en trouver dans certaines zones industrielles, aéroports ou ports maritimes ou fluviaux.

Si, dans le cas de PIV enclavés, la création d'une zone d'importance vitale n'apparaît pas utile au préfet de département, les opérateurs de ces points peuvent toutefois élaborer un protocole organisant les dispositions de sécurité communes. Ce protocole est adressé au préfet du département concerné.

Préalablement à la notification de sa décision de création d'une zone d'importance vitale, le préfet de département ou le préfet de département coordonnateur demande au SGDSN, par l'intermédiaire du préfet de zone de défense et de sécurité, l'attribution d'un numéro triplet d'identification de la zone. Les informations nécessaires à l'instruction de cette demande sont la délimitation de la zone d'importance vitale ainsi que la liste des PIV qui la constituent.

Lorsqu'un projet de création d'une zone d'importance vitale inclut au moins un point d'un OIV désigné au titre d'un secteur relevant du ministre de la défense, l'accord de l'officier général de zone de défense, membre de droit de la CZDS, est obligatoire.

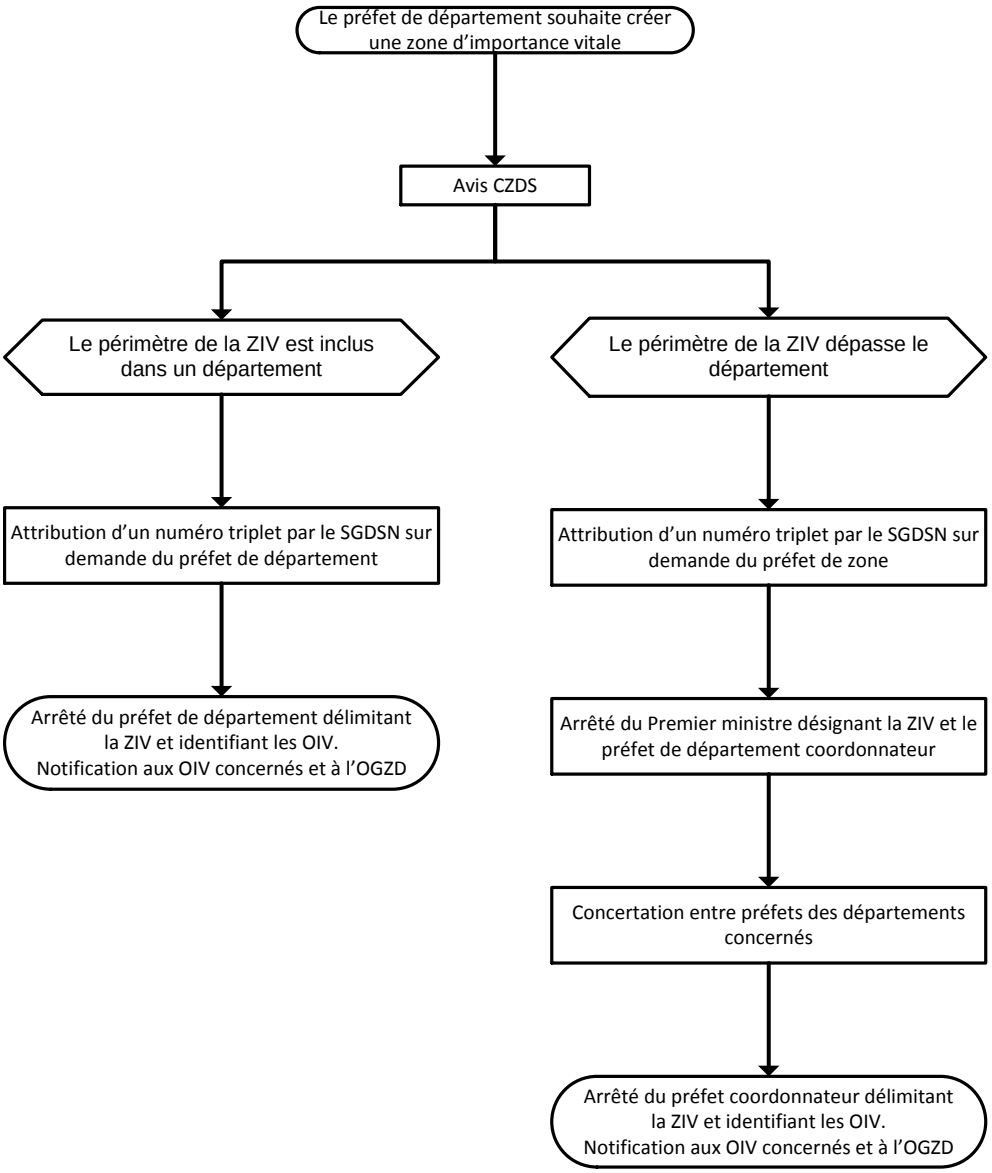


Figure 8 : Processus de désignation d'une ZIV

3.5. LE PLAN PARTICULIER DE PROTECTION (PPP)

La protection du PIV comprend des mesures de protection internes (*prévues par le PPP*) et externes (*prévues par le PPE*) qui relèvent d'une approche globale de la menace et des moyens utilisés pour y faire face. Elles sont destinées les unes et les autres à mettre en échec ou à défaut, retarder les tentatives malveillantes pouvant être effectuées par une ou plusieurs personnes, à en limiter les effets et à faciliter la continuité d'activité ou le rétablissement d'activité. Certaines mesures sont mises en œuvre en permanence, d'autres lorsque la nécessité s'en fait sentir ou sur décision du gouvernement ou de son représentant local, notamment dans le cadre du plan VIGIPIRATE.

L'opérateur élabore le PPP du PIV concerné, dans un délai de deux ans à compter de la notification de la dernière DNS qui lui est applicable. Pour son élaboration, il s'appuie :

- sur la DNS qui correspond au secteur d'activité dans le périmètre duquel se situe le PIV ;
- sur le PSO, dont il applique la politique de sûreté.

Il doit se conformer au plan type défini par arrêté du Premier ministre. A défaut de PSO (*cas d'un opérateur qui gère ou exploite un seul PIV*), le PPP **doit comporter une analyse de risque**.

3.5.1. Approbation du PPP

– POINT-CLE –
Approbation du PPP → pertinence du fond et conformité de la forme.

La décision d'approbation du préfet de département se fonde sur une évaluation **qualitative** du PPP soumis par l'opérateur. Cette évaluation prend en compte :

- l'avis de la CZDS s'il a été sollicité[16] ;
- la conformité du plan particulier de protection par rapport au plan-type ;
- la cohérence du dispositif proposé au regard de la politique générale de protection définie par le PSO ;
- la prise en compte des prescriptions de la DNS qui s'appliquent au PIV, notamment les scénarios de menace et les objectifs de sécurité ;
- l'adéquation du dispositif proposé aux infrastructures et aux modalités d'exploitation du PIV.

Le plan-type du PPP est un document élaboré par le SGDSN visant à maintenir une cohérence minimale de forme entre l'ensemble des plans particuliers de protection de l'ensemble des PIV situés sur le territoire national. Il constitue également un guide d'aide à l'élaboration d'un PPP pour l'opérateur. Néanmoins, en cas d'impossibilité manifeste de remplir certaines rubriques ou, au contraire, en cas d'absence manifeste de certaines autres rubriques, l'opérateur peut s'affranchir du plan-type dans les limites fixées par le préfet de département qui, *in fine*, approuve le PPP soumis par l'opérateur.

Dans le cadre de l'approbation d'un PPP, le préfet de département sollicite l'avis d'au moins un représentant des services de police, de gendarmerie, d'incendie et de secours ou du ministère de la défense et, idéalement, l'expertise d'une administration déconcentrée ayant une compétence particulière sur le point[17]. Il peut également effectuer une visite sur site de manière à apprécier la bonne adéquation du contenu du PPP, en vue de son approbation, avec les caractéristiques du PIV.

L'approbation des PPP des PIV du secteur nucléaire civil nécessite obligatoirement l'avis de l'autorité en charge de l'application des articles L.1333 et suivants du code de la défense[18].

Un guide d'aide à l'examen du PPP a été élaboré par le ministère de l'intérieur.

3.5.2. Mise en œuvre du PPP

Le PPP est décliné, en tant que de besoin, en consignes et en fiches réflexes qui ne sont pas nécessairement classifiées.

Il est mis en œuvre par une organisation de sécurité définie par l'opérateur et adaptée à la nature et aux caractéristiques du point et comprenant le délégué pour la défense et la sécurité du PIV.

La politique d'exercices et d'audits concourt à son évaluation, en vue de son adaptation et de son amélioration.

3.5.3. Révision du PPP

Le PPP peut être révisé :

- à la suite d'un contrôle portant sur la mise en œuvre du plan ;

[16] **La soumission d'un PPP à l'avis de la CZDS doit toutefois demeurer exceptionnelle.**
[17] La recherche de l'avis du service de police nationale ou de gendarmerie nationale territorialement compétent est à privilégier selon l'emplacement ou la nature du PIV.
[18] Service de défense, de sécurité et d'intelligence économique du ministère en charge de l'écologie.

- en cas de révision de la DNS du ou des secteurs d'activités concernés ;
- en cas de révision du PSO ;
- en cas de modification des conditions d'exploitation du PIV ou de certaines données d'environnement (*urbanisation, augmentation de la délinquance, incidents de sûreté, etc.*) ;
- en cas de cession du PIV.

Cette révision se fait à l'initiative de l'OIV ou sur injonction du ministre coordonnateur ou du préfet de département.

Pendant toute la durée du processus de révision, le plan en vigueur continue à s'appliquer. Le plan révisé remplace le plan préexistant dès réception de l'arrêté d'approbation.

Dans l'éventualité où l'opérateur contesterait le refus d'approbation du plan révisé, le PPP initial resterait en vigueur jusqu'à résolution du différend.

3.5.4. Modification du PPP par le préfet de département

Le préfet de département peut compléter ou modifier un PPP si l'opérateur n'a pas donné suite à l'injonction qui lui a été adressée ou si malgré les ajouts ou modifications apportés, les motifs[19] énoncés au I de l'article R. 1332-26 du code de la défense demeurent. Dans ce cas, le préfet de département sollicite l'avis de la CZDS sur les ajouts et modifications qu'il souhaite apporter au PPP. Ces ajouts et modifications portent sur les mesures ayant fait l'objet de l'injonction adressée à l'opérateur de compléter ou modifier ledit plan.

3.5.5. Diffusion du PPP

L'OIV établit, pour ce qui le concerne, les règles de diffusion interne du PPP de chacun de ses PIV, dans le respect de la réglementation relative à la protection du secret de la défense nationale.

Le préfet de département, ou l'autorité militaire désignée pour le SAIV « *Activités militaires de l'Etat* », ayant approuvé le PPP en conserve une copie, qu'il transmet également au ministre coordonnateur de l'OIV. La CIDS ou la CZDS concernée peuvent demander au préfet de département communication du PPP d'un PIV notamment en préparation d'un contrôle.

3.5.6. Mise en œuvre d'équivalences

Dans le domaine du transport maritime, le code des ports maritimes édicte une équivalence automatique entre les PPP et les plans de sûreté portuaire et plans de sûreté des installations portuaires approuvés (cf. articles R. 321-19 et R. 321-26 du code des ports maritimes).

Dans les autres secteurs (cf. article R. 1332-34 du code de la défense) et afin d'éviter des redondances, il appartient au préfet de département, après avis de la CIDS, de prononcer l'équivalence totale ou partielle des plans pris au titre d'autres réglementations et couvrant le domaine de la sûreté avec le PPP. Cela peut concerner, notamment, les dispositifs ci-après :

- les programmes de sûreté d'exploitant d'aéroport (PSEA) ;

  (références : article R. 213-1-1 du code de l'aviation civile)
- le plan interne de crise défini par la loi n°2004-811 du 13 août 2004 de modernisation de la sécurité civile ;
- les plans de sûreté élaborés en application d'accords internationaux ;

[19] S'il n'a pas été suffisamment tenu compte de l'avis de la CIDS ou de la CZDS, selon le cas, relatif au plan de sécurité de l'opérateur ou si une mesure au moins ne répond pas de manière satisfaisante à la DNS ou au PSO ou aux caractéristiques locales du PIV.

3.5.7. Le PPP de zone d'importance vitale

– POINT-CLE –
Constitution d'une zone d'importance vitale → Elaboration d'un PPP de zone.

Le délégué pour la défense et la sécurité de la zone d'importance vitale élabore un PPP de la zone qui prévoit des mesures communes de protection dont l'application doit être cohérente avec les mesures de protection des PIV qui constituent la zone. L'élaboration de ce plan s'appuie sur le plan-type de PPP de PIV. Les plans de sécurité des opérateurs constituant la zone d'importance vitale et leurs analyses de risque n'y sont pas annexés.

Le préfet de département ou le préfet coordonnateur prend en compte le PPP de la zone d'importance vitale dans l'élaboration ou la mise à jour du plan de protection externe des PIV.

