Fiche 2: Verordening agentschap ENISA en Europees kader voor cyberbeveiligingscertificering

1. Algemene gegevens

a) Titel voorstel
Verordening inzake ENISA, het agentschap van de Europese Unie voor cyberbeveiliging, tot intrekking van Verordening (EU) nr. 526/2013, en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie (de "cyberbeveiligingsverordening")

b) Datum ontvangst Commissiedocument
13 september 2017

c) Nr. Commissiedocument
COM (2017) 477

d) EUR-Lex
http://eur-lex.europa.eu/resource.html?uri=cellar:1985b4b4-985e-11e7-b92d-01aa75ed71a1.0001.02/DOC_1&format=PDF

e) Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing
SWD (2017) 500

f) Behandelingstraject Raad
Raad Justitie en Binnenlandse Zaken

g) Eerstverantwoordelijk ministerie
Ministerie van Veiligheid en Justitie en Ministerie van Economische Zaken

h) Rechtsbasis
Art. 114 VWEU

i) Besluitvormingsprocedure Raad
Gekwalificeerde meerderheid in de Raad

j) Rol Europees Parlement
Medebeslissing door het Europees Parlement

2. Essentie voorstel

a) Inhoud voorstel

De voorgestelde verordening bestaat uit twee delen:

- Een versterking van de rol van het EU Agentschap voor Netwerk- en Informatiebeveiliging (ENISA)
- De oprichting van een Europees kader voor cyberbeveiligingscertificering

ENISA

Het agentschap ENISA is in 2004 opgericht met het doel het waarborgen van een hoog niveau van netwerk- en informatiebeveiliging binnen de EU. Dit mandaat is verschillende malen verlengd en in 2013 is een nieuw mandaat voor een periode van zeven jaar aangenomen. Het agentschap ENISA ondersteunt Europese instituties, lidstaten en private bedrijven in het adresseren van, reageren op en het voorkomen van problemen op het gebied van netwerk- en informatiebeveiliging door verschillende activiteiten op vijf gebieden: expertise, beleid, capaciteit, gemeenschap en het creëren van mogelijkheden.

In reactie op de toegenomen digitale dreiging tegen de EU en diens economieën, democratische vrijheden en waarden en de adoptie van de Europese richtlijn voor Netwerk- en Informatiebeveiligingsrichtlijn (NIS-richtlijn)[1] wordt in het nieuwe mandaat voorgesteld om de rol van ENISA te versterken langs een drietal lijnen:

1) Permanente en centrale rol in het Europese cybersecurity ecosysteem
   In dit kader wordt voorgesteld om ENISA een permanent en uitgebreider mandaat te geven, waardoor het agentschap een centrale en sterke rol zal innemen in het Europese cybersecurity ecosysteem. In het voorstel krijgt ENISA onder meer de taak om Europese beleidsontwikkeling op cybersecuritygebied te ondersteunen en lidstaten te adviseren bij de implementatie van de Europese NIS-richtlijn.
2) Operationele taken
   Om specifieke dreigingen actief het hoofd te kunnen bieden zet de Commissie daarnaast in op het toekennen van ondersteunende operationele taken aan ENISA. De Commissie stelt onder meer voor dat ENISA gestructureerde samenwerking met het Computer Emergency Response Team (CERT) voor de Europese instituties, agentschappen en organen, CERT-EU, aangaat, waarbij het lidstaten kan ondersteunen bij uitvoeren van operationele analyses en op verzoek van lidstaten ex-post technisch onderzoek kan verrichten.
3) Een centrale rol in het Europees kader voor cyberbeveiligingscertificering
   Ten aanzien van certificering stelt de Commissie voor om ENISA een drietal taken uit te laten voeren ten behoeve van het ondersteunen en stimuleren van de implementatie van cybersecurity certificering van producten en diensten: voorbereiden van concept certificeringsschema's, ondersteuning van de Commissie bij het voeren van het

[1] Richtlijn (EU) 2016/1148 voor een hoog gemeenschappelijk niveau van network- en informatiebeveiliging (NIS-richtlijn)

secretariaat van de Europese Cybersecurity Certificering Groep (ECCG) en liaison met standaardisatie organisaties om juist gebruik van standaarden te garanderen en gebieden te identificeren waar additionele cybersecurity standaarden vereist zijn.

