

FR

FR

FR



COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 27.10.2008
COM(2008) 676 final

2008/0200 (CNS)

Proposition de

DÉCISION DU CONSEIL

relative au réseau d'alerte concernant les infrastructures critiques (CIWIN)

{SEC(2008)2701}
{SEC(2008)2702}

(présentée par la Commission)

EXPOSÉ DES MOTIFS

CONTEXTE DE LA PROPOSITION

Motivation et objectifs de la proposition

Le Conseil européen de juin 2004 avait invité la Commission à élaborer une stratégie globale aux fins de la protection des infrastructures critiques. Le 20 octobre 2004, la Commission avait ainsi adopté une communication intitulée «Protection des infrastructures critiques dans le cadre de la lutte contre le terrorisme», dans laquelle elle proposait des mesures en vue de renforcer la prévention, la préparation et la réponse de l'Union européenne face aux attaques terroristes contre des infrastructures critiques. Dans ses conclusions relatives à la prévention, la préparation et la réaction en cas d'attentats terroristes et dans son «Programme de solidarité de l'UE face aux conséquences des menaces et des attentats terroristes», adopté en décembre 2004, le Conseil se félicitait du projet de la Commission de proposer un programme européen de protection des infrastructures critiques (EPCIP) et approuvait la création par celle-ci d'un réseau d'alerte concernant les infrastructures critiques (CIWIN).

En décembre 2006, la Commission a proposé une directive du Conseil concernant le recensement et le classement des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Parallèlement, elle a adopté une communication relative à l'EPCIP. Ces deux documents ont ainsi créé le cadre de la protection des infrastructures dans l'Union. La communication présente le cadre horizontal de la protection des infrastructures critiques (PIC) dans l'Union et explique la manière dont l'EPCIP (y compris le CIWIN) pourrait être mis à exécution.

L'initiative CIWIN s'inscrit dans le cadre de l'EPCIP et porte plus précisément sur le processus de partage de l'information entre les États membres et sur le système informatique nécessaire à celui-ci.

Contexte général

La sécurité et l'économie de l'Union européenne, ainsi que le bien-être de nos citoyens, dépendent de certaines infrastructures et des services offerts par celles-ci. Par exemple, les réseaux de télécommunications et de distribution de l'énergie, les services financiers, les réseaux de transport, les services de santé, et l'approvisionnement en eau potable et en denrées alimentaires sont tous essentiels pour l'Union et ses États membres. Toute destruction ou interruption d'une infrastructure fournissant des services-clés, d'une part, et toute réponse inappropriée à ce type d'événement, d'autre part, pourraient entraîner des pertes humaines et matérielles, ainsi qu'une perte de confiance des citoyens européens dans l'UE. La complexité des interdépendances est telle qu'un événement donné peut avoir un effet en cascade sur d'autres secteurs et domaines fondamentaux avec lesquels il n'est pas directement lié à première vue. Comme ce type de relations d'interdépendance n'a pas fait l'objet de recherches suffisamment poussées, la protection des infrastructures critiques et la sécurité des citoyens de l'Union pourraient se révéler insuffisantes.

Les infrastructures critiques de l'Union sont actuellement soumises à une mosaïque de mesures et d'obligations en matière de protection, sans que des normes minimales soient appliquées horizontalement. Certains États membres sont déjà fort avancés dans le processus de recensement de leurs infrastructures critiques, imposent des mesures de protection strictes et ont déjà mis en place toute une série de pratiques et de structures pour assurer leur

protection. D'autres, en revanche, commencent juste à recenser leurs infrastructures critiques et auraient tout intérêt à appliquer les meilleures pratiques telles que la méthode d'évaluation des risques. Ces disparités se situent à deux niveaux, d'une part, au niveau géographique (c'est-à-dire entre les États membres) et, d'autre part, au niveau sectoriel (c'est-à-dire entre les différents secteurs PIC).

L'instauration d'un véritable échange d'informations entre les États membres est une tâche très complexe qui requiert une approche bien réfléchie. Il importe de prévenir les doubles emplois résultant d'un manque d'informations sur des situations comparables dans d'autres États membres: par exemple, la communication d'une bonne pratique établie dans l'un d'eux pourrait épargner à d'autres le coût du développement d'une pratique équivalente.

Par ailleurs, les parties prenantes sont réticentes à échanger des informations sensibles. Dès lors, tout échange efficace d'informations passera par l'instauration d'un climat de confiance et d'une certaine forme de souplesse.

Dispositions en vigueur dans le domaine de la proposition

Il n'existe aucune disposition relative à l'échange d'informations et d'alertes dans le domaine de la protection des infrastructures critiques, alors que la Commission avait proposé dès 2006 une directive concernant le recensement et le classement des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (COM(2006) 787 final). Parallèlement, la Commission avait adopté une communication sur un programme européen de protection des infrastructures critiques (COM(2006) 786 final). En juin 2008, le Conseil est parvenu à un accord politique sur la directive précitée, qui devrait être adoptée au second semestre 2008.

En outre, plusieurs systèmes d'alerte rapide (SAR) sectoriels existent dans l'Union. La principale différence du CIWIN par rapport aux SAR existants réside justement dans son caractère intersectoriel. Aucun des SAR actuels n'offre de fonctionnalité horizontale et intersectorielle qui soit accessible à un éventail d'acteurs (les services et ministères nationaux chargés de la protection des infrastructures critiques, etc.) plus large que les seuls services d'urgence:

- décision du Conseil instituant un mécanisme communautaire de protection civile (refonte) (2007/779/CE, Euratom);
- décision du Conseil concernant des modalités communautaires en vue de l'échange rapide d'informations dans le cas d'une situation d'urgence radiologique, établissant un système d'information communautaire sur les situations d'urgence radiologique (87/600/Euratom);
- directive du Conseil du 21 décembre 1982 concernant la notification des maladies des animaux dans la Communauté (82/894/CEE);
- directive du Conseil concernant les mesures de protection contre l'introduction dans la Communauté d'organismes nuisibles aux végétaux (2000/29/CE);
- décision du Parlement européen et du Conseil instaurant un réseau de surveillance épidémiologique et de contrôle des maladies transmissibles dans la Communauté (2119/98/CE);

- directive du Parlement européen et du Conseil relative à la sécurité générale des produits (2001/95/CE);
- règlement (CE) du Parlement européen et du Conseil établissant les principes généraux et les prescriptions générales de la législation alimentaire, instituant l'Autorité européenne de sécurité des aliments et fixant des procédures relatives à la sécurité des denrées alimentaires (178/2002);
- décision de la Commission concernant le développement d'un système informatique vétérinaire intégré dénommé TRACES (2003/623/CE);
- décision de la Commission modifiant son règlement intérieur (2006/25/CE, Euratom).