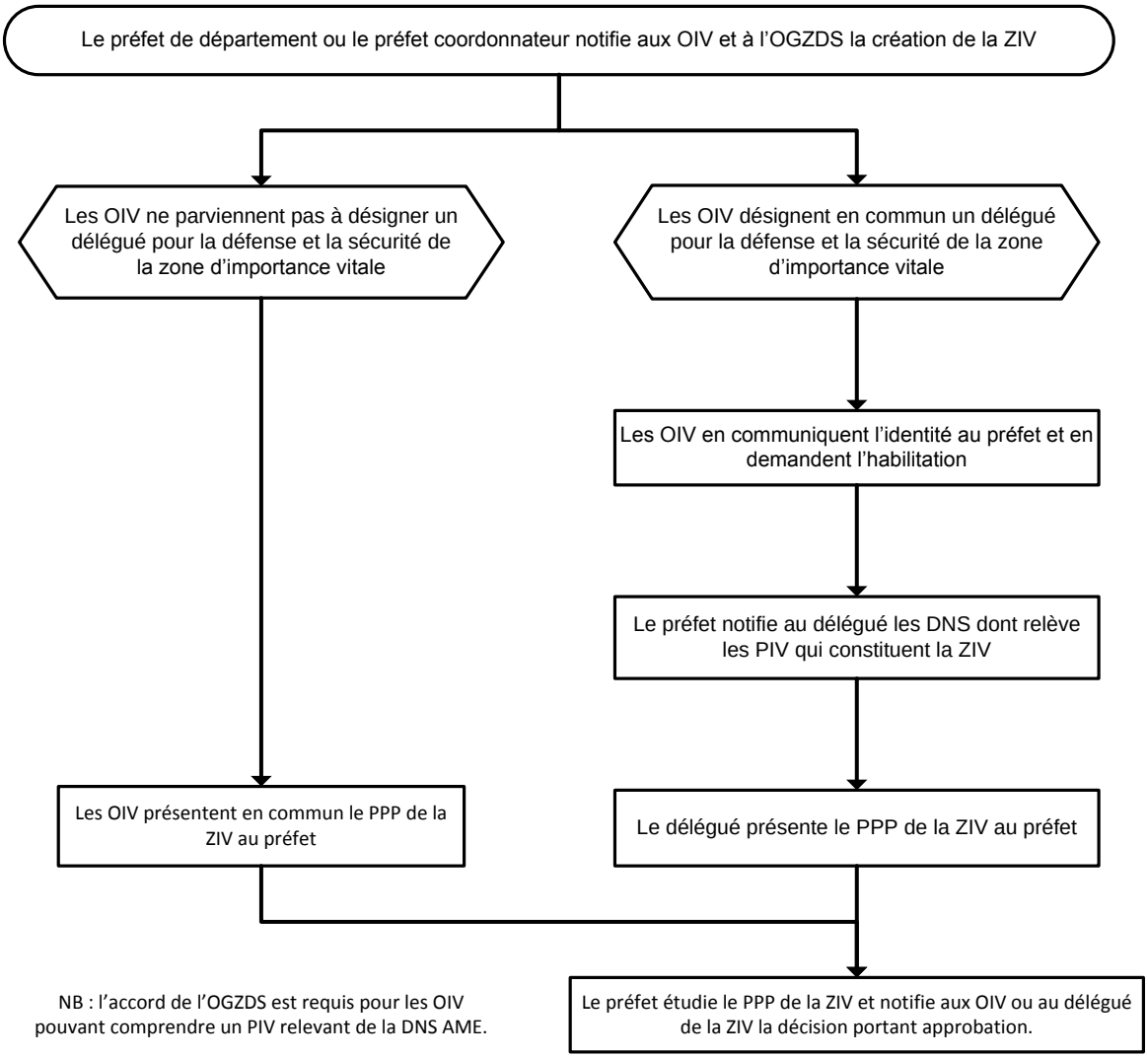


Figure 9 : Présentation du PPP de zone à l'autorité administrative

Le délégué pour la défense et la sécurité de la zone d'importance vitale, ou à défaut les OIV de ladite zone, disposent d'un **délai maximal de deux ans** à partir de la date la plus récente de notification d'une DNS à l'un des opérateurs pour présenter le PPP de la zone au préfet de département ou au préfet coordonnateur.

Le préfet de département ou le préfet coordonnateur dispose d'un délai de **six mois** à compter de la réception du PPP de la zone d'importance vitale pour statuer.

3.6. PLAN DE PROTECTION EXTERNE (PPE)

Le PPE est un document classifié, complémentaire du PPP. Il complète le dispositif particulier de protection du PIV qui est à la charge de l'opérateur.

Il définit les mesures planifiées de vigilance, de prévention, de protection et de réaction prévues par les pouvoirs publics, notamment par les forces de sécurité, sous l'autorité du préfet de département. Il décrit ainsi les modalités d'intervention sur le PIV en cas d'agression, en liaison avec l'opérateur. Il planifie les moyens humains et matériels à mettre en œuvre. Il peut prévoir des mesures de contrôle des zones périphériques au PIV. Il formalise les modalités d'échange d'informations avec l'opérateur (délégué pour la défense et la sécurité du PIV).

Une directive du ministre de l'intérieur a précisé le contenu des PPE.

En cas d'actualisation du PPP d'un PIV, le préfet de département apprécie la nécessité de réviser le PPE. L'approbation d'un PPP d'une zone d'importance vitale peut entraîner la révision des PPE des PIV qui constituent cette zone, vers un PPE unique s'appliquant à la dite ZIV.

Dans le cadre de l'élaboration du PPE, le préfet de département peut être amener à effectuer une visite sur site du PIV concerné.

Le préfet de département peut permettre à l'opérateur qui en fait la demande de prendre connaissance du PPE de son PIV.

Il est également recommandé de communiquer le PPE aux services de police et/ou de gendarmerie compétents, dans la mesure où il leur revient d'appliquer les mesures d'intervention prévues dans ce document.

Dans tous les cas, le PPE ne pourra être transmis ou communiqué qu'à une personne habilitée au niveau confidentiel défense et qui a besoin d'en connaître, conformément à la réglementation en vigueur.

3.7. GESTION DE LA CONFIDENTIALITE ET PROTECTION DU SECRET DE LA DEFENSE NATIONALE

3.7.1. Elaboration, conservation et transmission des documents classifiés

Les directives et plans établis en application du dispositif SAIV sont classifiés au niveau *Confidentiel Défense*, en application des règles définies dans l'instruction générale interministérielle sur la protection du secret de la défense nationale n°1300/SGDSN/PSE/PSD du 30 novembre 2011 (IGI 1300). Sont notamment concernés :

- les DNS ;
- les PSO, à l'exception d'un rapport de présentation résumant leurs principales dispositions ;
- les arrêtés de désignation des PIV ;
- les PPP et les arrêtés d'approbation (non publiés au recueil des actes administratifs) ;
- les PPE.

L'élaboration, la conservation et la transmission des documents classifiés par l'OIV sont réalisées selon les modalités définies dans l'IGI 1300.

Le schéma de transmission des documents en fonction du besoin d'en connaître est précisé dans l'annexe 6.

3.7.2. Destruction des documents classifiés

Qu'il en soit l'émetteur ou le destinataire, l'opérateur veille à la destruction des documents classifiés dont il n'a plus à faire usage, notamment lorsque :

- un document classifié est révisé ou abrogé ;
- un PIV est radié ;
- une ZIV est radiée
- un opérateur perd la qualification d'OIV.

3.7.3. Cas d'un opérateur ne souhaitant pas mentionner certaines informations jugées très sensibles dans le PSO ou les PPP

Un OIV peut ne pas vouloir faire apparaître certaines informations très sensibles touchant à la gestion des risques et des crises. Il doit, dans ce cas, justifier de l'existence de procédures ou de dispositions particulières en faisant référence à ses documents internes qui les prévoient. Les autorités administratives instruisant le plan de sécurité de l'opérateur et ses PPP peuvent interroger l'OIV à propos de ces informations si cela s'avère nécessaire à leur instruction. Les autorités administratives peuvent en prendre connaissance sans nécessairement en disposer.

4. AUDIT ET CONTROLE

Les procédures d'audit et de contrôle relatives au secteur des activités militaires de l'Etat sont définies par les DNS « activités militaires de l'Etat » et « activités industrielles de l'armement » ainsi que par les dispositions contenues au chapitre 5 de la présente instruction.

Les procédures d'audit et de contrôle relatives au sous-secteur nucléaire sont définies par la DNS « nucléaire » ainsi que par les dispositions contenues au chapitre 6 de la présente instruction.

Les procédures applicables aux autres secteurs sont définies dans le présent chapitre.

4.1. AUDIT INTERNE MENE PAR L'OIV

Les audits internes sont menés par l'OIV afin d'apprécier la validité du PPP de chacun de ses PIV. La périodicité d'audit, la composition de l'équipe d'audit et les modalités d'audit sont à l'appréciation de l'OIV. L'audit d'un PIV peut conduire l'OIV à réviser à son initiative le PPP. Il devra alors faire l'objet d'une nouvelle approbation par le préfet de département.

L'OIV n'est pas tenu d'adresser une copie du compte-rendu d'audit aux autorités administratives. Il tient néanmoins ces comptes rendus à la disposition de l'autorité administrative en cas de contrôle.

4.2. CONTROLES PAR LES PREFETS

Les préfets de département approuvent les PPP et élaborent les PPE. Ils ont également, conformément à l'article R.1332-29 du code de la défense, la responsabilité de s'assurer régulièrement du bon niveau de protection des PIV, par un dialogue permanent avec leurs délégués pour la défense et la sécurité. Cela comprend la possibilité de visite sur site du PIV concerné. Dans ce cas, le préfet de département ou son représentant peut être accompagné d'experts des services déconcentrés de l'Etat en fonction de la nature du PIV.

Par ailleurs, le préfet de département dispose de la possibilité de solliciter le contrôle d'un PIV par la CZDS (Article R 1332-15).

Afin de permettre à la CZDS d'effectuer une programmation des contrôles de PIV, les préfets de département la tiennent régulièrement informée de l'approbation des PPP (grâce à la remontée d'information prévue à l'annexe 7).

4.3. CONTROLES PAR LES COMMISSIONS DE DEFENSE ET DE SECURITE

La CIDS et la CZDS sont chargées d'une mission générale de contrôle de la mise en œuvre du dispositif de protection des PIV et ZIV, à l'exception de ceux dépendant d'OIV relevant du ministre de la défense. Elles peuvent, à leur initiative ou sur demande d'un ministre coordonnateur ou d'un préfet de département, contrôler les mesures prises pour la sécurité des PIV ou des ZIV. La CZDS ne contrôle que les points et les zones d'importance vitale situés dans sa zone de compétence.

La CIDS peut émettre des directives d'inspection. A cet égard, elle peut fixer annuellement, sur proposition du SGDSN (et de l'ANSSI en particulier), la liste des PIV qui en raison de la criticité potentielle de leur système d'information[20] doivent faire l'objet d'un contrôle. Des représentants de l'ANSSI font alors partie des équipes chargées du contrôle de ces PIV et réalisent le contrôle du système d'information. L'ANSSI peut également, à sa demande, se joindre aux équipes chargées des contrôles des autres PIV.

Afin de coordonner les prévisions de contrôle, en prenant en compte les éventuelles directives d'inspection émises par la CIDS, les CZDS transmettent au SGDSN ainsi qu'au ministère de l'intérieur, au titre de l'animation territoriale :

- un calendrier annuel prévisionnel de contrôles[21] ;
- un bilan annuel des contrôles effectués au titre de l'année passée.

Dans la perspective d'un contrôle, la CZDS demandera en tant que de besoin communication du PPP approuvé au préfet de département (cf. annexe 6).

Les dispositions ci-après donnent des indications sur le déroulement du contrôle, sans préjuger des adaptations nécessaires au cas par cas, laissées à l'appréciation de la CZDS.

4.3.1. Objectifs du contrôle

Le nombre total de PIV ne permet pas aux commissions de pouvoir contrôler seules l'intégralité des PIV de leur ressort territorial. Les contrôles de la commission sont ainsi complémentaires avec la mission générale de vérification de la réalisation des PPP dévolue aux préfets de département, qui sont associés à ce titre à la politique de contrôle.

Après un contrôle ayant donné lieu à des recommandations à l'opérateur, la vérification de la mise en œuvre de ces recommandations incombe à l'autorité de contrôle, qui en informera le préfet de département[22].

Si les documents de référence concernant la sécurité du PIV sont d'abord la DNS, le PSO et le PPP, la commission peut vérifier, plus généralement, que les mesures de sécurité ne contiennent pas de failles évidentes en matière de protection des installations contre la malveillance.

[20] Sauf cas particuliers, il faut considérer que le système d'information constitue un composant névralgique du PIV au sens du paragraphe 3.3.2 de la présente instruction.

[21] Ce calendrier est porté à la connaissance de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

[22] Lorsque les recommandations concernent la sécurité des systèmes d'information, le préfet de département peut demander l'assistance de l'ANSSI (cf. paragraphe 4.3.4).

4.3.2. Préparation du contrôle sur place

a - Annonce du contrôle à l'opérateur

Dans l'esprit de coopération avec les opérateurs qui sous-tend la démarche SAIV, les contrôles sont annoncés, et non impromptus. Le président de la commission informe par écrit le délégué pour la défense et la sécurité du PIV de la date et de l'objet du contrôle ou de la visite sur site, de la composition de l'équipe de contrôle et du programme prévisionnel et, si possible, de l'horaire. Il signale le cas échéant les points particuliers sur lesquels portera le contrôle. Lorsque le contrôle est mené par une commission, le préfet de département en est informé et peut formuler un avis quant à son opportunité.

En cas de contrôle d'une ZIV, le délégué pour la défense et la sécurité de la ZIV est le correspondant de l'équipe de contrôle.

b - Durée du contrôle

Le contrôle se déroule idéalement sur une seule journée. Lorsqu'il porte aussi sur la sécurité des systèmes d'information, le contrôle peut nécessiter normalement trois à quatre journées supplémentaires mais ne mobilise que les experts de la sécurité des systèmes d'information de l'équipe de contrôle (les représentants de l'ANSSI) et du PIV. Le contrôle peut être prolongé si l'étendue ou la complexité du PIV le justifie, sur décision du président de la commission ou du préfet de département en tant qu'autorité de contrôle.

c - Equipe de contrôle

Le contrôle des PIV est effectué par des membres de la CZDS ou leurs représentants, préalablement formés à la sécurité des activités d'importance vitale, accompagnés en tant que de besoin par des experts en fonction de la nature du PIV. Ils forment une équipe de contrôle. Tous les membres de l'équipe de contrôle doivent posséder une habilitation de niveau confidentiel défense.

La composition de l'équipe de contrôle est adaptée en fonction des enjeux de sécurité du PIV, de la durée du contrôle (sur un ou plusieurs jours) et des expertises particulières recherchées. Néanmoins, c'est au président de la commission ou à son représentant qu'il appartient de définir le format de cette équipe. Le chef de la délégation est le président de la commission ou son représentant. Les domaines d'expertise requis pour le contrôle sont notamment la gestion de risques, la sûreté, la sécurité physique des installations et la sécurité des systèmes d'information. A ce titre, l'équipe de contrôle de la CZDS est typiquement composée de la manière suivante :

- un représentant du préfet de zone de défense et de sécurité, chef de la délégation et chargé de produire le rapport ;
- un représentant du préfet de département ayant approuvé le PPP, s'il le souhaite ;
- un représentant du service de gendarmerie ou de police territorialement compétent[23] ;
- un représentant du ministère coordonnateur, au titre de son expertise ;
- des experts de l'Agence nationale de la sécurité des systèmes d'information notamment lorsqu'il s'agit d'un contrôle demandé par l'ANSSI (cf. paragraphe 4.3).

d - Réunion préparatoire

Une réunion préparatoire au contrôle est organisée avec les participants sélectionnés, le ministère coordonnateur concerné ou son représentant déconcentré et toute autre personne dont la présence lui paraît justifiée. La participation du DDS du PIV concernée est indispensable.