Certificering

Het voorstel heeft als doel te komen tot de oprichting van een Europees kader voor cyberbeveiligingscertificering voor ICT-producten en –diensten. Binnen het kader zal de Commissie, op voorstel van ENISA en na consultatie met stakeholders (inclusief lidstaten), certificeringsschema's vaststellen die EU-breed gebruikt worden. Producten en diensten die zijn gecertificeerd op basis van een vastgesteld certificeringsschema worden daarmee, op een omschreven beveiligingsniveau, weerbaar geacht tegen acties gericht op het aantasten van de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van data of de functionaliteiten en diensten die worden aangeboden. De beveiligingsniveaus en aanvullende elementen die in een schema thuishoren worden in de verordening vastgesteld.

Wanneer er voor een product of dienst een Europees certificeringsschema wordt vastgesteld zullen bestaande nationale schema's vervallen. Tevens is het lidstaten niet toegestaan om schema's in te richten voor producten en diensten waarvoor reeds een Europees certificeringsschema bestaat. Lidstaten zijn verplicht certificaten te erkennen die zijn uitgegeven in andere lidstaten. Een certificaat op basis van een Europees certificeringsschema kan ook gebruikt gaan worden om een vermoeden van overeenstemming met bepaalde wettelijke eisen in Europese dan wel nationale regelgeving aan te tonen.

Naast de inhoudelijke eisen voor schema's, komt de verordening ook tot de oprichting van een EU-breed bestuurlijk kader waarbinnen de vaststelling van certificeringsschema's tot stand moet gaan komen. De Commissie zal hierbinnen, zoals aangegeven, een centrale plaats innemen. De Commissie heeft verschillende rollen. Zo is de Commissie opdrachtgever van ENISA, stelt het de EU-brede schema's vast en is tevens voorzitter en secretaris van de Europese Cybersecurity Certificering Groep. In deze ECCG zullen de nationale certificeringstoezichthouders zitting hebben. De ECCG heeft een adviserende en ondersteunende rol voor de Commissie en kan voorstellen doen aan de Commissie voor de ontwikkeling van een schema.

Het instellen van bovengenoemde nationale certificeringstoezichthouders is een van de verplichtingen die de verordening voorstelt voor lidstaten. Een nationale toezichthouder zal verantwoordelijk worden voor toezicht op de uitvoering en toepassing van certificeringsschema's in het eigen land en op de conformiteitsbeoordelingsinstanties die de certificering zullen uitvoeren. De conformiteitsbeoordelingsinstanties, moeten worden geaccrediteerd door de nationale accreditatie-instantie in een lidstaat. In Nederland is dat de Raad voor Accreditatie.

De verordening stelt geen verplichtingen in voor het bedrijfsleven. Het aanvragen van certificering door bedrijven voor hun producten en/of diensten gebeurt op vrijwillige basis, tenzij anders voorgeschreven door EU- of nationale wetgeving.

b) Impact assessment Commissie

De conclusie die volgens de Commissie uit de impact assessment naar voren komt is dat ENISA een permanent karakter moet krijgen en dat de uitwerking van een Europees netwerk voor certificering gewenst is. ENISA kan ondersteuning geven op terreinen waar zij volgens de Commissie toegevoegde waarde heeft, zoals bij de implementatie van de NIS-richtlijn en operationele samenwerking. Bovendien kan ENISA het administratieve en technische management op zich nemen van het kader voor cyberbeveiligingscertificering. Door dit kader worden certificaten binnen alle lidstaten erkend, wat volgens de Commissie bevorderlijk werkt voor zowel het niveau van cybersecurity als voor de digitale interne markt.

