EUROPESE COMMISSIE

Brussel, 30.9.2010
COM(2010) 520 definitief

2010/0274 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

tot wijziging van Verordening (EG) nr. 460/2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging, ten aanzien van de looptijd van het Agentschap

TOELICHTING

1. ACHTERGROND

Het Europees Agentschap voor netwerk- en informatiebeveiliging (hierna "het ENISA") is in maart 2004 bij Verordening (EG) nr. 460/2004[1] opgericht voor een eerste periode van vijf jaar, en heeft als hoofddoel *"te zorgen voor een hoog en doeltreffend niveau van netwerk- en informatiebeveiliging in de [Unie] en […] een cultuur van netwerk- en informatiebeveiliging ten behoeve van de burgers, consumenten, bedrijven en publieke organen in de Europese Unie tot stand te brengen en op die manier bij te dragen tot de goede werking van de interne markt"*. Bij Verordening (EG) nr. 1007/2008[2] is het mandaat van het ENISA verlengd tot maart 2012.

De verlenging van het mandaat van het ENISA in 2008 heeft ook een debat op gang gebracht over de algemene richting van de Europese inspanningen op het gebied van netwerk- en informatiebeveiliging; de Commissie heeft een bijdrage geleverd tot dit debat door een publieke raadpleging op te starten over de mogelijke doelstellingen van een versterkt beleid voor netwerk- en informatiebeveiliging op het niveau van de Unie. Deze publieke raadpleging, die plaatsvond van november 2008 tot januari 2009, leverde bijna 600 reacties op[3].

Op 30 maart 2009 heeft de Commissie een mededeling betreffende de bescherming van kritieke informatie-infrastructuur vastgesteld[4], waarin met name aandacht wordt besteed aan de bescherming van Europa tegen cyberaanvallen en -verstoringen door de paraatheid, beveiliging en veerkracht te verbeteren; deze mededeling bevat ook een actieplan waarin het ENISA wordt opgeroepen om een rol te spelen, met name ter ondersteuning van de lidstaten. Tijdens de besprekingen in het kader van de ministeriële conferentie betreffende de bescherming van kritieke informatie-infrastructuur, die op 27 en 28 april 2009 plaatsvond in Tallinn, kon het actieplan op brede steun rekenen[5]. In de conclusies die het voorzitterschap van de Europese Unie uit deze conferentie heeft getrokken, wordt benadrukt dat het belangrijk is de operationele steun voor het ENISA op te drijven; volgens deze conclusies is het ENISA een waardevol instrument om de gezamenlijke inspanningen in de hele Unie op dit gebied te versterken en moet het mandaat van het Agentschap worden herbekeken en anders geformuleerd, zodat het beter is afgestemd op de prioriteiten en behoeften van de EU, zodat een flexibeler responscapaciteit kan worden opgebouwd, vaardigheden en bekwaamheden kunnen worden ontwikkeld en de operationele efficiëntie en algemene impact van het

---

1 Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging (PB L 77 van 13.3.2004, blz. 1).

2 Verordening (EG) nr. 1007/2008 van het Europees Parlement en de Raad van 24 september 2008 tot wijziging van Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging, ten aanzien van de looptijd van het Agentschap (PB L 293 van 31.10.2008, blz. 1).

3 Het samenvattend verslag van de resultaten van de openbare raadpleging 'Op weg naar een versterkt beleid inzake netwerk- en informatiebeveiliging in Europa' is als bijlage 11 bij de effectbeoordeling bij dit voorstel gevoegd.

4 COM(2009) 149 van 30.3.2009.

5 Discussienota: http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf
Conclusies van het voorzitterschap:
http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf.

Agentschap kunnen worden versterkt, teneinde ervoor te zorgen dat het Agentschap een permanente aanwinst wordt voor alle lidstaten en voor de Europese Unie in haar geheel.

Na de besprekingen in de Raad Telecommunicatie van 11 juni 2004, waar de lidstaten, gezien het belang van netwerk- en informatiebeveiliging, hun steun hebben uitgesproken voor een uitbreiding van het mandaat en een verhoging van de middelen van het ENISA, werd het debat afgesloten onder het Zweedse voorzitterschap van de Unie. In de resolutie van de Raad van 18 december 2009 over een coöperatieve Europese aanpak met betrekking tot netwerk- en informatiebeveiliging[6] worden de rol en het potentieel van het ENISA erkend, alsook de behoefte om het ENISA *'verder te ontwikkelen tot een doeltreffend orgaan'*. Volgens deze conclusies moet ook aandacht worden geschonken aan het moderniseren en versterken van het ENISA, zodat het de Commissie en de lidstaten kan helpen bij het overbruggen van de kloof tussen technologie en beleid en het centrum van deskundigheid van de EU kan worden in EU-aangelegenheden op het gebied van netwerk- en informatiebeveiliging.