Les objectifs de cette réunion sont de :

[23] Les forces régaliennes en charge de la protection de certains PIV y seront représentées (cas des PSPG).

- procéder à un examen rapide des caractéristiques du PIV contrôlé, sur la base des documents existants (PPP[24], PPE, PSO, DNS, rapport de contrôle antérieur) ;
- définir les axes principaux du contrôle sur site et les points saillants à vérifier, régler les aspects logistiques notamment les moyens d'accès aux composants névralgiques, les moyens de contrôle (droits d'accès, outils, etc.), les modalités pratiques du déplacement.

Le chef de délégation effectue la répartition des tâches entre les membres de l'équipe de contrôle.

L'équipe de contrôle doit prendre connaissance du référentiel de sécurité du site constitué par le PPP et le PSO. L'économie générale de la gestion de la sûreté du PIV, l'analyse de risque sur laquelle elle repose et l'organisation de la défense en profondeur du site doivent être assimilées et les composants névralgiques du PIV identifiés.

Le représentant de la préfecture de département, s'il est présent, fait connaître ce qu'il sait du PIV. Notamment, il fait savoir à l'équipe de contrôle l'état d'avancement de la mise en œuvre du PPP et si certaines des mesures de protection prévues dans celui-ci ne sont pas encore mises en place.

Des éléments de contexte et informations complémentaires à celles contenues dans le PPP sont apportés, comme :

- l'environnement du site (zone urbaine ou rurale, isolement, etc.) ;
- les autres réglementations de sécurité ou sûreté auxquelles il est éventuellement soumis (ISPS, OACI[25], ZRR[26], ICPE, Seveso, INB, zone d'interdiction de survol ou de prise de vues aériennes, zones protégées, etc.) ;
- d'une manière générale, toutes données intéressantes au titre de la sécurité du site (sensibilité ou vulnérabilité particulière, incidents de sécurité répertoriés, etc.).

4.3.3. Déroulement du contrôle

Le contrôle doit être exécuté de sorte à pouvoir déterminer si le dispositif de défense en profondeur du PIV est cohérent avec le PPP et les exigences minimales de sûreté attendues sur le site. De même l'adéquation avec le PPE peut être vérifiée.

a - Confidentialité du déroulement du contrôle

Les membres de l'équipe de contrôle font preuve sur place de discrétion vis-à-vis du personnel et des autres visiteurs présents sur le PIV. Les réunions se tiennent dans une salle dédiée au sein du PIV afin d'assurer la confidentialité des entretiens. Tous les participants doivent être habilités.

b - Etapes du contrôle

Les étapes prévues ci-après sont indicatives et s'adaptent à chaque cas.

- *Etape 1 : réunion de lancement du contrôle*

Le chef de délégation introduit la séance de lancement du contrôle en présentant un bref rappel des tenants et aboutissants du dispositif de la SAIV, du rôle des acteurs, de l'objectif du contrôle et de la composition de l'équipe de contrôle.

Le caractère classifié des informations échangées et des documents étudiés est rappelé. La présence des personnels du PIV participant au contrôle est nécessaire pour assurer que l'ensemble des intervenants de l'opérateur comprend le cadre général dans lequel s'inscrit le contrôle.

[24] Pour une ZIV, le PPP de la ZIV fait partie des documents de référence.
[25] Organisation de l'aviation civile internationale.
[26] Zone à régime restrictif.

- *Etape 2 : présentation sur table du PIV et du PPP par l'opérateur*

L'opérateur présente le PIV et le PPP pour permettre à l'équipe de contrôle d'apprécier sur table la politique générale de sécurité du PIV. Il précise l'activité du PIV, son organisation, son fonctionnement et les grandes lignes de l'analyse de risque du PPP (scénarios de menace, vulnérabilités).

- *Etape 3 : contrôle des mesures de protection*

- *Protection physique*

Le site est visité avec l'opérateur selon une logique concentrique, de l'extérieur (contour et entrée du PIV) vers l'intérieur (composants névralgiques du PIV). Le système de défense en profondeur doit ainsi pouvoir être identifié et compris, ses éventuelles lacunes détectées.

Les mesures de sécurité existantes sont comparées aux prescriptions du PPP et leur pertinence est jugée non seulement par rapport à l'analyse de risque qu'il contient mais aussi par rapport aux vulnérabilités identifiées par ailleurs par l'équipe de contrôle.

Le contrôle des mesures du plan VIGIPIRATE applicables au PIV est effectué. Sont notamment vérifiées l'application des mesures actives et la préparation des autres mesures graduées prévues dans le PPP comme par exemple le contrôle des personnes ou les mesures face aux menaces NRBC-E.

- *Sécurité des systèmes d'information*

Le contrôle de la sécurité des systèmes d'information est effectué lorsque un système d'information[27] constitue ou est susceptible de constituer un composant névralgique du PIV.

Le contrôle comporte une analyse technique du niveau de sécurité du système d'information, au regard des mesures de sécurité des systèmes d'information présentées dans le PPP, mais aussi par rapport aux menaces et vulnérabilités identifiées par ailleurs par l'équipe de contrôle, sur site, et à la lecture des documents transmis.

Les contrôles ne se limitent donc pas à un audit de l'organisation SSI (procédures, maintien en condition de sécurité) et à un contrôle de la sécurité physique des composants du système d'information, mais incluent également un examen technique du système d'information pouvant notamment comprendre :

- le relevé d'informations techniques (configurations du système, journaux d'évènements, traces d'incidents, etc.) ;
- la réalisation de tests d'intrusion dans le système d'information ;
- l'analyse du code source des logiciels ;
- la conduite d'entretiens avec les personnes en charge de l'administration du système ;
- et plus généralement toutes actions permettant d'analyser le niveau de sécurité.

Les interventions réalisées sont conformes à celles définies lors de la planification du contrôle. Une convention entre l'OIV et l'ANSSI peut être préalablement établie en tant que de besoin pour préciser les conditions dans lesquelles ces interventions sont effectuées. Sous son contrôle, le PIV met à disposition de l'ANSSI un accès direct à son système d'information pour permettre ces interventions.

[27] il peut s'agir de tout système d'information du PIV, y compris les systèmes d'information pilotant les systèmes industriels de l'OIV.

- *Dispositif de gestion de crise et plan de continuité d'activité*

L'organisation mise en place pour traiter les crises et assurer la continuité et le rétablissement d'activités du site font partie des éléments contrôlés. A ce titre, les membres de la commicssion de contrôle peuvent exiger d'avoir accès au plan de continuité d'activité de l'OIV, éventuellement décliné localement.

- *Etape 4 : bilan avec l'opérateur*

Un bilan immédiat est effectué à la fin du contrôle en présence du délégué à la défense et à la sécurité ainsi que du responsable de la sécurité des systèmes d'information de l'opérateur. Cette réunion de clôture a pour objectif de présenter à l'opérateur l'appréciation de l'équipe de contrôle sur la sécurité du PIV et de recueillir son avis en vue de tirer les conclusions initiales essentielles.

Les points suivants sont notamment abordés :

- conformité des mesures de sécurité avec le contenu du PPP ;
- pertinences des mesures de sécurité mises en place ;
- principales failles de sécurité détectées au regard des risques identifiés ;
- application des mesures VIGIPIRATE ;
- principaux axes d'amélioration.

La nature des principales non-conformités des mesures de protection avec le PPP est constatée avec le DDS. Les failles importantes dans l'analyse de risque, identifiées pendant le contrôle, mais non traitées par le PPP, sont aussi constatées.

4.3.4. Rapport de contrôle

a - Contenu du rapport

L'objectif du rapport de contrôle est de présenter à l'opérateur des recommandations pour améliorer la protection du PIV par rapport à son contexte, à l'état de l'art, et à son référentiel de sécurité (PPP, PSO, DNS). Il met donc en évidence les vulnérabilités du PIV face aux menaces identifiées et les mesures à prendre pour réduire la probabilité d'occurrence et/ou l'impact des risques. Parmi ces mesures, on distingue :

- les **recommandations simples** pour les problèmes les moins graves, qui ne donneront pas lieu à des suites particulières ;
- les **préconisations**, appelant une action de l'opérateur et/ou la révision du PPP.

Le rapport de contrôle est classifié et respecte le plan type dont le modèle figure en annexe 7.

Il commence par une brève description des modalités du contrôle, puis une page de synthèse sur le niveau de protection du PIV constaté pendant le contrôle, les principales failles détectées dans la sûreté du PIV, les recommandations et préconisations faites à l'opérateur.

Le rapport est rédigé par le chef de la délégation, approuvé par la commission et validé par son président. Il est ensuite transmis au DDS qui peut formuler des observations écrites, lesquelles pourront être annexées au rapport ou mener à sa révision.

b - Adoption du rapport et transmission à l'opérateur

Le rapport est soumis par le chef de délégation à l'autorité en charge du contrôle (CIDS, CZDS ou préfet de département) avant son adoption définitive.

Le rapport est adressé au :

- DDS du PIV ;
- DDS de l'OIV ;
- aux préfets de zone de défense et de sécurité et de département concernés ;
- au(x) ministre(s) coordonnateur(s) concernés ;
- au SHFD du ministère de l'intérieur, au titre de l'animation territoriale ;
- au SGDSN.

c - Suites du contrôle

Le suivi des préconisations figurant dans le rapport du contrôle incombe à l'autorité de contrôle. Lorsque les préconisations concernent la sécurité des systèmes d'information, l'autorité de contrôle peut faire appel aux personnes qualifiées ayant participé au contrôle (*i.e.* les experts de l'ANSSI) pour s'assurer du suivi de ces préconisations.

L'autorité de contrôle est informée des suites données à son rapport, tout comme le préfet de département.

De manière générale, le contrôle du PIV peut conduire à :

- la révision du PPP (Art. R. 1332-31 du code de la défense) ;
- la mise en demeure de l'OIV d'exécuter, dans un délai compris entre un et trois mois, une ou plusieurs mesures du PPP qui n'auraient pas été réalisées (Art. R. 1332-30 du code la défense) ;
- la saisine de l'autorité judiciaire aux fins de poursuite de l'auteur du délit (Art. R. 1332-30 du code de la défense).

5. PARTICULARITES DU SECTEUR D'ACTIVITES D'IMPORTANCE VITALE « ACTIVITES MILITAIRES DE L'ETAT »

Ce chapitre précise les spécificités liées au secteur d'activités d'importance vitale « Activités militaires de l'Etat » lorsque des modalités d'application diffèrent du schéma général de mise en œuvre du dispositif de sécurité des activités d'importance vitale. Le détail des procédures spécifiques à ce secteur figure dans les DNS « *Activités militaires de l'Etat* » et « *Activités industrielles de l'armement* », relevant toutes deux de la coordination du ministère de la défense.

5.1. LE PROCESSUS DE SECURITE DES ACTIVITES D'IMPORTANCE VITALE APPLIQUE AU SECTEUR « ACTIVITES MILITAIRES DE L'ETAT »

L'autorité militaire[28] désignée par le chef d'état-major des armées (CEMA) est, selon le cas :

- le délégué général pour l'armement en ce qui concerne l'approbation des PPP de ses installations classées installations prioritaires de défense (IPD) et PIV mais également de ceux des OIV de l'armement relevant du secteur « *Activités militaires de l'Etat* » ;
- le chef d'état-major de l'armée concernée, les officiers généraux commandants supérieurs des forces armées, le directeur général ou le directeur du service suivant le cas, en ce qui concerne l'approbation des PPP de ses installations classées IPD et PIV ;

[28] Ou l'autorité compétente.

- éventuellement le chef d'état-major des armées en ce qui concerne des PIV des organismes interarmées qui pourraient être classés comme IPD ainsi que des installations nucléaires intéressant la dissuasion, relevant ou non du ministère de la défense, lorsqu'aucune autorité n'a été désignée.

Chaque autorité militaire désignée par le CEMA se fait communiquer le nom de la personne chargée d'exercer la fonction de délégué pour la défense et la sécurité du PIV situé dans son domaine de compétence.

Pour les OIV relevant de la DNS « *Activités industrielles de l'armement* », le nom de la personne chargée d'exercer la fonction de délégué pour la défense et la sécurité de l'OIV est transmis au délégué général pour l'armement.

L'autorité militaire ayant approuvé le PPP d'un PIV conserve une copie dudit plan. L'autorité militaire informe le préfet de département d'implantation du PIV de l'approbation du PPP et lui communique dans les conditions fixées par sa hiérarchie (§ 5.4) les éléments du PPP strictement nécessaires à la réalisation du PPE. Le ministre de la défense, le chef d'état-major des armées ou leur représentant peut demander à l'autorité militaire concernée communication du PPP. L'OIV peut demander, au préfet de département concerné, à prendre connaissance du PPE de son PIV. L'ensemble des installations du secteur d'activités d'importance vitale « *Activités militaires de l'Etat* » est périodiquement contrôlé par la direction de la protection et de la sécurité de la défense (DPSD), par l'inspection des armées (IDA) dans le cadre de leurs attributions fixées par décret, par les OGZDS et les COMSUP dans leur zone de responsabilité et selon les modalités définies dans les DNS *« Activités militaires de l'Etat »* et « *Activités industrielles de l'armement »*. Le ministère de la défense peut faire appel à l'ANSSI pour effectuer le contrôle des systèmes d'information de ces installations dans les conditions prévues au paragraphe 5.5. Les rapports d'inspection sont adressés au ministre de la défense et aux OIV dont relèvent les installations.

Le préfet de département d'implantation du PIV est informé de toute nouvelle approbation du PPP consécutive à une opération de contrôle.

