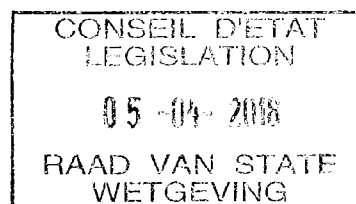


MIJ BEKEND :

: VU



63296/4

Wetsontwerp tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.	Projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.
Titel 1. - Definities en algemene bepalingen	Titre 1er. - Définitions et dispositions générales
Hoofdstuk 1. Onderwerp en toepassingsgebied	Chapitre 1er. Objet et champ d'application
Afdeling 1. Onderwerp	Section 1. Objet
Art. 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.	Art. 1. La présente loi règle une matière visée à l'article 74 de la Constitution.
Art. 2. Deze wet voorziet in de omzetting van de Europese richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, hierna de "NIS-richtlijn" genoemd.	Art. 2. La présente loi vise à transposer la directive européenne (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, ci-après dénommée la "directive NIS".
Afdeling 2. Toepassingsgebied	Section 2. Champ d'application
Art. 3. § 1. Deze wet is van toepassing op de aanbieders van essentiële diensten, zoals gedefinieerd in artikel 6, 11°, die minstens één vestiging op Belgisch grondgebied hebben en daadwerkelijk een activiteit uitoefenen die betrekking heeft op de verlening van minstens één essentiële dienst op Belgisch grondgebied. § 2. Deze wet is van toepassing op de digitaaldienstverleners, zoals gedefinieerd in artikel 6, 20°, die hun hoofdvestiging in België hebben. Een digitaaldienstverlener wordt geacht zijn hoofdvestiging in België te hebben als zijn hoofdkantoor zich daar bevindt.	Art. 3. § 1er. La présente loi s'applique aux opérateurs de services essentiels, tels que définis à l'article 6, 11°, ayant au moins un établissement sur le territoire belge et exerçant effectivement une activité liée à la fourniture d'au moins un service essentiel sur le territoire belge. § 2. La présente loi s'applique aux fournisseurs de service numérique, tels que définis à l'article 6, 20°, dont l'établissement principal est situé en Belgique. Un fournisseur de service numérique est réputé avoir son établissement principal en Belgique lorsque son siège social s'y trouve.

Deze wet is ook van toepassing op de digitaaldienstverleners die niet in de Europese Unie gevestigd zijn wanneer zij in België diensten verlenen als bedoeld in bijlage III en hun vertegenwoordiger in België gevestigd is in het kader van de NIS-richtlijn.	La présente loi est également applicable aux fournisseurs de service numérique qui ne disposent pas d'un établissement dans l'Union européenne lorsque ceux-ci fournissent en Belgique des services visés à l'annexe III et qu'ils établissent en Belgique leur représentant pour les besoins de la directive NIS.
Art. 4. § 1. De beveiligings- en meldingseisen bedoeld in deze wet zijn niet van toepassing op ondernemingen die onderworpen zijn aan de eisen van de artikelen 114 en 114/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, wat hun activiteiten betreft op het gebied van het aanbieden van openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten, en op verleners van vertrouwensdiensten die onderworpen zijn aan de eisen van artikel 19 van de Europese verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, wat hun activiteiten inzake vertrouwensdiensten betreft. § 2. Deze wet is niet van toepassing op de aanbieders die behoren tot de sector financiën in de zin van bijlage II van de wet. Er wordt een uitzondering gemaakt in het vorige lid voor de bepalingen van titel I, van hoofdstuk 1 van titel II, en van artikel 17, §§ 2 en 3, van deze wet. In afwijking van het eerste lid is artikel 27 van deze wet van toepassing op de aanbieders die behoren tot de sector financiën in de zin van bijlage II van de wet, met uitzondering van de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU. § 3. Wanneer een sectorspecifieke rechtshandeling van de Europese Unie vereist dat aanbieders van essentiële diensten of digitaaldienstverleners zorgen voor de beveiliging van hun netwerk- en informatiesystemen of voor de melding van incidenten, en op voorwaarde dat die eisen ten minste feitelijk gelijkwaardig zijn aan de verplichtingen van deze wet, kunnen de bepalingen betreffende de beveiliging van netwerk- en informatiesystemen en de melding van incidenten van deze handeling afwijken van de bepalingen van deze wet.	Art. 4. § 1. Les exigences en matière de sécurité et de notification prévues par la présente loi ne s'appliquent pas, pour leurs activités de fourniture de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public, aux entreprises soumises aux exigences énoncées aux articles 114 et 114/1 de la loi du 13 juin 2005 relative aux communications électroniques, et, pour leurs activités de services de confiance, aux prestataires de services de confiance soumis aux exigences énoncées à l'article 19 du règlement européen (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. § 2. La présente loi n'est pas applicable aux opérateurs relevant du secteur des finances au sens de l'annexe II de la loi. Il est fait exception à l'alinéa précédent pour les dispositions du titre I, du chapitre 1 du titre II, et de l'article 17, §§ 2 et 3 de la présente loi. Par dérogation à l'alinéa 1er, l'article 27 de la présente loi est applicable aux opérateurs relevant du secteur des finances au sens de l'annexe II de la loi, à l'exception des opérateurs de plate-forme de négociation au sens de l'article 3, 6° de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE. § 3. Lorsqu'un acte juridique sectoriel de l'Union européenne exige des opérateurs de services essentiels ou des fournisseurs de service numérique qu'ils assurent la sécurité de leurs réseaux et systèmes d'information ou qu'ils procèdent à la notification des incidents, et à condition que les exigences en question aient un effet au moins équivalent à celui des obligations prévues par la présente loi, les dispositions relatives à la sécurité des réseaux et des systèmes d'information et à la notification d'incidents de cet acte peuvent déroger aux dispositions de la présente loi.

De Koning is ermee belast de eventuele gelijkwaardige sectorspecifieke handelingen, als bedoeld in het vorige lid, nader te bepalen.	Le Roi est chargé de préciser les éventuels actes sectoriels équivalents visés à l'alinéa précédent.
§ 4. Deze wet is niet van toepassing op de nucleaire installaties bedoeld in de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, met uitzondering van de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit.	§. 4. La présente loi n'est pas applicable aux installations nucléaires visées par la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, à l'exception des éléments d'une installation nucléaire destinée à la production industrielle d'électricité qui servent au transport de l'électricité.
Art. 5. § 1. Deze wet doet geen afbreuk aan de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, aan de artikelen 259bis, 314bis, 380, 382quinquies, 383bis, 383bis/1, 433septies, 433novies/1, 458bis, 550bis en 550ter van het Strafwetboek, of aan andere bepalingen van het Belgisch recht tot omzetting van richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad en van richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad.	Art. 5. § 1er. La présente loi est sans préjudice de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, des articles 259bis, 314bis, 380, 382quinquies, 383bis, 383bis/1, 433septies, 433novies/1, 458bis, 550bis et 550ter du Code pénal, ou d'autres dispositions du droit belge transposant la directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil, ainsi que la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.
§ 2. Deze wet doet geen afbreuk aan de verplichte beveiligingsmaatregelen voor netwerk- en informatiesystemen die geclassificeerde informatie verwerken, in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, of nucleaire documenten, in de zin van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.	§ 2. La présente loi est sans préjudice des mesures de sécurité imposées aux systèmes et réseaux informatiques traitant des informations classifiées, au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, ou des documents nucléaires au sens de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire.
Hoofdstuk 2. Definities	Chapitre 2. Définitions
Art. 6. Voor de toepassing van deze wet moet worden verstaan onder:	Art. 6. Pour l'application de la présente loi, il faut entendre par :
1° "CCB": het Centrum voor Cybersecurity België opgericht bij het koninklijk besluit van 10 oktober 2014;	1° "CCB" : le Centre pour la Cybersécurité Belgique créé par l'arrêté royal du 10 octobre 2014 ;

2° "sectorale overheid": de overheid bedoeld in bijlage IV van de wet of aangewezen door de Koning bij in Ministerraad overlegd besluit;	2° "autorité sectorielle" : l'autorité publique reprise à l'annexe IV de la loi, ou désignée par le Roi, par arrêté délibéré en Conseil des Ministres;
3° "ADCC": de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken, opgericht bij het koninklijk besluit van 18 april 1988 tot oprichting van het Coördinatie- en Crisiscentrum van de regering;	3° "DGCC" : la Direction générale Centre de Crise du Service public fédéral Intérieur, créée par l'arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise ;
4° "nationaal CSIRT ": het Computer Security Incident Response Team, belast met de coördinatie op nationaal en internationaal niveau van het beheer van computerbeveiligingsincidenten voor de in de wet bedoelde aanbieders en diensten;	4° "CSIRT national" : le centre de réponse aux incidents de sécurité informatique, chargé de la coordination, au niveau national et international, de la gestion des incidents de sécurité informatique pour les opérateurs et les services visés par la loi ;
5° "sectoraal CSIRT": dienst van de sectorale overheid waarvan de taken bedoeld worden in bijlage I van deze wet;	5° "CSIRT sectoriel": service de l'autorité sectorielle dont les tâches sont visées à l'annexe I de la présente loi ;
6° "BELAC": de accreditatie-instelling opgericht bij het koninklijk besluit van 31 januari 2006 tot oprichting van het BELAC-accreditatiesysteem van instellingen voor de conformiteitsbeoordeling;	6° "BELAC" : l'organisme d'accréditation créé par l'arrêté royal du 31 janvier 2006 portant création du système BELAC d'accréditation des organismes d'évaluation de la conformité ;
7° "instelling voor de conformiteitsbeoordeling": instelling bedoeld in artikel 1.9 van het Wetboek van economisch recht die conformiteitsbeoordelingsactiviteiten verricht, zoals onder meer kalibratie, proeven, certificatie en keuring;	7° "organisme d'évaluation de la conformité" : organisme visé à l'article 1.9 du Code de droit économique et qui effectue des opérations d'évaluation de la conformité, comme l'étalonnage, les essais, la certification et l'inspection ;
8° "netwerk- en informatiesysteem":	8° "réseau et système d'information" :
a) een elektronische-communicatienetwerk in de zin van artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;	a) un réseau de communications électroniques au sens de l'article 2, 3° de la loi du 13 juin 2005 relative aux communications électroniques ;
b) een apparaat of groep van permanent of tijdelijk gekoppelde of bij elkaar behorende apparaten, waarvan een of meer elementen, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische componenten van dat apparaat die met name de automatisering van het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken;	b) tout dispositif, tout ensemble de dispositifs interconnectés ou apparentés, de manière permanente ou temporaire, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation du processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel ;
c) of digitale gegevens die via in de punten a) en b) bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan;	c) ou les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance ;