2. ALGEMENE CONTEXT

Informatie- en communicatietechnologieën (ICT) vormen de ruggengraat van de Europese economie en samenleving. ICT zijn kwetsbaar voor bedreigingen die niet langer nationale grenzen volgen en die veranderd zijn door technologische en marktontwikkelingen. Aangezien ICT een mondiale dimensie hebben en nauw met elkaar en met andere infrastructuren zijn verweven, kan de beveiliging en veerkracht ervan niet worden gewaarborgd door een louter nationale en niet-gecoördineerde aanpak. Tegelijk evolueren de uitdagingen met betrekking tot netwerk- en informatiebeveiliging zeer snel. Netwerk- en informatiesystemen moeten effectief worden beveiligd tegen alle soorten verstoringen en defecten, inclusief aanvallen door mensen.

Beleidsmaatregelen op het gebied van netwerk- en informatiebeveiliging spelen een centrale rol in de digitale agenda voor Europa[7], een vlaggenschipinitiatief van de EU 2020-strategie, om het potentieel van ICT te exploiteren en te bevorderen en om dit potentieel te vertalen in duurzame groei en innovatie. De benutting van ICT stimuleren en het vertrouwen in de informatiemaatschappij bevorderen, zijn sleutelprioriteiten van de digitale agenda voor Europa. Het ENISA is dan ook nodig om ervoor te zorgen dat de Unie, de lidstaten en belanghebbenden over de nodige bekwaamheden en paraatheid beschikken om problemen op het gebied van netwerk- en informatiebeveiliging te voorkomen, op te sporen en aan te pakken.

3. REDENEN OM DE MAATREGELEN TE NEMEN

Samen met dit voorstel stelt de Commissie ook een verordening voor inzake het ENISA, ter vervanging van Verordening (EG) nr. 460/2004; deze verordening houdt een grondige herziening in van de bepalingen met betrekking tot het beheer van het Agentschap en richt het Agentschap op voor een periode van vijf jaar. De Commissie is zich er echter van bewust dat in het kader van de wetgevingsprocedure met betrekking tot dat voorstel lange besprekingen kunnen plaatsvinden in het Europees Parlement en de Raad, met het risico op een juridisch

---

6 Resolutie van de Raad van 18 december 2009 over een coöperatieve Europese aanpak met betrekking tot netwerk- en informatiebeveiliging (PB C 321 van 29.12.2009, blz. 1). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:NL:PDF.

7 COM(2010) 245 van 19.5.2010.

vacuüm als het nieuwe mandaat van het Agentschap niet wordt goedgekeurd vóór het huidige mandaat verstrijkt.

Daarom stelt de Commissie de onderhavige verordening voor, waarbij het huidige mandaat van het Agentschap met 18 maanden wordt verlengd, zodat er voldoende tijd is voor de besprekingen.

2010/0274 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

tot wijziging van Verordening (EG) nr. 460/2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging, ten aanzien van de looptijd van het Agentschap

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Gezien het advies van het Europees Economisch en Sociaal Comité[8],

Gezien het advies van het Comité van de Regio's[9],

Na toezending van het voorstel aan de nationale parlementen,

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) In 2004 hebben het Europees Parlement en de Raad Verordening (EG) nr. 460/2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging[10] (hierna "het Agentschap" genoemd) aangenomen.

(2) In 2008 hebben het Europees Parlement en de Raad Verordening (EG) nr. 1007/2008 aangenomen, waarbij Verordening (EG) nr. 460/2004 wordt gewijzigd voor wat de looptijd van het Agentschap betreft[11].

(3) Vanaf november 2008 vond een publiek debat plaats over de algemene richting van de Europese inspanningen voor betere netwerk- en informatiebeveiliging; dit debat had ook betrekking op het Agentschap. In overeenstemming met de strategie van de Commissie inzake betere regelgeving heeft de Commissie, bij wijze van bijdrage tot

---

8 PB C van , blz. .

9 PB C van , blz. .

10 Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging (PB L 77 van 13.3.2004, blz. 1).

11 Verordening (EG) nr. 1007/2008 van het Europees Parlement en de Raad van 24 september 2008 tot wijziging van Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging, ten aanzien van de looptijd van het Agentschap (PB L 293 van 31.10.2008, blz. 1).

dit debat, het initiatief genomen tot een publieke raadpleging over de doelstellingen voor versterkt beleid inzake netwerk- en informatiebeveiliging op het niveau van de Unie; deze raadpleging vond plaats tussen november 2008 en januari 2009. Dit debat is uitgemond in een resolutie van de Raad van 18 december 2009 over een coöperatieve Europese aanpak met betrekking tot netwerk- en informatiebeveiliging[12].

(4) Rekening houdende met de resultaten van het publieke debat wordt voorgenomen Verordening (EG) nr. 460/2004 te vervangen.

(5) Aangezien een wetgevende procedure om het ENISA te hervormen veel tijd voor debat kan vragen en het mandaat van het Agentschap op 13 maart 2012 afloopt, is het noodzakelijk een verlenging goed te keuren die voldoende besprekingen in het Europees Parlement mogelijk maakt en tegelijk samenhang en continuïteit garandeert.