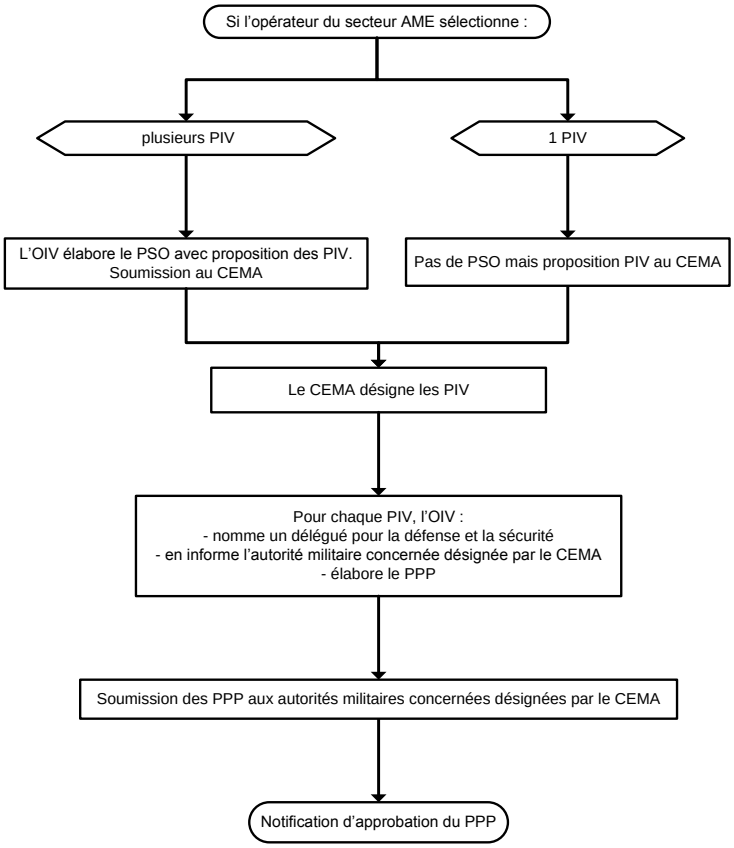


Figure 10 : Processus SAIV du secteur AME

5.2. LE PLAN DE SECURITE D'OPERATEUR

Le PSO est soumis à l'approbation du CEMA. Les PSO relevant de la DNS « *Activités industrielles de l'armement* » sont préalablement validés par le délégué général pour l'armement.

5.3. LE PLAN PARTICULIER DE PROTECTION

5.3.1. Approbation du PPP

Les PPP relevant de la DNS AME sont approuvés par l'autorité militaire désignée par le CEMA et ceux relevant de la DNS AIA sont approuvés par le délégué général pour l'armement (DGA). La révision du PPP se fait à l'initiative de l'opérateur ou sur injonction du ministre de la défense ou de son représentant.

Toute nouvelle approbation de PPP est portée à la connaissance du préfet de département d'implantation du PIV.

5.3.2. Modification du PPP par l'autorité militaire.

L'autorité militaire peut compléter ou modifier un PPP si le chef de site de l'installation prioritaire de défense ou le délégué pour la défense et la sécurité du PIV n'a pas donné suite à l'injonction qui lui a été adressée, ou si malgré les ajouts ou modifications apportées, les motifs énoncés au I de l'article R. 1332-26 du code de la défense demeurent. Dans ce cas, l'autorité militaire apporte elle-même les modifications et les ajouts qu'elle juge utiles de voir apparaître dans le PPP. Ces ajouts et modifications portent sur les mesures ayant fait l'objet de l'injonction adressée au chef de site de l'installation prioritaire de défense ou au délégué pour la défense et la sécurité du PIV de compléter ou modifier ledit plan.

Toute nouvelle approbation de PPP est portée à la connaissance du préfet de département d'implantation du PIV.

5.4. PLAN DE PROTECTION EXTERNE

Le préfet du département où est situé le PIV élabore le PPE de ce point, en liaison avec le délégué pour la défense et la sécurité du point, en tenant compte du PPP, et en coordination avec l'officier général de zone de défense et de sécurité.

Les PSO et les PPP de la DNS AME ne sont pas diffusés dans leur intégralité aux préfectures. Seules les informations extraites des PPP strictement nécessaires à l'élaboration des PPE des PIV leur sont communiquées par les DDS des PIV. Toutefois, après accord du DMD ou de l'OGZD, ces documents peuvent être consultés dans leur intégralité par les préfectures afin de recueillir les informations utiles et nécessaires à l'élaboration des PPE des PIV militaires.

5.5. MODALITES DE CONTROLE

L'autorité militaire désignée par le CEMA et ayant approuvé le PPP d'un PIV peut, à son initiative, sur demande d'un ministre coordonnateur ou du préfet de département concerné, contrôler les modalités de mise en œuvre dudit plan. Dans ce cadre, le SGDSN (ANSSI) peut proposer au ministre de la défense une liste de PIV qui, en raison de la criticité potentielle de leur système d'information, devraient être contrôlés. Le ministre de la défense et l'ANSSI s'accordent sur un mandat fixant les modalités du contrôle et permettant à des représentants de l'ANSSI, accompagnés de représentants du ministère, de faire partie des équipes chargées du contrôle de ces PIV.

a - Périodicité

Le CEMA fournit au ministre de la défense :

- son calendrier annuel prévisionnel de contrôles des PIV ;
- un bilan annuel des contrôles effectués au titre de l'année écoulée.

Pour les PIV dont l'ANSSI demande le contrôle, le ministère de la défense fournit à l'ANSSI la liste de ceux retenus et le calendrier prévisionnel de contrôle. Une copie du rapport de contrôle est alors adressé au secrétariat général de la défense et de la sécurité nationale.

b - Directives d'inspection

L'autorité militaire désignée par le CEMA (ou le haut-commissaire à l'énergie atomique pour les INID) est chargée d'une mission générale de contrôle de la mise en œuvre des PPP des PIV des opérateurs relevant du ministre de la défense.

c - Rapport de contrôle

Le modèle de rapport d'inspection des IPD et PIV relevant du SAIV AME approuvé par le CEMA, s'applique à l'autorité militaire chargée de contrôler et d'inspecter les IPD et les PIV.

Le rapport de contrôle est adressée au CEMA, au délégué pour la défense et la sécurité de l'opérateur et au délégué pour la défense et la sécurité du PIV.

d - Préconisations et/ou sanction

Le contrôle du PIV peut conduire à :

- la révision du PPP (*Art. R. 1332-31 du code de la défense*). Dans ce cas, le préfet de département d'implantation du PIV est informé à l'issue de celle-ci;
- la mise en demeure de l'OIV d'exécuter, dans un délai compris entre un et trois mois, une ou plusieurs mesures du PPP qui n'auraient pas été réalisées (*Art. R. 1332-30 du code de la défense*).

L'autorité militaire désignée par le CEMA veille à l'application des préconisations formulées à l'occasion d'un contrôle. Elle tient l'ANSSI informée lorsque cette dernière a participé au contrôle du système d'information, de l'application des préconisations qu'elle a formulées et peut demander au besoin son assistance.

6. ARTICULATION AVEC D'AUTRES PLANS ET DISPOSITIONS REGLEMENTAIRES

6.1. LIEN AVEC LES PLANS D'INTERVENTION : PLANS PIRATE ET DISPOSITIF ORSEC

Les plans PIRATE s'intègrent dans le dispositif global de vigilance, de prévention, de protection et de lutte contre le terrorisme.

Dans la continuité du plan VIGIPIRATE, ils visent à permettre aux autorités gouvernementales de réagir rapidement à tout événement grave. Le dispositif de sécurité des activités d'importance vitale et le plan VIGIPIRATE se placent essentiellement en amont de cet événement alors que les plans d'intervention se situent en aval. Par conséquent, il s'agit de prévoir dans les PSO selon les orientations fixées par la DNS, dans les PPP et dans les PPE les mesures favorisant, d'une part, l'application des mesures du plan VIGIPIRATE et, d'autre part, la mise en œuvre des plans d'intervention éventuelle.

Le plan ORSEC départemental détermine, compte tenu des risques existants dans le département l'organisation générale des secours et recense l'ensemble des moyens publics et privés susceptibles d'être mis en œuvre. Il définit les conditions de leur emploi par l'autorité compétente pour diriger les secours. A ce titre, il s'intègre dans le dispositif global de réponse de l'Etat.

6.2. AUTRES DISPOSITIFS

6.2.1. Lien avec les installations prioritaires de défense

En cas de menace portant sur une ou plusieurs installations prioritaires de défense, le commandement militaire désigné à cet effet peut être chargé, par décret en conseil des ministres, de la responsabilité de l'ordre public et de la coordination des mesures de défense civile avec les mesures militaires de défense à l'intérieur du ou des secteurs de sécurité délimités autour de ces installations par le Président de la République en conseil de défense[29].

Une aire spéciale de surveillance (ASS) doit être délimitée autour des installations prioritaires de défense. Dans celle-ci s'exerce en permanence une recherche coordonnée du renseignement au profit du service centralisateur des autorités locales désignées par le préfet. Ces autorités sont en charge, localement, de la sécurité de l'installation. Les aires spéciales de surveillance sont harmonisées sur l'ensemble du territoire et adaptées à la menace.

Les principes de mise en œuvre qui en découlent, pour les secteurs de sécurité des installations prioritaires de défense, sont définis dans les articles R. 1311-39 à R. 1311-43 du code de la défense.

6.2.2. Lien avec les zones protégées

Une zone protégée[30] peut être créée, sur décision du ministre coordonnateur compétent, sur tout ou partie du périmètre d'un PIV.

L'objet de la zone protégée est d'assurer aux lieux intéressant la défense nationale, qu'il s'agisse de services, d'établissements ou d'entreprises, publiques ou privées, une protection juridique contre les intrusions, complémentaire de la protection physique évoquée précédemment. Elles sont érigées en fonction du besoin de protection déterminé par le ministre coordonnateur compétent.

6.2.3. Lien avec les lieux abritant des éléments couverts par le secret de la défense nationale

Les disposition relatives à l'accès des magistrats aux lieux abritant des éléments couverts par le secret de la défense nationale, prévues aux chapitre VI du titre IV de l'IGI n°1300 du 30 novembre 2011 relative à la protection du secret de la défense nationale, ne concernent que l'accès des magistrats de l'ordre judiciaire à ces lieux.

6.2.4. Lien avec les zones interdites à la prise de vue aérienne et les zones interdites de survol

a - <u>Zones interdites à la prise de vue aérienne</u>

Le code de l'aviation civile (articles D. 133-10 à D. 133-14) règlemente l'usage aérien des appareils photographiques, cinématographiques, de télédétection et d'enregistrement de données de toute nature. La liste des zones interdites à la prise de vue aérienne est fixée par arrêté interministériel. Les zones concernées sont en principe sélectionnées parmi les PIV, sur proposition des ministères coordonnateurs. Les sites sont sélectionnés en fonction de leur vulnérabilité à une action de ciblage, c'est-à-dire à l'aune de leur environnement immédiat (zone urbanisée, emprise isolée) et de leur

[29] Article L. 1321-2 du code de la défense.
[30] Articles 413-7 et R 413-1 à R. 413-5 du code pénal.

configuration propre, afin de ne pas attirer inutilement l'attention sur des sites extérieurement anodins.

b - Zones interdites de survol

Le code des transports (article L. 6211-4) prévoit que certaines zones peuvent être interdites de survol, pour des raisons d'ordre militaire ou de sécurité publique. Elles sont définies par l'arrêté ministériel du 7 octobre 2006 modifié fixant les zones interdites de survol en France. Ces zones sont en principe également sélectionnées parmi les PIV par les ministères coordonnateurs.

6.2.5. Lien avec les zones maritimes réglementées

Le code des transports (article L. 5242-2) prévoit que le ministre chargé de la mer ou les préfets maritimes peuvent prendre des dispositions, pour certaines zones et/ou périodes temporelles, d'interdiction de la navigation, du mouillage ou de certaines activités, édictés en vue d'assurer la sécurité de la navigation ou le maintien de l'ordre public en mer. Certains PIV peuvent être concerné par ces restrictions de circulations.

6.2.6. Lien avec la défense opérationnelle du territoire

La défense opérationnelle du territoire, en liaison avec les autres formes de la défense militaire et avec la défense civile, concourt au maintien de la liberté et de la continuité d'action du Gouvernement, ainsi qu'à la sauvegarde des organes essentiels à la défense de la Nation.

Les autorités militaires auxquelles incombe son exécution ont notamment pour mission, en tout temps, de participer à la protection des installations militaires et, en priorité, de celles de la force nucléaire stratégique[31].

Les modalités de mise en œuvre de la défense opérationnelle du territoire font l'objet des articles R*.1422-1 à R*.1422-4 du code de la défense.

Le CEMA adresse aux officiers généraux de zones de défense les directives nécessaires à l'établissement des plans de défense opérationnelle du territoire. Ces plans, élaborés en accord avec les préfets de zone ou les hauts fonctionnaires de zone, doivent être cohérents avec les plans relevant de la compétence de ces derniers, conformément à l'article R.1311-3 du code de la défense. Ils sont arrêtés par le Premier ministre ou, en cas de délégation, par le ministre de la défense[32].

Les plans de défense pour la mise en œuvre (*partielle ou totale*) des mesures qui découlent de ces cas doivent être élaborés dans un souci de continuité (*ascendante et descendante*) avec les mesures de protection décidées par l'autorité territoriale du temps de paix, en cohérence avec les plans cités supra. Les mesures prises par l'autorité militaire pour la sécurité et la protection doivent être cohérentes et compatibles avec les autres mesures décidées par l'autorité territoriale (PPE) et par les opérateurs (PPP) pour le fonctionnement des secteurs d'activités d'importance vitale.

Les ministres coordonnateurs doivent, dès le temps de paix, définir les mesures de protection des installations prioritaires de défense et des PIV, propres à la défense opérationnelle du territoire.

6.2.7. Lien avec les régimes d'application exceptionnelle

a - Etat de siège

L'état de siège est défini dans les articles L. 2121-1 à L. 2121-8 du code de la défense.

Pendant l'état de siège, le renfort militaire envisagé peut être mis en place en priorité autour des installations prioritaires de défense, des zones d'importance vitale et des PIV.

[31] article R. 1421-1 du code de la défense.
[32] Cf. article R. 1422-1 du code de la défense.

b - Etat d'urgence

L'état d'urgence est défini par la loi n° 55-385 du 3 avril 1955. (Article L 2131-1 du code de la défense).

Pour toutes les installations prioritaires de défense, les zones d'importance vitale et les PIV de son ressort, le préfet peut déterminer des lieux faisant l'objet de restrictions de séjour ou de circulation.