9° "beveiliging van netwerk- en informatiesystemen": het vermogen van netwerk- en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen;	9° "sécurité des réseaux et des systèmes d'information" : la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles ;
10° "nationale strategie voor de beveiliging van netwerk- en informatiesystemen": een kader met strategische doelstellingen en prioriteiten op het gebied van de beveiliging van netwerk- en informatiesystemen op nationaal niveau;	10° "stratégie nationale en matière de sécurité des réseaux et des systèmes d'information": un cadre prévoyant des objectifs et priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information au niveau national ;
11° "aanbieder van essentiële diensten": een publieke of private entiteit die voldoet aan de criteria bedoeld in artikel 11, § 2;	11° "opérateur de services essentiels" : une entité publique ou privée qui répond aux critères visés à l'article 11, § 2 ;
12° "incident": elke gebeurtenis met een reële negatieve impact op de beveiliging van netwerk- en informatiesystemen;	12° "incident" : tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information ;
13° "incidentenbehandeling": alle procedures ter ondersteuning van de opsporing, analyse en beheersing van en reactie op een incident;	13° "gestion d'incident" : toutes les procédures utiles à la détection, à l'analyse et au confinement d'un incident et toutes les procédures utiles à l'intervention en cas d'incident ;
14° "risico": elke redelijkerwijs vast te stellen omstandigheid of gebeurtenis met een mogelijke negatieve impact op de beveiliging van netwerk- en informatiesystemen;	14° "risque" : toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information ;
15° "intersectoraal criterium": factor die gemeenschappelijk is voor alle sectoren bedoeld in bijlage II van deze wet en die het belang van een verstorend effect voor de verlening van een essentiële dienst in de zin van artikel 11, § 2, c bepaalt;	15° "critère intersectoriel" : facteur commun à tous les secteurs visés à l'annexe II de la présente loi et déterminant l'importance d'un effet perturbateur sur la fourniture d'un service essentiel au sens de l'article 11, § 2, c;
16° "sectoraal criterium": factor die eigen is aan een sector of deelsector bedoeld in bijlage II van deze wet en die het belang van een verstorend effect voor de verlening van een essentiële dienst in de zin van artikel 11, § 2, c bepaalt;	16° "critère sectoriel" : facteur propre à un secteur ou sous-secteur visé à l'annexe II de la présente loi et déterminant l'importance d'un effet perturbateur sur la fourniture d'un service essentiel au sens de l'article 11, § 2, c;
17° "beveiligingsbeleid voor de netwerk- en informatiesystemen" (I.B.B.): een document als bedoeld in artikel 14, § 2, van deze wet met de maatregelen voor de beveiliging van de netwerk- en informatiesystemen die de aanbieders van essentiële diensten of de digitaaldienstverleners hebben genomen;	17° "politique de sécurité des systèmes et réseaux d'information" (P.S.I.) : un document visé à l'article 14, § 2 de la présente loi, reprenant les mesures de sécurité des réseaux et des systèmes d'information adoptées

18° "contactpunt voor de beveiliging van de netwerk- en informatiesystemen": is het contactpunt aangewezen door de aanbieders van essentiële diensten of de digitaledienstverleners dat de functie van contactpunt uitoefent ten aanzien van de sectorale overheid, het CCB en de ADCC, voor elke vraag in verband met de beveiliging van de netwerk- en informatiesystemen waarvan de verleende essentiële diensten afhankelijk zijn.	par un opérateur de services essentiels ou par un fournisseur de service numérique ;
19° "digitale dienst": een dienst in de zin van artikel 1, lid 1, punt b), van de Europese richtlijn 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij, en waarvan de soort is vermeld in de lijst in bijlage III;	18° "point de contact pour la sécurité des systèmes et réseaux d'information" : est le point de contact désigné par l'opérateur de services essentiels ou le fournisseur de service numérique et qui exerce la fonction de point de contact vis-à-vis de l'autorité sectorielle, du CCB, et de la DGCC pour toute question liée à la sécurité des réseaux et des systèmes d'information dont sont tributaires les services essentiels fournis.
20° "digitaledienstverlener": elke rechtspersoon die een digitale dienst aanbiedt als bedoeld in bijlage III van deze wet;	19° "service numérique" : un service au sens de l'article 1er, paragraphe 1, point b), de la directive européenne 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information et dont le type figure dans la liste de l'annexe III ;
21° "vertegenwoordiger van een digitaledienstverlener": elke in België gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om voor rekening van een niet in de Unie gevestigde digitaledienstverlener op te treden en die door het CCB of de bevoegde sectorale overheid kan worden gecontacteerd in plaats van de digitaledienstverlener, wat de uit deze wet voortvloeiende verplichtingen betreft;	20° "fournisseur de service numérique" : une personne morale qui fournit un service numérique visé à l'annexe III de la présente loi ;
22° "internetknooppunt (IXP)": een netwerkinfrastructuur die de onderlinge verbinding van meer dan twee onafhankelijke autonome systemen mogelijk maakt, voornamelijk met als doel de uitwisseling van internetverkeer te vergemakkelijken; een internetknooppunt zorgt enkel voor onderlinge verbinding voor autonome systemen; een internetknooppunt vereist niet dat het internetverkeer tussen twee deelnemende autonome systemen via een derde autonoom systeem verloopt, noch dat het internetknooppunt dergelijk verkeer wijzigt of anderszins daartussen komt;	21° "représentant d'un fournisseur de service numérique" : une personne physique ou morale établie en Belgique qui est expressément désignée pour agir pour le compte d'un fournisseur de service numérique non établi dans l'Union, qui peut être contactée par le CCB ou l'autorité sectorielle compétente à la place du fournisseur de service numérique concernant ses obligations découlant de la présente loi ;
23° "domeinnaamsysteem" of "DNS": een hiërarchisch opgebouwd adresseringssysteem in een netwerk dat een zoekvraag naar een domeinnaam beantwoordt;	22° "point d'échange internet (IXP)" : une structure de réseau qui permet l'interconnexion de plus de deux systèmes autonomes indépendants, essentiellement aux fins de faciliter l'échange de trafic internet; un IXP n'assure l'interconnexion que pour des systèmes autonomes; un IXP n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic ;
24° "DNS-dienstverlener": een entiteit die DNS-diensten op het internet verleent;	23° "système de noms de domaine (DNS)" : un système hiérarchique et distribué d'affectation de noms dans un réseau qui résout les questions liées aux noms de domaines ;
	24° "fournisseur de services DNS" : une entité qui fournit des services DNS sur l'internet ;

25° "register voor topleveldomeinnamen": een entiteit die de internetdomeinnamen van een specifiek topleveldomein registreert en beheert; 26° "onlinemarktplaats": een digitale dienst die het consumenten, zoals gedefinieerd in artikel 1.1., 2°, van het Wetboek van economisch recht, en/of ondernemers, zoals gedefinieerd in artikel 1.8, 39°, van hetzelfde Wetboek, mogelijk maakt online verkoop- of diensten-overeenkomsten met ondernemers te sluiten op de website van de onlinemarktplaats of op de website van een ondernemer die gebruikmaakt van door de onlinemarktplaats aangeboden informaticadiensten; 27° "onlinezoekmachine": een digitale dienst die het gebruikers mogelijk maakt zoekacties uit te voeren op in principe alle websites of websites in een bepaalde taal op basis van een zoekvraag over om het even welk onderwerp in de vorm van een trefwoord, een zin of andere input; het resultaat zijn hyperlinks naar informatie over de opgevraagde inhoud; 28° "cloudcomputerdienst": een digitale dienst die toegang mogelijk maakt tot een schaalbare en elastische pool van deelbare computercapaciteit; 29° "certificeringsaudit": een audit uitgevoerd door een instelling voor de conformiteitsbeoordeling bedoeld in artikel 6, 7°, die, overeenkomstig artikel 21, § 3, van deze wet, geaccrediteerd is door BELAC of door een instelling die de erkenningsakkoorden van de "European Cooperation for Accreditation" medeondertekend heeft.	25° "registre de noms de domaine de haut niveau" : une entité qui administre et gère l'enregistrement de noms de domaine internet dans un domaine de haut niveau donné ; 26° "place de marché en ligne" : un service numérique qui permet à des consommateurs au sens de l'article 1.1., 2° du Code de droit économique et/ou à des professionnels, au sens de l'article 1.8, 39° du même Code, de conclure des contrats de vente ou de service en ligne avec des professionnels, soit sur le site internet de la place de marché en ligne, soit sur le site internet d'un professionnel qui utilise les services informatiques fournis par la place de marché en ligne ; 27° "moteur de recherche en ligne" : un service numérique qui permet aux utilisateurs d'effectuer des recherches sur, en principe, tous les sites internet ou sur les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot clé, d'une phrase ou d'une autre entrée, et qui renvoie des liens à partir desquels il est possible de trouver des informations en rapport avec le contenu demandé ; 28° "service d'informatique en nuage" : un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées ; 29° "audit de certification" : un audit réalisé par un organisme d'évaluation de la conformité visé à l'article 6, 7° et accrédité, conformément à l'article 21, § 3 de la présente loi, par BELAC ou par une institution qui est co-signataire des accords de reconnaissance du « European Cooperation for Accreditation ».
Hoofdstuk 3. Bevoegde autoriteiten en samenwerking op nationaal niveau	Chapitre 3. Autorités compétentes et coopération au niveau national
Afdeling 1. Bevoegde autoriteiten	Section 1. Autorités compétentes
Art. 7. § 1. Het CCB is, als nationale autoriteit, belast met de opvolging en de coördinatie van de uitvoering van deze wet. § 2. De sectorale overheden zijn, voor hun respectievelijke sector, belast met het toezicht op de uitvoering van de bepalingen van deze wet.	Art. 7. § 1er. Le CCB est chargé, au titre d'autorité nationale, du suivi et de la coordination de la mise en œuvre de la présente loi. § 2. Les autorités sectorielles sont chargées, pour leur secteur respectif, de veiller à la mise en œuvre des dispositions de la présente loi.

De Koning kan sectorale overheden oprichten, bestaande uit vertegenwoordigers van de Federale Staat, de Gemeenschappen en de Gewesten, overeenkomstig de modaliteiten bepaald in artikel 92ter van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen. § 3. Het CCB wordt aangewezen als centraal nationaal contactpunt inzake de beveiliging van de netwerk- en informatiesystemen, hierna "NIS-contactpunt" genoemd, voor het geheel van de aanbieders van essentiële diensten en digitaledienstverleners, voor België in zijn relatie met de Europese Commissie, de lidstaten van de Europese Unie, de Samenwerkingsgroep en het CSIRT-netwerk. Daartoe vertegenwoordigt het België binnen de Samenwerkingsgroep bedoeld in artikel 11 van de NIS-richtlijn. § 4. Het CCB oefent de functie van nationaal CSIRT uit om meldingen van incidenten door aanbieders van essentiële diensten en digitaledienstverleners te ontvangen. Het ontvangt ook de meldingen van incidenten in andere landen. § 5. Ter ondersteuning van het nationale CSIRT kan elke sectorale overheid ervoor kiezen om een sectoraal CSIRT uit te bouwen, mits naleving van de verplichtingen bedoeld in bijlage I van deze wet. § 6. Het CCB vertegenwoordigt België binnen het CSIRT-netwerk bedoeld in artikel 12 van de NIS-richtlijn. Het werkt op doeltreffende, efficiënte en beveiligde wijze mee aan de opdrachten van het CSIRT-netwerk.	Le Roi peut créer des autorités sectorielles, composées de représentants de l'Etat fédéral, des Communautés et des Régions, conformément aux modalités prévues à l'article 92 ter de la loi spéciale du 8 août 1980 de réformes institutionnelles. § 3. Le CCB est désigné comme point de contact national unique en matière de sécurité des réseaux et des systèmes d'information, ci-après dénommé "point de contact NIS" pour l'ensemble des opérateurs de services essentiels et des fournisseurs de services numériques, pour la Belgique dans ses relations avec la Commission européenne, les États membres de l'Union européenne, le Groupe de coopération et le réseau des CSIRT. A cette fin, il représente la Belgique au sein du Groupe de coopération visé à l'article 11 de la directive NIS. § 4. Le CCB exerce la fonction de CSIRT national afin de recevoir les notifications d'incidents des opérateurs de services essentiels et des fournisseurs de service numérique. Il reçoit également les notifications d'incidents d'autres Etats. § 5. En appui du CSIRT national, chaque autorité sectorielle peut choisir de développer un CSIRT sectoriel, moyennant le respect des obligations visées à l'annexe I de la présente loi. § 6. Le CCB représente la Belgique au sein du réseau des CSIRT visé à l'article 12 de la directive NIS. Il coopère de manière effective, efficace et sécurisée aux missions du réseau des CSIRT.
Afdeling 2. Samenwerking op nationaal niveau	Section 2. Coopération au niveau national
Art. 8. § 1. Het CCB, de ADCC en de sectorale overheden werken nauw samen om de in deze wet vastgestelde verplichtingen te vervullen. § 2. Naargelang de behoeften en overeenkomstig de toepasselijke wettelijke bepalingen werken de overheden bedoeld in het eerste lid ook samen met, onder meer, de diensten van het Openbaar Ministerie, de politie en de Gegevensbeschermingsautoriteit.	Art. 8. § 1. Le CCB, la DGCC et les autorités sectorielles coopèrent étroitement aux fins du respect des obligations énoncées dans la présente loi. § 2. En fonction des besoins et conformément aux dispositions légales applicables, les autorités visées à l'alinéa 1 coopèrent également, entre autres, avec les services du Ministère public, de la police et de l'Autorité de protection des données.
Hoofdstuk 4. Informatie-uitwisseling	Chapitre 4. Echanges d'information
Art. 9. § 1. Onverminderd de wettelijke bepalingen die de vertrouwelijkheid van de informatie m.b.t. de wezenlijke belangen van de openbare veiligheid	Art. 9. § 1. Sous réserve des dispositions légales garantissant la confidentialité des informations liées aux intérêts essentiels de la sécurité publique, les

