COMMISSION EUROPÉENNE

Bruxelles, le 30.9.2010
COM(2010) 520 final

2010/0274 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

modifiant le règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée

EXPOSÉ DES MOTIFS

1. CONTEXTE

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ci-après dénommée «l'ENISA») a été créée en mars 2004 pour une période initiale de cinq ans par le règlement (CE) n° 460/2004[1]. Elle avait pour principal objet «*d'assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de [l'Union] et […] de favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des organismes du secteur public de l'Union européenne, contribuant ainsi au bon fonctionnement du marché intérieur*». Le règlement (CE) n° 1007/2008[2] a prolongé le mandat de l'ENISA jusqu'en mars 2012.

La prolongation du mandat de l'ENISA en 2008 a aussi fourni l'occasion d'entamer un débat concernant l'orientation générale que doivent suivre les efforts européens en faveur de la sécurité des réseaux et de l'information (SRI), débat auquel la Commission a contribué en lançant une consultation publique sur les objectifs possibles d'une politique SRI renforcée au niveau de l'Union. Cette consultation publique s'est déroulée de novembre 2008 à janvier 2009 et a permis de recueillir près de 600 contributions[3].

Le 30 mars 2009, la Commission a adopté une communication relative à la protection des infrastructures d'information critiques[4] (PIIC) visant à protéger l'Europe des cyberattaques et des perturbations en améliorant la préparation, la sécurité et la résilience, qui comportait un plan d'action invitant l'ENISA à jouer un rôle, principalement de soutien aux États membres. Le plan d'action a été largement approuvé lors des discussions de la conférence ministérielle sur la PIIC qui s'est tenue à Tallinn, en Estonie, les 27 et 28 avril 2009[5]. Dans ses conclusions, la conférence de la présidence de l'Union européenne souligne combien il est important de «*mettre à profit le soutien opérationnel*» de l'ENISA; elle affirme que l'ENISA «*constitue un instrument précieux permettant d'appuyer les efforts de coopération menés à travers l'UE en la matière*» et souligne la nécessité de repenser et de reformuler le mandat de l'Agence «*afin de mieux mettre l'accent sur les priorités et les besoins de l'UE, de pouvoir y répondre de manière plus souple, de développer des savoirs et des compétences, et de soutenir l'efficacité opérationnelle de l'Agence ainsi que son impact général*» de sorte que l'Agence devienne *«un atout permanent pour chaque État membre et l'Union européenne dans son ensemble»*.

Après discussion au Conseil Télécommunications du 11 juin 2009, à l'occasion duquel les États membres ont approuvé la prolongation du mandat de l'ENISA et l'accroissement de ses ressources eu égard à l'importance de la SRI et aux problèmes en constante évolution qui se

---

1 Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (JO L 77 du 13.3.2004, p. 1).

2 Règlement (CE) n° 1007/2008 du Parlement européen et du Conseil du 24 septembre 2008 modifiant le règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée (JO L 293 du 31.10.2008, p. 1).

3 Le rapport de synthèse contenant les résultats de la consultation publique «Vers une politique renforcée de la sécurité des réseaux et de l'information en Europe» est joint en annexe 11 à l'analyse d'impact qui accompagne la présente proposition.

4 COM(2009) 149 du 30.3.2009.

5 Document de réflexion: http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf Conclusions de la présidence: http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf.

posent dans ce domaine, il a été mis un terme au débat sous la présidence suédoise de l'Union. La résolution du Conseil du 18 décembre 2009 sur une approche européenne concertée en matière de SRI[6] reconnaît le rôle et le potentiel de l'ENISA ainsi que la nécessité de «*continuer à développer cette agence pour en faire un organisme efficace*». Elle souligne aussi la nécessité de moderniser et de renforcer l'Agence pour que celle-ci aide la Commission et les États membres à combler le fossé entre technologie et politiques, servant ainsi de centre d'expertise de l'Union pour les questions de SRI.

2. CONTEXTE GENERAL

L'ensemble de l'économie et de la société européenne repose désormais sur les technologies de l'information et des communications (TIC). Les TIC peuvent faire l'objet de menaces que les frontières nationales n'arrêtent plus et qui ont pris de nouvelles formes du fait de l'évolution des technologies et du marché. Étant donné que les TIC ont une dimension planétaire et qu'elles sont interconnectées avec d'autres infrastructures, dont elles sont interdépendantes, il est impossible de garantir leur sécurité et leur résilience en adoptant des approches strictement nationales et non coordonnées. En même temps, les problèmes liés à la SRI évoluent rapidement. Aussi les réseaux et systèmes informatiques doivent-ils être protégés efficacement contre toutes sortes de perturbations et de pannes, y compris contre les attaques délibérées.