Cohérence avec les autres politiques et les objectifs de l'Union

La présente proposition est parfaitement compatible avec les objectifs de l'Union et en particulier avec l'objectif consistant à «maintenir et [à] développer l'Union en tant qu'espace de liberté, de sécurité et de justice au sein duquel est assurée la libre circulation des personnes, en liaison avec des mesures appropriées en matière de contrôle des frontières extérieures, d'asile, d'immigration ainsi que de prévention de la criminalité et de lutte contre ce phénomène».

Elle est également compatible avec les autres politiques puisqu'elle ne vise pas à remplacer les mesures existantes, mais à les compléter afin d'améliorer la protection des infrastructures critiques européennes.

CONSULTATION DES PARTIES INTERESSEES ET ANALYSE D'IMPACT

Consultation des parties intéressées

Méthodes de consultation utilisées, principaux secteurs visés et profil général des répondants

Tous les acteurs concernés ont été consultés au sujet du CIWIN dans le cadre de la consultation sur l'EPCIP. Cette dernière a pris les formes suivantes:

- le Livre vert sur l'EPCIP, adopté le 17 novembre 2005, qui prévoyait une période de consultation jusqu'au 15 janvier 2006 et auquel 22 États membres ont répondu officiellement. Une centaine de représentants du secteur privé ont également présenté des observations. Les réponses ont généralement été favorables à l'idée de la création du CIWIN;
- plusieurs réunions informelles des points de contact PIC nationaux organisées par la Commission (décembre 2005, février 2006, décembre 2006, novembre 2007, février 2008 et mars 2008);
- une étude sur la création d'un réseau d'alerte concernant les infrastructures critiques (CIWIN), achevée en janvier 2008 par un prestataire extérieur: Unisys. Dans le cadre de cette étude, le prestataire a procédé à des entretiens sur le CIWIN dans l'ensemble des 27 États membres;
- des réunions informelles avec des représentants du secteur privé, dont un grand nombre avec des représentants d'entreprises privées ainsi qu'avec des associations professionnelles.

Synthèse des réponses reçues et de la façon dont elles ont été prises en compte

Si le Livre vert sur l'EPCIP avait une portée plus large et consultait les acteurs sur de nombreux aspects de ce programme (par exemple, ses objectifs et principes-clés, ses étapes de mise en œuvre, etc.), une de ses parties était consacrée au CIWIN.

Les réponses à ce livre vert et les discussions régulières avec l'ensemble des acteurs ont eu un impact majeur sur l'élaboration de la proposition relative au CIWIN. Au départ, les États membres ne s'accordaient pas sur le type de réseau d'alerte à mettre en place. Certains souhaitaient un système de communication/d'alerte à plusieurs niveaux assurant deux fonctions distinctes: un système d'alerte rapide et un forum électronique destiné à l'échange d'idées et des meilleures pratiques en matière de protection des infrastructures critiques, tandis que d'autres préféraient limiter le CIWIN à sa fonction de forum ou bien à un SAR reliant les États membres à la Commission. À l'époque de la consultation, deux États membres étaient même opposés à l'idée d'un tel réseau d'alerte. Compte tenu de ces divergences de vues, cette question a été abordée lors des réunions régulières des points de contact PIC avec les États membres. Le projet de CIWIN qui a finalement été retenu est le fruit de ces discussions.

Obtention et utilisation d'expertise

Domaines scientifiques/d'expertise concernés

L'expertise de spécialistes a pu être obtenue lors d'un grand nombre de réunions et de séminaires qui se sont tenus en 2006, 2007 et 2008, ainsi que dans le cadre du processus de consultation au sujet du livre vert sur l'EPCIP. La Commission a recueilli des informations auprès de tous les acteurs concernés.

Méthodologie utilisée

En mars 2006, la Commission a attribué un marché qui comprenait une étude de faisabilité du CIWIN, l'objectif étant de recueillir des informations sur les meilleures pratiques en matière de protection des infrastructures critiques et d'interroger des experts nationaux sur les exigences d'un tel réseau, tant pour la fonction de réseau d'échange que pour celle de système d'alerte rapide, compte tenu des infrastructures et réseaux existant aux niveaux national et international.

Un autre objectif était d'établir une plate-forme commune aux fins de l'échange d'informations utiles à la protection des infrastructures critiques.

Principales organisations/principaux experts consultés

Tous les États membres

Résumé des avis reçus et pris en considération

Il n'a été fait mention d'aucun risque potentiellement grave pouvant avoir des conséquences irréversibles.

Moyens utilisés pour mettre les résultats de l'expertise à la disposition du public

Les annexes de l'analyse d'impact

Analyse d'impact

L'accord sur l'adoption d'une proposition distincte pour le CIWIN a déjà été obtenu dans le cadre du paquet EPCIP, à savoir dans la communication de la Commission relative à ce programme. Cinq options ont été examinées dans l'analyse d'impact:

Option 1: Statu quo. Aucune action horizontale ne serait entreprise au niveau européen; il appartiendrait à chaque État membre de prendre des mesures.

Option 2: Cette option (qui exigerait à la fois une révision fonctionnelle des réseaux informatiques existants et une modification de leur base juridique) envisage le CIWIN comme une mise à niveau des SAR existants. Son rôle consisterait à assurer l'interopérabilité de ces derniers, en les rendant accessibles aux différents services, dans l'Union et dans les ministères nationaux. Puisque celui-ci ne remplirait qu'une fonction d'alerte rapide, toute modification en vue d'ajouter une plate-forme destinée à l'échange d'informations et des meilleures pratiques nécessiterait de procéder à une révision majeure des SAR existants et, partant, d'y consacrer des ressources importantes.

Option 3: Cette option envisage le CIWIN comme une plate-forme ouverte destinée à l'échange (non sécurisé) d'informations relatives à la protection des installations critiques. Elle exigerait un outil informatique qui soit accessible au public et qui fonctionne comme un site internet classique. Un tel outil permettrait certainement de sensibiliser le public à la protection des infrastructures critiques en Europe et d'accroître les échanges directs d'informations entre les acteurs concernés. Cependant, comme le propriétaire de toute information chargée dans le système ne connaîtrait pas l'identité de l'utilisateur final, le volume des chargements serait très limité.