waarborgen, mag de informatie uitgewisseld in het kader van deze wet met de autoriteiten van de Europese Unie en buitenlandse of nationale autoriteiten worden uitgewisseld wanneer die uitwisseling noodzakelijk is voor de toepassing van deze wet. De uitgewisselde informatie wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van die uitwisseling. Bij die uitwisseling van informatie wordt de vertrouwelijkheid van de informatie gewaarborgd en worden de veiligheids- en commerciële belangen van aanbieders van essentiële diensten en digitaaldienstverleners beschermd. Met inachtneming van het eerste en tweede lid wordt, voor de toepassing van deze wet, afgeweken van de door andere wetgeving opgelegde verplichtingen inzake het beroepsgeheim. § 2. De sectorale overheid, de inspectiedienst, het CCB en de ADCC beperken de toegang tot de informatie bedoeld in de titels 2 en 3 en tot de informatie die hun wordt toevertrouwd door de aanbieders van essentiële diensten of de digitaaldienstverleners, tot de personen die er de kennis van nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met deze wet. § 3. Onverminderd andere strengere wettelijke bepalingen moeten de aanbieder van essentiële diensten, zijn medewerkers en onderaannemers de toegang tot de inhoud van de maatregelen in het I.B.B. beperken tot de personen die er de kennis van nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functie in het kader van hun activiteit voor de aanbieder van essentiële diensten of opdracht die verband houdt met deze wet. Ze zijn gebonden aan het beroepsgeheim wat deze informatie betreft. § 4. De aanbieder van essentiële diensten, de digitaaldienstverlener, het CCB, de sectorale overheid, de inspectiedienst en de ADCC werken te allen tijde samen door een adequate informatie-uitwisseling betreffende de beveiliging van de netwerk- en informatiesystemen.	informations échangées dans le cadre de la présente loi peuvent faire l'objet d'un échange avec des autorités de l'Union européenne, avec des autorités étrangères ou nationales, lorsque cet échange est nécessaire à l'application de la présente loi. Les informations échangées se limitent au minimum nécessaire et sont proportionnées à l'objectif de cet échange. Cet échange d'informations préserve la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des opérateurs de services essentiels et des fournisseurs de service numérique. Dans le respect des alinéas 1 et 2, il est dérogé, pour l'exécution de la présente loi, aux obligations de secret professionnel imposés par d'autres législations. § 2. L'autorité sectorielle, le service d'inspection, le CCB et la DGCC limitent l'accès aux informations visées aux titres 2 et 3 et aux informations qui leur sont confiées par l'opérateur de services essentiels ou le fournisseur de service numérique, aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec la présente loi. § 3. Sans préjudice d'autres dispositions légales plus contraignantes, l'opérateur de services essentiels, ses agents et ses sous-traitants ne peuvent donner accès au contenu des mesures figurant dans la P.S.I. qu'aux personnes qui ont besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions dans le cadre de leur activité pour l'opérateur de services essentiels ou de leur mission en lien avec la présente loi. Ils sont tenus au secret professionnel en ce qui concerne ces informations. § 4. L'opérateur de services essentiels, le fournisseur de service numérique, le CCB, l'autorité sectorielle, le service d'inspection et la DGCC collaborent en tout temps, par un échange adéquat d'informations concernant la sécurité des systèmes et réseaux d'informations.
Hoofdstuk 5. Nationale strategie voor de beveiliging van netwerk- en informatiesystemen	Chapitre 5. Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information

Art. 10. § 1. Na raadpleging van het CCB, de ADCC, de sectorale overheden en de Gegevensbeschermingsautoriteit keurt de Koning, bij in Ministerraad overlegd besluit, de nationale strategie voor de beveiliging van netwerk- en informatiesystemen goed. In deze strategie worden passende strategische en regelgevingsdoelstellingen bepaald om een hoog beveiligingsniveau van de netwerk- en informatiesystemen tot stand te brengen en te handhaven. Ze moet minstens betrekking hebben op de in bijlage II van deze wet bedoelde sectoren en de in bijlage III van deze wet bedoelde diensten. § 2. De nationale strategie voor de beveiliging van netwerk- en informatiesystemen betreft onder meer de volgende punten: a) de doelstellingen en de prioriteiten van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen; b) een governancekader ter verwezenlijking van de doelstellingen en de prioriteiten van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen, met inbegrip van de taken en verantwoordelijkheden van de overheidsorganen en de andere betrokken actoren; c) de bepaling van maatregelen inzake paraatheid, reactie en herstel, met inbegrip van samenwerking tussen de publieke en de particuliere sector; d) een overzicht van de onderwijs-, bewustmakings- en opleidingsprogramma's met betrekking tot de nationale strategie voor de beveiliging van netwerk- en informatiesystemen; e) een overzicht van de plannen voor onderzoek en ontwikkeling met betrekking tot de nationale strategie voor de beveiliging van netwerk- en informatiesystemen; f) een risicobeoordelingsplan om risico's te identificeren; g) een lijst van de verschillende actoren die betrokken zijn bij de uitvoering van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen.	Art. 10. § 1er. Après consultation du CCB, de la DGCC, des autorités sectorielles et de l'Autorité de protection des données, le Roi adopte, par arrêté délibéré en Conseil des Ministres, la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information qui définit les objectifs stratégiques et réglementaires appropriées en vue de parvenir à un niveau élevé de sécurité des réseaux et des systèmes d'information et de le maintenir et de couvrir au moins les secteurs visés à l'annexe II et les services visés à l'annexe III de la présente loi. § 2. La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information porte, entre autres, sur les points suivants : a) les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information; b) un cadre de gouvernance permettant d'atteindre les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, prévoyant notamment les rôles et les responsabilités des organismes publics et des autres acteurs pertinents; c) l'inventaire des mesures en matière de préparation, d'intervention et de récupération, y compris la coopération entre les secteurs public et privé; d) un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ; e) un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ; f) un plan d'évaluation des risques permettant d'identifier les risques ; g) une liste des différents acteurs concernés par la mise en œuvre de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information.
Titel 2. - Netwerk- en informatiesystemen van de aanbieders van essentiële diensten	Titre 2. - Réseaux et systèmes d'information des opérateurs de services essentiels

Hoofdstuk 1. Identificatie van de aanbieders van essentiële diensten	Chapitre 1. Identification des opérateurs de services essentiels
Art. 11. § 1. De sectorale overheid identificeert de potentiële aanbieders van essentiële diensten van haar sector en houdt hierbij minstens rekening met de soorten aanbieders in bijlage II van deze wet en met de door hen verleende essentiële diensten. Binnen de grenzen van hun respectievelijke bevoegdheden overleggen het CCB en de ADCC met de sectorale overheid om over te gaan tot deze identificatie. De sectorale overheid raadpleegt, in voorkomend geval, de betrokken gewesten en/of gemeenschappen en de vertegenwoordigers van de in bijlage II bedoelde entiteiten. § 2. Om de in paragraaf 1 bedoelde aanbieders te identificeren, moet de sectorale overheid de volgende criteria toepassen: a) de entiteit verleent een dienst die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten; b) de verlening van die dienst is afhankelijk van netwerken en informatiesystemen; en c) een incident zou aanzienlijke verstorende effecten hebben voor de verlening van die dienst; d) de in § 4 bedoelde criteria en weerslag niveaus of drempelwaarden. Voor een identificatie volstaat het dat de potentiële aanbieder van essentiële diensten minstens aan een van de vastgestelde criteria, drempelwaarden of weerslag niveaus voldoet. § 3. Behoudens tegenbewijs wordt de verlening van een essentiële dienst geacht afhankelijk te zijn van netwerken en informatiesystemen. § 4. Om het belang van het in artikel 11, § 2, c), bedoelde verstorende effect te bepalen, stelt de sectorale overheid sectorale of intersectorale criteria, weerslag niveaus of drempelwaarden vast. Binnen de grenzen van hun respectievelijke bevoegdheden overleggen het CCB en de ADCC met de sectorale overheid om over te gaan tot deze vaststelling, na raadpleging, in voorkomend geval, van de betrokken gewesten en/of gemeenschappen en van de vertegenwoordigers van de in bijlage II bedoelde entiteiten.	Art. 11. § 1er. L'autorité sectorielle identifie les opérateurs de services essentiels potentiels de son secteur, en prenant au minimum en compte les types d'opérateurs qui figurent à l'annexe II de la présente loi, et les services essentiels qu'ils fournissent. Dans les limites de leurs compétences respectives, le CCB et la DGCC se concertent avec l'autorité sectorielle pour procéder à cette identification. L'autorité sectorielle consulte, le cas échéant, les régions et/ou les communautés concernées et les représentants des entités visées à l'annexe II. § 2. Pour identifier les opérateurs visés au paragraphe 1er, l'autorité sectorielle doit appliquer les critères suivants : a) l'entité fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques ; b) la fourniture de ce service est tributaire des réseaux et des systèmes d'information ; et c) un incident aurait un effet perturbateur important sur la fourniture dudit service ; d) les critères et les niveaux d'incidence ou les seuils visés au § 4. Pour ce faire, il suffit que l'opérateur de services essentiels potentiel réponde au moins soit à un critère, soit un seuil et soit un niveau d'incidence fixé pour être identifié. § 3. Sauf preuve contraire, la fourniture d'un service essentiel est présumée être tributaire des réseaux et systèmes d'information. § 4. Afin de déterminer l'importance de l'effet perturbateur visé à l'article 11, § 2, c), l'autorité sectorielle établit des critères sectoriels ou intersectoriels, des niveaux d'incidence ou des seuils. Dans les limites de leurs compétences respectives, le CCB et la DGCC se concertent avec l'autorité sectorielle pour procéder à cette détermination après consultation, le cas échéant, des régions et/ou des communautés concernées et des représentants des entités visées à l'annexe II.