Les politiques concernant la SRI ont une fonction essentielle dans la stratégie numérique pour l'Europe[7], initiative phare au titre de la stratégie Europe 2020, visant à exploiter et développer le potentiel des TIC et à le transformer en croissance durable et en innovation. Encourager l'adoption des TIC et susciter la confiance dans la société de l'information sont des priorités absolues de la stratégie numérique pour l'Europe. Il est nécessaire, à cet effet, de réformer l'ENISA afin de permettre à l'Union, aux États membres et aux parties prenantes de se doter de moyens importants et d'atteindre un degré élevé de préparation pour prévenir et détecter les problèmes SRI et mieux y répondre.

3. POURQUOI FAUT-IL AGIR?

Parallèlement à la présente proposition, la Commission présente une proposition de règlement relatif à l'ENISA destiné à remplacer le règlement (CE) n° 460/2004. Elle prévoit une révision en profondeur des dispositions régissant l'Agence et établit cette dernière pour une durée de cinq ans. Cependant, la Commission est consciente du fait que la procédure législative au Parlement européen et au Conseil peut demander un certain temps pour que la proposition soit débattue et il y a donc un risque de vide juridique au cas où le nouveau mandat de l'Agence ne serait pas adopté avant expiration du mandat actuel.

Aussi la Commission soumet-elle la présente proposition de règlement prolongeant de 18 mois le mandat actuel de l'Agence pour qu'un délai suffisant permette le déroulement des débats.

---

6 Résolution du Conseil du 18 décembre 2009 sur une approche européenne concertée en matière de sécurité des réseaux et de l'information (JO C 321 du 29.12.2009, p. 1). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:FR:PDF.

7 COM(2010) 245 du 19.5.2010.

2010/0274 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

modifiant le règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

vu l'avis du Comité économique et social européen[8],

vu l'avis du Comité des régions[9],

après transmission de la proposition aux parlements nationaux,

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) En 2004, le Parlement européen et le Conseil ont adopté le règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information[10] (ci-après dénommée «l'Agence»).

(2) En 2008, le Parlement européen et le Conseil ont adopté le règlement (CE) n° 1007/2008 modifiant le règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée[11].

(3) À partir de novembre 2008 s'est tenu un débat sur l'orientation générale que doivent suivre les efforts européens en faveur de la sécurité des réseaux et de l'information (SRI) concernant également l'Agence. Conformément à sa stratégie visant à «Mieux légiférer» et afin de contribuer à ce débat, la Commission a lancé une consultation publique sur les objectifs possibles d'une politique de la sécurité des réseaux et de l'information renforcée au niveau de l'Union, qui a eu lieu de novembre 2008 à janvier 2009. Ce débat a débouché, en décembre 2009, sur la résolution du Conseil du

---

8 JO C … du …, p. ...

9 JO C … du …, p. ...

10 Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (JO L 77 du 13.3.2004, p. 1).

11 Règlement (CE) n° 1007/2008 du Parlement européen et du Conseil du 24 septembre 2008 modifiant le règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée (JO L 293 du 31.10.2008, p. 1).

18 décembre 2009 sur une approche européenne concertée en matière de sécurité des réseaux et de l'information (SRI)[12].

(4) Compte tenu des résultats de la discussion publique, il est envisagé de remplacer le règlement (CE) n° 460/2004.

(5) Une procédure législative visant à réformer l'ENISA peut demander un certain temps pour que la proposition soit débattue et, étant donné que le mandat de l'Agence prendra fin le 13 mars 2012, il est nécessaire d'adopter une prolongation qui permettra à la fois d'assurer la cohérence et la continuité et de laisser suffisamment de temps pour organiser les débats au Conseil et au Parlement européen.

(6) Il convient dès lors de prolonger la durée de l'Agence jusqu'au 13 septembre 2013,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Le règlement (CE) n° 460/2004 est modifié comme suit:

L'article 27 est remplacé par le texte suivant:

«Article 27 - Durée

L'Agence est instituée à partir du 14 mars 2004 pour une période de neuf ans et six mois».