Option 4: Cette option envisage le CIWIN comme un réseau sécurisé de communication/d'alerte à plusieurs niveaux, facultatif et assurant deux fonctions distinctes: un système d'alerte rapide et un forum électronique destiné à l'échange d'idées et des meilleures pratiques en matière de protection des infrastructures critiques. Le CIWIN prendrait la forme d'un outil informatique capable de contenir et de transmettre des informations sensibles, classées jusqu'au niveau «UE RESTREINT». Ce réseau aurait deux fonctions principales: 1) celle d'un forum sécurisé destiné à l'échange d'informations, priorité étant donnée à l'échange des meilleures pratiques, au dialogue et à l'instauration d'un climat de confiance au niveau de l'Union; 2) celle d'un système d'alerte rapide pour les infrastructures critiques. Les États membres auraient la faculté d'utiliser l'ensemble du système, l'une ou l'autre fonction, ou bien aucune.

Option 5: Cette option envisage le CIWIN comme un réseau de communication/d'alerte à plusieurs niveaux, de caractère obligatoire et assurant deux fonctions distinctes: un système d'alerte rapide et un forum électronique destiné à l'échange d'idées et des meilleures pratiques en matière de protection des infrastructures critiques. Le CIWIN serait un réseau obligatoire, chaque État membre étant obligé de charger et de mettre à jour régulièrement les informations pertinentes.

La Commission a réalisé l'analyse d'impact prévue dans le programme de travail. L'option 4, qui envisage le CIWIN comme un réseau sécurisé de communication/d'alerte à plusieurs niveaux, facultatif et assurant deux fonctions distinctes: un système d'alerte rapide et un forum électronique destiné à l'échange d'idées et des meilleures pratiques en matière de protection des infrastructures critiques, présente clairement le meilleur rapport

avantages/inconvénients. Dans ce scénario, le CIWIN offrirait un environnement sécurisé pour l'échange d'informations, contribuerait grandement à l'instauration d'un climat de confiance entre les acteurs concernés et permettrait l'échange d'alertes.

L'analyse d'impact du CIWIN figure en annexe à la présente proposition.

ÉLÉMENTS JURIDIQUES DE LA PROPOSITION

Résumé des mesures proposées

Les mesures proposées ont pour objet d'assister les États membres dans l'échange d'informations sur les menaces et les vulnérabilités qui leur sont communes, ainsi que sur les mesures et les stratégies de nature à limiter les risques pour protéger les infrastructures critiques.

Base juridique

L'article 308 du traité instituant la Communauté européenne et l'article 203 du traité instituant la Communauté européenne de l'énergie atomique constituent la base juridique de la proposition.

Principe de subsidiarité

Le principe de subsidiarité s'applique, dans la mesure où la proposition ne relève pas de la compétence exclusive de la Communauté.

Les objectifs de la proposition ne peuvent être réalisés d'une manière suffisante par les États membres pour la ou les raisons suivantes.

Le principe de subsidiarité est respecté puisque les mesures envisagées par la présente proposition ne peuvent être réalisées par un seul État membre de l'Union et doivent donc être réalisées au niveau européen.

Bien qu'il appartienne à chaque État membre de protéger les infrastructures critiques qui sont dans son ressort, il est évident qu'une plate-forme d'échange d'informations transfrontalière et couvrant toute l'Union, garantissant que les informations soient disponibles pour tous les États membres qui pourraient en avoir besoin, ne peut être réalisée qu'au niveau européen.

L'action communautaire permettra de mieux réaliser les objectifs de la proposition pour la ou les raisons suivantes.

Aucun État membre isolé ne peut assurer un échange paneuropéen d'informations ou l'échange d'alertes rapides. Il est donc manifeste qu'une action au niveau européen apporte en plus la coordination d'éléments d'information éventuellement déjà disponibles mais non partagés avec les autres.

Seule une approche européenne assurera une égalité de traitement entre les États membres qui souhaitent partager et recevoir des informations, une coopération qui ne crée pas de discrimination géographique entre eux et la bonne transmission des informations à ceux qui souhaitent les recevoir.

Il existe un lien direct entre coopération interdisciplinaire européenne, d'une part, et sûreté nationale et sécurité intérieure, d'autre part. Du fait des interdépendances sectorielles et transfrontalières actuelles, des États membres sont susceptibles d'offrir des services à d'autres États membres ou d'avoir une incidence sur la fourniture de services dans d'autres États membres. Le fait qu'un État membre n'ait pas suffisamment protégé les infrastructures se trouvant sur son territoire pourrait ainsi avoir des répercussions sur un autre État membre.

Les infrastructures de dimension européenne étant de plus en plus nombreuses, une approche purement nationale est insuffisante. Il est donc indispensable de prendre des mesures pour faire face au large éventail de menaces qui pèsent sur les infrastructures critiques de l'Europe.

Par conséquent, la proposition est conforme au principe de subsidiarité.

Principe de proportionnalité

La proposition respecte le principe de proportionnalité pour la ou les raisons suivantes.

La présente proposition ne va pas au-delà de ce qui est nécessaire pour réaliser les objectifs de coopération des États membres dans ce domaine, d'autant plus que ces derniers sont disposés à participer. Du reste, les mesures proposées permettent aux États membres ne souhaitant pas participer au CIWIN de ne pas l'utiliser.

Par rapport aux avantages qui en découleront, le CIWIN n'aura pas d'incidence financière directe notable, que ce soit sur les budgets nationaux ou le budget de l'Union. À titre d'exemple, les coûts de maintenance devraient s'élever à quelque 550 000 EUR par an, alors que le coût des incidents que le CIWIN pourrait potentiellement prévenir ou dont il pourrait réduire les effets est bien supérieur.

Choix des instruments

Instrument proposé: décision du Conseil.

D'autres moyens ne seraient pas appropriés pour la ou les raisons suivantes:

Le prototype du CIWIN ne peut devenir pleinement opérationnel et disponible dans tous les États membres, sans une base juridique. Étant donné que l'objet de la présente proposition est spécifique et non de portée générale, une décision du Conseil constitue l'instrument juridique le plus approprié pour réaliser cet objectif et obliger, parallèlement, les utilisateurs du système (États membres et Commission) à respecter la nature éventuellement confidentielle des informations échangées.

INCIDENCE BUDGETAIRE

L'incidence budgétaire est estimée dans la fiche financière ci-jointe. Le programme «Prévention, préparation et gestion des conséquences en matière de terrorisme et d'autres risques liés à la sécurité» pour la période 2007-2013 interviendra dans la mise en œuvre de la présente décision.