§ 5. De sectorale overheid houdt minstens rekening met de volgende intersectorale criteria: a) het aantal gebruikers dat afhankelijk is van de door de betrokken entiteit verleende dienst; b) de afhankelijkheid van de andere in bijlage II bedoelde sectoren van de door die entiteit verleende dienst; c) de gevolgen die incidenten kunnen hebben, wat betreft mate en duur, voor economische of maatschappelijke activiteiten of de openbare veiligheid; d) het marktaandeel van die entiteit; e) de omvang van het geografische gebied dat door een incident kan worden getroffen; f) het belang van de entiteit voor de instandhouding van een toereikend dienstverleningsniveau, rekening houdend met de beschikbare alternatieven voor het verlenen van die dienst.	§ 5. L'autorité sectorielle prend en compte, au moins les critères intersectoriels suivants : a) le nombre d'utilisateurs tributaires du service fourni par l'entité concernée ; b) la dépendance des autres secteurs visés à l'annexe II à l'égard du service fourni par cette entité ; c) les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques ou sociétales ou sur la sécurité publique ; d) la part de marché de cette entité ; e) la portée géographique eu égard à la zone susceptible d'être touchée par un incident ; f) l'importance que revêt l'entité pour garantir un niveau de service suffisant, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service.
Na raadpleging van het CCB en de ADCC kan de Koning deze intersectorale criteria aanvullen na raadpleging van de sectorale overheden, de gewesten en gemeenschappen.	Après consultation du CCB et de la DGCC, le Roi peut compléter ces critères intersectoriels, après consultation des autorités sectorielles, des régions et des communautés.
§ 6. De potentiële aanbieder van essentiële diensten bezorgt de sectorale overheid, op haar verzoek of op verzoek van het CCB of de ADCC, alle nuttige informatie over zijn eventuele identificatie als aanbieder van essentiële diensten, met inbegrip van de informatie die toelaat te objectiveren of de verlening van de essentiële dienst al dan niet afhankelijk is van netwerk- en informatiesystemen.	§ 6. L'opérateur de services essentiels potentiel transmet à l'autorité sectorielle, à la demande de celle-ci, du CCB ou de la DGCC, toutes les informations utiles quant à son éventuelle identification en tant qu'opérateur de services essentiels, en ce compris celles permettant d'objectiver la dépendance ou non de la fourniture du service essentiel aux réseaux et systèmes de l'information.
De sectorale overheid maakt de door de potentiële aanbieder meegedeelde relevante informatie over aan het CCB en de ADCC.	Les informations pertinentes transmises par l'opérateur potentiel sont communiquées par l'autorité sectorielle au CCB et à la DGCC.
§ 7. De sectorale overheid bezorgt het CCB en de ADCC een gemotiveerd voorstel van lijst van potentiële aanbieders van essentiële diensten in haar sector, samen met een of meer toegepaste identificatiecriteria.	§ 7. L'autorité sectorielle communique au CCB et à la DGCC une proposition motivée de liste des opérateurs de services essentiels potentiels dans son secteur avec le ou les critères d'identification retenus.
Wanneer geen enkele potentiële aanbieder van essentiële diensten is geïdentificeerd binnen een sector of deelsector, licht de sectorale overheid de redenen hiervoor schriftelijk toe.	Lorsqu'aucun opérateur de services essentiels potentiel n'a été identifiée au sein d'un secteur ou d'un sous-secteur, l'autorité sectorielle en expose par écrit les raisons.
Het CCB en de ADCC brengen, binnen de grenzen van hun respectievelijke bevoegdheden, advies uit over het gemotiveerde voorstel van lijst, in voorkomend geval na raadpleging van de gewesten en gemeenschappen.	Le CCB et la DGCC, dans les limites de leurs compétences respectives, rendent un avis sur la proposition motivée de liste, le cas échéant après consultation des régions et des communautés.

§ 8. Wanneer de sectorale overheid vaststelt dat de aanbieder van essentiële diensten een of meer essentiële diensten in minstens één andere lidstaat van de Europese Unie verleent, brengt ze het CCB en de ADCC daarvan op de hoogte. Deze laatste organiseren, in samenwerking met de betrokken sectorale overheden, de besprekingen met de betrokken buitenlandse nationale autoriteit of autoriteiten en, in voorkomend geval, met de betrokken gewesten of gemeenschappen. § 9. De sectorale overheid brengt de aanbieder op de hoogte van haar gemotiveerde beslissing betreffende zijn aanwijzing als aanbieder van essentiële diensten. Deze kennisgeving gebeurt op beveiligde wijze. De Koning kan de hierbij toe te passen beveiligingsmaatregelen bepalen. Ze bezorgt ook een kopie van deze beslissing aan het CCB en de ADCC. In voorkomend geval brengt de sectorale overheid de betrokken gewesten en/of gemeenschappen hiervan op de hoogte. § 10. Binnen de 3 maanden na zijn aanwijzing bezorgt de aanbieder van essentiële diensten de sectorale overheid een beschrijving van de netwerk- en informatiesystemen waarvan de verlening van de betrokken essentiële dienst of diensten afhankelijk is. De sectorale overheid bezorgt deze beschrijving aan het CCB. § 11. De sectorale overheid zorgt voor een permanente opvolging van het identificatie- en aanwijzingsproces van de aanbieders van essentiële diensten en van hun essentiële diensten, volgens de in dit hoofdstuk beschreven procedures. De sectorale overheid evalueert en, in voorkomend geval, actualiseert minstens om de twee jaar de identificatie van de aanbieders van essentiële diensten en van hun essentiële diensten. De bijwerkingen worden naar het CCB en de ADCC gestuurd. § 12. Onverminderd de toepassing van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen worden de bestuursdocumenten	§ 8. Lorsque l'autorité sectorielle constate que l'opérateur de services essentiels fournit un ou des services essentiels dans au moins un autre Etat membre de l'Union européenne, elle en informe le CCB et la DGCC. Ces derniers, en collaboration avec les autorités sectorielles concernées, organisent les discussions avec la ou les autorités nationales étrangères concernées et, le cas échéant, avec les régions ou les communautés concernées. § 9. L'autorité sectorielle notifie à l'opérateur sa décision motivée de désignation en qualité d'opérateur de services essentiels. Cette notification est réalisée de manière sécurisée. Le Roi peut préciser les mesures de sécurité à appliquer à cette notification. Elle communique également copie de cette décision au CCB et à la DGCC. L'autorité sectorielle en informe, le cas échéant, les régions et/ou les communautés concernées. § 10. Dans les 3 mois de sa désignation, l'opérateur de services essentiels transmet à l'autorité sectorielle un descriptif des réseaux et des systèmes d'information dont la fourniture du ou des services essentiels concernés est tributaire. L'autorité sectorielle communique ce descriptif au CCB. § 11. L'autorité sectorielle assure le suivi permanent du processus d'identification et de désignation des opérateurs de services essentiels et de leurs services essentiels, selon les procédures décrites au présent chapitre. Au minimum, l'autorité sectorielle réexamine et, le cas échéant, met à jour l'identification des opérateurs de services essentiels et de leurs services essentiels tous les deux ans. Les actualisations sont adressées au CCB et à la DGCC. § 12. Sans préjudice de l'application de la loi du 11 décembre 1998 relative à la classification, aux habilitations, attestations et avis de sécurité, les documents administratifs liés à l'application du présent article, sont considérés comme des documents administratifs liés à la sécurité de la population, à l'ordre public et la sûreté, au sens de l'article 6, § 1er de la loi du 11 avril 1994 relative à la publicité de l'administration, qui ne peuvent être consultés, faire
---	---

betreffende de toepassing van dit artikel als bestuursdocumenten beschouwd die verband houden met de veiligheid van de bevolking, de openbare orde en de veiligheid, in de zin van artikel 6, § 1, van de wet van 11 april 1994 betreffende de openbaarheid van bestuur, en die niet het voorwerp mogen uitmaken van inzage, uitleg of mededeling in afschrift voor het publiek.	l'objet d'explications ou être communiqué sous forme d'une copie pour le public.
Art. 12. § 1. In afwijking van artikel 11 wijst de sectorale overheid de exploitanten van kritieke infrastructuur aan, zoals aangeduid krachtens artikel 8 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur en artikel 6 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuur in de deelsector van het luchtvervoer, als aanbieders van essentiële diensten, wanneer hun sector is opgenomen in bijlage II van deze wet en de verlening van hun essentiële diensten afhankelijk is van netwerk- en informatiesystemen. Deze aanwijzing gebeurt in overleg met het CCB en de ADCC binnen de grenzen van hun respectievelijke bevoegdheden. § 2. Behoudens tegenbewijs wordt de exploitatie van een kritieke infrastructuur geacht afhankelijk te zijn van netwerk- en informatiesystemen. § 3. De exploitant bezorgt de sectorale overheid, op haar verzoek of op verzoek van het CCB of de ADCC, alle nuttige informatie over zijn eventuele identificatie als aanbieder van essentiële diensten, met inbegrip van de informatie die toelaat te objectiveren of hij al dan niet afhankelijk is van netwerk- en informatiesystemen. De sectorale overheid maakt de door de exploitant meegedeelde relevante informatie over aan het CCB en de ADCC. § 4. Artikel 11, § 9, is van toepassing op de gemotiveerde beslissing tot aanwijzing van een exploitant van kritieke infrastructuur als aanbieder van essentiële diensten.	Art. 12. § 1er Par dérogation à l'article 11, l'autorité sectorielle désigne les exploitants d'infrastructures critiques, telles que désignées en vertu de l'article 8 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques et de l'article 6 de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien, comme des opérateurs de services essentiels lorsque leur secteur est repris dans l'annexe II de la présente loi et que la fourniture des services essentiels qu'ils délivrent est tributaire des réseaux et des systèmes d'information. Cette désignation se fait en concertation avec le CCB et la DGCC dans les limites de leurs compétences respectives. § 2. Sauf preuve contraire, l'exploitation d'une infrastructure critique est présumée être tributaire des réseaux et systèmes d'information. § 3. L'exploitant transmet à l'autorité sectorielle, à la demande de celle-ci, du CCB ou de la DGCC, toutes les informations utiles quant à son éventuelle identification en tant qu'opérateur de services essentiels, en ce compris celles permettant d'objectiver sa dépendance ou non aux réseaux et systèmes de l'information. Les informations pertinentes transmises par l'exploitant sont communiquées par l'autorité sectorielle au CCB et à la DGCC. § 4. L'article 11, § 9 est applicable à la décision motivée de désignation d'un exploitant d'une infrastructure critique en qualité d'opérateur de services essentiels.
Art 13. De Koning kan, bij in Ministerraad overlegd besluit, andere sectoren of soorten aanbieders toevoegen aan bijlage II van deze wet.	Art. 13. Le Roi peut, par arrêté délibéré en Conseil des Ministres, ajouter d'autres secteurs ou types d'opérateurs à l'annexe II de la présente loi.
Hoofdstuk 2. Beveiligingsmaatregelen	Chapitre 2. Mesures de sécurité