Article 2
Entrée en vigueur

Le présent règlement entre en vigueur le jour suivant celui de sa publication *au Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à […], le […]

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*

[12] Résolution du Conseil du 18 décembre 2009 sur une approche européenne concertée en matière de sécurité des réseaux et de l'information (JO C 321 du 29.12.2009, p. 1).

FICHE FINANCIÈRE LÉGISLATIVE DES PROPOSITIONS

1. CADRE DE LA PROPOSITION/INITIATIVE

1.1. Dénomination de la proposition/initiative

Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information.

1.2. Domaine(s) politique(s) concerné(s) dans la structure GPA/EBA[13]

Société de l'information et médias

Cadre réglementaire pour la stratégie numérique

1.3. Nature de la proposition/initiative

☐ La proposition/initiative porte sur une **action nouvelle**

☐ La proposition/initiative porte sur une **action nouvelle suite à un projet pilote/une action préparatoire**[14]

☑ La proposition/initiative est relative à **la prolongation d'une action existante**

☐ La proposition/initiative porte sur une **action réorientée vers une nouvelle action**

1.4. Objectifs

1.4.1. Objectif(s) stratégique(s) pluriannuel(s) de la Commission visé(s) par la proposition/initiative

Améliorer la résilience des réseaux de communications électroniques européens

L'Agence continuera à travailler sur la résilience, en exécutant notamment des enquêtes sur les obligations, les besoins et les bonnes pratiques mises en œuvre en matière de résilience[15], ainsi que des analyses de méthodes et procédures supplémentaires destinées à améliorer la résilience. D'autres projets pilotes seront entrepris en vue d'évaluer la validité des exigences, des méthodes et des pratiques. L'Agence contribuera à l'amélioration de la sécurité et de la résilience des infrastructures d'information critiques ainsi qu'à la constitution du Partenariat public-privé européen pour la résilience (EP3R) et du Forum européen des États membres (EFMS).

Développer et maintenir la coopération entre les États membres

---

13 GPA: gestion par activités – EBA: établissement du budget par activités.

14 Tels que visé à l'article 49, paragraphe 6, points a) ou b), du règlement financier.

15 Ces enquêtes seront fondées sur celles menées par l'ENISA en 2006 et 2007 concernant les mesures de sécurité mises en œuvre par les opérateurs de communications électroniques.

L'ENISA devrait poursuivre ses efforts pour identifier, à l'échelle européenne, des cercles de compétences en matière de sécurité sur des thèmes tels que la sensibilisation et la gestion des incidents, la coopération en matière d'interopérabilité des cartes d'identité électroniques au niveau paneuropéen[16], ainsi que le maintien d'une plateforme de soutien aux échanges de bonnes pratiques en matière de sécurité des réseaux et de l'information à l'échelle européenne[17]. La coopération entre les États membres devrait être renforcée en vue d'améliorer les capacités de tous les États membres et de rehausser le niveau général de cohérence et d'interopérabilité.

Répertorier les risques émergents pour établir la confiance

L'Agence continuera à travailler à la mise en place d'un cadre qui permettra aux décideurs de mieux comprendre et de mieux évaluer les risques émergents qui découlent de technologies et d'applications nouvelles, grâce à une pratique systématique de collecte, de traitement, et de diffusion des données et de retour d'informations sur celles-ci.

Renforcer la confiance des microentreprises dans l'information

L'ère de l'information numérique continue à ouvrir de nombreuses possibilités commerciales aux entreprises, et notamment aux plus petites d'entre elles. Cependant, le développement des TIC et leur adoption par les utilisateurs présentent encore des faiblesses. L'objectif est de faire le point sur les besoins et attentes des microentreprises dans ce domaine. Pour ce faire, l'ENISA encouragera et pilotera des modèles de coopération transfrontières entre des multiplicateurs et des associations dans le domaine du renforcement des capacités en matière de SRI en faveur des microentreprises, travaillera au développement de systèmes de certification ciblant les microentreprises et de cadres de conformité pour les non-experts, produira et pilotera des bonnes pratiques pour la continuité de l'activité et œuvrera, dans le domaine de la conformité, pour permettre aux PME et aux microentreprises de formuler leurs objectifs de sécurité et d'établir des feuilles de route pour les atteindre.