INFORMATIONS SUPPLEMENTAIRES

Simulation, phase-pilote et période de transition

La proposition a fait ou fera l'objet d'une simulation ou d'une phase-pilote.

Réexamen / révision / clause de suppression automatique

La proposition contient une clause de réexamen.

La proposition contient une clause de révision.

Proposition de

DÉCISION DU CONSEIL

relative au réseau d'alerte concernant les infrastructures critiques (CIWIN)

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité instituant la Communauté européenne, et notamment son article 308,

vu le traité instituant la Communauté européenne de l'énergie atomique, et notamment son article 203,

vu la proposition de la Commission¹,

vu l'avis du Parlement européen²,

considérant ce qui suit:

- (1) Dans ses conclusions relatives à la prévention, la préparation et la réaction en cas d'attentats terroristes et dans son «Programme de solidarité de l'UE face aux conséquences des menaces et des attentats terroristes», adopté en décembre 2004, le Conseil s'était félicité de l'intention de la Commission de proposer un programme européen de protection des infrastructures critiques et avait approuvé la création par celle-ci d'un réseau d'alerte concernant les infrastructures critiques (CIWIN)³.
- (2) En novembre 2005, la Commission a adopté un livre vert sur le programme européen de protection des infrastructures critiques (EPCIP), présentant différentes options pour la mise en place de ce programme et du CIWIN. Les résultats de la consultation consécutive au livre vert ont confirmé l'intérêt de la majorité des États membres pour la création du CIWIN.
- (3) En décembre 2006, la Commission a adopté une communication relative à l'EPCIP⁴ qui annonçait que le CIWIN ferait l'objet d'une proposition distincte de sa part et fournirait une plate-forme pour l'échange sécurisé des meilleures pratiques.
- (4) Plusieurs incidents ayant touché des infrastructures critiques en Europe, tels que par exemple la «panne d'électricité européenne» de 2006, ont démontré qu'un meilleur échange d'informations, plus efficace, était nécessaire pour prévenir ce type d'incidents ou en limiter la portée.

¹ JO C [...] du [...], p. [...].

² JO C [...] du [...], p. [...].

³ 14894/04.

⁴ COM(2006) 786 final.

- (5) Il convient de mettre en place un système d'information permettant aux États membres et à la Commission d'échanger des informations et des alertes dans le domaine de la protection des infrastructures critiques (PIC) et de renforcer leur dialogue à ce sujet, tout en favorisant l'intégration et une meilleure coordination des différents programmes de recherche PIC nationaux, qui demeurent très cloisonnés.
- (6) Le CIWIN devrait, d'une part, contribuer à l'amélioration de la protection des infrastructures critiques dans l'Union, en fournissant un système d'information de nature à faciliter la coopération entre les États membres et, d'autre part, offrir une alternative efficace et rapide aux méthodes chronophages de recherche d'informations sur les infrastructures critiques dans la Communauté.
- (7) Il devrait, notamment, accélérer la définition de mesures appropriées visant à faciliter l'échange sécurisé des meilleures pratiques, et servir de moyen de transmission des alertes et des informations sur des menaces immédiates.
- (8) Le CIWIN devrait éviter les doubles emplois et tenir compte des caractéristiques, de l'expertise, des modalités de fonctionnement et des domaines de compétence propres à chacun des systèmes d'alerte rapide (SAR) sectoriels existants.
- (9) Au fil des années, la Commission a développé une capacité opérationnelle d'intervention dans toute une série de situations d'urgence, grâce à différents SAR sectoriels, réservés aux services spécialisés de l'Union. Les SAR existants ne comportent toutefois pas de fonction PIC accessible à d'autres acteurs en dehors des autorités sectorielles ou des services d'urgence.
- (10) Eu égard à l'interdépendance des infrastructures critiques et au niveau variable de leur protection dans les États membres, la création d'un instrument communautaire horizontal et intersectoriel destiné à l'échange d'informations et d'alertes dans le domaine de la PIC renforcerait la sécurité des citoyens.
- (11) Compte tenu de la future mise en service du réseau de communication «Services télématiques transeuropéens entre administrations (s-TESTA)» ou d'un autre réseau sécurisé exploité par la Commission, cette dernière devrait opter pour la plate-forme technologique la plus appropriée au CIWIN et obliger les utilisateurs finals à se conformer aux exigences techniques qu'elle aura établies.
- (12) Le partage d'informations concernant la PIC entre les acteurs concernés requiert une relation de confiance, de sorte que les renseignements confidentiels ou sensibles qui ont été volontairement partagés ne soient pas divulgués et que ces données sensibles bénéficient d'une protection adéquate.
- (13) L'accès au CIWIN devrait être réservé aux utilisateurs autorisés conformément aux modalités, procédures et mesures de sécurité établies: dans les États membres, il serait ainsi réservé aux autorités nationales compétentes, tandis qu'au sein de la Commission, il serait réservé aux services compétents.
- (14) Les coûts liés à l'exploitation du CIWIN au niveau de la Communauté devraient être couverts par des ressources communautaires et/ou par les programmes communautaires correspondants.

- (15) Les coûts liés à l'exploitation du CIWIN au niveau national devraient, sauf modalités communautaires contraires, être à la charge des États membres eux-mêmes.
- (16) Les objectifs de l'action envisagée, à savoir un échange d'informations sécurisé et rapide entre les États membres, ne pouvant pas être réalisés de manière suffisante par les États membres et pouvant donc, en raison des effets de l'action envisagée, être mieux réalisés au niveau communautaire, la Communauté peut adopter des mesures en vertu du principe de subsidiarité énoncé à l'article 5 du traité. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente décision n'excède pas ce qui est nécessaire pour atteindre ces objectifs.
- (17) La présente décision respecte les droits fondamentaux et observe les principes reconnus, en particulier, par la Charte des droits fondamentaux de l'Union européenne,

A ARRÊTÉ LA PRÉSENTE DÉCISION:

Article premier
Objet

La présente décision porte création d'un système sécurisé d'information, de communication et d'alerte, le réseau d'alerte concernant les infrastructures critiques (CIWIN), en vue d'assister les États membres dans l'échange d'informations sur les menaces et les vulnérabilités qui leur sont communes, ainsi que sur les mesures et les stratégies de nature à limiter les risques liés à la protection des infrastructures critiques.