6.2.8. Lien avec les plans de continuité d'activité et les plans d'urgence[33]

Les plans de continuité et de rétablissement d'activité visent à assurer le fonctionnement des activités essentielles des administrations et des opérateurs et la disponibilité des ressources indispensables au déroulement de leurs activités. Ils doivent par conséquent permettre la poursuite des activités au sein des PIV auxquels ils se rapportent, même en cas de crise grave.

Le dispositif de sécurité des activités d'importance vitale et les plans de continuité et de rétablissement d'activité s'intègrent dans une même logique de gestion de crise. Ils doivent être parfaitement compatibles entre eux et tendre vers les mêmes objectifs de continuité de l'activité et de sauvegarde de la ressource.

Les opérateurs d'importance vitale sont désormais tenus de rédiger un plan de continuité d'activité (article L. 2151-1 du code de la défense). A cette fin, le SGDSN a élaboré un guide méthodologique d'aide à l'élaboration des plans de continuité d'activité qui permet aux opérateurs d'importance vitale de concevoir un PCA répondant aux objectifs précités.

6.3. CAS PARTICULIER DU SECTEUR NUCLEAIRE[34]

6.3.1. Installations nucléaires civiles[35]

Les installations nucléaires civiles représentent des enjeux à la fois économiques, sanitaires et environnementaux majeurs. C'est pourquoi le secteur nucléaire doit être traité de façon particulière et de telle manière que la sécurité des matières, des transports et des installations nucléaires soit assurée de façon permanente et homogène contre tout acte de malveillance, en parfaite cohérence avec la Convention sur la Protection Physique des Matières Nucléaires adoptée par l'Agence Internationale de l'Energie Atomique.

Le sous-secteur nucléaire est composé des OIV au titre de l'article L. 1332-2 du code de la défense autorisés à importer, exporter, élaborer, détenir, transférer, utiliser ou transporter des matières nucléaires définies à l'article R. 1333-1 du même code, à savoir le plutonium, l'uranium, le thorium, le deutérium, le tritium et le lithium 6.

Il bénéficie, depuis la loi du 25 juillet 1980, codifiée aux articles L. 1333-1 et suivants du code de la défense, d'une réglementation forte visant à la protection et au contrôle de ces matières nucléaires, sur les sites ou en cours de transport.

---

[33] les plans d'urgence sont les suivants :
- le plan d'urgence interne (PUI), qui est établi et mis en œuvre par l'industriel responsable d'une installation ; il a pour objet d'une part de protéger le personnel travaillant sur le site en cas d'incident ou d'accident, et, d'autre part, de limiter au maximum les conséquences de l'accident à l'extérieur du site ;
- le plan particulier d'intervention (PPI), qui est établi et mis en œuvre par le préfet dont relève l'installation, et qui définit les moyens et l'organisation nécessaires pour protéger les populations en cas d'accident et apporter à l'industriel exploitant l'installation accidentée l'appui des moyens d'intervention extérieurs [*pompiers, gendarmes, police, service d'aide médicale urgente (SAMU), etc.*].

[34] articles R. 1333-13, R. 1333-37 à R. 1333-74 du code de la défense.

[35] installations nucléaires de base (INB).

Les articles R. 1333-1 et suivants (notamment l'article R. 1333-14) du code de la défense organisent, en cohérence avec la DNS propre à ce secteur, la protection et le contrôle des matières, des transports et des installations nucléaires.

Une aire spéciale de surveillance (ASS) est délimitée autour des installations nucléaires civiles les plus sensibles et dans laquelle s'exerce en permanence une recherche coordonnée du renseignement au profit des autorités responsables localement de la sécurité de l'installation (service centralisateur désigné par le préfet). Les ASS sont délimitées conformément aux prescriptions de la directive interministérielle en vigueur relative au recueil du renseignement en matière de surveillance dans le domaine nucléaire.

Tous les OIV du sous-secteur nucléaire sont désignés parmi les opérateurs autorisés à exercer les activités indiquées supra, par le ministre coordonnateur dudit sous-secteur, y compris lorsqu'ils ne possèdent ou n'opèrent qu'un PIV.

Toutefois, un préfet de département peut désigner un tel OIV qui gère une seule installation nucléaire de base (Article R1332-3 et L 1332-2).

Afin de garder la plus grande cohérence et une totale homogénéité dans l'application de ces réglementations, l'article VIII.4 de la DNS du sous-secteur nucléaire prévoit que les inspecteurs des matières nucléaires prévus à l'article L.1333-5 du code de la défense, spécialement habilités par les autorités de l'Etat, effectuent à la demande du ministre coordonnateur du sous-secteur nucléaire, et après information du préfet de zone de défense et de sécurité et du préfet de département territorialement compétent, le contrôle de l'application par les OIV de la DNS du sous-secteur nucléaire et de ses annexes et qu'ils informent les préfets concernés de leurs actions et de leurs constats.

La DNS du sous-secteur nucléaire organise les relations entre le service central chargé de la sécurité nucléaire et les préfets territorialement compétents, sans préjudice des concertations prévues dans la présente instruction.

De façon générale, les préfets de département ayant dans leur ressort un PIV dépendant de ce sous-secteur agissent en permanence en liaison étroite avec le service central spécialement chargé de la sécurité nucléaire auprès du ministre coordonnateur. De même, ce service tient systématiquement informé les préfets des inspections réalisées dans le cadre de la présente instruction, et recherche leur participation chaque fois qu'il est possible.

6.3.2. Installations nucléaires intéressant la dissuasion (INID) [36]

Au plan de la protection physique des installations, les dispositions de la directive nationale de sécurité « activités militaires de l'Etat » (DNS AME) sont applicables aux opérateurs d'importance vitale (OIV) détenant des INID dépendant ou non du ministère de la défense. Elles sont complétées par le référentiel de menaces spécifiques élaboré par le chef d'état-major des armées et les objectifs de protection applicables qui en découlent.

A ce titre, le ministre de la défense est le ministre coordonnateur pour l'ensemble des INID, que celles-ci dépendent ou non de son ministère. Dans le cas des INID situées dans l'emprise d'établissements industriels, le ministre de la défense doit être tenu informé par le ministre de tutelle de toute évolution des prescriptions applicables en matière de protection physique. Les hauts fonctionnaires de défense et de sécurité (HFDS) concernés se concertent étroitement.

L'inspecteur des armements nucléaires est chargé de vérifier la pertinence et la bonne application de l'ensemble des mesures concourant au contrôle gouvernemental de la dissuasion nucléaire. Il est consulté lors de la définition des procédures du contrôle gouvernemental et donne son avis sur la

[36] Installations prioritaires de défense (IPD), installations nucléaires de base secrètes (INBS) et installations nucléaires intéressant la dissuasion (INID).

validité des dispositions ou mesures prises et propose toute modification qui lui apparaîtrait nécessaire (articles R.* 1411-13 et R.* 1411-15 du code de la défense).

7. LES INFRASTRUCTURES CRITIQUES EUROPEENNES

Le programme européen de protection des infrastructures critiques[37] (PEPIC) a été adopté en 2006. Les menaces contre lesquelles il doit répondre ne se limitent pas seulement au terrorisme, mais englobent les activités criminelles, les catastrophes naturelles et d'autres causes d'accidents, selon une approche tous risques. L'objectif général est d'améliorer la protection des infrastructures critiques dans l'Union européenne. C'est dans ce cadre qu'a été adoptée la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.

7.1. DIRECTIVE DU CONSEIL SUR LE RECENSEMENT DES INFRASTRUCTURES CRITIQUES EUROPEENNES

Le dispositif prévu au niveau national pour la sécurité des secteurs d'activités d'importance vitale s'inscrit dans une logique sensiblement comparable et complémentaire à celle menée au niveau de l'Union européenne. La directive 2008/114/CE prévoit un mécanisme d'identification et de désignation des infrastructures critiques européennes (ICE) « *dont l'arrêt ou la destruction aurait un impact considérable sur deux Etats membres au moins* ». La mise en œuvre de ce mécanisme s'appuie sur des lignes directrices (non contraignantes) élaborées conjointement par la Commission et les Etats membres.

Une infrastructure critique est un « *point, système ou partie de celui-ci, situé dans les États membres, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif dans un État membre du fait de la défaillance de ces fonctions* ».

Le dispositif communautaire est mis en place dans un premier temps dans deux secteurs d'activités[38] :

- les transports (*transport routier, ferroviaire, aérien, navigation intérieure, transport hauturier, cabotage et ports*) ;
- l'énergie (*infrastructures et installations permettant la production et le transport d'électricité, production pétrolière, raffinage, traitement, stockage et distribution par oléoducs, production gazière, raffinage, traitement, stockage et distribution par gazoducs et terminaux de gaz naturel liquéfié*).

Les Etats membres désignent un point de contact pour la protection des infrastructures critiques européennes, chargé de coordonner les questions liées à l'application de la directive tant à l'intérieur de l'État membre qu'avec les autres États membres et la Commission. Pour la France, il s'agit du SGDSN.

[37] Communication de la Commission du 12 décembre 2006 sur un programme européen de protection des infrastructures critiques.

[38] A l'occasion d'un prochain réexamen, le champ d'application de la directive pourra être étendu à d'autres secteurs d'activités (celui des technologies de l'information et de la communication est particulièrement visé par une éventuelle extension).

7.2. OBLIGATIONS POUR L'ETAT ET LES OPERATEURS

La directive rappelle le rôle prééminent des Etats membres dans ce dispositif. Ils doivent veiller à son application effective par les opérateurs et doivent également présenter à la Commission, tous les 24 mois, des données générales de synthèse sur les types de points vulnérables, de menaces et de risques rencontrés dans les différents secteurs d'infrastructures critiques européennes. Pour la désignation des infrastructures concernées, un dialogue doit être recherché entre les Etats membres concernés, avec le soutien éventuel de la Commission.

Selon la directive, l'opérateur d'une infrastructure critique européenne a deux obligations :

- désigner un correspondant pour la sécurité ;
- rédiger un PSO.

Ces deux obligations sont parfaitement comparables à celles qui existent en droit français, qu'il s'agisse du délégué pour la défense et la sécurité (DDS) de l'opérateur ou du PSO.

Valent PSO au titre de la directive, selon le cas de figure :

- le PPP ou plan reconnu équivalent au titre de l'article R. 1332-34 du code de la défense ;
- le PSO prévu par l'article R. 1332-19 du code de la défense.

7.3. IDENTIFICATION D'UNE INFRASTRUCTURE CRITIQUE EUROPEENNE

Pour les secteurs auxquels la directive s'applique, les ministères coordonnateurs concernés procèdent, en liaison avec les OIV et avec l'appui méthodologique du SGDSN, à une analyse sectorielle visant à identifier les infrastructures répondant aux critères mentionnés supra, tant en France que dans les autres Etats membres (ICE potentielles).

Les ICE en France sont normalement sélectionnées parmi les PIV. Dans le cas contraire, l'infrastructure désignée doit au moins être couverte globalement par un PSO au titre du dispositif de la SAIV ou se voir préalablement appliquer ce dispositif[39]. Dans tout autre cas de figure, l'infrastructure n'est pas désignée ICE. L'Etat membre qui en a fait la demande en est informé.

Le travail d'identification des ICE à l'étranger est entrepris également lors de l'élaboration des DNS et des PSO, tous secteurs d'activités confondus, dans le cadre de l'analyse des interdépendances internationales. Une fois cette sélection effectuée, le SGDSN en informe les Etats membres sur les territoires desquels se trouvent une ou plusieurs ICE potentielles. Les modalités des discussions bilatérales sont déterminées au cas par cas (réunion, échange de courrier, etc.), sous la responsabilité du SGDSN.

La directive européenne n'impose aucune règle quant à la forme que doit prendre l'accord entre les États membres sur la désignation définitive d'une ICE. Elle précise seulement que « *l'État membre sur le territoire duquel se situe une ICE potentielle la désigne en tant qu'ICE après accord entre cet État membre et les États membres qui sont susceptibles d'être affectés considérablement par l'infrastructure. L'accord de l'État membre sur le territoire duquel se situe l'infrastructure à désigner comme ICE est requis* ». Cet accord peut se concrétiser par un simple échange de lettres entre les deux parties.

[39] Ce dernier cas de figure ne peut être écarté mais ne doit être envisagé que de manière exceptionnelle ; en tout état de cause l'opérateur concerné n'est désigné OIV que dans la mesure où il répond aux conditions prévues à l'article R. 1332-1 du code de la défense.

7.4. DESIGNATION D'UNE INFRASTRUCTURE CRITIQUE EUROPEENNE EN FRANCE

Une fois l'accord obtenu, le ministère coordonnateur informe les opérateurs d'ICE situées en France du choix effectué, en précisant le n° d'identification du PIV. Les préfets de zone et de départements sont informés spécifiquement de cette désignation. Les infrastructures critiques européennes font l'objet d'une mention particulière dans la base de données DIVA tenue et mise à jour par le SGDSN.

8. CONTESTATION DES ACTES PRIS PAR L'AUTORITE ADMINISTRATIVE (ART. R. 1332-33 DU CODE DE LA DEFENSE)

– POINT-CLE –
Le recours administratif est préalable au recours contentieux.

8.1. PRINCIPE

L'opérateur qui conteste un acte pris dans le cadre de la mise en œuvre du dispositif de sécurité des secteurs d'activités d'importance vitale doit adresser préalablement un recours administratif à l'autorité administrative concernée.

a - Autorité destinataire du recours administratif

Lorsqu'un opérateur est désigné d'importance vitale au titre d'un secteur d'activités d'importance vitale, l'éventuel recours administratif est adressé au ministre coordonnateur dudit secteur.

Lorsqu'un opérateur est désigné d'importance vitale au titre de plusieurs secteurs d'activités d'importance vitale, l'éventuel recours administratif est adressé au correspondant privilégié.

Lorsqu'un opérateur est désigné d'importance vitale par le préfet de département, l'éventuel recours administratif est adressé au ministre coordonnateur du secteur d'activités d'importance vitale mentionné dans l'arrêté de désignation du préfet.

b - Décisions pouvant faire l'objet d'un recours administratif

Les décisions administratives prises pour l'application du dispositif de sécurité des activités d'importance vitale peuvent faire l'objet d'une contestation dans le cadre général de l'article R. 1332-33 du code de la défense.

Les avis rendus par la CIDS et par les CZDS ne sont pas susceptibles de faire l'objet d'un recours administratif ou contentieux car ce ne sont pas des décisions administratives.