(6) De looptijd van het Agentschap dient daarom tot 13 september 2013 te worden verlengd,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD :

Artikel 1

Verordening (EG) nr. 460/2004 wordt als volgt gewijzigd:

Artikel 27 wordt vervangen door:

'Artikel 27 - Looptijd

Het Agentschap wordt opgericht met ingang van 14 maart 2004 voor een periode van negen jaar en zes maanden'.

Artikel 2
Inwerkingtreding

Deze verordening treedt in werking op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te […], […]

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*

[12] Resolutie van de Raad van 18 december 2009 over een coöperatieve Europese aanpak met betrekking tot netwerk- en informatiebeveiliging (PB C 321 van 29.12.2009, blz. 1).

FINANCIEEL MEMORANDUM VOOR VOORSTELLEN

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

Voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging.

1.2. Betrokken beleidsterrein(en) in de ABM/ABB-structuur[13]

Informatiemaatschappij en media

Regelgevingskader voor de digitale agenda

1.3. Aard van het voorstel/initiatief

☐ Het voorstel/initiatief betreft **een nieuwe actie**

☐ Het voorstel/initiatief betreft **een nieuwe actie na een proefproject/een voorbereidende actie**[14]

☑ Het voorstel/initiatief betreft **de verlenging van een bestaande actie**

☐ Het voorstel/initiatief betreft **een actie die wordt omgebogen naar een nieuwe actie**

1.4. Doelstellingen

1.4.1. De met het voorstel/initiatief beoogde strategische meerjarendoelstelling(en) van de Commissie

Verbeteren van de robuustheid van de Europese e-communicatienetwerken

Het Agentschap zal blijven werken aan problemen met de veerkracht door bijv. onderzoeken uit te voeren met betrekking tot de verplichtingen, eisen en goede praktijken op het gebied van veerkracht[15], en door methoden en procedures voor het verbeteren van de veerkracht te analyseren. Er zullen extra proefprojecten worden uitgevoerd om de geldigheid van de eisen, methoden en praktijken te beoordelen. Het Agentschap zal bijdragen tot het verbeteren van de beveiliging en de veerkracht van kritieke communicatie- en informatie-infrastructuur en tot het opbouwen van het pan-Europese publiek-private partnerschap inzake veerkracht en het pan-Europese forum van de lidstaten.

Ontwikkeling en instandhouding van samenwerking tussen de lidstaten

---

13 ABM: Activity Based Management – ABB: Activity Based Budgeting.

14 In de zin van artikel 49, lid 6, onder a) of b), van het Financieel Reglement.

15 Dergelijke onderzoeken bouwen voort op onderzoeken van het ENISA in 2006 en 2007 naar de door de e-communicatiebeheerders uitgevoerde beveiligingsmaatregelen.

Het ENISA moet blijven voortbouwen op zijn inspanningen om Europawijde competentiekringen inzake veiligheid te identificeren over onderwerpen als bewustmaking en reactie op incidenten, samenwerking rond de interoperabiliteit van de pan-Europese e-ID[16] en instandhouding van een platform voor de ondersteuning van de makelaardij in goede praktijken inzake netwerk- en informatiebeveiliging op Europees niveau[17]. Verdere samenwerking tussen de lidstaten moet tot stand worden gebracht om de capaciteiten van alle lidstaten te verbeteren en het algemene coherentie- en interoperabiliteitsniveau te verhogen.

Identificeren van ontluikende, vertrouwensondermijnende risico's

Het Agentschap zal blijven werken aan het opstellen van een kader dat beleidmakers in staat zal stellen ontluikende risico's, die het gevolg zijn van nieuwe technologieën en toepassingen, beter te begrijpen en te beoordelen via systematische gegevensverzameling, -verwerking, -verspreiding en feedback.

Scheppen van informatievertrouwen bij micro-ondernemingen

In het digitale informatietijdperk blijven tal van kansen voor ondernemingen, vooral micro-ondernemingen ontstaan. De verdere ontwikkeling en oppak door de gebruiker van ICT blijft evenwel kwetsbaar. Het doel is de behoeften en verwachtingen van micro-ondernemingen op dit gebied te verzamelen en te beoordelen. Het ENISA zal deze doelstelling nastreven door proefmodellen op te stellen voor grensoverschrijdende samenwerking tussen multipliers en verenigingen op het gebied van capaciteitsopbouw voor netwerk- en informatiebeveiliging, gericht op micro-ondernemingen, door certificeringsregelingen voor micro-ondernemingen en nalevingskaders voor niet-deskundigen op te stellen, door goede praktijken uit te werken en proefprojecten voor deze praktijken op te zetten met het oog op bedrijfscontinuïteit, door werk te maken van nalevingskwesties die het mkb en micro-ondernemingen in staat stellen hun beveiligingsdoelstellingen uit te drukken en stappenplannen op te stellen om deze doelstellingen te verwezenlijken.