Article 2
Définitions

Aux fins de la présente décision, on entend par:

«infrastructures critiques»: les éléments, les systèmes ou parties de ceux-ci, situés dans les États membres, qui sont indispensables au maintien des fonctions sociétales vitales, de la santé, de la sécurité et du bien-être économique et social des citoyens, et dont l'arrêt ou la destruction aurait une incidence importante dans un État membre s'il l'on ne parvenait pas à maintenir ces fonctions;

«États membres participants»: les États membres qui ont signé un protocole d'accord avec la Commission;

«responsable CIWIN»: le point de contact CIWIN de l'État membre concerné ou de la Commission qui veille à la bonne utilisation du réseau et au respect des consignes d'utilisation dans cet État membre ou au sein de la Commission;

«menace»: toute information, toute circonstance ou tout événement pouvant potentiellement provoquer l'arrêt ou la destruction d'une infrastructure critique, ou d'un de ses éléments.

Article 3
Participation

La participation au CIWIN et son utilisation sont ouvertes à tous les États membres. La participation au CIWIN est subordonnée à la signature d'un protocole d'accord spécifiant les exigences techniques et en matière de sécurité applicables au réseau, et contenant des informations sur les sites qui lui seront raccordés.

Article 4
Fonctions

- (1) Le CIWIN remplit les deux fonctions suivantes:
 - (a) un forum électronique pour l'échange d'informations concernant la protection des infrastructures critiques;
 - (b) un système d'alerte rapide permettant aux États membres participants et à la Commission de signaler les menaces et risques immédiats pesant sur les infrastructures critiques.
- (2) Le forum électronique se compose d'espaces fixes et d'espaces dynamiques.

Les espaces fixes sont présents dans le système en permanence. Si leur contenu peut être adapté, ces espaces ne peuvent être supprimés, renommés ou ajoutés. L'annexe I contient la liste des espaces fixes.

Les espaces dynamiques sont créés à la demande et répondent à un objectif précis. Ils sont supprimés une fois leur objectif initial rempli. L'annexe II contient la liste des espaces dynamiques à créer lors de la mise en place du CIWIN.

Article 5
Rôle des États membres

- (1) Les États membres participants désignent un responsable CIWIN et en informe la Commission. Le responsable CIWIN signe le protocole d'accord et gère les droits d'accès au réseau dans l'État membre concerné.
- (2) Les États membres participants fournissent l'accès au CIWIN conformément aux consignes adoptées par la Commission.
- (3) Les États membres participants fournissent des informations d'intérêt communautaire sur la protection des infrastructures critiques et les mettent régulièrement à jour.

Article 6
Rôle de la Commission

- (1) La Commission est chargée:
 - (a) du développement et de la gestion techniques du CIWIN, y compris la structure informatique de celui-ci et les éléments nécessaires à l'échange d'informations;

- (b) de l'établissement de consignes fixant les conditions d'utilisation du réseau, notamment la confidentialité, la transmission, le stockage, le classement et la suppression des informations. La Commission fixe également les conditions et modalités d'octroi d'un accès illimité ou restreint au CIWIN.
- (2) La Commission désigne le responsable CIWIN qui est chargé de la gestion des droits d'accès au réseau au sein de la Commission.
- (3) La Commission fournit des informations d'intérêt communautaire sur la protection des infrastructures critiques et les met régulièrement à jour.

Article 7 *Sécurité*

- (1) Le CIWIN étant un réseau sécurisé, il peut traiter des informations jusqu'au niveau «RESTREINT UE».

La Commission opte pour la plate-forme technologique la plus appropriée au CIWIN, et les utilisateurs se conforment aux exigences techniques établies par la Commission.

La classification de sécurité du CIWIN est mise à niveau en fonction des besoins.

- (2) Les droits d'accès aux documents sont accordés en fonction du «besoin d'en connaître» des utilisateurs et doivent à tout moment respecter les instructions précises de l'auteur en ce qui concerne la protection et la diffusion du document.
- (3) Les États membres et la Commission prennent les mesures de sécurité nécessaires pour:
 - (a) empêcher toute personne non autorisée d'accéder au CIWIN;
 - (b) garantir que les personnes autorisées aient accès aux seules données relevant de leur compétence lorsqu'elles utilisent le CIWIN;
 - (c) empêcher que des informations stockées sur le réseau ne soient lues, copiées, modifiées ou effacées par des personnes non autorisées.
- (4) Le chargement d'informations sur le CIWIN n'affecte pas la propriété des informations concernées. Les utilisateurs autorisés sont uniquement responsables des informations qu'ils fournissent et doivent s'assurer que leur contenu est parfaitement conforme au droit national et communautaire en vigueur.

Article 8 *Consignes d'utilisation*

La Commission élabore des consignes d'utilisation contenant toutes les informations utiles sur les fonctions et rôles du CIWIN, et les met régulièrement à jour.

Article 9
Coûts

Les coûts liés à l'exploitation, à la maintenance et au fonctionnement central du CIWIN sont à la charge du budget communautaire. Les coûts liés à l'accès des utilisateurs au CIWIN dans les États membres sont à la charge des États membres participants.

Article 10
Réexamen

La Commission réexamine et évalue le fonctionnement du CIWIN tous les trois ans, et présente des rapports réguliers aux États membres.

Le premier rapport, qui est soumis dans les trois ans suivant l'entrée en vigueur de la présente décision, indique notamment les éléments du réseau communautaire qui doivent être améliorés ou adaptés. Il contient également toute proposition de modification ou d'adaptation de la présente décision jugée nécessaire par la Commission.

Article 11
Date d'application

La présente décision est applicable à partir du 1^{er} janvier 2009.

Article 12
Destinataires

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles,

Par le Conseil
Le Président

ANNEXE I

ESPACES FIXES DU CIWIN

Les espaces fixes visés à l'article 4 sont les suivants:

- (1) les espaces «États membres», offrant à chaque État membre participant la possibilité de créer son propre espace sur le portail CIWIN. L'organisation, l'administration et le contenu de cet espace relèvent de la responsabilité exclusive des États membres. L'espace est réservé aux utilisateurs de l'État membre concerné;
- (2) les espaces sectoriels, correspondant à 11 secteurs distincts: industrie chimique; énergie; finances; produits alimentaires; santé; TIC; industrie du cycle du combustible nucléaire; installations de recherche; espace; transports; et eau. Un sous-espace intersectoriel pour les thèmes génériques et les questions intéressant plusieurs secteurs est également prévu;
- (3) l'espace «responsables CIWIN», servant de plate-forme stratégique de coordination et de coopération destinée à favoriser et intensifier les travaux et les communications concernant la protection des infrastructures critiques. Cet espace est réservé aux responsables CIWIN;
- (4) l'espace «coopération extérieure de l'Union», axé sur la sensibilisation à la coopération extérieure en matière de protection des infrastructures critiques et sur la sensibilisation aux normes de protection des infrastructures critiques en dehors de l'Union;
- (5) le répertoire de contacts, destiné à faciliter la recherche des coordonnées des autres utilisateurs du CIWIN ou des experts en protection des infrastructures critiques.