3. Nederlandse positie ten aanzien van het voorstel

a) *Essentie Nederlands beleid op dit terrein*

Nederland is als open en internationaal georiënteerde economie gebaat bij een stabiel en vrij toegankelijk cyberdomein. Hiertoe zet Nederland samen met zijn internationale partners en door middel van effectieve Multi stakeholder samenwerking in op een veilig en open cyberdomein, waarin de kansen die digitalisering onze economie en samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd.

De samenhang tussen veiligheid, vrijheid en maatschappelijke groei wordt hiertoe, in een dynamische balans, tot stand gebracht in een constante open en pragmatische dialoog tussen alle stakeholders, waaronder overheden, bedrijven, het maatschappelijke middenveld, academici en de technische gemeenschap, zowel nationaal als internationaal. De concrete uitwerking van deze visie op het gebied van digitale veiligheid is vastgelegd in de Nederlandse Nationale Cyber Security Strategie 2 (NCSS2) uit 2013.[2] Gezien het inherent grensoverschrijdende karakter van cyberbeveiliging en cyberdreiging staat Europese en internationale samenwerking in de Nederlandse aanpak centraal.

Nederland zet in op een verdere integratie en versterking van de Digitale Interne Markt. Vertrouwen van bedrijven en consumenten in de veiligheid van deze markt is hiervoor essentieel. Hiertoe werkt Nederland in mondiaal en in EU-verband mee aan het ontwikkelen van normen, standaarden en een certificeringsstelsel met wederzijdse erkenning. Dit laatste gebeurt bijvoorbeeld binnen de SOG-IS overeenkomst. SOG-IS MRA (Senior Officials Group for Information Security Mutual Recognition Agreement) is een overeenkomst tussen 14 landen[3] op het gebied van wederzijdse erkenning van certificaten voor informatiebeveiligingsproducten. Ook werkt de Nederlandse overheid als toezichthouder samen met de private sector om beveiligingscertificaten uit te geven voor cyberproducten in de overheidssector. In de Nationale Cybersecurity Strategie

[2] Nationale Cyber Security Strategie 2 (https://www.ncsc.nl/organisatie/nationale+cybersecurity+strategie)
[3] Duitsland, Estland, Finland, Frankrijk, Italië, Kroatië, Luxemburg, Nederland, Noorwegen, Oostenrijk, Polen, Spanje, Verenigd Koninkrijk en Zweden,

uit 2013 is ingezet op certificering en diplomering van informatiebeveiligers.

b) *Beoordeling + inzet ten aanzien van dit voorstel*

ENISA

ENISA is een belangrijke speler in het Europese cyberlandschap en het aantal taken van ENISA is uitgebreid binnen de door het vorige mandaat gezette kaders. Onder meer door de inwerkingtreding van de NIS-richtlijn en het secretariaat van het Europese netwerk van computer security incident response teams, CSIRTs Network, dat met de adoptie van de NIS-richtlijn is opgericht. Dit is ook gebleken uit de evaluatie van ENISA. Nederland staat dan ook positief tegenover het voorstel voor een permanent mandaat.

De toegevoegde waarden van het agentschap zitten in capaciteitsopbouw, het leveren van expertise over producten en het faciliteren en ondersteunen van (multilaterale) activiteiten. Daarbij valt te denken aan onder meer de implementatie van de NIS-richtlijn, het organiseren van de jaarlijkse Europese cyberoefeningen en het secretariaat van het CSIRTs Network. Bovendien is Nederland positief over de expliciete rol van ENISA in het bevorderen van publiek-private samenwerking in Europa middels het faciliteren van sectorale Information Sharing and Analysis Centres (ISACs).

Nederland zal in de onderhandelingen scherp zijn op plannen die strijdig zijn met de verdragsrechtelijke afspraken betreffende de bevoegdheid van lidstaten op het gebied van nationale veiligheid, omdat de verantwoordelijkheid voor hun nationale veiligheid bij de lidstaten zelf ligt. Mede vanuit dit oogpunt heeft Nederland een negatieve grondhouding ten opzichte van operationele taken voor ENISA met name als deze zich ontwikkelen tot CSIRT-functionaliteiten, zoals het zelfstandig monitoren van- en plegen van respons op incidenten, omdat dit een verantwoordelijkheid betreft van nationale lidstaten. Mede daarom zal Nederland kritisch zijn ten opzichte van de voorgestelde operationele samenwerking tussen ENISA en CERT-EU.