Il en va de même des avis rendus par les autorités administratives dans le cadre de l'enquête administrative éventuellement sollicitée préalablement à l'accès à un PIV. L'avis rendu par cette autorité n'est pas une décision administrative.

8.2. EXCEPTION

En cas de contestation du PPP complété ou modifié par le préfet de département ou l'autorité militaire, la décision du préfet de département ou de l'autorité militaire fait l'objet d'un recours devant le tribunal administratif qui statuent en urgence.

9. BASE DE DONNEES « DIVA »

Une base de données unique tenue et mise à jour par le SGDSN rassemble l'ensemble des informations spécifiques du dispositif de sécurité des activités d'importance vitale. Elle porte le nom de « DIVA » (*Données d'Importance VitAle*s).

9.1. ATTRIBUTION DU NUMERO D'IDENTIFICATION (TRIPLET) DES PIV ET DES ZIV

Chaque PIV et chaque ZIV doivent être identifiés par un numéro d'identification (dit aussi « triplet »), délivré par le SGDSN, avant toute notification de désignation d'un PIV ou de création d'une ZIV par l'autorité administrative.

9.2. INFORMATIONS CONCERNANT LES OIV

Dès désignation d'un OIV, l'autorité administrative (ministre coordonnateur ou préfet de département) en informe le SGDSN en lui précisant la référence et la date de l'arrêté de désignation, le ou les ministre(s) coordonnateurs associé(s) et le ou les secteur(s) d'activité(s) concerné(s).

Par la suite, l'autorité administrative informe le SGDSN :

- de la date de notification à l'OIV de la dernière DNS devant lui être communiquée ;
- de la date de présentation du PSO à la commission interministérielle ou zonale de défense et de sécurité ;
- de la date de désignation des PIV.

L'autorité administrative ayant connaissance d'une modification d'une des informations ci-dessus en informe le SGDSN afin de mettre à jour la base de données.

9.3. INFORMATIONS CONCERNANT LES PIV ET LES ZIV

Dès qu'il approuve un PPP d'un PIV ou d'une ZIV, le préfet de département transmet, par l'intermédiaire du préfet de zone de défense et de sécurité, au ministère de l'intérieur en charge de l'animation territoriale, au SGDSN ainsi qu'aux ministres coordonnateurs intéressés, les informations utiles concernant le PIV ou la ZIV. La nature de ces informations est précisée en annexe 8. Les autorités ayant connaissance d'une modification de ces informations en informent le SGDSN (et le préfet de département d'implantation du PIV ou de la ZIV) afin de mettre à jour la base de données. Il en va de même pour les PIV relevant du ministère de la Défense selon ses propres directives.

* * * * * * *

L'instruction générale interministérielle n° 6600/SGSDN/PSE/PPS du 26 septembre 2008 relative à la sécurité des activités d'importance vitale est abrogée.

Paris, le 7 janvier 2014,
Pour le Premier ministre et par délégation,
Le secrétaire général de la défense et de la sécurité nationale

Francis DELON

LISTE DES ANNEXES

A L'INSTRUCTION GENERALE INTERMINISTERIELLE

N° 6600/SGDSN/PSE/PSN DU 7 JANVIER 2014

RELATIVE A LA SECURITE DES ACTIVITES D'IMPORTANCE VITALE

1.	Glossaire
2.	Répertoire des acronymes
3.	Architecture générale de la planification anti-terroriste
4.	Synoptique des actions à mener selon le niveau de responsabilité
5.	Repères chronologiques pour la mise en œuvre du dispositif de sécurité des activités d'importance vitale
6.	Transmission des documents
7.	Modèle de rapport de contrôle d'un PIV par une commission interministérielle ou zonale de défense et de sécurité des secteurs d'activités d'importance vitale
8.	Informations à transmettre pour la mise à jour de la base de données DIVA
9.	Modèle de formulaire de demande d'avis adressée par l'OIV à l'autorité administrative avant l'accès d'une personne à un PIV
10.	Modèle de formulaire d'information de la personne concernée par l'enquête administrative
11.	Modèle de formulaire de rejet de demande d'accès à un PIV en cas de demande non recevable
12.	Modèle de formulaire de réponse de la préfecture à l'OIV

Annexe 1

Glossaire

Aire Spéciale de Surveillance[1] (ASS) : aire géographique définie par le préfet autour d'un point estimé particulièrement sensible et dans laquelle s'exerce en permanence une recherche coordonnée du renseignement au profit des autorités responsables de la sécurité de l'installation.

Attractivité : attrait d'une cible pour un acte de malveillance ou de terrorisme, par suite des effets attendus sur les plans humain, économique, médiatique ou psychologique.

Composant névralgique : élément à la fois indispensable au fonctionnement d'une installation prioritaire de défense ou d'un point d'importance vitale et vulnérable, de niveau plus fin que ce point (salle de contrôle ou de commande…).

Danger : toute situation, condition ou pratique qui comporte en elle-même une capacité à occasionner des dommages aux personnes, aux biens ou à l'environnement[2].

Défense dans la profondeur : la défense en profondeur consiste en la superposition de plusieurs lignes de défense, composées d'un ensemble de mesures de sécurité, chaque ligne devant contribuer à affaiblir l'attaque et à permettre aux suivantes de se renforcer en vue soit d'empêcher la destruction ou la prise de contrôle des composants névralgiques du PIV, soit d'en limiter les effets.

Directive nationale de sécurité (DNS) : fondées sur une analyse de risque du secteur concerné en tenant compte des scénarios de menaces élaborés par le ministre coordonnateur, la ou les directives nationales de sécurité d'un secteur d'activités d'importance vitale précisent les **objectifs et les politiques de sécurité du secteur ou d'une partie du secteur**.

Etablissement : unité géographique de production ou d'exploitation.

Exigences de sécurité : éléments requis pour atteindre les objectifs de sécurité, exprimés dans un ou plusieurs des cinq domaines *planification*, *sensibilisation*, *organisation*, *prévention* et *protection.*

Faisabilité d'une action malveillante ou d'un acte de terrorisme : possibilité de conduire une telle action à partir de connaissances, de l'acquisition de moyens, de l'exploitation de vulnérabilités, de la capacité à accéder à la cible sans être détecté dans un délai qui rendrait l'action impossible.

Infrastructure critique européenne (ICE) : infrastructure critique située dans les États membres de l'Union Européenne dont l'arrêt ou la destruction aurait un impact considérable sur deux États membres au moins.

Impacts (ou conséquences dommageables) : effets prévisibles d'une agression réussie sur une cible, estimés en termes d'atteinte aux activités du pays ou de danger pour la population.

Installation : ensemble des objets, des dispositifs et des bâtiments installés en vue d'un usage déterminé.

Installation prioritaire de défense[3] (IPD) : Installation autour de laquelle a été délimité par le

[1] cf. I.I n°1200/SGDN/AC/REC/CD du 8.12. 1973 et I.I n°10008/SGDN/ANS/CD du 24.01.1979.
[2] cf. référentiel international de bonnes pratiques *Occupational Health and Safety Assessment Series* [18001].
[3] Articles L. 1321 et R. 1311-39 à R. 1311-43 2 du code de la défense, instruction interministérielle n°1100/SGDN/AC/REG/CD du 8 août 1973 relative à la délimitation des secteurs de sécurité des installations

président de la République en conseil de défense un secteur de sécurité et dont la sécurité doit être assurée en priorité et en tout temps. Une aire spéciale de surveillance (ASS) est par ailleurs définie par le préfet autour de chaque IPD (cf. définition de l'ASS plus haut).

Les autorités militaires auxquelles incombe l'exécution de la défense opérationnelle du territoire ont pour mission en tout temps, de participer à la protection des installations militaires et, en priorité, de celles de la force nucléaire stratégique[4]. Les IPD sont concernées par ces mesures.

Menace : tout événement physique, phénomène ou activité humaine potentiellement préjudiciable, susceptible de provoquer des décès ou des lésions corporelles, des dégâts matériels ou immatériels, des perturbations sociales et économiques ou une détérioration de l'environnement. Pour la démarche de sécurité des secteurs d'activités d'importance vitale, les menaces seront réputées avoir un caractère malveillant ou être de nature terroriste.

Mesures de sécurité : systèmes ou procédures identifiés pour répondre aux exigences de sécurité.

Ministre coordonnateur : le ministre coordonnateur d'un secteur d'activités d'importance vitale *désigne* les opérateurs d'importance vitale relevant du ou des secteurs d'activités dont il a la charge, *élabore* la ou les directives nationales de sécurité du ou de ces secteurs et *notifie* la liste des points d'importance vitale. Il est responsable de la coordination du secteur vis-à-vis des autres secteurs et, pour chaque secteur dont il est chargé, de la prise en compte des intérêts des autres ministères. Ce rôle ne lui donne toutefois aucune tutelle sur les opérateurs du secteur concerné par la directive nationale de sécurité qui relèvent d'autres ministères.

Objectif de sécurité : but à atteindre pour amener un risque identifié à un niveau acceptable, en agissant sur l'attractivité, la faisabilité, la vulnérabilité ou les impacts.

Ouvrage : construction.

Plan de sécurité d'opérateur (PSO) : plan définissant la politique générale de protection de l'ensemble des activités de l'opérateur, notamment celles organisées en réseau, comportant des mesures permanentes de protection et des mesures temporaires et graduées. Il n'est requis que si l'opérateur gère plusieurs points d'importance vitale.

Plan particulier de protection (PPP) : plan établi pour chaque point d'importance vitale à partir du plan de sécurité d'opérateur d'importance vitale, qui lui est annexé, et comportant des mesures permanentes de protection et des mesures temporaires et graduées.

Plan de protection externe (PPE) : plan établi pour chaque point d'importance vitale par le préfet de département en liaison avec le délégué de l'opérateur pour la défense et la sécurité de ce point, récapitulant les mesures planifiées de vigilance, de prévention, de protection et de réaction prévues par les pouvoirs publics.

Point d'importance vitale (PIV) : tout établissement, installation ou ouvrage dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement :

- si son activité est difficilement substituable ou remplaçable, d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation,
- ou de mettre gravement en cause la santé ou la vie de la population.

---

prioritaires de défense, instruction interministérielle n° 1200/SGDN/AC/REG/CD du 8 décembre 1973, relative à la sécurité des installations prioritaires de défense.

[4] Article R. 1421-1 du code de la défense.

Risque encouru : appréciation combinée de la vraisemblance d'une agression réussie (résultant des scénarios de menace et de l'analyse des vulnérabilités) et de ses impacts.

Secteur d'activités d'importance vitale (SAIV) : secteur constitué d'activités concourant à un même objectif :

- qui ont trait à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie des populations, ou à l'exercice de l'autorité de l'État, ou au fonctionnement de l'économie, ou au maintien du potentiel de défense, ou à la sécurité de la nation, dès lors que ces activités sont difficilement substituables ou remplaçables ;

- ou qui peuvent présenter un danger grave pour la population.

Vulnérabilité : propension d'un milieu, d'un bien ou d'une personne à subir des conséquences dommageables à la suite d'un événement. Elle ne produit pas nécessairement de dommage par elle-même[5].

Zone d'importance vitale (ZIV) : zone géographique continue dans laquelle sont implantés plusieurs points d'importance vitale relevant d'opérateurs différents et interdépendants.

Zone protégée : zone créée par arrêté des ministres intéressés et faisant l'objet d'une interdiction d'accès sans autorisation, sanctionnée pénalement en cas d'infraction (articles 413-7 et R. 413-1 à R. 413-5 du code pénal).

[5] Par exemple, par la porte d'un local contenant des matières dangereuses restant ouverte en permanence (vulnérabilité), des personnes mal intentionnées pourraient pénétrer pour commettre un vol (menace) ; un temps très long peut s'écouler avant que des personnes identifient la vulnérabilité et s'introduisent dans les locaux pour voler les matières en vue d'un usage malveillant.