ANNEXE II

ESPACES DYNAMIQUES DU CIWIN

Les espaces dynamiques visés à l'article 4 sont les suivants:

- (1) l'espace «groupes d'experts», destiné à l'appui des travaux des groupes d'experts en PIC;
- (2) l'espace «projets», contenant des informations sur les projets financés par la Commission;
- (3) les espaces «alerte», qui peuvent être créés en cas d'alerte donnée dans le SAR et qui constitueront le canal de communication pendant les activités liées à la PIC;
- (4) l'espace «thèmes particuliers», réservé à des thèmes spécifiques.

FICHE FINANCIÈRE LÉGISLATIVE

1. DÉNOMINATION DE LA PROPOSITION:

Décision du Conseil relative au réseau d'alerte concernant les infrastructures critiques (CIWIN)

2. CADRE GPA / EBA (GESTION PAR ACTIVITE/ETABLISSEMENT DU BUDGET PAR ACTIVITE)

Activité 18.05: Sécurité et protection des libertés

Objectif 2: Protection des infrastructures critiques

3. LIGNES BUDGÉTAIRES

3.1. Lignes budgétaires [lignes opérationnelles et lignes connexes d'assistance technique et administrative (anciennes lignes BA)], y compris leurs intitulés:

Ligne budgétaire: 18.050800

Intitulé: Prévention, préparation et gestion des conséquences en matière de terrorisme

3.2. Durée de l'action et de l'incidence financière:

À partir de 2009

3.3. Caractéristiques budgétaires:

| Ligne budgétaire | Nature de la dépense | | Nouvelle | Participation AELE | Participation pays candidats | Rubrique perspectives financières |
|------------------|----------------------|-------------------|----------|--------------------|------------------------------|-----------------------------------|
| 18.050800 | DNO | Diff ⁵ | NON | NON | NON | 3A |

⁵ Crédits dissociés

4. RÉCAPITULATIF DES RESSOURCES

4.1. Ressources financières

4.1.1. Récapitulatif des crédits d'engagement (CE) et des crédits de paiement (CP)

en millions d'euros (à la 3^e décimale)

| Nature de la dépense | Section n° | | 2009 | 2010 | 2011 | 2012 | 2013 | Total |
|----------------------|------------|--|------|------|------|------|------|-------|
|----------------------|------------|--|------|------|------|------|------|-------|

Dépenses opérationnelles⁶

| | | | | | | | | |
|---------------------------|------|---|------|------|------|------|------|------|
| Crédits d'engagement (CE) | 8.1. | a | 0,95 | 0,55 | 0,55 | 0,55 | 0,55 | 3,15 |
| Crédits de paiement (CP) | | b | 0,95 | 0,55 | 0,55 | 0,55 | 0,55 | 3,15 |

Dépenses administratives incluses dans le montant de référence⁷

| | | | | | | | | |
|--|--------|---|----|----|----|----|----|----|
| Assistance technique et administrative – ATA (CND) | 8.2.4. | c | NA | NA | NA | NA | NA | NA |
|--|--------|---|----|----|----|----|----|----|

MONTANT TOTAL DE RÉFÉRENCE

| | | | | | | | | |
|----------------------|--|-----|------|------|------|------|------|------|
| Crédits d'engagement | | a+c | 0,95 | 0,55 | 0,55 | 0,55 | 0,55 | 3,15 |
| Crédits de paiement | | b+c | 0,95 | 0,55 | 0,55 | 0,55 | 0,55 | 3,15 |

Dépenses administratives non incluses dans le montant de référence⁸

| | | | | | | | | |
|--|--------|---|-------|-------|-------|-------|-------|-------|
| Ressources humaines et dépenses connexes (CND) | 8.2.5. | d | 0,117 | 0,117 | 0,117 | 0,117 | 0,117 | 0,585 |
| Frais administratifs autres que les ressources humaines et coûts connexes, hors montant de référence (CND) | 8.2.6. | e | 0,015 | 0,015 | 0,015 | 0,015 | 0,015 | 0,075 |

| | | | | | | | | |
|---|--|-----------------|-------|-------|-------|-------|------|--|
| TOTAL CE, y compris coût des ressources humaines | | a+c +d +e | 1,082 | 0,682 | 0,682 | 0,682 | 3,81 | |
| TOTAL CP, y compris coût des ressources humaines | | b+c +d +e | 1,082 | 0,682 | 0,682 | 0,682 | 3,81 | |

⁶ Dépenses ne relevant pas du chapitre xx 01 du titre xx concerné.

⁷ Dépenses relevant de l'article xx 01 04 du titre xx.

⁸ Dépenses relevant du chapitre xx 01, sauf articles xx 01 04 et xx 01 05.

4.1.2. *Compatibilité avec la programmation financière*

- Proposition compatible avec la programmation financière existante.
- Cette proposition nécessite une reprogrammation de la rubrique concernée des perspectives financières.
- Cette proposition peut nécessiter un recours aux dispositions de l'accord interinstitutionnel⁹ (relatives à l'instrument de flexibilité ou à la révision des perspectives financières).

4.1.3. *Incidence financière sur les recettes*

- Proposition sans incidence financière sur les recettes
- Incidence financière — L'effet sur les recettes est le suivant:

4.2. **Ressources humaines en ETP (y compris fonctionnaires, personnel temporaire et externe) - voir détails au point 8.2.1.**

| Besoins annuels | 2009 | 2010 | 2011 | 2012 | 2013 |
|---------------------|------|------|------|------|------|
| Total des effectifs | 1 | 1 | 1 | 1 | 1 |

5. **CARACTÉRISTIQUES ET OBJECTIFS**

5.1. **Réalisation nécessaire à court ou à long terme**

Le CIWIN a pour objectif spécifique de permettre une coordination et une coopération au niveau de l'Union en matière d'information sur la protection des infrastructures critiques. Il doit surtout assurer un échange d'informations sécurisé et structuré, permettre ainsi à ses utilisateurs d'acquérir rapidement et efficacement les meilleures pratiques appliquées dans les autres États membres et mettre les États membres en mesure d'utiliser le système d'alerte rapide prévu pour la PIC.