Daarnaast zal Nederland inzetten op zoveel als mogelijk gebruik maken van- en aansluiting zoeken bij reeds bestaande netwerken, structuren, organisaties, initiatieven en mechanismen. Het CSIRTs Network is een centraal gremium hiervoor. In dit verband zal het voorgestelde nieuw op te richten Europees onderzoeks- en kenniscentrum voor cyberbeveiliging en de relatie van dit instituut met ENISA kritisch worden beschouwd.

Ten aanzien van de rol van ENISA op het gebied van certificering zal benadrukt worden dat dit zeer specifieke expertise vereist waarbij Nederland geen rol ziet voor ENISA op het gebied van de goedkeuring van high-assurance producten welke ingezet worden ten behoeve van de nationale veiligheid. Daarnaast mogen de extra taken met betrekking tot certificering haar andere taken en bevoegdheden van ENISA niet in de weg zitten.

Certificering

Het voorstel sluit aan bij de Nederlandse inzet op het gebied van de digitale interne markt en certificering. Het is de Nederlandse inschatting dat het voorstel kan bijdragen aan het versterken van vertrouwen van burgers en bedrijven in de veiligheid van producten en de kwaliteit van aangeboden diensten. De schaalvergroting die optreedt door ontwikkeling van Europees geharmoniseerde certificeringsschema's kan certificering op EU-niveau efficiënter en goedkoper maken. Daarmee is het tevens een kans voor Nederlandse certificeringsinstanties, wiens markt nu in potentie groter wordt. Een dergelijke samenhangende EU-brede benadering van certificering moet daarbij geen uitsluitende werking hebben voor niet-EU-aanbieders.

Wat betreft de inrichting van het voorgestelde kader voor cyberbeveiligingscertificering en de actoren en hun onderlinge relatie is het kabinet kritischer. Het kabinet mist hierin een aanpak die voortbouwt op de jarenlange ervaring en expertise van bestaande certificeringsinstellingen en een meer 'bottom up' aanpak met stakeholders. Daarnaast is voldoende ruimte nodig voor lidstaten om eigen eisen te kunnen blijven stellen en controles te kunnen uitvoeren als het gaat om producten en diensten die van belang zijn voor de nationale veiligheid.

Het kabinet zal inzetten op zoveel mogelijk behoud van invloed en beleidsautonomie en –flexibiliteit van de lidstaten bij de certificering van producten en diensten. In de huidige voorgestelde structuren worden de lidstaten vooral in een adviserende en ondersteunende rol gepositioneerd. Medezeggenschap in de besluitvorming door de lidstaten over EU-brede schema's, en behoud van nationale ruimte om eigen eisen te mogen stellen in het kader van nationale veiligheid wordt een belangrijke inzet van het kabinet.

In het voorstel wordt onvoldoende onderscheid gemaakt tussen de verschillende veiligheidsniveaus van producten. Voor Nederland is ruimte voor flexibiliteit en maatwerk van belang. High-assurance producten en diensten moeten aan hogere certificeringseisen voldoen. NL zet in op het behoud en integreren van de bestaande SOG-IS samenwerking op het gebied van certificering van beveiligingsproducten, waarbij de kennis, expertise en samenwerking met de (internationale) industrie wordt gehandhaafd en geïntensiveerd.

De voorgestelde verordening richt zich primair op een stelsel dat verplichtingen met zich meebrengt voor lidstaten (zoals het instellen van een certificeringstoezichthouder). De rol van de private sector in het werken met en inrichten van stelsels is onderbelicht. Met inachtneming van het uitgangspunt dat verdere versterking van cyberbeveiliging op Europees niveau noodzakelijk is, is de betrokkenheid van de private sector bij de ontwikkeling van certificatieschema's van belang voor voldoende draagvlak wat bijdraagt aan de acceptatie en het gebruik van de certificeringsschema's door de markt, zoals is gebleken in het kader van de SOG-IS. Ook zorgt de ontwikkeling van certificatieschema's in samenwerking met de private sector voor economische kansen. Dergelijke publiek-private samenwerking past binnen de Nederlandse beleidsvisie op cybersecurity. Een sterkere borging van deze samenwerking in de verordening wordt daarom nagestreefd.