Artikel 14. § 1. De aanbieder van essentiële diensten neemt passende en evenredige technische en organisatorische maatregelen om de risico's voor de beveiliging van netwerk- en informatiesystemen waarvan zijn essentiële diensten afhankelijk zijn, te beheersen. Deze maatregelen zorgen, gezien de stand van de techniek, voor een niveau van fysieke en logische beveiliging van netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen. De aanbieder neemt ook passende maatregelen om incidenten die de beveiliging van de voor de verlening van die essentiële diensten gebruikte netwerk- en informatiesystemen aantasten, te voorkomen of de gevolgen ervan te minimaliseren, teneinde de continuïteit van deze diensten te waarborgen. § 2. De aanbieder van essentiële diensten werkt een beveiligingsbeleid uit voor zijn netwerk- en informatiesystemen (hierna "I.B.B." genoemd) dat minstens de in de paragrafen 1 en 4 bedoelde concrete beveiligingsdoelstellingen en -maatregelen bevat. § 3. De aanbieder van essentiële diensten werkt zijn I.B.B. uiterlijk uit binnen een termijn van twaalf maanden na de kennisgeving van zijn aanwijzing. Hij implementeert de in zijn I.B.B. beschreven maatregelen uiterlijk binnen een termijn van vierentwintig maanden na de kennisgeving van zijn aanwijzing. Voor een welbepaalde sector of, in voorkomend geval, per deelsector kan de bevoegde sectorale overheid deze termijn aanpassen in functie van het soort maatregelen in het I.B.B. § 4. Op voorstel van de Eerste Minister en van de bevoegde ministers kan de Koning beveiligingsmaatregelen opleggen aan de aanbieders van essentiële diensten van verschillende sectoren. Het voorstel wordt geformuleerd na advies van het CCB, de ADCC, de sectorale overheden en, in voorkomend geval, van de gewesten of gemeenschappen. De sectorale overheid kan, in overleg met het CCB en, in voorkomend geval, na raadpleging van de gewesten of gemeenschappen, eisen dat de aanbieders van essentiële diensten die tot haar sector of deelsectoren behoren bijkomende beveiligingsmaatregelen naleven.	Art. 14. § 1er. L'opérateur de services essentiels prend les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information dont sont tributaires ses services essentiels. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité physique et logique adapté aux risques existants, compte tenu de l'état des connaissances. L'opérateur prend également les mesures appropriées en vue de prévenir les incidents qui compromettent la sécurité des réseaux et des systèmes d'information utilisés pour la fourniture de ces services essentiels ou d'en limiter l'impact, en vue d'assurer la continuité de ces services. § 2. L'opérateur de services essentiels élabore une politique de sécurité de ses systèmes et réseaux d'information (ci-après dénommé « P.S.I. ») reprenant au moins les objectifs et les mesures de sécurité concrètes, visés aux paragraphes 1er et 4. § 3. L'opérateur de services essentiels élabore sa P.S.I. au plus tard dans un délai de douze mois à dater de la notification de sa désignation. Dans un délai de vingt-quatre mois au plus tard à dater de la notification de sa désignation, il met en œuvre les mesures prévues dans sa P.S.I. Pour un secteur déterminé ou le cas échéant par sous-secteur, l'autorité sectorielle compétente peut moduler ce délai en fonction du type de mesures prévues dans la P.S.I. § 4. Sur proposition du Premier Ministre et des Ministres compétents, le Roi peut imposer certaines mesures de sécurité applicables aux opérateurs de services essentiels de plusieurs secteurs. La proposition est formulée après avis du CCB, de la DGCC, des autorités sectorielles et, le cas échéant, des régions ou des communautés. L'autorité sectorielle, en concertation avec le CCB et, le cas échéant, après consultation des régions ou des communautés, peut exiger certaines mesures complémentaires de sécurité aux opérateurs de services essentiels relevant de son secteur ou de ses sous-secteurs.
---	--

§ 5. De maatregelen voor de fysieke en logische beveiliging van netwerk- en informatiesystemen die zijn opgenomen in het beveiligingsplan van de exploitant (B.P.E.) bedoeld in artikel 13 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur en in artikel 11 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuur in de deelsector van het luchtvervoer, worden gelijkgesteld met het I.B.B. indien alle in paragraaf 2 bedoelde informatie erin opgenomen is.	§ 5. Les mesures de sécurité physique et logique des réseaux et systèmes d'information contenues dans le plan de sécurité de l'exploitant (P.S.E.) visé à l'article 13 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et à l'article 11 de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien sont assimilées à la P.S.I. lorsque toutes les informations visées au paragraphe 2 y sont reprises.
Art. 15. Behoudens tegenbewijs geniet de aanbieder van essentiële diensten het vermoeden dat de inhoud van het I.B.B. bedoeld in artikel 14, § 2, conform is, wanneer zijn beveiligingsmaatregelen voldoen aan de eisen van de norm ISO/IEC 27001 of aan een nationale, buitenlandse of internationale norm die door de Koning als gelijkwaardig wordt erkend, na advies van BELAC, de sectorale overheid en het CCB. Het in het vorige lid bedoelde conformiteitsbewijs wordt geleverd aan de hand van een certificaat uitgereikt door een instelling voor de conformiteitsbeoordeling, bedoeld in artikel 6, 7°, van deze wet, die volgens de norm ISO/IEC 17021 of ISO/IEC 17065 geaccrediteerd is door BELAC of door een instelling die de erkenningsakkoorden van de "European Cooperation for Accreditation" medeondertekend heeft. Het uitgereikte certificaat moet betrekking hebben op het certificeringsdomein waarvoor de instelling geaccrediteerd is.	Art. 15. Sauf preuve contraire, l'opérateur de services essentiels bénéficie d'une présomption de conformité du contenu de la PSI visée à l'article 14, § 2, lorsque ses mesures de sécurité répondent aux exigences de la norme ISO/IEC 27001 ou à une norme nationale, étrangère ou internationale reconnue équivalente par le Roi, après avis de BELAC, de l'autorité sectorielle et du CCB. La preuve de la conformité visée à l'alinéa précédent est fournie par un certificat délivré par un organisme d'évaluation de la conformité, visé à l'article 6, 7° de la présente loi et accrédité selon la norme ISO/IEC 17021 ou ISO/IEC 17065 par BELAC ou par une institution qui est co-signataire des accords de reconnaissance du « European Cooperation for Accreditation ». Le certificat délivré doit être dans le domaine de certification pour lequel l'organisme est accrédité.
Art. 16. § 1. De aanbieder van essentiële diensten wijst zijn contactpunt aan voor de beveiliging van netwerk- en informatiesystemen en deelt de gegevens ervan mee aan de bevoegde sectorale overheid binnen een termijn van drie maanden na de kennisgeving van de aanwijzing als aanbieder van essentiële diensten, alsook na elke bijwerking van deze gegevens. De sectorale overheid bezorgt deze gegevens aan het CCB en de ADCC. § 2. Indien er reeds een beveiligingscontactpunt bestaat krachtens nationale of internationale bepalingen die van toepassing zijn in een sector of een deelsector, bezorgt de aanbieder van essentiële diensten de contactgegevens ervan aan de in paragraaf 1 bedoelde sectorale overheid.	Art. 16. § 1. L'opérateur de services essentiels désigne son point de contact pour la sécurité des systèmes et réseaux d'information et en communique les données à l'autorité sectorielle compétente dans un délai de trois mois à dater de la notification de la désignation comme opérateur de services essentiels, ainsi qu'après chaque mise à jour de ces données. L'autorité sectorielle transmet ces données au CCB et à la DGCC. § 2. Lorsqu'il existe déjà un point de contact pour sécurité en vertu de dispositions nationales ou internationales applicables dans un secteur ou un sous-secteur, l'opérateur de services essentiels communique les coordonnées à l'autorité sectorielle visée au paragraphe 1er.

§ 3. Het in paragraaf 1 bedoelde contactpunt voor de beveiliging van netwerk- en informatiesystemen is te allen tijde beschikbaar.	§ 3. Le point de contact pour la sécurité des systèmes et réseaux d'information visé au paragraphe 1er est disponible à tout moment.
Hoofdstuk 3. Melding van incidenten	Chapitre 3. Notification d'incidents
Art. 17. § 1. De aanbieder van essentiële diensten meldt het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT, en de ADCC onverwijld alle incidenten die een aanzienlijke impact hebben op de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn. De meldingsplicht is van toepassing zelfs wanneer de aanbieder van essentiële diensten slechts gedeeltelijk over de relevante informatie beschikt om te bepalen of het incident een aanzienlijke impact heeft. § 2. Dit artikel is van toepassing op de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU. § 3. Aanbieders die behoren tot de sector financiën in de zin van bijlage II van de wet, met uitzondering van de exploitanten van een handelsplatform, melden beveiligingsincidenten onverwijld aan de Nationale Bank van België. Deze laatste bezorgt de melding vervolgens onverwijld aan het nationale CSIRT en de ADCC. § 4. Wanneer een aanbieder van essentiële diensten afhankelijk is van een derde digitaledienstverlener, meldt de aanbieder van essentiële diensten alle gevallen waarin een incident bij zijn digitaledienstverlener aanzienlijke gevolgen heeft voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn, en dit volgens de in dit artikel beschreven procedures. § 5. De Koning is belast met de oprichting van een gemeenschappelijk en beveiligd meldingsplatform om de uitvoering en verwerking van de meldingen te vergemakkelijken die deze wet oplegt aan de aanbieders van essentiële diensten en digitaledienstverleners.	Art. 17. § 1er. L'opérateur de services essentiels notifie au CSIRT national, à l'autorité sectorielle ou à son CSIRT sectoriel, et à la DGCC, sans retard injustifié, tous les incidents ayant un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des systèmes d'information dont sont tributaires le ou les services essentiels qu'il fournit. L'obligation de notifier s'applique même si l'opérateur de services essentiels ne dispose que d'une partie des informations pertinentes pour évaluer le caractère significatif de l'impact de l'incident. § 2. Le présent article s'applique aux opérateurs de plate-forme de négociation au sens de l'article 3, 6° de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE. § 3. Les opérateurs relevant des secteur des finances au sens de l'annexe II de la loi, à l'exception des opérateurs de plate-forme de négociation, notifient, sans retard injustifié, les incidents de sécurité à la Banque nationale de Belgique. Cette dernière transmet alors la notification, sans retard injustifié, au CSIRT national et à la DGCC. § 4. Lorsqu'un opérateur de services essentiels s'appuie sur un tiers fournisseur de service numérique, l'opérateur de services essentiels notifie tout incident ayant un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des systèmes d'information dont sont tributaires le ou les services essentiels qu'il fournit, en raison d'un incident touchant son fournisseur de service numérique, selon les procédures décrites au présent article. § 5. Le Roi est chargé de créer une plate-forme commune et sécurisée de notification afin de faciliter la mise en œuvre et le traitement des notifications imposées aux opérateurs de services essentiels et aux fournisseurs de service numérique par la présente loi. Sur proposition du Premier Ministre, des Ministres compétents, et après avis de l'Autorité de protection