5.2. **Valeur ajoutée de l'intervention communautaire, compatibilité de la proposition avec d'autres instruments financiers et synergies éventuelles**

Bien qu'il appartienne à chaque État membre de protéger les infrastructures critiques qui sont dans son ressort, il est évident qu'une plateforme d'échange d'informations transfrontalière et couvrant toute l'Union, garantissant que les informations soient disponibles pour tous les États membres qui pourraient en avoir besoin, ne peut être réalisée qu'au niveau européen. Aucun État membre isolé ne peut assurer un échange paneuropéen d'informations ou l'échange d'alertes rapides. Il est donc manifeste qu'une action au niveau européen apporte en plus la coordination d'éléments d'information éventuellement déjà disponibles mais non partagés avec les autres. Seule une approche européenne assurera une égalité de traitement entre les États membres qui souhaitent partager et recevoir des informations, une coopération

⁹ Voir points 19 et 24 de l'accord interinstitutionnel.

qui ne crée pas de discrimination géographique entre eux et la bonne transmission des informations à ceux qui souhaitent les recevoir.

5.3. Objectifs, résultats escomptés et indicateurs connexes de la proposition dans le contexte de la gestion par activité (GPA)

Le CIWIN a pour objectif spécifique d'accélérer la définition de mesures appropriées visant à faciliter l'échange sécurisé des meilleures pratiques et de servir de moyen de transmission des alertes et des informations sur des menaces immédiates. Le système devrait faire en sorte que les bonnes personnes obtiennent les bonnes informations au bon moment.

La création du CIWIN avait déjà été envisagée dans la communication relative à un programme européen de protection des infrastructures critiques, et le CIWIN en tant qu'outil informatique constitue lui-même un des objectifs opérationnels de ce programme. Néanmoins, le (sous-)objectif opérationnel que poursuit le CIWIN peut être décrit comme suit:

- créer un outil informatique facilitant la coopération PIC entre les États membres, offrant une alternative efficace et rapide aux méthodes souvent chronophages de recherche d'informations et donnant aux États membres la possibilité de communiquer directement et de charger les informations qu'ils jugent utiles.

5.4. Modalités de mise en œuvre (indicatives)

Gestion centralisée

directement par la Commission

indirectement par délégation à:

des agences exécutives

des organismes créés par les Communautés, tels que visés à l'article 185 du règlement financier

des organismes publics nationaux/organismes avec mission de service public

Gestion partagée ou décentralisée

avec des États membres

avec des pays tiers

Gestion conjointe avec des organisations internationales (à préciser)

Remarques:

6. CONTRÔLE ET ÉVALUATION

6.1. Système de contrôle

Il conviendrait d'utiliser les indicateurs de progrès suivants pour mesurer les progrès réalisés par le CIWIN:

- nombre d'États membres participant au CIWIN (au moins 20 États membres devraient l'utiliser régulièrement pour qu'il soit considéré comme un succès);
- degré de confidentialité des informations échangées (les États membres chargent-ils uniquement des informations non classifiées ou également des informations classifiées?);
- les groupes d'experts en PIC se servent-ils du CIWIN comme principal outil d'échange d'avis pour atteindre leurs objectifs (par exemple, définition des critères d'identification des infrastructures critiques dans certains secteurs)?

6.2. Évaluation

6.2.1. Évaluation ex ante

Au terme de la période d'essai (projet-pilote CIWIN) en 2009, la Commission enverra des questionnaires succincts aux autorités des États membres pour évaluer leur satisfaction à l'égard du réseau et vérifier s'il contribue aux objectifs généraux de l'initiative CIWIN (et elle proposera éventuellement d'ajouter de nouvelles fonctions ou de supprimer celles qui ne donnent pas de bons résultats).

Une analyse d'impact a été réalisée et est annexée à la présente proposition.

6.2.2. Mesures prises à la suite d'une évaluation intermédiaire/ex post (enseignements tirés d'expériences antérieures similaires)

Le principal dispositif de contrôle et d'évaluation devrait mettre en avant le principe de «satisfaction du client».

- Le système fonctionnel devrait ensuite être contrôlé par la Commission tous les trois ans. Pour ce faire, la Commission s'appuiera sur les avis des États membres recueillis lors des réunions régulières des points de contact PIC.

6.2.3. Conditions et fréquence des futures évaluations

Le CIWIN sera évalué par rapport aux indicateurs mentionnés au point 6.1., au terme de ses trois premières années d'existence.

7. MESURES ANTIFRAUDE

La protection des intérêts financiers de la Communauté et la lutte contre les fraudes et les irrégularités font partie intégrante de la présente décision.

Le contrôle administratif des contrats et des paiements incombera au service compétent de la Commission. Chaque opération financée au titre de la présente décision sera supervisée à tous les stades du cycle du projet par les services compétents de la Commission. Cette supervision

tiendra compte des obligations contractuelles ainsi que des principes d'analyse coût-efficacité et de saine gestion financière.

En outre, les conventions ou contrats conclus en application de la présente décision prévoiront expressément un contrôle des dépenses autorisées dans le cadre des projets/programmes et de la bonne exécution des activités, ainsi qu'un contrôle financier par la Commission, notamment par l'Office européen de lutte antifraude (OLAF), et par la Cour des comptes, si nécessaire sur place. Ils autoriseront la Commission (OLAF) à effectuer des contrôles et vérifications sur place conformément au règlement (Euratom, CE) n° 2185/96 du Conseil du 11 novembre 1996 relatif aux contrôles et vérifications sur place effectués par la Commission pour la protection des intérêts financiers des Communautés européennes contre les fraudes et autres irrégularités.

Une attention particulière sera accordée à la nature des dépenses (éligibilité), au respect des budgets (effectivité) et aux informations et justificatifs (preuve de la dépense).