Het kabinet is van mening dat in eerste instantie de kwaliteit van en het draagvlak voor de Europese certificatieschema's ertoe moet leiden dat partijen gebruik maken van de Europese certificatieschema's en de daarop gebaseerde certificaten. Het kabinet zet vraagtekens bij de verplichting in het voorstel dat bestaande nationale schema's vervallen wanneer een Europees certificeringsschema wordt vastgesteld. Voorts zal het kabinet inzetten op de verbetering van de onvolkomenheden in het voorstel van technische aard in relatie tot onder meer de Europese verordening over accreditatie.

c) Eerste inschatting van krachtenveld

Van de lidstaten wordt een positieve grondhouding verwacht ten aanzien van een permanent mandaat voor ENISA. Naast Nederland zullen ook andere lidstaten kritisch zijn ten opzichte van een operationele rol voor ENISA. De verwachting is dat in lijn met de Nederlandse inzet, andere lidstaten aandacht zullen vragen voor het belang van nationale bevoegdheden.

Nederland verwacht in de Raad een positieve grondhouding van de lidstaten voor het versterken van de cyberbeveiliging in de EU onder meer door certificering van producten en diensten. Daarbij wordt tevens verwacht dat er medestanders zijn van de Nederlandse bezwaren en aandachtspunten wat betreft high-assurance producten voor de nationale veiligheid, beleidsautonomie voor lidstaten bij het certificeren van producten en diensten, goed bestuur en het belang van het overeind houden van bestaande schema's, waaronder de schema's vallende onder de SOG-IS overeenkomst.

4. Beoordeling bevoegdheid, subsidiariteit en proportionaliteit

a) Bevoegdheid

De voorgestelde bevoegdheidsgrondslag is artikel 114 VWEU. Dit artikel geeft de EU de bevoegdheid tot harmonisatie van nationale wetgeving die de instelling en de goede werking van de interne markt betreft. Het betreft een gedeelde bevoegdheid tussen de EU en de lidstaten (artikel 4, lid 2, onder a, VWEU). Het kabinet acht dit de juiste rechtsgrondslag voor het voorstel.

Een aantal van de in de voorgestelde verordening opgenomen elementen, met name de certificering van producten raken aan de nationale veiligheid. Op grond van artikel 4, lid 2, VEU dient de Unie de essentiële staatsfuncties, zoals de bescherming van de nationale veiligheid te eerbiedigen. Met name de nationale veiligheid blijft de uitsluitende verantwoordelijkheid van elke lidstaat. In de uitwerking zal daarom nauwgezet moeten worden gekeken of de Unie haar bevoegdheden niet overschrijdt.

b) Subsidiariteit

Nederland heeft een positief oordeel ten aanzien van de subsidiariteit van het voorstel gezien het inherent grensoverschrijdende karakter van cyberbeveiliging en cyberdreiging met een negatieve kanttekening ten aanzien van de operationele taken van ENISA, onder meer omdat het onderling

samenwerken en rechtstreeks uitwisselen van operationele informatie een nationale aangelegenheid is. Ten aanzien van het certificeringsraamwerk zijn de voordelen van schaalvergroting het grootst wanneer certificaten EU-breed gelden en de Digitale Interne Markt wordt hierdoor versterkt.

c) Proportionaliteit

Ten aanzien van het nieuwe mandaat van ENISA heeft Nederland een positief oordeel aangaande de proportionaliteit. Het vergroten van de rol van ENISA zoals voorgesteld door de Commissie wordt beoordeeld als een geschikt en effectief middel om de cyberbeveiliging op Europees niveau naar een hoger niveau te brengen. Door uitbreiding van ENISA kan het agentschap meer capaciteit en expertise ontwikkelen, waardoor betere ondersteuning mogelijk wordt.