Op voorstel van de Eerste Minister, de bevoegde ministers en na advies van de Gegevensbeschermingsautoriteit kan de Koning in dit platform ook de meldingen opnemen van aanbieders van essentiële diensten en digitaledienstverleners, opgelegd door verordening EU 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. § 6. De Koning kan specifieke modaliteiten voor de melding en rapportering van incidenten bepalen. § 7. Op voorstel van de bevoegde minister kan de Koning, per sector of deelsector, de weerslagniveaus of de drempelwaarden bepalen die noodzakelijkerwijs een aanzienlijke impact hebben in de zin van paragraaf 1. Het voorstel van koninklijk besluit wordt geformuleerd na advies van het nationale CSIRT, de ADCC, de sectorale overheid en, in voorkomend geval, van de betrokken gewesten of gemeenschappen.	des données, le Roi peut inclure dans cette plate-forme les notifications faites par les opérateurs de services essentiels et les fournisseurs de service numérique, imposés par le règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. § 6. Le Roi peut déterminer des modalités particulières de notification et de rapportage des incidents. § 7. Sur proposition du Ministre compétent, le Roi peut établir des niveaux d'incidence ou des seuils, par secteur ou sous-secteur, constituant nécessairement un impact significatif au sens du paragraphe 1er. La proposition d'arrêté royal est formulée après avis du CSIRT national, de la DGCC, de l'autorité sectorielle et, le cas échéant, des régions ou des communautés concernées.
Titel 3. - Netwerk- en informatiesystemen van digitaledienstverleners	Titre 3. - Réseaux et systèmes d'information des fournisseurs de service numérique
Art. 18. Deze titel is niet van toepassing op micro- en kleine ondernemingen zoals gedefinieerd in de aanbeveling van de Europese Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (2003/361/EG).	Art. 18. Le présent titre ne s'applique pas aux micro et petites entreprises telles qu'elles sont définies dans la recommandation de la Commission européenne du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (2003/361/CE).
Hoofdstuk 1. De beveiligingseisen	Chapitre 1. Les exigences de sécurité
Art. 19. § 1. De digitaledienstverleners identificeren de risico's voor de beveiliging van de netwerk- en informatiesystemen die zij gebruiken voor het aanbieden in de Europese Unie van de in bijlage III bedoelde diensten en nemen passende en evenredige technische en organisatorische maatregelen om die risico's te beheersen. Deze maatregelen zorgen, gezien de stand van de techniek, voor een niveau van beveiliging van netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen, en houden rekening met de volgende aspecten: a) de beveiliging van systemen en voorzieningen; b) de behandeling van incidenten; c) het beheer van de bedrijfscontinuïteit;	Art. 19. § 1er. Les fournisseurs de service numérique identifient les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent pour offrir, dans l'Union, les services visés à l'annexe III et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer. Ces mesures garantissent, compte tenu de l'état des connaissances, un niveau de sécurité des réseaux et des systèmes d'information adapté au risque existant et prennent en considération les éléments suivants : a) la sécurité des systèmes et des installations ; b) la gestion des incidents ; c) la gestion de la continuité des activités; d) le suivi, l'audit et le contrôle;

d) toezicht, controle en testen; e) de inachtneming van de internationale normen. § 2. De digitaledienstverleners nemen ook maatregelen om incidenten die de beveiliging van hun netwerk- en informatiesystemen aantasten, voor de in bijlage III van deze wet bedoelde diensten die in de Europese Unie worden aangeboden, te voorkomen en te minimaliseren, teneinde de continuïteit van deze diensten te waarborgen. § 3. De digitaledienstverleners duiden een contactpunt aan voor de informatiebeveiliging en delen de gegevens ervan mee aan de sectorale overheid die bevoegd is voor de digitaledienstverleners, alsook na elke bijwerking van deze gegevens. De sectorale overheid bezorgt deze informatie aan het CCB.	e) le respect des normes internationales. § 2. Les fournisseurs de service numérique prennent également des mesures pour éviter les incidents portant atteinte à la sécurité de leurs réseaux et systèmes d'information, et réduire au minimum l'impact de ces incidents sur les services visés à l'annexe III de la présente loi qui sont offerts dans l'Union européenne, de manière à garantir la continuité de ces services. § 3. Les fournisseurs de service numérique renseignent un point de contact pour la sécurité informatique et en communiquent les données à l'autorité sectorielle compétente pour les fournisseurs de services numériques, ainsi qu'après chaque mise à jour de ces données. L'autorité sectorielle communique ces informations au CCB.
Hoofdstuk 2. Melding van incidenten	Chapitre 2. Notification d'incidents
Art. 20. § 1. De digitaledienstverleners melden ieder incident dat aanzienlijke gevolgen heeft voor de verlening van een door hen in de Europese Unie aangeboden dienst als bedoeld in bijlage III, onverwijld aan het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT. De meldingen bevatten informatie om te bepalen of de eventuele grensoverschrijdende impact van het incident aanzienlijk is. Melding leidt voor de meldende partij niet tot een verhoogde aansprakelijkheid. § 2. De melding gebeurt overeenkomstig de uitvoeringsverordeningen van de Europese Commissie, waaronder de Uitvoeringsverordening (EU) 2018/151 van 30 januari 2018 tot vaststelling van toepassingsbepalingen voor Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad wat betreft de nadere specificatie van de door digitaledienstverleners in aanmerking te nemen elementen voor het beheer van de risico's in verband met de beveiliging van netwerk- en informatiesystemen en van de parameters om te bepalen of een incident aanzienlijke gevolgen heeft. § 3. De verplichting om een incident te melden geldt alleen wanneer de digitaledienstverlener toegang heeft tot de informatie die nodig is om de gevolgen van een incident volledig of gedeeltelijk te beoordelen.	Art. 20. § 1er. Les fournisseurs de service numérique notifient au CSIRT national, à l'autorité sectorielle ou à son CSIRT sectoriel, sans retard injustifié, tout incident ayant un impact significatif sur la fourniture d'un service visé à l'annexe III qu'ils offrent, dans l'Union européenne. Les notifications contiennent des informations permettant d'évaluer l'ampleur de l'éventuel impact au niveau transfrontalier. Cette notification n'accroît pas la responsabilité de la partie qui en est à l'origine. § 2. La notification se fait conformément aux règlements d'exécution de la Commission européenne, dont celui du 30 janvier 2018 (UE) 2018/151 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif. § 3. L'obligation de notifier un incident ne s'applique que lorsque le fournisseur de service numérique a accès aux informations nécessaires pour évaluer complètement ou partiellement, l'impact de l'incident.

§ 4. Deze melding gebeurt overeenkomstig de door de Koning bepaalde modaliteiten en via het platform bedoeld in artikel 17, § 5, van deze wet. § 5. Het CCB stelt in voorkomend geval, en in het bijzonder indien het in paragraaf 1 bedoelde incident op minstens één andere lidstaat van de Europese Unie betrekking heeft, de andere getroffen lidstaat of lidstaten in kennis. Het CCB beschermt daarbij, overeenkomstig het Unierecht of de nationale wetgeving, de veiligheids- en commerciële belangen van de digitaledienstverlener alsook de vertrouwelijkheid van de verstrekte informatie. § 6. Wanneer publieke bewustwording nodig is om een incident te voorkomen of een lopend incident te beheersen, of wanneer de openbaarmaking van het incident anderszins in het algemeen belang is, kunnen het CCB en, in voorkomend geval, de autoriteiten of CSIRT's van andere betrokken lidstaten van de Europese Unie na overleg met de betrokken digitaledienstverlener het publiek informeren over afzonderlijke incidenten of verlangen dat de digitaledienstverlener dit doet.	§ 4. Cette notification est réalisée conformément aux modalités prévues par le Roi et via la plate-forme visée à l'article 17, § 5 de la présente loi. § 5. Lorsque c'est approprié, et notamment si l'incident visé au paragraphe 1 concerne au moins un autre Etat membre de l'Union européenne, le CCB informe le ou les autres États membres touchés. Ce faisant, le CCB doit, dans le respect du droit national et de l'Union, préserver la sécurité et les intérêts commerciaux du fournisseur de service numérique ainsi que la confidentialité des informations communiquées. § 6. Après avoir consulté le fournisseur de service numérique concerné, le CCB et, lorsque c'est approprié, les autorités ou les CSIRT des autres États membres de l'Union européenne concernés peuvent informer le public d'incidents particuliers ou imposer au fournisseur de service numérique de le faire, dans le cas où la sensibilisation du public est nécessaire pour prévenir un incident ou pour gérer un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards.
Titel 4. - Toezicht en sancties	Titre 4. - Contrôle et sanctions
Hoofdstuk 1. Toezicht op de aanbieders van essentiële diensten	Chapitre 1^{er}. Les contrôles des opérateurs de services essentiels
Afdeling 1. Audits	Section 1. Audits
Art. 21. § 1. De aanbieder van essentiële diensten realiseert, jaarlijks en op zijn kosten, een interne audit van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële diensten afhankelijk zijn. Deze interne audit moet de aanbieder van essentiële diensten toelaten zich ervan te vergewissen dat de in zijn I.B.B. bepaalde maatregelen en processen goed worden toegepast en regelmatig worden gecontroleerd. De sectorale overheid kan, in overleg met het CCB, de inhoud en de overige regels die van toepassing zijn op deze interne audit bepalen. De aanbieder van essentiële diensten bezorgt de interne auditverslagen binnen de dertig dagen aan de sectorale overheid. § 2. Certificeringsaudits of interne audits uitgevoerd bij aanbieders van essentiële diensten die het in artikel 15 van de wet bedoelde vermoeden genieten, kunnen door	Art. 21. § 1^{er}. L'opérateur de services essentiels réalise, chaque année et à ses frais, un audit interne des réseaux et systèmes d'information dont sont tributaires les services essentiels qu'il fournit. Cet audit interne doit permettre à l'opérateur de services essentiels de s'assurer que les mesures et les processus définis dans sa P.S.I. sont bien appliqués et font l'objet de contrôles réguliers. L'autorité sectorielle peut déterminer, en concertation avec le CCB, le contenu et les autres règles applicables à l'audit interne. L'opérateur de services essentiels transmet les rapports d'audit interne, dans les trente jours, à l'autorité sectorielle. § 2. Les audits de certification ou les audits internes réalisés auprès des opérateurs de services essentiels bénéficiant de la présomption visée à l'article 15 de la

de inspectiedienst of de sectorale overheid worden gelijkgesteld met de verplichte jaarlijkse interne audit bedoeld in paragraaf 1. De verslagen van deze audits worden binnen de dertig dagen door de aanbieder van essentiële diensten aan de sectorale overheid bezorgd. § 3. De aanbieder van essentiële diensten laat, minstens om de drie jaar en op zijn kosten, een externe audit uitvoeren door een geaccrediteerde of door de sectorale overheid erkende instelling voor de conformiteitsbeoordeling als bedoeld in artikel 6, 7°. De in het vorige lid bedoelde accreditatie is een accreditatie van de in artikel 6, 7°, bedoelde instelling voor de conformiteitsbeoordeling die wordt uitgereikt door BELAC of door een instelling die de erkenningsakkoorden van de "European Cooperation for Accreditation" medeondertekend heeft en die aan de minimumeisen van de ISO/IEC 17021 of ISO/IEC 17065 en aan eventuele bijkomende sectorale eisen voldoet. De lijst van de geaccrediteerde of erkende instellingen voor de conformiteitsbeoordeling is beschikbaar bij de sectorale overheid die ze actueel houdt. De sectorale overheid bepaalt, in overleg met het CCB, de bijkomende sectorale eisen waaraan de in artikel 6, 7°, bedoelde instelling voor de conformiteitsbeoordeling onderworpen kan zijn en de regels die van toepassing zijn op de externe audit. De Koning bepaalt, bij in Ministerraad overlegd besluit, de voorwaarden en modaliteiten van de eventuele erkenning bedoeld in het eerste lid die door de sectorale overheid aan de instelling voor de conformiteitsbeoordeling wordt verleend. De aanbieder van essentiële diensten bezorgt de externe auditverslagen binnen de dertig dagen aan de sectorale overheid. § 4. Certificeringsaudits uitgevoerd bij aanbieders van essentiële diensten die het in artikel 15 van de wet bedoelde vermoeden genieten, kunnen door de inspectiedienst of de sectorale overheid worden gelijkgesteld met de verplichte externe audit bedoeld in paragraaf 3. De verslagen van deze audits worden binnen de dertig dagen door de aanbieder van essentiële diensten aan de sectorale overheid bezorgd.	loi peuvent être assimilés, par le service d'inspection ou l'autorité sectorielle, à l'audit interne annuel obligatoire visé au paragraphe 1. Les rapports de ces audits sont transmis, par l'opérateur de services essentiels, dans les trente jours, à l'autorité sectorielle. § 3. L'opérateur de services essentiels fait réaliser, au moins tous les trois ans et à ses frais, un audit externe réalisé par un organisme d'évaluation de la conformité visé à l'article 6, 7°, accrédité ou agréé par l'autorité sectorielle. L'accréditation visée à l'alinéa précédent est une accréditation de l'organisme d'évaluation de la conformité visé à l'article 6, 7° délivrée par BELAC, ou par une institution qui est co-signataire des accords de reconnaissance du « European Cooperation for Accreditation », répondant aux exigences minimales de l'ISO/IEC 17021 ou ISO/IEC 17065 et aux éventuelles exigences supplémentaires sectorielles. La liste des organismes d'évaluation de la conformité accrédités ou agréés est disponible auprès de l'autorité sectorielle qui la tient à jour. L'autorité sectorielle détermine, en concertation le CCB, les exigences supplémentaires sectorielles auxquels peut être soumis l'organisme d'évaluation de la conformité visé à l'article 6, 7° et les règles applicables à l'audit externe. Le Roi détermine, par arrêté délibéré en Conseil des Ministres, les conditions et les modalités de l'éventuel agrément visé à l'alinéa 1^{er} et accordé par l'autorité sectorielle à l'organisme d'évaluation de la conformité. L'opérateur de services essentiels transmet les rapports d'audit externe, dans les trente jours, à l'autorité sectorielle. § 4. Les audits de certification réalisés auprès des opérateurs de services essentiels bénéficiant de la présomption visée à l'article 15 de la loi peuvent être assimilés, par le service d'inspection ou l'autorité sectorielle, à l'audit externe obligatoire visé au paragraphe 3. Les rapports de ces audits sont transmis, dans les trente jours, par l'opérateur de services essentiels, à l'autorité sectorielle. § 5. Le CCB peut solliciter, de manière motivée, de l'autorité sectorielle la transmission des rapports de
--	---