1.4.2. Objectif(s) spécifique(s) et activité(s) GPA/EBA concernée(s)

Objectif spécifique

Accroître la sécurité des réseaux et de l'information (SRI), favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des organismes du secteur public, et recenser les défis politiques que représentent les réseaux et l'internet futurs.

Activité(s) GPA/EBA concernée(s)

Politique des communications électroniques et sécurité des réseaux.

[16] Ce soutien permettra le suivi des travaux menés par l'ENISA en 2006 et 2007 à propos d'un langage commun pour améliorer l'interopérabilité des cartes d'identité électroniques.

[17] Cette plateforme fait suite aux travaux menés en 2007 pour définir une feuille de route sur la mise en place d'un courtage des bonnes pratiques en matière de sécurité des réseaux et de l'information à l'échelle européenne.

1.4.3. Résultat(s) et impact(s) attendu(s)

L'Agence devrait contribuer à un niveau élevé de sécurité des réseaux et de l'information dans l'Union et à l'émergence d'une culture de la sécurité des réseaux et de l'information, dans l'intérêt des citoyens, des consommateurs, des entreprises et des organismes du secteur public de l'Union européenne, prenant part ainsi au bon fonctionnement du marché intérieur.

1.4.4. Indicateurs de résultats et d'impacts

Voir le point 1.4.1 ci-dessus.

1.5. Justification(s) de la proposition/initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme

L'ENISA a été créée à l'origine en 2004 afin de faire face aux menaces pour la SRI et aux atteintes à la SRI pouvant en découler. Depuis lors, les défis concernant la sécurité des réseaux et de l'information ont changé en fonction des évolutions technologiques et commerciales et ont fait l'objet de réflexions et de débats approfondis, ce qui implique aujourd'hui d'actualiser et de décrire plus en détail les problèmes précis qui se posent et la façon dont ils sont impactés par les changements dans le paysage SRI. Dans les conclusions de la présidence de la conférence ministérielle sur la protection des infrastructures d'information critiques, qui s'est tenue à Tallinn, il est déclaré que «les nouveaux défis auxquels nous serons confrontés durant de nombreuses années exigent que le mandat de l'Agence soit profondément repensé et reformulé afin de mieux mettre l'accent sur les priorités et les besoins de l'UE, de pouvoir y répondre de manière plus souple, de développer des savoirs et des compétences européennes, et de soutenir l'efficacité opérationnelle de l'Agence ainsi que son impact général. C'est de cette façon que l'ENISA pourra devenir un atout permanent pour chaque État membre et l'Union européenne dans son ensemble».

La Commission présente, parallèlement à la présente proposition, une proposition de règlement concernant l'ENISA destinée à remplacer le règlement (CE) n° 460/2004, qui prévoit une révision en profondeur des dispositions régissant l'Agence et établit cette dernière pour une durée de cinq ans. Cependant, la Commission est consciente du fait que la procédure législative au Parlement européen et au Conseil peut demander un certain temps pour que la proposition soit débattue et il y a donc un risque de vide juridique si le nouveau mandat de l'Agence n'était pas adopté avant expiration du mandat actuel.

Aussi la Commission soumet-elle la présente proposition de règlement prolongeant de 18 mois le mandat actuel de l'Agence pour qu'un délai suffisant permette le déroulement des débats.

1.5.2. Valeur ajoutée de l'intervention de l'UE

Les problèmes de SRI ne s'arrêtent pas aux frontières nationales et ne peuvent donc pas être réglés efficacement au seul niveau national. En même temps, les façons dont le problème est traité par les pouvoirs publics des différents États membres sont très diverses. Ces différences constituent un obstacle de taille à l'instauration de mécanismes appropriés, à l'échelle de l'Union, pour une SRI accrue en Europe. Comme les infrastructures TIC sont par nature interconnectées, l'efficacité des mesures prises au niveau national dans un État membre est

toujours fortement affectée par l'ampleur plus limitée des mesures dans les autres États membres et par le manque de coopération transnationale systématique. Si l'insuffisance des mesures de SRI provoque un incident dans un État membre, elle peut aussi entraîner des perturbations dans d'autres États membres.

De plus, la multiplication des exigences de sécurité implique un coût pour les entreprises opérant au niveau de l'Union européenne et entraîne un morcellement et un manque de compétitivité sur le marché intérieur européen.

Compte tenu de la dépendance croissante vis-à-vis des réseaux et systèmes informatiques, la préparation pour faire face aux incidents s'avère insuffisante.