1.4.2. Specifieke doelstelling(en) en betrokken ABM/ABB-activiteiten

Specifieke doelstelling

De netwerk- en informatiebeveiliging vergroten, een cultuur van netwerk- en informatiebeveiliging ontwikkelen ten bate van burgers, consumenten, bedrijven en organisaties uit de publieke sector en beleidsuitdagingen ten gevolge van toekomstige netwerken en het internet identificeren.

Betrokken AMB/ABB-activiteit(en)

Beleid inzake elektronische communicatie en netwerkveiligheid

[16] Deze ondersteuning vormt de voortzetting van de werkzaamheden die het ENISA in 2006 en 2007 heeft verricht rond een gemeenschappelijke taal voor het verbeteren van de e-ID-interoperabiliteit.

[17] Dit platform is een vervolg op de werkzaamheden die in 2007 zijn verricht voor het vaststellen van een stappenplan over het opzetten van een makelaardij in goede praktijk inzake netwerk- en informatiebeveiliging op Europees niveau.

1.4.3. Verwachte resulta(a)t(en) en gevolg(en)

Bijdragen tot een hoog niveau van netwerk- en informatiebeveiliging in de Unie en een cultuur van netwerk- en informatiebeveiliging ten behoeve van de burgers, consumenten, bedrijven en organisaties uit de publieke sector in de Europese Unie, en aldus bijdragen tot de goede werking van de interne markt.

1.4.4. Resultaat- en effectindicatoren

Zie 1.4.1 hierboven

1.5. Motivering van het voorstel/initiatief

1.5.1. Behoefte(n) waarin op korte of lange termijn moet worden voorzien

Het ENISA is opgericht in 2004 om bedreigingen van de netwerk- en informatiebeveiliging en mogelijke inbreuken op die beveiliging aan te pakken. Sindsdien zijn de uitdagingen in verband met netwerk- en informatiebeveiliging geëvolueerd door technologische en marktontwikkelingen en zijn ze het voorwerp geweest van verdere beschouwing en debat, waardoor het vandaag mogelijk is nauwkeuriger te beschrijven wat de exacte problemen zijn en hoe deze worden beïnvloed door de veranderingen op het gebied van netwerk- en informatiebeveiliging. In de conclusies van het voorzitterschap van de ministeriële conferentie betreffende de bescherming van kritieke informatie-infrastructuur in Tallinn is met name vermeld dat "de nieuwe en langdurige uitdagingen voor de toekomst vereisen dat het mandaat van het Agentschap (het ENISA) grondig opnieuw wordt bekeken en geformuleerd, zodat het beter is afgestemd op de prioriteiten en behoeften van de Unie, een flexibeler responscapaciteit kan worden opgebouwd, vaardigheden en bekwaamheden kunnen worden ontwikkeld en de operationele efficiëntie en algemene impact van het Agentschap kunnen worden versterkt, teneinde ervoor te zorgen dat het Agentschap een permanente aanwinst wordt voor alle lidstaten en voor de Europese Unie in haar geheel." Samen met dit voorstel stelt de Commissie een verordening inzake het ENISA voor ter vervanging van Verordening (EG) nr. 460/2004; deze verordening voorziet in een grondige herziening van de bepalingen inzake het beheer van het Agentschap en richt het Agentschap op met een looptijd van vijf jaar. De Commissie is zich er echter van bewust dat in het kader van de wetgevingsprocedure met betrekking tot dat voorstel lange besprekingen kunnen plaatsvinden in het Europees Parlement en de Raad, met het mogelijke risico op een juridisch vacuüm als het nieuwe mandaat van het Agentschap niet wordt goedgekeurd vóór het huidige mandaat verstrijkt. Daarom stelt de Commissie de onderhavige verordening voor, waarbij het huidige mandaat van het Agentschap met 18 maanden wordt verlengd, zodat er voldoende tijd is voor de besprekingen.

1.5.2. Toegevoegde waarde van de deelname van de EU

Problemen met netwerk- en informatiebeveiliging stoppen niet aan nationale grenzen en kunnen dus ook niet efficiënt worden aangepakt op nationaal niveau alleen. Tegelijk zijn er grote verschillen in de manier waarop het probleem wordt aangepakt door publieke

autoriteiten in verschillende lidstaten. Deze verschillen kunnen een belangrijke hinderpaal vormen voor de toepassing van passende mechanismen ter verbetering van netwerk- en informatiebeveiliging in de hele Unie. Gezien de verwevenheid van ICT-infrastructuren wordt de effectiviteit van nationale maatregelen in een lidstaat nog steeds in grote mate beïnvloed door maatregelen van een lager niveau in andere lidstaten en door het gebrek aan systematische grensoverschrijdende samenwerking. Een gebrek aan maatregelen voor netwerk- en informatiebeveiliging in één lidstaat kan verstoringen van de dienstverlening in andere lidstaten veroorzaken.