8. DÉTAIL DES RESSOURCES

8.1. Objectifs de la proposition en termes de coûts

Crédits d'engagement en millions d'euros (à la 3^e décimale)

| (Indiquer les intitulés des objectifs, des actions et des réalisations) | Type de réalisation | Coût moyen | 2009 | | 2010 | | 2011 | | 2012 | | 2013 | | TOTAL | |
|---|--|------------|----------------------|------------|----------------------|------------|----------------------|------------|----------------------|------------|----------------------|------------|----------------------|------------|
| | | | Nbre de réalisations | Coût total |
| OBJECTIF OPÉRATIONNEL n°1 ¹⁰ créer un outil informatique facilitant la coopération PIC entre les États membres | | | | | | | | | | | | | | |
| Action: créer et gérer un SAR PIC, et créer un forum d'échange des meilleures pratiques | | | | | | | | | | | | | | |
| - Réalisation 1 | Hébergement de la fonction SAR du CIWIN (environnement sécurisé) | 0,3 | 1 | 0,3 | 1 | 0,3 | 1 | 0,3 | 1 | 0,3 | 1 | 0,3 | 5 | 1,5 |

¹⁰ Tel que décrit dans la partie 5.3.

| (Indiquer les intitulés des objectifs, des actions et des réalisations) | Type de réalisation | Coût moyen | 2009 | | 2010 | | 2011 | | 2012 | | 2013 | | TOTAL | |
|---|--|------------|----------------------|------------|----------------------|------------|----------------------|------------|----------------------|------------|----------------------|------------|----------------------|------------|
| | | | Nbre de réalisations | Coût total |
| - Réalisation 2 | Support et maintenance du réseau | 0,25 | 1 | 0,25 | 1 | 0,25 | 1 | 0,25 | 1 | 0,25 | 1 | 0,25 | 5 | 1,25 |
| - Réalisation 3 | Support technique nécessaire à l'accréditation de sécurité, maintenance, fourniture d'un helpdesk et de formations | 0,07 | 1 | 0,4 | | | | | | | | | 1 | 0,4 |
| COÛT TOTAL 1 | | 0,617 | 1 | 0,95 | 1 | 0,55 | 1 | 0,55 | 1 | 0,55 | 1 | 0,55 | 5 | 3,15 |

8.2. Dépenses administratives

8.2.1. Effectifs et types de ressources humaines

| Types d'emplois | | Effectifs à affecter à la gestion de l'action par l'utilisation de ressources existantes et/ou supplémentaires (nombre de postes/ETP) | | | | |
|--|------|--|------|------|------|------|
| | | 2009 | 2010 | 2011 | 2012 | 2013 |
| (18) | (20) | (21) | (22) | (23) | (24) | (25) |
| Fonctionnaires | | | 0 | 0 | 0 | 0 |
| ou agents temporaires ¹¹ | | | 5 | 5 | 5 | 5 |
| (XX 01 01) | AST | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| (19) | | | | | | |
| Personnel financé ¹² au titre de l'art. XX 01 02 | | | | | | |
| Autres effectifs ¹³ financés au titre de l'art. XX 01 04/05 | | | | | | |
| TOTAL | | 1 | 1 | 1 | 1 | 1 |

8.2.2. Description des tâches découlant de l'action

La principale tâche des fonctionnaires de la Commission sera celle d'administrateur CIWIN. Ces fonctionnaires seront donc chargés de configurer la solution, ils géreront les demandes de création d'espaces dynamiques, créeront lesdits espaces et supprimeront les espaces inutilisés ou abandonnés. Le rôle d'administrateur sera réservé à la Commission.

8.2.3. Origine des ressources humaines (statutaires)

- Postes actuellement affectés à la gestion du programme à remplacer ou à prolonger
- Postes préalloués dans le contexte de l'exercice de SPA/APB pour l'année n
- Postes à demander lors de la prochaine procédure de SPA/APB

¹¹ Dont le coût n'est PAS couvert par le montant de référence.

¹² Dont le coût n'est PAS couvert par le montant de référence.

¹³ Dont le coût est inclus dans le montant de référence.

- Postes à redéployer en utilisant les ressources existantes dans le service concerné (redéploiement interne)
- Postes nécessaires pour l'année n, mais non prévus dans l'exercice de SPA/APB de l'année concernée

8.2.4. *Autres dépenses administratives incluses dans le montant de référence (XX 01 04/05 – Dépenses de gestion administrative)*

en millions d'euros (à la 3^e décimale)

| Ligne budgétaire (n° et intitulé) | 2009 | 2010 | 2011 | 2012 | 2013 | TOTAL |
|---|------|------|------|------|------|-------|
| 1 Assistance technique et administrative (comprenant les coûts de personnel afférents) | | | | | | |
| Agences exécutives ¹⁴ | NA | NA | NA | NA | NA | NA |
| Autre assistance technique et administrative | NA | NA | NA | NA | NA | NA |
| - <i>intra muros</i> | | | | | | |
| - <i>extra muros</i> | | | | | | |
| Total assistance technique et administrative | NA | NA | NA | NA | NA | NA |

8.2.5. *Coût des ressources humaines et coûts connexes non inclus dans le montant de référence*

en millions d'euros (à la 3^e décimale)

| Type de ressources humaines | 2009 | 2010 | 2011 | 2012 | 2013 |
|--|-------|-------|-------|-------|-------|
| Fonctionnaires et agents temporaires (XX 01 01) | 0,117 | 0,117 | 0,117 | 0,117 | 0,117 |
| Personnel financé au titre de l'art. XX 01 02 (auxiliaires, END, agents contractuels, etc.) (indiquer la ligne budgétaire) | | | | | |
| Coût total des ressources humaines et coûts connexes (NON inclus dans le montant de référence) | 0,117 | 0,117 | 0,117 | 0,117 | 0,117 |

Calcul – *Fonctionnaires et agents temporaires*

¹⁴ Il convient de mentionner la fiche financière législative se rapportant spécifiquement à l'agence/aux agences exécutive(s) concernée(s).

Voir au point 8.2.1.

Calcul - *Personnel financé au titre de l'article XX 01 02*

NA

| | 2009 | 2010 | 2011 | 2012 | 2013 | TOTAL |
|--|-------|-------|-------|-------|-------|-------|
| XX 01 02 11 01 — Missions | 0,01 | 0,01 | 0,01 | 0,01 | 0,01 | 0,05 |
| XX 01 02 11 02 – Réunions et conférences | 0,005 | 0,005 | 0,005 | 0,005 | 0,005 | 0,025 |
| XX 01 02 11 03 - Comités ¹⁵ | NA | NA | NA | NA | NA | NA |
| XX 01 02 11 04 — Études et consultations | NA | NA | NA | NA | NA | NA |
| XX 01 02 11 05 — Systèmes d'information | NA | NA | NA | NA | NA | NA |
| Total autres dépenses de gestion (XX 01 02 11) | NA | NA | NA | NA | NA | NA |
| 3 Autres dépenses de nature administrative (préciser en indiquant la ligne budgétaire) | NA | NA | NA | NA | NA | NA |
| Total des dépenses administratives autres que ressources humaines et coûts connexes (NON inclus dans le montant de référence) | 0,015 | 0,015 | 0,015 | 0,015 | 0,015 | 0,075 |

Calcul — *Autres dépenses administratives non incluses dans le montant de référence*

NA

¹⁵ Préciser le type de comité, ainsi que le groupe auquel il appartient.