Les systèmes nationaux actuels d'alerte rapide et d'intervention en cas d'incident ont des défauts importants. Les processus et les pratiques en matière de surveillance et de notification des incidents dans le domaine de la sécurité des réseaux varient considérablement selon les États membres. Dans certains pays, les processus ne sont pas formalisés tandis que, dans d'autres, il n'y a pas d'autorité compétente pour recevoir et traiter les rapports d'incident. En fait, il n'existe pas de systèmes européens. Par conséquent, un incident SRI pourrait perturber complètement les systèmes permettant de répondre aux besoins de base et il convient d'anticiper les réactions appropriées. Dans sa communication sur la PIIC, la Commission a également souligné la nécessité de moyens européens en matière d'alerte rapide et d'intervention en cas d'incident, éventuellement étayés par des exercices à l'échelle européenne.

Le besoin se fait nettement sentir de disposer d'instruments politiques destinés à recenser, de façon proactive, les risques et faiblesses SRI, d'instaurer les mécanismes d'intervention appropriés (par exemple, en recensant et en diffusant de bonnes pratiques), et de faire en sorte que ces mécanismes soient connus et appliqués par les parties prenantes.

1.5.3. Principales leçons tirées d'expériences similaires

Conformément à l'article 25 du règlement instituant l'ENISA, une évaluation de l'ENISA a été réalisée par un groupe d'experts externes en 2006/2007, en vue de fournir une évaluation formative des méthodes de travail, de l'organisation et du mandat de l'Agence, et de recommander le cas échéant des améliorations. Il convient de noter que cette évaluation a été réalisée un an seulement après que l'ENISA est devenue opérationnelle. Le rapport d'évaluation[18] a confirmé la validité des motifs politiques initiaux ayant justifié la création de l'ENISA, a soulevé certains problèmes à résoudre concernant la visibilité de l'Agence et sa capacité à produire des effets de grande ampleur. Au nombre de ces problèmes figuraient la structure organisationnelle, l'éventail de compétences du personnel opérationnel de l'Agence et les difficultés organisationnelles liées à son éloignement géographique.

Voir aussi le point 1.5.1 ci-dessus.

[18] Voir http://ec.europa.eu/dgs/information_society/evaluation/studies/s2006_enisa/docs/final_report.pdf

1.5.4. Compatibilité et synergie éventuelle avec d'autres instruments financiers

L'avenir de l'ENISA a été évoqué dans le cadre du débat général sur la SRI et d'autres initiatives politiques axées sur l'avenir de la SRI.

1.6. Durée de l'action et de son impact financier

☑ Proposition/initiative à **durée limitée**

– ☑ Proposition/initiative en vigueur du 14/3/2012 au 13/9/2013

– ☑ Impact financier de 2012 à 2013.

☐ Proposition/initiative à **durée illimitée**

– Mise en œuvre avec une période de démarrage de AAAA à AAAA,

– suivie d'un fonctionnement à plein rendement.

1.7. Mode(s) de gestion prévu(s)[19]

☐ **Gestion centralisée directe** par la Commission.

☑ **Gestion centralisée indirecte** par délégation de tâches d'exécution à:

– ☐ des agences exécutives

– ☑ des organismes créés par les Communautés[20]

– ☐ des organismes publics nationaux/organismes avec mission de service public

– ☐ des personnes chargées de l'exécution d'actions spécifiques en vertu du titre V du traité sur l'Union Européenne, identifiées dans l'acte de base concerné au sens de l'article 49 du Règlement financier.

☐ **Gestion partagée** avec des États membres.

☐ **Gestion décentralisée** avec des pays tiers.

☐ **Gestion conjointe** avec des organisations internationales ***(à préciser)***.

---

[19] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_fr.html

[20] Tels que visés à l'article 185 du règlement financier.

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Le directeur exécutif est responsable du contrôle effectif et de l'évaluation des performances de l'Agence par rapport à ses objectifs, et rend compte de son activité chaque année au conseil d'administration.

Le directeur exécutif rédige un rapport général couvrant toutes les activités de l'Agence au cours de l'année précédente, qui compare notamment les résultats obtenus avec les objectifs du programme de travail annuel. Une fois adopté par le conseil d'administration, ce rapport est transmis au Parlement européen, au Conseil, à la Commission, à la Cour des comptes, au Comité économique et social européen ainsi qu'au Comité des régions, et est publié.