Bovendien leidt de vermenigvuldiging van beveiligingseisen tot kosten voor bedrijven die op Europese schaal actief zijn en tot een versnippering en gebrek aan concurrentievermogen op de Europese interne markt.

De afhankelijkheid van netwerk- en informatiesystemen neemt toe, maar er lijkt onvoldoende bereidheid te zijn om incidenten aan te pakken.

De huidige nationale systemen voor vroegtijdige waarschuwing en aanpak van incidenten vertonen belangrijke gebreken. De procedures en praktijken voor het monitoren en rapporteren van incidenten op het gebied van netwerkbeveiliging verschillen sterk per lidstaat. In sommige landen zijn de procedures onvoldoende geformaliseerd, terwijl er in andere landen geen bevoegde autoriteit is voor het ontvangen en verwerken van verslagen over incidenten. Er bestaan geen Europese systemen. Ten gevolge daarvan kan de basisdienstverlening grondig worden verstoord door incidenten op het gebied van netwerk- en informatiebeveiliging; daarom moeten passende reacties worden voorbereid. In de mededeling van de Commissie betreffende de bescherming van kritieke informatie-infrastructuur wordt ook benadrukt dat er behoefte is aan Europese capaciteit voor vroegtijdige waarschuwing en incidentenrespons, eventueel ondersteund door oefeningen op Europese schaal.

Er is een duidelijke behoefte aan beleidsinstrumenten die erop gericht zijn risico's en kwetsbare plekken met betrekking tot netwerk- en informatiebeveiliging proactief te identificeren, passende responsmechanismen vast te stellen (bijv. via de identificatie en verspreiding van goede praktijken) en te garanderen dat de belanghebbenden deze responsmechanismen kennen en toepassen.

1.5.3. De lessen die uit reeds verrichte soortgelijke activiteiten zijn getrokken

Overeenkomstig artikel 25 van de ENISA-verordening heeft een panel van externe deskundigen in 2006/2007 een evaluatie van het ENISA uitgevoerd om een formele beoordeling van de praktijken, de organisatie en het toepassingsgebied van het Agentschap op te stellen en, voor zover nodig, aanbevelingen te doen voor verbeteringen. Er zij op gewezen dat het ENISA nog maar één jaar operationeel was toen deze evaluatie werd uitgevoerd. Het evaluatieverslag[18] bevestigde de geldigheid van de oorspronkelijke beleidsargumenten achter de oprichting van het ENISA, en stelde punten aan de orde met betrekking tot de zichtbaarheid van het Agentschap en het vermogen van het Agentschap om een grote impact te hebben. Deze punten hadden onder meer betrekking op de organisatiestructuur, de mix van vaardigheden, de omvang van het operationele personeelsbestand van het Agentschap en de organisatorische uitdagingen ten gevolge van de afgelegen locatie.

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

Zie ook punt 1.5.1.

1.5.4. Samenhang en eventuele synergie met andere relevante instrumenten

De toekomst van het ENISA maakte deel uit van het algemene debat over netwerk- en informatiebeveiliging en andere beleidsinitiatieven die gericht zijn op de toekomst van netwerk- en informatiebeveiliging.

1.6. Duur en financiële gevolgen

☑ Voorstel/initiatief met een **beperkte geldigheidsduur**

– ☑ Voorstel/initiatief van kracht vanaf 14.3.2012 tot en met 13.9.2013

– ☑ Financiële gevolgen in 2012 en 2013

☐ Voorstel/initiatief met een **onbeperkte geldigheidsduur**

– Uitvoering met een opstartperiode vanaf JJJJ tot en met JJJJ,

– gevolgd door een volledige uitvoering.

1.7. Beheersvorm(en)[19]

☐ **Direct gecentraliseerd beheer** door de Commissie

☑ **Indirect gecentraliseerd beheer** door uitvoeringstaken te delegeren aan:

– ☐ uitvoerende agentschappen

– ☑ door de Gemeenschappen opgerichte organen[20]

– ☐ nationale publiekrechtelijke organen of organen met een openbaredienstverleningstaak

– ☐ personen aan wie de uitvoering van specifieke acties in het kader van titel V van het Verdrag betreffende de Europese Unie is toevertrouwd en die worden genoemd in het betrokken basisbesluit in de zin van artikel 49 van het Financieel Reglement.

☐ **Gedeeld beheer** met de lidstaten

☐ **Gedecentraliseerd beheer** met derde landen

☐ **Gezamenlijk beheer** met internationale organisaties ***(geef aan welke)***

[19] Nadere gegevens over de beheersvormen en verwijzingen naar het Financieel Reglement zijn beschikbaar op BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[20] In de zin van artikel 185 van het Financieel Reglement.