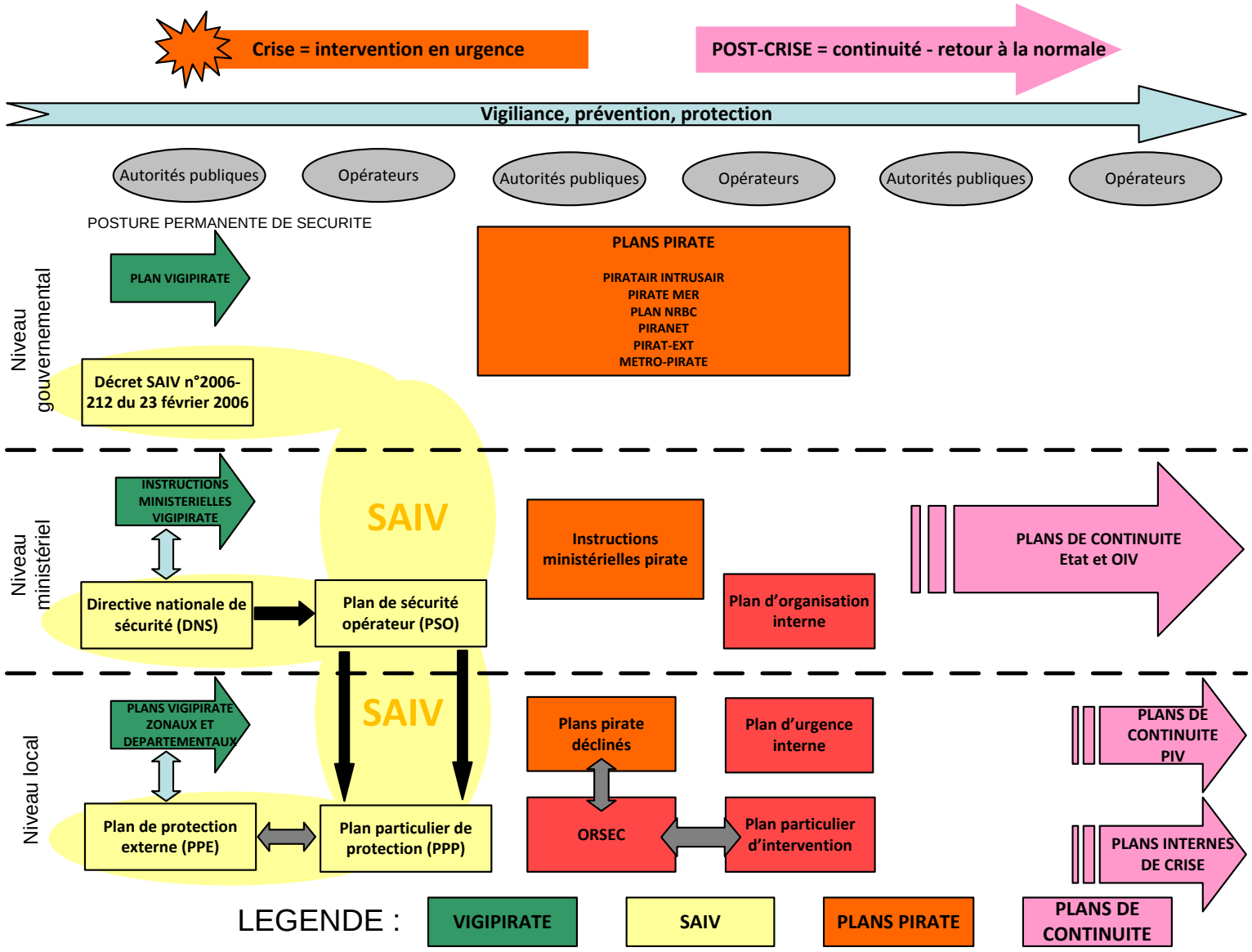
Annexe 2

Répertoire des acronymes

AME	Activités militaires de l'Etat
CEMA	Chef d'état-major des armées
CIDS	Commission interministérielle de défense et de sécurité
DDS	Délégué pour la défense et la sécurité
DOT	Défense opérationnelle du territoire
CDAOA	Commandement de la défense aérienne et des opérations aériennes
CZDS	Commission zonale de défense et de sécurité
IAN	Inspection des armements nucléaires
ICE	Infrastructure critique européenne
ICPE	Installation classée pour la protection de l'environnement
IDA	Inspection des armées
INB	Installation nucléaire de base
IPD	Installation prioritaire de défense
OIV	Opérateur d'importance vitale
PPE	Plan de protection externe
PPP	Plan particulier de protection
PSO	Plan de sécurité d'opérateur
PIV	Point d'importance vitale
SAIV	Secteur d'activités d'importance vitale
SHFD	Service du haut fonctionnaire de défense
ZIV	Zone d'importance vitale

Annexe 3

Architecture générale de la planification antiterroriste



Annexe 4

Synoptique des actions à mener selon le niveau de responsabilité

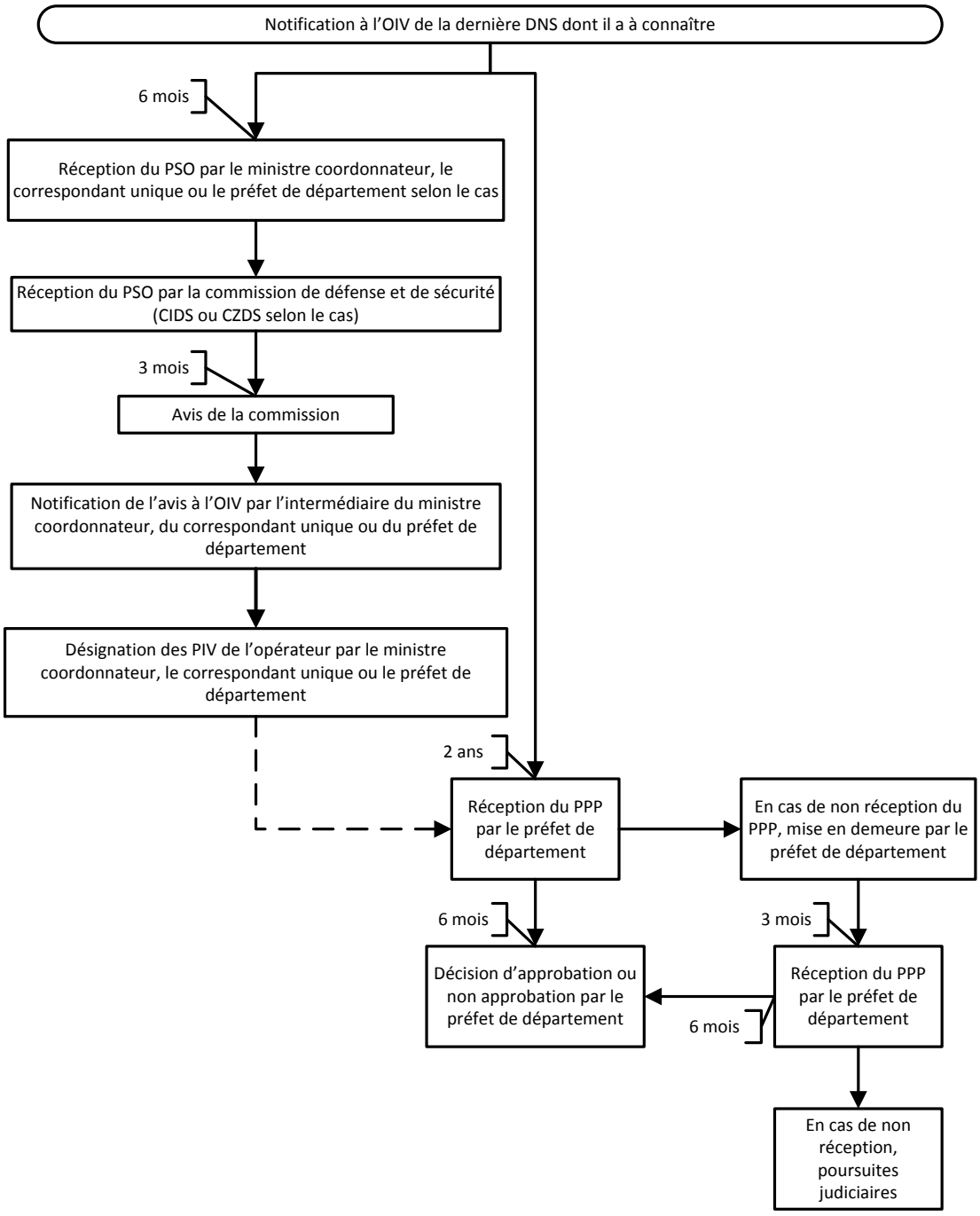
	REALISATION	DESIGNATION	APPROBATION	CONSULTATION	CONTROLE
Premier ministre	- Définition des secteurs d'activités d'importance vitale et des ministres coordonnateurs - Documents de méthode et plans type		- DNS	Désignation d'une ZIV sur plusieurs départements ainsi que le préfet coordonnateur	
Ministre de l'intérieur	Guide d'aide à l'élaboration des plans				Animation et suivi de la mise en œuvre territoriales
Ministre coordonnateur	- DNS	- OIV - PIV			
CIDS				- DNS - OIV - PSO y compris la liste des PIV	- Contrôle sur place des PIV
CZDS				- Désignation des OIV opérateurs d'un seul établissement (ICPE ou INB) - PSO dont le périmètre ne dépasse pas celui de la zone - Désignation d'une ZIV (1 seul département) - PPP de la ZIV	- Contrôle sur place des PIV
Préfet	- PPE	- OIV opérateurs d'une seule ICPE ou INB et PIV afférents - ZIV (1 seul département)	- PPP (PIV et ZIV)		- Inspection des PIV - Injonction et mise en demeure - Saisine de l'autorité judiciaire
Opérateur	- PSO - PPP				

Annexe 5

Repères chronologiques
pour la mise en œuvre du dispositif de sécurité des activités d'importance vitale

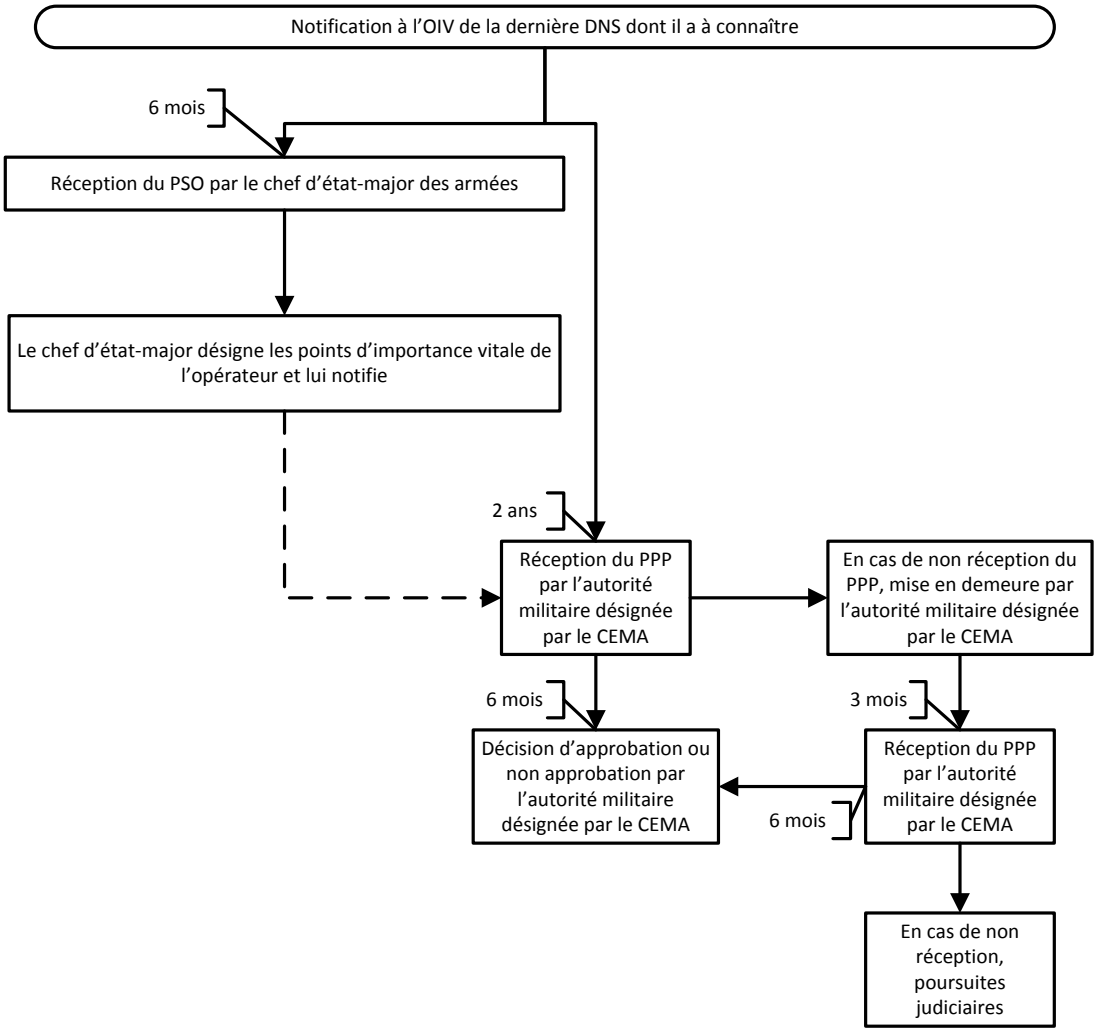
1. Principe général

Les délais indiqués courent à partir de l'étape précédente.



2. Cas des opérateurs d'importance vitale relevant du ministre de la défense

Les délais indiqués courent à partir de l'étape précédente.

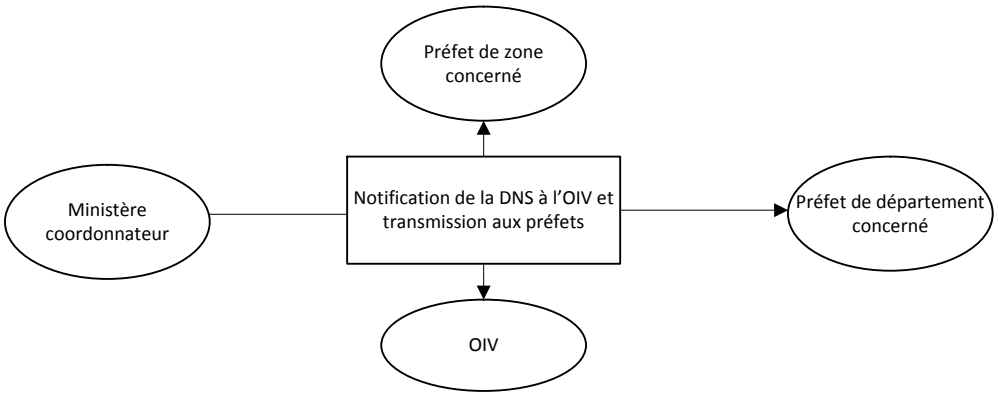


Annexe 6

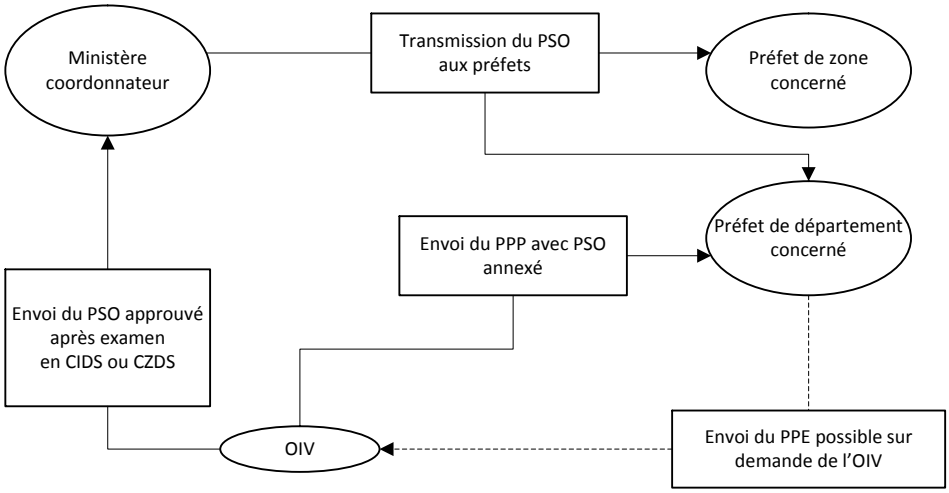
Transmission des documents

Les échelons territoriaux reçoivent les documents en application du droit d'en connaître. Les DNS et PSO sont transmis sans délai par les ministères coordonnateurs aux préfets de zone et aux préfets de département, dès lors que ceux-ci ont un PIV afférents dans leur ressort territorial.