Nederland acht het voorstel voor een Europees-breed certificeringsraamwerk proportioneel. Het raamwerk zal bijdragen aan de verbetering van de Europese cyberbeveiliging en tegelijkertijd de Digitale Interne Markt versterken. Het is hierin belangrijk dat gebruik wordt gemaakt van bestaande certificeringsstructuren en ervaring en expertise van lidstaten op dit gebied om dubbelingen en overlap te voorkomen en om zo een effectief en adequaat raamwerk te ontwikkelen.

5. Financiële implicaties, gevolgen voor regeldruk en administratieve lasten

a) Consequenties EU-begroting

Nederland is van mening dat de benodigde EU-middelen zoals gemeld in het voorstel gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2014-2020 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting en de gemeenschappelijke aanpak inzake gedecentraliseerde EU-agentschappen. Daarnaast moet een eventuele verhoging van het aantal werknemers elders worden gecompenseerd, in lijn met de Nederlandse visie op de afspraken over stafreductie uit de inter-institutionele overeenkomst (IIA) bij het Meerjarig Financieel Kader (MFK). Nederland wil niet vooruitlopen op de omvang en inhoud van het volgende MFK (na 2020). De uitvoerend directeur van ENISA wordt aangesteld voor een periode van 5 jaar met een optie om te verlengen voor nog eens 5 jaar. Aangezien vanaf een ambtstermijn van 10 jaar een langlopende pensioenverplichting in de Europese begroting ontstaat, wil Nederland de tweede termijn van de uitvoerend directeur beperken tot 4 jaar.

b) Financiële consequenties (incl. personele) voor Rijksoverheid en/ of decentrale overheden

Door het verplichtende karakter van onder meer het hebben van een certificeringstoezichthouder per lidstaat ontstaat naar verwachting de noodzaak tot een personele uitbreiding van de Rijksoverheid op dit terrein. Hierbij wordt gekeken hoe efficiënt van bestaande kennis en expertise binnen de Rijksoverheid gebruik kan worden gemaakt. Voor decentrale overheden worden geen consequenties verwacht. Eventuele budgettaire gevolgen worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.

c) Financiële consequenties (incl. personele) voor bedrijfsleven en burger

Het certificeren van producten en diensten zal enige kosten met zich meebrengen voor het bedrijfsleven. De voorgestelde certificering is echter niet verplicht, tenzij nationale of Europese wetsbepalingen anders bepaalt. Een bedrijf kan zelf de afweging maken of het voor hen van toegevoegde waarde is.

d) Gevolgen voor regeldruk/administratieve lasten voor Rijksoverheid, decentrale overheden, bedrijfsleven en burger

Het instellen van een certificeringstoezichthouder en daarmee het toezicht houden op het certificeringsproces zal extra administratieve lasten met zich meebrengen voor de Rijksoverheid. De rol van de Rijksoverheid blijft daarbij beperkt tot internationale afstemming over certificering en het houden van toezicht (inclusief de behandeling van individuele klachten en het zo nodig opleggen van sancties).

Vanwege het voorgestelde voor bedrijven niet-verplichte karakter van het kader voor cyberbeveiligingscertificering leidt de verordening niet tot extra regeldruk voor het bedrijfsleven, tenzij nationale of Europese wetsbepalingen anders bepalen. Voor decentrale overheden en burgers zijn geen administratieve lasten voorzien.

e) Gevolgen voor concurrentiekracht

Vanwege het EU-brede en niet-verplichtende karakter worden positieve consequenties verwacht voor de Nederlandse concurrentiekracht. Door de voorgestane versterkte integratie is de verwachting dat Nederlandse bedrijven en certificeringsinstanties gemakkelijker toegang tot en aansluiting bij de Europese markt vinden.