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

De uitvoerend directeur is verantwoordelijk voor het effectieve toezicht en het toetsen van de prestaties van het Agentschap aan zijn doelstellingen en rapporteert jaarlijks aan de raad van bestuur.

De uitvoerend directeur stelt een algemeen verslag op betreffende alle activiteiten van het Agentschap in het afgelopen jaar, waarin met name de behaalde resultaten worden vergeleken met de doelstellingen van het jaarlijks werkprogramma. Na goedkeuring door de raad van bestuur wordt dit verslag aan het Europees Parlement, de Raad, de Commissie, de Rekenkamer, het Europees Economisch en Sociaal Comité en het Comité van de Regio's toegezonden en gepubliceerd.

2.2. Beheers- en controlesysteem

2.2.1. Geconstateerde risico's

Sinds het ENISA in 2004 is opgericht, werd het aan externe en interne evaluaties onderworpen.

Overeenkomstig artikel 25 van de ENISA-Verordening was de eerste stap in dit proces de onafhankelijke evaluatie van het ENISA door een panel van externe deskundigen in 2006/2007. Het verslag van het panel van externe deskundigen[21] bevestigde dat de oorspronkelijke beleidsredenen voor het oprichten van het ENISA en de oorspronkelijke doelstellingen ervan nog steeds geldig zijn en speelde een rol in het aan de orde stellen van sommige problemen die moeten worden aangepakt.

In maart 2007 heeft de Commissie over de evaluatie verslag uitgebracht aan de raad van bestuur, die vervolgens zelf aanbevelingen heeft gedaan over de toekomst van het Agentschap en over wijzigingen van de ENISA-Verordening[22].

In juni 2007 heeft de Commissie haar eigen beoordeling van de resultaten van de externe evaluatie en de aanbevelingen van de raad van bestuur in een Mededeling aan het Europees Parlement en de Raad voorgelegd[23]. Volgens de Mededeling moet worden gekozen tussen de verlenging van het mandaat van het Agentschap of de vervanging van het Agentschap door een ander mechanisme zoals een permanent forum van stakeholders of een netwerk van organisaties op het gebied van veiligheid. De Mededeling lanceerde ook een publieke

---

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

22 Overeenkomstig artikel 25 van de ENISA-verordening. De volledige tekst van het door de raad van bestuur van het ENISA aangenomen document, dat ook de overwegingen van de raad van bestuur bevat, is beschikbaar op de volgende website: http://enisa.europa.eu/pages/03_02.htm.

23 Mededeling van de Commissie aan het Europees Parlement en de Raad inzake de evaluatie van het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA), COM(2007) 285 definitief van 1.6.2007: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:EN:NOT.

raadpleging over het onderwerp, en vroeg de Europese stakeholders om inbreng aan de hand van een vragenlijst ter oriëntatie van de verdere besprekingen[24].

In 2009 heeft de Commissie een effectbeoordeling opgezet om de opties voor de toekomst van het ENISA te onderzoeken. Deze effectbeoordeling begeleidt het voorstel voor een verordening inzake het ENISA die Verordening (EG) nr. 460/2004 zou vervangen.

2.2.2. Controlemiddel(en)

Zie 2.2.1

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

De rekeningen voor alle uitbestede diensten en studies worden door het personeel van het Agentschap vóór de feitelijke uitbetaling gecontroleerd, met inachtneming van eventuele contractuele verplichtingen, economische beginselen en goede financiële of beheerspraktijken. In alle overeenkomsten en contracten tussen het Agentschap en de begunstigden van eventuele betalingen worden fraudebestrijdingsbepalingen (eisen ten aanzien van toezicht, verslaglegging, enz.) opgenomen.

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

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarige financiële kader en betrokken begrotingsonderde(e)l(en) van de uitgaven

- Bestaande begrotingsonderdelen voor uitgaven

Rubriek van het meerjarige financiële kader	Begrotingsonderdeel	Soort krediet	Bijdrage			
	Nummer / Beschrijving	GK/ NGK (25)	van EVA-landen[26]	van kandidaat-lidstaten[27]	van derde landen	in de zin van artikel 18, lid 1, onder a bis), van het Financieel Reglement
1.a Concurrentievermogen voor groei en werkgelegenheid	09 02 03 01 Europees Agentschap voor netwerk- en informatiebeveiliging – Subsidie op grond van titels 1 en 2	GK	JA	NEE	NEE	NEE
	09 02 03 02 Europees Agentschap voor netwerk- en informatiebeveiliging – Subsidie op grond van titel 3	GK	JA	NEE	NEE	NEE
5 Administratieve uitgaven	09 01 01 Uitgaven voor personeel in actieve dienst voor het beleidsterrein "Informatiemaatschappij en media"	NGK	NEE	NEE	NEE	NEE
	09 01 02 11 Andere beheersuitgaven	NGK	NEE	NEE	NEE	NEE