2.2. Système de gestion et de contrôle

2.2.1. Risque(s) identifié(s)

Depuis la création de l'ENISA en 2004, celle-ci a fait l'objet d'évaluations externes et internes.

Conformément à l'article 25 du règlement instituant l'ENISA, la première étape de ce processus a été une évaluation indépendante de l'ENISA réalisée par un groupe d'experts externes en 2006/2007. Le rapport[21] qu'il a établi a confirmé la validité du raisonnement politique à la base de la création de l'ENISA et des objectifs initiaux, et a largement contribué à soulever certaines des questions qui devaient être traitées.

En mars 2007, la Commission a présenté son rapport sur l'évaluation au conseil d'administration qui a ensuite formulé ses propres recommandations sur l'avenir de l'Agence et sur les modifications à apporter au règlement ENISA[22].

En juin 2007, la Commission a soumis sa propre appréciation des résultats de l'évaluation externe et des recommandations du conseil d'administration dans le cadre d'une communication au Parlement européen et au Conseil[23]. La Commission y exposait le choix à faire entre la prolongation du mandat de l'Agence et le remplacement de celle-ci par un autre mécanisme tel qu'une assemblée permanente des parties prenantes ou un réseau d'organisations travaillant dans le domaine de la sécurité des réseaux. Elle lançait aussi une consultation publique sur ce sujet, en sollicitant les suggestions et réactions des parties prenantes européennes par une liste de questions visant à orienter les débats ultérieurs[24].

---

21 http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm.

22 Conformément à l'article 25 du règlement ENISA. L'intégralité du document adopté par le conseil d'administration de l'ENISA, qui contient aussi les réflexions de celui-ci, est disponible sur le site web suivant: http://enisa.europa.eu/pages/03_02.htm.

23 Communication de la Commission au Parlement européen et au Conseil sur l'évaluation de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), COM(2007) 285 final du 1.6.2007: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:FR:NOT.

24 http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=EnisaFuture&lang=en.

En 2009, la Commission a lancé une analyse d'impact destinée à examiner les options possibles pour l'avenir de l'ENISA. Cette analyse d'impact est jointe à la proposition de règlement concernant l'ENISA destiné à remplacer le règlement (CE) n° 460/2004.

2.2.2. Moyen(s) de contrôle prévu(s)

Voir 2.2.1

2.3. Mesures de prévention des fraudes et irrégularités

Le contrôle du paiement de tout service ou étude nécessaire est effectué par le personnel de l'Agence avant le paiement, compte tenu de toute obligation contractuelle, des principes économiques et des bonnes pratiques financières ou de gestion. Des dispositions antifraude (surveillance, exigences en matière de rapports) seront introduites dans tous les accords et contrats conclus entre l'Agence et les bénéficiaires de tous paiements.

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses impactées

- Lignes budgétaires existantes

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Nature de **la dépense**	Participation			
	Numéro/Description	CD/CND (25)	de pays AELE[26]	de pays candidats[27]	de pays tiers	au sens de l'article 18, paragraphe 1, point a) *bis*, du règlement financier
1.a Compétitivité pour la croissance et l'emploi	09 02 03 01 Agence européenne chargée de la sécurité des réseaux et de l'information – Subvention aux titres 1 et 2	CD	OUI	NON	NON	NON
	09 02 03 02 Agence européenne chargée de la sécurité des réseaux et de l'information – Subvention au titre 3	CD	OUI	NON	NON	NON
5 Dépenses administratives	09 01 01 Dépenses liées au personnel en activité du domaine politique «Société de l'information et médias»	CND	NON	NON	NON	NON
	09 01 02 11 Autres dépenses de gestion	CND	NON	NON	NON	NON

25 CD= Crédits dissociés/CND= Crédits non dissociés.

26 AELE: Association européenne de libre-échange.

27 Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

3.2. Impact estimé sur les dépenses

3.2.1. Synthèse de l'impact estimé sur les dépenses

Millions d'euros (à la 3e décimale)

Rubrique du cadre financier pluriannuel:	1.a	Compétitivité pour la croissance et l'emploi