6. Implicaties juridisch

a) Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)

De verordening is rechtstreeks toepasselijk in de lidstaten. De volledige en effectieve toepassing van de verordening vereist echter dat er nationale uitvoeringsmaatregelen getroffen worden. De verordening verplicht elke lidstaat om één instantie aan te wijzen (of op te richten) die toezicht houdt op certificerende instellingen (de vraag of certificaten terecht zijn verstrekt) en op houders van certificaten (de vraag of producten en diensten voldoen aan het certificatieschema). Deze toezichthouder moet onafhankelijk zijn van de organisaties waarop hij toezicht houdt. De toezichthouder moet bevoegd zijn om informatie te vorderen, gegevens over mogelijke niet-naleving te verstrekken aan andere toezichthoudende instanties, audits uit te voeren, naleving af te dwingen, binnen te treden in panden van certificeerders en certificaathouders, certificaten in te trekken en sancties op te leggen. Dit zijn ingrijpende overheidsbevoegdheden. Ook moet de toezichthouder klachten behandelen van natuurlijke en rechtspersonen over verstrekte certificaten. Bij de verdere implementatie zal worden bezien hoe de taken en bevoegdheden van de door de verordening vereiste nationale toezichthouder zich verhouden tot de taken en

bevoegdheden van de Stichting Raad voor Accreditatie. Daarbij zal ook worden betrokken dat de verordening de mogelijkheid kent dat voor bepaalde cybersecuritycertificaten wordt voorgeschreven dat zij alleen verstrekt mogen worden door een overheidsinstantie ("public body", art. 48 lid 4).

b) Gedelegeerde en/of uitvoeringshandelingen, incl. NL-beoordeling daarvan

Het voorstel kent twee bepalingen waarin aan de Commissie de bevoegdheid wordt toegekend om uitvoeringshandelingen vast te stellen. Artikel 44 kent de Commissie de bevoegdheid toe om certificeringsschema's vast te stellen (op voorstel van ENISA en door middel van de onderzoeksprocedure). Artikel 52 geeft de Commissie de bevoegdheid (door middel van de onderzoeksprocedure) om nadere regels te stellen over het aanmelden, door de nationale toezichthouder bij de Commissie, van de door die lidstaat erkende certificeerders.
Het kabinet kan instemmen met de voorgestelde uitvoeringsbevoegdheden omdat deze erop gericht zijn eenvormige voorwaarden te waarborgen voor de uitvoering van de verordening.
De keuze voor de onderzoeksprocedure acht het kabinet geschikt omdat het hier gaat om handelingen van algemene strekking (de regels over het aanmelden die vastgesteld moeten worden gelden immers voor alle nationale toezichthouders).

c) Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en besluiten) met commentaar t.a.v. haalbaarheid

De verordening treedt in werking op de twintigste dag na de dag van publicatie. Om de verordening in Nederland te kunnen uitvoeren is formele wetgeving vereist. Daarvoor is doorgaans minstens anderhalf jaar nodig. Vervolgens moet wellicht een nieuwe overheidsinstantie worden opgericht en bemenst (de toezichthouder). Het in het voorstel opgenomen tijdpad is dan ook niet realistisch.

d) Wenselijkheid evaluatie-/horizonbepaling

De verordening bepaalt dat de Commissie de verordening iedere vijf jaar evalueert (art. 56) en dat die evaluatie ertoe kan leiden dat de Commissie voorstelt om de taken van ENISA te wijzigen of om ENISA op te heffen.

7. Implicaties voor uitvoering en/of handhaving

De toezichthouder moet bevoegd zijn "to impose penalties". Volgens de verklaring van de Raad van 27 april 2006, PbEU 2006, L 114, moet de term "penalties" in rechtsinstrumenten van de EU vertaald worden als "sancties". Zo gelezen vereist de verordening *niet* dat de toezichthouder bevoegd is om punitieve sancties op te leggen (zoals een bestuurlijke boete of bijvoorbeeld een punitief bedoelde intrekking van een erkenning) en staat zij ook bestuursrechtelijke herstelsancties toe. De verordening laat ook ruimte voor strafrechtelijke handhaving.

8. Implicaties voor ontwikkelingslanden

Geen.