25 GK = gesplitste kredieten/NGK = niet-gesplitste kredieten.

26 EVA: Europese Vrijhandelsassociatie.

27 Kandidaat-lidstaten en, in voorkomend geval, potentiële kandidaat-lidstaten van de Westelijke Balkan.

3.2. Geraamde gevolgen voor de uitgaven

3.2.1. Samenvatting van de geraamde gevolgen voor de uitgaven

in miljoenen euro's (tot op 3 decimalen)

Rubriek van het meerjarige financiële kader:	1.a	Concurrentiekracht ter bevordering van groei en werkgelegenheid

ENISA			14 maart – 31 dec. 2012	1 jan. – 13 sept. 2013	**TOTAAL**
Beleidskredieten					
09 02 03 02 Europees Agentschap voor netwerk- en informatiebeveiliging – Subsidie op grond van titel 3	Vastleggingen	(1)	2,073	1,734	**3,807**
	Betalingen	(2)	2,073	1,734	**3,807**
Administratieve kredieten					
09 02 03 01 Europees Agentschap voor netwerk- en informatiebeveiliging – Subsidie op grond van titels 1 en 2		(3)	4,600	4,291	**8,891**
TOTAAL kredieten onder Rubriek 1a	Vastleggingen	=1 +3	6,673	6,025	**12,698**
	Betalingen	=2+3	6,673	6,025	**12,698**

• TOTAAL operationele kredieten	Vastleggingen	(4)	2,073	1,734	**3,807**
	Betalingen	(5)	2,073	1,734	**3,807**
• TOTAAL uit het budget van specifieke programma's gefinancierde administratieve kredieten		(6)	4,600	4,291	**8,891**

TOTAAL kredieten onder RUBRIEK 1.a Concurrentievermogen voor groei en werkgelegenheid van het meerjarige financiële kader	Vastleggingen	=4+ 6	6,673	6,025	**12,698**
	Betalingen	=5+ 6	6,673	6,025	**12,698**

in miljoenen euro's (tot op 3 decimalen)

Rubriek van het meerjarige financiële kader:	5	Administratieve uitgaven

		14 maart – 31 dec. 2012	1 jan. – 13 sept. 2013	Totaal
Personele middelen		0,342	0,299	**0,641**
Andere administratieve uitgaven		0,008	0,007	**0,015**
TOTAAL DG INFSO	Kredieten	0,350	0,306	**0,656**

TOTAAL kredieten onder RUBRIEK 5 van het meerjarige financiële kader	(Totaal vastleggingen = totaal betalingen)	0,350	0,306	**0,656**

		14 maart – 31 dec. 2012	1 jan. – 13 sept. 2013	Totaal
TOTAAL kredieten onder RUBRIEKEN 1 tot en met 5 van het meerjarige financiële kader	Vastleggingen	7,023	6,331	**13,354**
	Betaling	7,023	6,331	**13,354**

3.2.2. Geraamde gevolgen voor de beleidskredieten

– ☐ Voor het voorstel/initiatief zijn geen beleidskredieten nodig

– ☑ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

Vastleggingskredieten, in miljoenen euro's (tot op 3 decimalen)

Vermeld doelstellingen en outputs ⇩	14 maart - 31 december 2012	1 januari - 13 september 2013	**TOTAAL**
Verbeteren van de robuustheid van de Europese e-communicatienetwerken	0,237	0,198	**0,435**
Ontwikkeling en instandhouding van samenwerking tussen de	0,237	0,198	**0,435**
Identificeren van opkomende risico's voor het scheppen van	0,169	0,141	**0,310**
Scheppen van informatievertrouwen bij micro-ondernemingen	0,087	0,072	**0,159**
Beheer van horizontale activiteiten	1,344	1,124	**2,468**
TOTALE KOSTEN	2,073	1,734	**3,807**

3.2.3. Geraamde gevolgen voor de administratieve kredieten[28]

3.2.3.1. Samenvatting

– ☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

– ☑ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

a) Administratieve uitgaven onder Rubriek 5 van het meerjarige financiële kader

in miljoenen euro's (tot op 3 decimalen)

RUBRIEK 5 van het meerjarige financiële kader	14 maart – 31 dec. 2012	1 jan. – 13 sept. 2013	**TOTAAL**
Personele middelen	0,342	0,299	**0,641**
Andere administratieve uitgaven	0,008	0,007	**0,015**
TOTAAL	0,350	0,306	**0,656**

b) Administratieve uitgaven met betrekking tot het ENISA - onder begrotingsonderdeel "09.020301 Europees Agentschap voor netwerk- en informatiebeveiliging: Titel 1 – Personeel en Titel 2 – Werking van het Agentschap".

in miljoenen euro's (tot op 3 decimalen)

	14 maart – 31 dec. 2012	1 jan. – 13 sept. 2013	**TOTAAL**
Personele middelen - Titel 1 – Personeel	4,216	3,916	**8,132**
Andere uitgaven van administratieve aard – Titel 2 – Werking van het Agentschap	0,384	0,375	**0,759**
TOTAAL	**4,600**	**4,291**	**8,891**

[28] De bijlage bij het financieel memorandum is niet ingevuld omdat ze niet van toepassing is op het huidige voorstel.