§ 5. Het CCB kan de sectorale overheid, mits motivering, vragen hem de certificerings- of auditverslagen van een aanbieder van essentiële diensten te bezorgen. § 6. De aanbieder van essentiële diensten voert zijn eerste interne audit uit uiterlijk binnen de drie maanden na de uitwerking van zijn I.B.B. Hij voert zijn eerste externe audit uit uiterlijk binnen de vierentwintig maanden na de uitvoering van zijn eerste interne audit.	certification ou d'audits d'un opérateur de services essentiels. § 6. Au plus tard dans les trois mois de l'élaboration de sa P.S.I., l'opérateur de services essentiels réalise son premier audit interne. Au plus tard vingt-quatre mois après la réalisation de son premier audit interne, l'opérateur de services essentiels réalise son premier audit externe.
Afdeling 2. Inspectiedienst	Section 2. Service d'inspection
Art. 22. § 1. Voor de aanbieders van essentiële diensten wordt per sector of, in voorkomend geval, per deelsector een inspectiedienst opgericht die belast is met het toezicht op de naleving van de bepalingen van deze wet en van de uitvoeringsbesluiten ervan door de aanbieders van essentiële diensten van die sector of deelsector. De Koning wijst voor een welbepaalde sector of, in voorkomend geval, per deelsector de inspectiedienst aan die bevoegd is voor het toezicht. Hij kan de eventuele sectorale praktische controlemodaliteiten bepalen. Voor de sector van de digitale infrastructuur wordt het Belgisch Instituut voor postdiensten en telecommunicatie aangewezen als inspectiedienst. De Koning kan de praktische controlemodaliteiten voor deze sector bepalen, na advies van het Instituut. § 2. De leden van de inspectiedienst beschikken over een legitimatiekaart waarvan het model, per sector of, in voorkomend geval, per deelsector, door de Koning wordt bepaald. § 3. Onverminderd artikel 21 kunnen de inspectiediensten en de sectorale overheden op elk ogenblik grondige controles uitvoeren op de naleving door de aanbieder van essentiële diensten van de beveiligingsmaatregelen en van de regels voor het melden van incidenten. Het CCB kan de inspectiedienst of de sectorale overheid, mits motivering, aanbevelen om deze controles uit te voeren. § 4. De aanbieder van essentiële diensten verleent zijn volledige medewerking aan de leden van de inspectiedienst of de sectorale overheid bij de	Art. 22. § 1er. Pour les opérateurs de services essentiels, un service d'inspection par secteur, ou, le cas échéant, par sous-secteur, est mis en place, chargé du contrôle du respect des dispositions de la présente loi et de ses actes d'exécution par les opérateurs de services essentiels dudit secteur ou sous-secteur. Le Roi désigne, pour un secteur déterminé ou, le cas échéant, par sous-secteur, le service d'inspection compétent pour effectuer le contrôle. Il peut fixer les éventuelles modalités sectorielles pratiques du contrôle. Pour le secteur des infrastructures numériques, l'Institut belge pour les services postaux et les télécommunications est désigné en tant que service d'inspection. Le Roi peut fixer les modalités pratiques du contrôle pour ce secteur, après avis de l'Institut. § 2. Les membres du service d'inspection sont dotés d'une carte de légitimation dont le modèle est fixé par le Roi, par secteur, ou, le cas échéant, par sous-secteur. § 3. Sans préjudice de l'article 21, les services d'inspection et les autorités sectorielles peuvent à tout moment réaliser des contrôles approfondis du respect par l'opérateur de services essentiels des mesures de sécurité et des règles de notification des incidents. Le CCB peut recommander, de manière motivée, au service d'inspection ou à l'autorité sectorielle de réaliser des contrôles. § 4. L'opérateur de services essentiels apporte son entière collaboration aux membres du service d'inspection ou de l'autorité sectorielle dans l'exercice de leurs fonctions et notamment pour informer ceux-ci au mieux de toutes les mesures de sécurité existantes.

uitoefening van hun functie en met name om deze zo goed mogelijk te informeren over alle bestaande beveiligingsmaatregelen. Indien nodig stelt de aanbieder van essentiële diensten het nodige materiaal ter beschikking van de leden van de inspectiedienst of van de sectorale overheid zodat ze de veiligheidsvoorschriften kunnen naleven tijdens de inspecties. § 5. Onverminderd de bevoegdheden van de officieren van gerechtelijke politie bedoeld in artikel 8 van het Wetboek van strafvordering beschikken de beëdigde leden van de inspectiedienst of van de sectorale overheid op elk ogenblik over de volgende toezichtbevoegdheden bij de uitoefening van hun opdracht, en dit zowel in het kader van administratieve handelingen als in het kader van de vaststelling van inbreuken bij proces-verbaal: 1° zonder voorafgaande verwittiging, op vertoon van hun legitimatiekaart, alle plaatsen betreden die de aanbieder van essentiële diensten gebruikt; zij hebben slechts toegang tot bewoonde lokalen mits een machtiging die vooraf is uitgereikt door de onderzoeksrechter. 2° ter plaatse kennis nemen van het I.B.B., de auditverslagen, alle bescheiden, documenten en andere informatiebronnen die nodig zijn voor de uitoefening van hun opdracht; 3° overgaan tot elk onderzoek, elke controle en elk verhoor, alsook alle inlichtingen inwinnen die zij nodig achten voor de uitoefening van hun opdracht; 4° de identiteit opnemen van de personen die zich bevinden op de plaatsen die de aanbieder van essentiële diensten gebruikt en van wie ze het verhoor noodzakelijk achten voor de uitoefening van hun opdracht. Daartoe kunnen ze van deze personen eisen dat ze hun officiële identiteitsdocumenten voorleggen. Bij het formuleren van een eis tot informatie of bewijs vermeldt de inspectiedienst of de sectorale overheid het doel van de eis en specificeert ze welke informatie moet worden verstrekt. § 6. Voor het bekomen van een machtiging tot betreding van bewoonde ruimten richten de leden van de inspectiedienst of de sectorale overheid een met redenen omkleed verzoek aan de onderzoeksrechter. Dit verzoek bevat minstens de volgende gegevens: - de identificatie van de bewoonde ruimten waartoe de leden van de inspectiedienst of de sectorale overheid toegang wensen te hebben;	Si nécessaire, l'opérateur de services essentiels met à disposition des membres du service d'inspection ou de l'autorité sectorielle le matériel nécessaire de manière à ce qu'ils remplissent les consignes de sécurité lors des inspections. § 5. Sans préjudice des attributions des officiers de police judiciaire visées à l'article 8 du Code d'instruction criminelle, les membres assermentés du service d'inspection ou de l'autorité sectorielle disposent, à tout moment, des compétences de contrôle suivantes dans l'exercice de leur mission, tant dans le cadre de démarches administratives, que dans le cadre de la constatation d'infractions par procès-verbal : 1° pénétrer sans avertissement préalable, sur présentation de leur carte de légitimation, dans tous les lieux utilisés par l'opérateur de services essentiels ; ils n'ont accès aux locaux habités que moyennant autorisation préalable délivrée par le juge d'instruction. 2° prendre connaissance sur place de la P.S.I., des rapports d'audits, de tout acte, tout document et toute autre source d'informations nécessaires à l'exercice de leur mission ; 3° procéder à tout examen, contrôle et audition, et requérir toutes les informations qu'ils estiment nécessaires à l'exercice de leur mission ; 4° prendre l'identité des personnes qui se trouvent sur les lieux utilisés par l'opérateur de services essentiels et dont ils estiment l'audition nécessaire pour l'exercice de leur mission. À cet effet, ils peuvent exiger de ces personnes la présentation de documents officiels d'identification. Au moment de formuler une demande d'informations ou de preuves, le service d'inspection ou l'autorité sectorielle mentionne la finalité de la demande et précise quelles sont les informations exigées. § 6. Pour obtenir l'autorisation de pénétrer dans des locaux habités, les membres du personnel du service d'inspection ou de l'autorité sectorielle adressent une demande motivée au juge d'instruction. Cette demande contient au moins les données suivantes : - l'identification des espaces habités auxquels les membres du personnel du service d'inspection ou de l'autorité sectorielle souhaitent avoir accès - les infractions éventuelles qui font l'objet du contrôle
---	--