ENISA			14 mars -31 déc. 2012	1er janv. -13 sept 2013	**TOTAL**
Crédits d'exploitation					
09 02 03 02 Agence européenne chargée de la sécurité des réseaux et de l'information – Subvention au titre 3	Engagements	(1)	2,073	1,734	**3,807**
	Paiements	(2)	2,073	1,734	**3,807**
Crédits administratifs					
09 02 03 01 Agence européenne chargée de la sécurité des réseaux et de l'information – Subvention aux titres 1 et 2		(3)	4,600	4,291	**8,891**
TOTAL des crédits sous la rubrique 1.a	Engagements	=1+3	6,673	6,025	**12,698**
	Paiements	=2+3	6,673	6,025	**12,698**

• TOTAL des crédits d'exploitation	Engagements	(4)	2,073	1,734	**3,807**
	Paiements	(5)	2,073	1,734	**3,807**
• TOTAL des crédits de nature administrative financés par l'enveloppe des programmes spécifiques		(6)	4,600	4,291	**8,891**

TOTAL des crédits sous la rubrique 1.a Compétitivité pour la croissance et l'emploi du cadre financier pluriannuel	Engagements	=4+6	6,673	6,025	**12,698**
	Paiements	=5+6	6,673	6,025	**12,698**

Millions d'euros (à la 3e décimale)

Rubrique du cadre financier pluriannuel:	5	Dépenses administratives

		14 mars-31 déc. 2012	1er janv.-13 sept 2013	Total
Ressources humaines		0,342	0,299	**0,641**
Autres dépenses administratives		0,008	0,007	**0,015**
TOTAL DG INFSO	Crédits	0,350	0,306	**0,656**

TOTAL des crédits sous la rubrique 5 du cadre financier pluriannuel	(Total des engagements = total des paiements)	0,350	0,306	**0,656**

		14 mars-31 déc. 2012	1er janv.-13 sept 2013	Total
TOTAL des crédits sous les rubriques 1 à 5 du cadre financier pluriannuel	Engagements	7,023	6,331	**13,354**
	Paiement	7,023	6,331	**13,354**

3.2.2. Impact estimé sur les crédits opérationnels

– ☐ La proposition/l'initiative n'implique pas l'utilisation de crédits opérationnels.

– ☑ La proposition/l'initiative implique l'utilisation de crédits opérationnels, comme expliqué ci-après:

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

Indiquer les objectifs et résultats ⇩	14 mars – 31 décembre 2012	1 janvier - 13 septembre 2013	**TOTAL**
Améliorer la résilience des réseaux de communications électroniques européens	0,237	0,198	**0,435**
Développer et maintenir la coopération entre les États membres	0,237	0,198	**0,435**
Répertorier les risques émergents pour établir la confiance	0,169	0,141	**0,310**
Renforcer la confiance des microentreprises dans l'information	0,087	0,072	**0,159**
Gestion des activités horizontales	1,344	1,124	**2,468**
COÛT TOTAL	2,073	1,734	**3,807**

3.2.3. Impact estimé sur les crédits de nature administrative[28]

3.2.3.1. Résumé

– ☐ La proposition/l'initiative n'implique pas l'utilisation de crédits de nature administrative.

– ☑ La proposition/l'initiative implique l'utilisation de crédits de nature administrative, comme expliqué ci-après:

a) Dépenses administratives sous la rubrique 5 du cadre financier pluriannuel

Millions d'euros (à la 3e décimale)

RUBRIQUE 5 du cadre financier pluriannuel	14 mars-31 déc. 2012	1er janv.-13 sept 2013	**TOTAL**
Ressources humaines	0,342	0,299	**0,641**
Autres dépenses administratives	0,008	0,007	**0,015**
TOTAL	0,350	0,306	**0,656**

b) Dépenses administratives relatives à l'ENISA – couvertes par la ligne budgétaire «09.020301 Agence européenne chargée de la sécurité des réseaux et de l'information: Titre 1 – Personnel et Titre 2 – Fonctionnement de l'Agence».

Millions d'euros (à la 3e décimale)

	14 mars-31 déc. 2012	1er janv.-13 sept 2013	**TOTAL**
Ressources humaines – Titre 1 – Personnel	4,216	3,916	**8,132**
Autres dépenses de nature administrative – Titre 2 – Fonctionnement de l'Agence	0,384	0,375	**0,759**

[28] L'annexe de la fiche financière législative n'est pas remplie car elle ne s'applique pas à la présente proposition.

TOTAL	**4,600**	**4,291**	**8,891**

3.2.3.2. Besoins estimés en ressources humaines

– ☐ La proposition/l'initiative n'implique pas l'utilisation de ressources humaines.