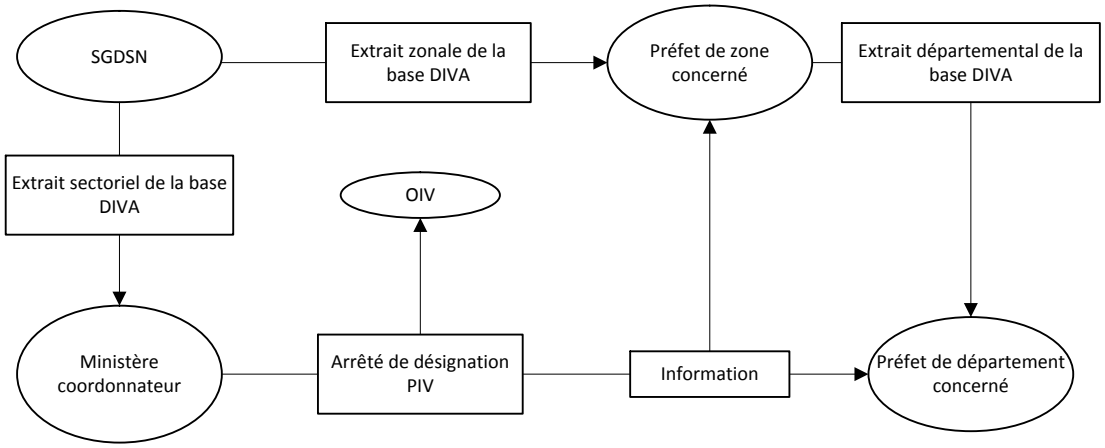
Directives nationales de sécurité



Plans de sécurité d'opérateur – Plans particuliers de protection



Points d'importance vitale



Annexe 7

Modèle de rapport de contrôle d'un point d'importance vitale par une commission de défense et de sécurité des secteurs d'activités d'importance vitale

Objet : Visite du [désignation du point d'importance vitale]

Références : Articles R.1332-10 à R.1332-10 (commission interministérielle) ou R.1332-13 à R.1332-15 (commission zonale) du code de la défense

Classification : Confidentiel défense

Pièce jointe : Feuille de présence

a. Caractéristiques du point d'importance vitale

Cette partie reprend la partie 1 du plan particulier de protection du point d'importance vitale, à laquelle s'ajoutent :

- la dénomination de l'opérateur d'importance vitale ;
- la référence de la notification de désignation du point d'importance vitale ;
- l'identification du ministre coordonnateur ou correspondant unique ;
- l'identification des autres ministres coordonnateurs concernés ;
- l'identification des directives nationales de sécurité de référence ;
- la mention d'appartenance éventuelle à une zone d'importance vitale identifiée par son numéro triplet ;
- l'identification des forces de l'ordre territorialement compétentes (police ou gendarmerie nationale) dans la zone dans laquelle se situe le point d'importance vitale ;
- un descriptif succinct des éventuels incidents de sécurité survenus depuis le précédent contrôle
- l'existence d'un plan de continuité d'activité de l'OIV décliné localement et l'identification du responsable de sa mise en œuvre.

a.1 Identification

a Désignation du point d'importance vitale et numéro de triplet

b Classement éventuel du site selon les réglementations concernant la protection

c Nature des activités

d Secteur(s) d'activité(s) d'importance vitale concerné(s)

e Localisation du point d'importance vitale (adresse, numéro de téléphone, environnement alentour, plan d'accès)

a.2 Présentation

a Organisation hiérarchique (autorité, responsables, permanence de direction)

b Délégué pour la défense et la sécurité du point d'importance vitale (titulaire, suppléant, autres fonctions du délégué)

c Description du fonctionnement de l'établissement, des installations et de l'environnement

d Effectif employé dans le point d'importance vitale (personnel d'exécution, cadres, nombre d'étrangers (Union européenne et hors Union européenne), employés et sous-traitants…)

a.3 Vulnérabilités spécifiques du site

a Vulnérabilités particulières (locales, interdépendances)

b Points névralgiques (vulnérabilités particulières)

a.4 Objectifs de sécurité et stratégie de réponse

a.5 Organisation pour la gestion de crise

a.6 Responsables de la protection du site

b. <u>Analyse de l'efficacité des dispositifs de sûreté en place</u>

Pour chacun des items ci-dessous un commentaire qualitatif apprécie :

- la réalité des dispositifs en place par rapport à ceux prévus par le plan particulier de protection ;
- et l'efficacité des dispositifs en place par rapport aux contraintes géographiques et d'exploitation du point d'importance vitale. Zonages, clôtures et obstacles retardateurs

b.1 Protection des bâtiments, des accès, des parkings

b.2 Contrôle des entrées et des sorties de personnes et de véhicules (employés, sous-traitants, clients, fournisseurs)[6]

b.3 Dispositifs de détection d'intrusion

b.4 Éclairage

b.5 Énergie

b.6 PC de sécurité

b.7 Systèmes d'information, y compris télécommunications

b.8 Protection des systèmes de sécurité

b.9 Autres (capteurs physiques ou logiques, détecteurs de signaux faibles, mécanismes de mise en sûreté, etc.)

c. <u>Analyse de l'efficacité des systèmes d'alerte</u>

Pour chacun des items ci-dessous un commentaire qualitatif apprécie :

- la réalité des systèmes en place par rapport à ceux prévus par le plan particulier de protection ;
- et l'efficacité des systèmes en place par rapport aux contraintes géographiques et d'exploitation du point d'importance vitale.

c.1 Systèmes internes à l'opérateur (moyens d'alerte : téléphone, interphone, réseaux spécialisés, sirènes, etc.)

c.2 Systèmes externes à l'opérateur (réseau téléphonique public : préfecture, autorité militaire, brigade de gendarmerie, service de police, pompiers) ; éventuellement liaisons d'alerte spécialisées de la force publique

[6] un dispositif particulier de contrôle est mis en place pour les sites relevant de la directive nationale de sécurité des activités militaires de l'Etat.

d. <u>Analyse de l'efficacité des dispositions concernant le personnel et des consignes de sécurité</u>

Pour chacun des items ci-dessous un commentaire qualitatif apprécie :

- la réalité des dispositions et des consignes en place par rapport à celles prévues par le plan particulier de protection ;
- et l'efficacité des dispositions et des consignes en place par rapport aux contraintes géographiques et d'exploitation du point d'importance vitale.

d.1 Sensibilisation du personnel de l'établissement et des tiers (clients, fournisseurs…)

d.2 Procédures de recrutement et d'accès des personnes

d.3 Habilitation du personnel

d.4 Relations avec les sous-traitants

d.5 Équipes de protection et de gardiennage

a Personnel : effectif, provenance, formation

b Organisation du gardiennage, postes tenus, rondes, moyens complémentaires

d.6 Systèmes d'astreinte et de permanence

d.7 Consignes en cas d'alerte

d.8 Rôle éventuel du personnel des autres branches de la sécurité

d.9 Consignes pour les tests et les contrôles périodiques du matériel et du personnel de protection

e. <u>Analyse qualitative des mesures de renforcement de la protection incombant au responsable du point d'importance vitale en cas de crise</u>

Pour chacun des items ci-dessous un commentaire qualitatif apprécie :

- la réalité de la préparation au renforcement de la protection au regard du dispositif prévu au chapitre 6 du plan particulier de protection ;
- et l'adaptation de ces mesures de renforcement compte tenu des contraintes géographiques et d'exploitation du point d'importance vitale.

e.1 Dispositions matérielles (renforcement du PC de sécurité)

e.2 Dispositions intéressant le personnel et renforcement du gardiennage

e.3 Modification des consignes

e.4 Modalités d'assistance à l'intervention éventuelle de la force publique

f. <u>Analyse qualitative des plans d'intervention en cas d'alerte</u>

Un commentaire qualitatif apprécie la bonne tenue à jour des plans d'intervention en cas d'alerte compte tenu des éventuelles modifications d'exploitation du point d'importance vitale ou de facteurs extérieurs dont l'opérateur d'importance vitale aurait eu connaissance.

g. Analyse qualitative de la gestion de la sécurité

Pour chacun des items ci-dessous un commentaire qualitatif apprécie :

- l'application des principes de gestion de la sécurité au regard des éléments contenus dans le chapitre 8 du plan particulier de protection ;
- et l'efficacité de ces principes compte tenu des contraintes d'exploitation du point d'importance vitale.

g.1 Principes d'organisation

g.2 Audits

g.3 Entraînement et exercices

g.4 Formation

g.5 Principes de révision des procédures

g.6 Prescriptions de sécurité dues aux concertations avec d'autres opérateurs impliqués du fait d'une interdépendance

g.7 Prescriptions de sécurité à l'égard des sous-traitants et des fournisseurs (une attention particulière sera portée aux modalités de délégation d'activités)

h. Analyse qualitative de la déclinaison du plan particulier de protection

Un commentaire qualitatif apprécie la pertinence des consignes mises en place et diffusées compte tenu des contraintes d'exploitation du point d'importance vitale.

i. Conclusions

i.1 Appréciation générale de la vulnérabilité du point d'importance vitale et du niveau de protection

i.2 Appréciation de l'opportunité de la désignation comme point d'importance vitale

i.3 Actions correctrices à mesures et suites à donner.

Pièce jointe : Participants à la visite de la commission zonale de défense et de sécurité des secteurs d'activités d'importance vitale

- Membres permanents
- Membres associés
- Autres participants

Annexe 8

Informations à transmettre pour
la mise à jour de la base de données DIVA

Ces informations sont transmises par le préfet de département ou le préfet de département coordonnateur, par l'intermédiaire du préfet de zone de défense :

- au service du haut fonctionnaire de défense du ministère de l'intérieur, au titre de sa mission d'animation territoriale,
- au secrétariat général de la défense et de la sécurité nationale qui tient à jour la base de donnée DIVA relative aux points d'importance vitale.

Ces données sont transmises dès notification de l'approbation du plan particulier de protection puis, dans les meilleurs délais, dès qu'une modification de ces données intervient.

Informations concernant un point d'importance vitale

Dénomination du point d'importance vitale

a. Opérateur d'importance vitale concerné
b. Numéro de triplet attribué (9 chiffres) au PIV
c. Localisation : adresse postale, coordonnées géographiques (latitude/longitude)
d. Numéros de téléphone du PIV
e. Identité, coordonnées téléphoniques et courrier électronique délégué pour la défense et la sécurité du PIV
f. Identification et coordonnées des forces de l'ordre compétentes (police nationale ou gendarmerie) dans la zone d'implantation du PIV
g. Classement éventuel selon d'autres réglementations : ERR, ICPE, INB, ISPS, etc.
h. Référence de la notification d'approbation du PPP (sauf secteur AME)
i. Référence du PPE

Informations concernant une zone d'importance vitale

Dénomination de la zone d'importance vitale

a. Liste des points d'importance vitale constituant la zone / suivi du nom de l'OIV
b. Numéro de triplet de chacun des PIV constituant la ZIV
c. Numéro de triplet attribué (9 chiffres) à la ZIV
d. Localisation de la ZIV
e. Préfet de département ou préfet de département coordonnateur désigné
f. Identification et coordonnées des forces de l'ordre compétentes (police nationale ou gendarmerie) dans la zone d'implantation de la ZIV
g. Référence de la notification d'approbation du PPP de la ZIV

Annexe 9

Modèle de formulaire de demande d'avis adressée par l'OIV à l'autorité administrative avant l'accès d'une personne à un PIV

DEMANDE DE CRIBLAGE

(IGI n°6600 du 7 janvier 2014)

Données relatives à l'opérateur et au PIV :

- Année / numéro d'ordre de la demande :

- Numéro de triplet :

Données relatives à la personne :

- Nom et prénom :

- Date et lieu de naissance :

- Domicile actuel :

- Nom de l'employeur (si différent du demandeur) :

- Profession ou fonction :

Données relatives à l'accès au site :

- Désignation de la partie du PIV concernée :

- Justification de la nécessité de l'accès à la partie du PIV concernée :

- Justification de l'impossibilité de mettre en place des mesures de prévention autres :

- Durée prévue de l'accès au site :

- Numéro d'immatriculation du véhicule :

A . . . . . , le . . . . . .

Nom, qualité, signature de l'autorité compétente et cachet de l'organisme

Annexe 10

Modèle de formulaire d'information de la personne concernée par l'enquête administrative

Nom de l'opérateur
Raison sociale
Adresse

Objet : sécurisation de l'accès au site (*dénomination*) sis à (*adresse*/*commune*).

Madame, Monsieur,

Dans le cadre de …(1), vous allez être amené à accéder à un/des site(s) relevant de la responsabilité de notre société. Afin de sécuriser l'accès à ce(s) site(s), et conformément aux dispositions législatives et réglementaires du code de la défense (article L1332-2-1 et les articles R1332-22-1 et suivants), nous avons sollicité préalablement l'avis de l'autorité administrative. Dans ce cadre, une enquête administrative destinée à vérifier qu'aucun fait vous concernant n'est incompatible avec l'accès envisagé est susceptible d'être réalisée par l'autorité administrative.

(1) à compléter selon la raison de l'accès au site : activités professionnelles, stage de longue durée, visite sollicitée par la personne…

A . . . . . , le . . . . . .
Nom, qualité, signature de l'autorité compétente
et cachet de l'organisme

Annexe 11

Modèle de formulaire de rejet de demande d'accès à un PIV
en cas de demande non recevable

Par courriel en date du date du JJ/MM/AA, vous sollicitez l'avis de la préfecture quant à l'accès de M./Mme/MM…… à un site relevant de votre responsabilité.
J'ai le regret de vous informer que la demande que vous avez formulée ne répond pas aux conditions permettant de diligenter une enquête administrative en vue de sécuriser l'accès à ce site. Ces conditions sont explicitées au paragraphe « encadrement des possibilités de demandes d'avis » du chapitre « modalités de contrôle des personnes accédant à un PIV ».

Annexe 12

Modèle de formulaire de réponse de la préfecture à l'OIV

Par courriel en date du date du JJ/MM/AA, vous sollicitez l'avis du préfet de/du……. quant à l'accès de M./Mme/MM…… à un site relevant de votre responsabilité.

Votre demande reçoit un avis favorable / défavorable.

L'enquête administrative diligentée a/n'a pas permis de vérifier que les caractéristiques de la personne physique ou morale intéressée ne sont pas incompatibles avec l'accès envisagé.