3.2.3.2. Geraamde personeelsbehoeften

– ☐ Voor het voorstel/initiatief zijn geen personele middelen nodig

– ☑ Voor het voorstel/initiatief zijn personele middelen nodig, zoals hieronder nader wordt beschreven:

a) Personele middelen binnen de Commissie

	14 maart – 31 dec. 2012	1 jan. – 13 sept. 2013
Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen) (in voltijdequivalenten, VTE)		
XX 01 01 01 (zetel en vertegenwoordigingen van de Commissie)	3,5	3,5
TOTAAL	**3,5**	**3,5**

b) Personele middelen van het ENISA

		14 maart – 31 dec. 2012	1 jan. – 13 sept. 2013
Lijst van het aantal ambten van het ENISA (in voltijdequivalent, VTE)			
Ambtenaren en tijdelijk personeel	**AD**	29	29
	AST	15	15
TOTAAL Ambtenaren en tijdelijk personeel		44	44
Ander personeel (in VTE)			
Arbeidscontractanten		**13**	**13**
Gedetacheerde nationaal deskundigen		**5**	**5**
TOTAAL ander personeel		**18**	**18**
TOTAAL		**62**	**62**

Beschrijving van de taken die het personeel van het Agentschap moet uitvoeren:

Ambtenaren en tijdelijke functionarissen	Het Agentschap blijft verder: – adviserende en coördinerende functies vervullen voor zover het **gegevens** over informatiebeveiliging **verzamelt en analyseert**. Tegenwoordig verzamelen zowel openbare als particuliere instellingen met uiteenlopende bedoelingen gegevens over IT-incidenten en andere gegevens die relevant zijn voor informatiebeveiliging. Er is echter geen centrale entiteit op Europees niveau die algemeen gegevens kan verzamelen en analyseren en opinies en advies kan verstrekken voor het ondersteunen van het beleidswerk van de Unie inzake netwerk- en informatiebeveiliging; – **optreden** als een **centrum van deskundigheid** waartoe zowel de lidstaten als de Europese instellingen zich kunnen wenden voor **opinies en advies over technische aangelegenheden** betreffende beveiliging; – bijdragen tot **brede samenwerking tussen verschillende actoren** op het gebied van informatiebeveiliging, bijv. assistentie verlenen bij de vervolgactiviteiten ter ondersteuning van beveiligd e-zakendoen. Dergelijke samenwerking is een essentiële eerste voorwaarde voor een veilige werking van netwerken en informatiesystemen in Europa. Deelname en betrokkenheid van alle stakeholders is nodig; – bijdragen tot een gecoördineerde aanpak van informatiebeveiliging door **ondersteuning van lidstaten**, bijv. inzake de **bevordering van risicobeoordeling** en bewustmakingsactiviteiten; – de **interoperabiliteit van netwerken en informatiesystemen** waarborgen wanneer lidstaten technische eisen **toepassen** die van invloed zijn op de veiligheid; – de **relevante normaliseringseisen** identificeren, bestaande beveiligingsnormen en certificeringssystemen beoordelen en het gebruik op zo breed mogelijke schaal ervan ter ondersteuning van de Europese wetgeving bevorderen; – **internationale samenwerking** op dit gebied ondersteunen, die steeds meer nodig is aangezien netwerk- en informatiebeveiligingsproblemen een mondiaal karakter hebben.
Extern personeel	– Zie hoger

3.2.4. Verenigbaarheid met het huidige meerjarige financiële kader

– ☑ Het voorstel/initiatief is verenigbaar met het huidige meerjarige financiële kader

– ☐ Het voorstel/initiatief vergt herprogrammering van de betrokken rubriek van het meerjarige financiële kader

– ☐ Het voorstel/initiatief vergt toepassing van het flexibiliteitsinstrument of herziening van het meerjarige financiële kader[29]

3.2.5. Bijdrage van derden aan de financiering

– ☐ Het voorstel/initiatief voorziet niet in medefinanciering door derden

– ☑ Het voorstel/initiatief voorziet in medefinanciering, zoals hieronder wordt geraamd (van toepassing op de begrotingsonderdelen 09.020301 en 09.020302):

Indicatieve kredieten, in miljoen euro (tot op 3 decimalen)

	14 maart – 31 dec. 2012	1 jan. – 13 sept. 2013	Totaal
EVA	0,160	0,145	0,305

3.3. Geraamde gevolgen voor de ontvangsten

– ☑ Het voorstel/initiatief heeft geen financiële gevolgen voor de ontvangsten

– ☐ Het voorstel/initiatief heeft de hieronder beschreven financiële gevolgen:

  – ☐ voor de eigen middelen

  – ☐ voor de diverse ontvangsten

[29] Zie de punten 19 en 24 van het Interinstitutioneel Akkoord.