– ☑ La proposition/l'initiative implique l'utilisation de ressources humaines, comme expliqué ci-après:

a) Ressources humaines au sein de la Commission

	14 mars-31 déc. 2012	1er janv.-13 sept 2013
Tableau des effectifs de l'ENISA (postes de fonctionnaires et d'agents temporaires) (en équivalent temps plein - ETP)		
XX 01 01 01 (au siège et dans les bureaux de représentation de la Commission)	3,5	3,5
TOTAL	**3,5**	**3,5**

b) Ressources humaines de l'ENISA

		14 mars-31 déc. 2012	1er janv.-13 sept 2013
Tableau des effectifs de l'ENISA (en équivalent temps plein - ETP)			
Fonctionnaires ou agents temporaires	**AD**	29	29
	AST	15	15
TOTAL des fonctionnaires ou agents temporaires		44	44
Autre personnel (en ETP)			
Agents contractuels		**13**	**13**
Experts nationaux détachés (END)		**5**	**5**
TOTAL autre personnel		**18**	**18**
TOTAL		**62**	**62**

Description des tâches devant être exécutées par le personnel de l'Agence:

Fonctionnaires et agents temporaires	L'Agence continuera à: – avoir une fonction consultative et de coordination, dans le cadre de laquelle elle **recueillera et analysera des données** sur la sécurité de l'information. Actuellement, des organismes tant publics que privés, poursuivant des objectifs différents, recueillent des données sur les incidents dans le domaine des technologies de l'information et d'autres renseignements pertinents pour la sécurité de l'information. Cependant, il n'existe pas, au niveau européen, d'organe central capable de mettre en œuvre une démarche d'ensemble pour la collecte et l'analyse des données et la formulation d'avis et de conseils en vue de soutenir l'activité politique de l'Union sur la sécurité des réseaux et de l'information; – **faire office** de **centre d'expertise** auprès duquel les États membres comme les institutions européennes pourront demander **des avis et des conseils sur des questions techniques** liées à la sécurité; – contribuer à l'instauration d'une **coopération de grande envergure entre les différents acteurs** dans le domaine de la sécurité de l'information, en apportant par exemple une assistance aux activités de suivi qui accompagnent les travaux sur la sécurité du commerce électronique. Cette coopération sera une condition préalable capitale pour la sécurité du fonctionnement des réseaux et des systèmes d'information en Europe. La participation et l'engagement de tous les intéressés sont donc requis; – contribuer à l'instauration d'une approche coordonnée de la sécurité de l'information en fournissant une **assistance aux États membres**, par exemple en ce qui concerne la **promotion de l'évaluation des risques** et des actions de sensibilisation; – assurer l'**interopérabilité des réseaux et systèmes d'information** lorsque les États membres **appliquent** des exigences techniques qui ont une incidence sur la sécurité; – recenser les besoins **pertinents en matière de normalisation**, évaluer les normes de sécurité et systèmes de certification existants et œuvrer pour que leur utilisation par les États membres soit la plus large possible afin de soutenir l'application de la législation européenne; – favoriser, dans ce domaine, une **coopération internationale** qui devient de plus en plus nécessaire car les problèmes de sécurité des réseaux et de l'information ont une dimension mondiale.
Personnel externe	– Voir ci-dessus.

3.2.4. Compatibilité avec la programmation financière existante

– ☑ La proposition/l'initiative est compatible avec la programmation financière existante.

– ☐ La proposition/l'initiative nécessite une reprogrammation de la rubrique concernée du cadre financier pluriannuel.

– ☐ La proposition/l'initiative nécessite le recours à l'instrument de flexibilité ou à la révision du cadre financier pluriannuel[29].

3.2.5. Participation de tiers au financement

– ☐ La proposition/l'initiative ne prévoit pas de cofinancement par des tiers.

– ☑ La proposition prévoit un cofinancement par des tiers estimé ci-après (applicable aux lignes budgétaires 09.020301 et 09.020302):

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

	14 mars-31 déc. 2012	1er janv.-13 sept 2013	Total
AELE	0,160	0,145	0,305

3.3. Incidence estimée sur les recettes

– ☑ La proposition/l'initiative n'a pas d'incidence financière sur les recettes.

– ☐ La proposition/l'initiative a l'incidence financière suivante:

  – ☐ sur ses ressources propres

  – ☐ sur les recettes diverses.

[29] Voir les points 19 et 24 de l'accord interinstitutionnel.