- de eventuele inbreuken die het voorwerp zijn van het toezicht; - alle bescheiden en inlichtingen waaruit blijkt dat het gebruik van dit middel nodig is. De onderzoeksrechter beslist binnen een termijn van maximum 48 uur na de ontvangst van het verzoek. De beslissing van de onderzoeksrechter is met redenen omkleed. De bezoeken aan de bewoonde lokalen zonder machtiging van de bewoner gebeuren tussen vijf en eenentwintig uur door minstens twee leden van de inspectiedienst of de sectorale overheid die samen optreden. § 7. Bij het begin van elk verhoor wordt aan de ondervraagde persoon meegedeeld: 1° dat zijn verklaringen gebruikt kunnen worden als bewijs in rechte; 2° dat hij mag vragen dat alle vragen die gesteld worden, en zijn antwoorden genoteerd worden met de gebruikte woorden. Elke ondervraagde persoon mag de documenten in zijn/haar bezit gebruiken, zonder dat daardoor het verhoor uitgesteld wordt. Hij/zij kan tijdens het verhoor of later vragen om die documenten bij te voegen bij het verhoor. Het verhoor vermeldt nauwkeurig het tijdstip waarop het begint, eventueel onderbroken en hernomen wordt, en eindigt. Het vermeldt de identiteit van de personen die in het verhoor of in een deel ervan tussenkomen. Aan het einde van het verhoor heeft de ondervraagde persoon het recht om zijn verhoor te lezen of het te laten voorlezen. Hij mag zijn verklaringen laten verbeteren of er iets aan laten toevoegen. De leden van de inspectiedienst of de sectorale overheid die een persoon ondervragen, informeren hem erover dat hij een kopie mag vragen van de tekst van het verhoor. Deze kopie wordt gratis geleverd. § 8. De leden van de inspectiedienst of de sectorale overheid mogen elk informaticasysteem en de erin opgenomen gegevens raadplegen. Zij mogen zich ter plaatse het informaticasysteem en de erin opgenomen gegevens die zij nodig hebben voor hun onderzoeken en vaststellingen doen voorleggen en er kosteloos uittreksels, duplicaten of kopieën van nemen of vragen	- tous les documents et renseignements desquels il ressort que l'utilisation de ce moyen est nécessaire. Le juge d'instruction décide dans un délai de 48 heures maximum après réception de la demande. La décision du juge d'instruction est motivée. Les visites sans autorisation de l'occupant dans des locaux habités se font entre cinq et vingt-et-une heures par au moins deux membres du service d'inspection ou de l'autorité sectorielle agissant conjointement. § 7. Au début de toute audition, il est communiqué à la personne interrogée : 1° que ses déclarations peuvent être utilisées comme preuve en justice ; 2° qu'elle peut demander que toutes les questions qui lui sont posées et les réponses qu'elle donne soient actées dans les termes utilisés. Toute personne interrogée peut utiliser les documents en sa possession, sans que cela puisse entraîner le report de l'audition. Elle peut, lors de l'audition ou ultérieurement, exiger que ces documents soient joints à l'audition. L'audition mentionne avec précision l'heure à laquelle elle a pris cours, est éventuellement interrompue et reprise, et prend fin. Elle mentionne l'identité des personnes qui interviennent lors de l'audition ou à une partie de celle-ci. A la fin de l'audition, la personne interrogée a le droit de relire celle-ci ou de demander que lecture lui en soit faite. Elle peut demander à ce que ses déclarations soient corrigées ou complétées. Les membres du personnel du service d'inspection ou de l'autorité sectorielle qui interrogent une personne l'informent qu'elle peut demander une copie du texte de son audition. Cette copie lui est délivrée gratuitement. § 8. Les membres du service d'inspection ou l'autorité sectorielle peuvent consulter tous les supports d'information et les données qu'ils contiennent peuvent se faire produire sur place le système informatique et les données qu'il contient dont ils ont besoin pour leurs examens et constatations, en prendre ou en demander gratuitement des extraits ou des copies, sous une forme lisible et intelligible qu'ils ont demandée.
---	---

in een door hen gevraagde leesbare en verstaanbare vorm. Indien het niet mogelijk is om ter plaatse kopieën te nemen, mogen de leden van de inspectiedienst of de sectorale overheid, tegen een ontvangstbewijs dat een inventaris bevat, het informaticasysteem en de erin opgenomen gegevens in beslag nemen. § 9. De leden van de inspectiedienst of de sectorale overheid kunnen een beroep doen op experts. § 10. Na elke inspectie stelt de inspectiedienst een verslag op en bezorgt een kopie daarvan aan de geïnspecteerde aanbieder van essentiële diensten en aan de bevoegde sectorale overheid. Als het toezicht wordt verhinderd, kunnen de beëdigde leden van de inspectiedienst de bijstand vorderen van de federale of lokale politiediensten. § 11. Wanneer de netwerk- en informatiesystemen van een aanbieder van essentiële diensten zich buiten het Belgische grondgebied bevinden, kan de inspectiedienst of de sectorale overheid, in overleg met het CCB, de bevoegde toezichthouders van deze andere landen om samenwerking en bijstand verzoeken. Deze bijstand en samenwerking kunnen betrekking hebben op informatie-uitwisseling en verzoeken om toezichtmaatregelen. § 12. De leden van de inspectiedienst of sectorale overheid waarborgen het vertrouwelijke karakter van de gegevens van vertrouwelijke aard of bedrijfsgeheimen waarvan ze kennis nemen bij de uitoefening van hun opdracht en zien erop toe dat deze gegevens uitsluitend worden aangewend voor de uitoefening van hun toezichtsoptocht krachtens deze wet. § 13. De leden van de inspectiedienst of de experts die deelnemen aan de inspectie, mogen geen enkel rechtstreeks of onrechtstreeks belang hebben in de ondernemingen of instellingen waarop zij toezicht dienen uit te oefenen, waardoor hun objectiviteit in het gedrang zou kunnen komen. § 14. Het CCB kan de inspectiedienst, mits motivering, vragen om zijn inspectieverslagen te bezorgen. § 15. Voor iedere sector of deelsector kan de Koning, bij in Ministerraad overlegd besluit en na advies van de sectorale overheid, retributies bepalen voor de	S'il n'est pas possible de prendre des copies sur place, les membres du service d'inspection ou l'autorité sectorielle peuvent saisir, contre récépissé contenant un inventaire, le système informatique et les données qu'il contient. § 9. Les membres du service d'inspection ou de l'autorité sectorielle peuvent faire appel à des experts. § 10. Après chaque inspection, le service d'inspection rédige un rapport et en transmet une copie à l'opérateur de services essentiels inspecté et à l'autorité sectorielle compétente. En cas d'obstacle au contrôle, les membres assermentés du service d'inspection peuvent requérir l'assistance des services de police, fédérale ou locale. § 11. Lorsque les réseaux et les systèmes d'information d'un opérateur de services essentiels sont situés en dehors du territoire belge, le service d'inspection ou l'autorité sectorielle, en concertation avec le CCB, peut solliciter la coopération et l'assistance des autorités de contrôle compétentes de ces autres États. Cette assistance et cette coopération peuvent porter sur des échanges d'informations et sur des demandes de prise de mesures de contrôle. § 12. Les membres du service d'inspection ou de l'autorité sectorielle garantissent le caractère confidentiel des données confidentielles ou des secrets d'entreprise dont ils prennent connaissance dans l'exercice de leur mission et s'assurent que ces données ne seront utilisées que dans l'exercice de leur mission de contrôle en vertu de la présente loi. § 13. Les membres du service d'inspection ou les experts appelés à participer à l'inspection ne peuvent avoir un intérêt quelconque, direct ou indirect, dans les entreprises ou institutions qu'ils sont chargés de contrôler, susceptible de compromettre leur objectivité. § 14. Le CCB peut solliciter, de manière motivée, du service d'inspection la transmission de ses rapports d'inspection. § 15. Le Roi peut déterminer, par secteur ou sous-secteur, par arrêté délibéré en Conseil des Ministres et après avis de l'autorité sectorielle, des rétributions relatives aux prestations d'inspections. Ces rétributions
---	---

inspectieprestaties. Deze retributies zijn ten laste van de aanbieders van essentiële diensten. De Koning bepaalt de berekenings- en betalingsmodaliteiten.	sont à charge des opérateurs de services essentiels. Il fixe les modalités de calcul et de paiement.
Hoofdstuk 2. Toezicht op de digitaaldienstverleners	Chapitre 2. Contrôle des fournisseurs de service numérique
Art. 23. § 1. De Koning kan de praktische controlemodaliteiten van de digitaaldienstverleners bepalen.	Art. 23. § 1er Le Roi peut fixer les modalités pratiques du contrôle des fournisseurs de service numérique.
§ 2. De sectorale overheid kan een digitaaldienstverlener verplichten: a) haar, binnen de door haar vastgestelde termijn, de informatie te verstrekken die nodig is om de beveiliging van zijn netwerk- en informatiesystemen te beoordelen, met inbegrip van gedocumenteerde beleidsmaatregelen op het gebied van beveiliging; b) elke niet-inachtneming van de beveiligingseisen en de eisen inzake het melden van incidenten recht te zetten binnen de door haar vastgestelde termijn.	§ 2. L'autorité sectorielle peut imposer à un fournisseur de service numérique : a) de lui communiquer, dans le délai qu'elle lui fixe, les informations nécessaires pour évaluer la sécurité de ses réseaux et systèmes d'information, y compris les documents relatifs à ses politiques de sécurité ; b) de corriger tout manquement aux exigences de sécurité et de notification d'incidents, dans le délai qu'elle lui fixe.
§ 3. De sectorale overheid kan, indien nodig, door middel van toezichtmaatregelen achteraf, maatregelen nemen wanneer ze het bewijs in handen krijgt dat een digitaaldienstverlener niet voldoet aan de beveiligingseisen of de eisen inzake het melden van incidenten. Dit bewijs kan worden voorgelegd door een bevoegde autoriteit van een andere lidstaat van de Europese Unie waar de dienst wordt verleend.	§ 3. L'autorité sectorielle peut adopter des mesures, au besoin, dans le cadre de mesures de contrôle a posteriori, lorsque, selon les éléments communiqués, un fournisseur de service numérique ne satisfait pas aux exigences de sécurité ou de notification d'incidents. Ces éléments peuvent être communiqués par une autorité compétente d'un autre État membre de l'Union européenne dans lequel le service est fourni.
§ 4. In het kader van haar controles achteraf beschikt de sectorale overheid over dezelfde bevoegdheden als deze bedoeld in artikel 22.	§ 4. Dans le cadre de ses contrôles a posteriori, l'autorité sectorielle dispose des mêmes pouvoirs que ceux prévues à l'article 22.
§ 5. Wanneer een digitaaldienstverlener zijn hoofdvestiging of een vertegenwoordiger in België heeft maar zijn netwerk- en informatiesystemen in een of meer andere landen, kan de sectorale overheid, in overleg met het CCB, de bevoegde toezichthouders van deze andere landen om samenwerking en bijstand verzoeken. Deze bijstand en samenwerking kunnen betrekking hebben op informatie-uitwisseling en verzoeken om toezichtmaatregelen.	§ 5. Si un fournisseur de service numérique a son établissement principal ou un représentant en Belgique alors que ses réseaux et systèmes d'information sont situés dans un ou plusieurs autres États, l'autorité sectorielle, en concertation avec le CCB, peut solliciter la coopération et l'assistance des autorités de contrôle compétentes de ces autres États. Cette assistance et cette coopération peuvent porter sur les échanges d'informations et sur les demandes de prise de mesures de contrôle.
§ 6. De sectorale overheid kan de in dit artikel bedoelde bevoegdheden ook uitoefenen op verzoek van bevoegde overheden van een andere lidstaat van de Europese Unie.	§ 6. L'autorité sectorielle peut exercer également les compétences prévues au présent article, à la demande d'autorités compétentes d'un autre Etat membre de l'Union européenne.

§ 7. Het CCB kan de sectorale overheid vragen hem de controleverslagen van een digitaaldienstverlener te bezorgen. § 8. De Koning kan, bij in Ministerraad overlegd besluit en na advies van de sectorale overheid, retributies bepalen voor de controleprestaties. Deze retributies zijn ten laste van de digitale dienstverleners. De Koning bepaalt de berekenings- en betalingsmodaliteiten.	§ 7. Le CCB peut solliciter de l'autorité sectorielle la transmission des rapports de contrôle d'un fournisseur de service numérique. § 8. Le Roi peut déterminer, par arrêté délibéré en Conseil des Ministres et après avis de l'autorité sectorielle, des rétributions relatives aux prestations de contrôles. Ces rétributions sont à charge des fournisseurs de service numérique. Le Roi fixe les modalités de calcul et de paiement.
Hoofdstuk 3. De sancties	Chapitre 3. Les sanctions
Afdeling 1. Procedure	Section 1. Procédure
Art. 24. § 1. Wanneer in een inspectieverslag of een externe auditverslag wordt vastgesteld dat een inbreuk is begaan op deze wet of op de uitvoeringsbesluiten ervan, kan de inspectiedienst of de sectorale overheid de betrokken aanbieder van essentiële diensten of digitaaldienstverlener in gebreke stellen om zijn verplichtingen na te komen binnen een door deze dienst of overheid vastgestelde termijn. De termijn wordt bepaald rekening houdend met de werkingsvoorwaarden van de aanbieder van essentiële diensten of digitaaldienstverlener en met de te nemen maatregelen. Het CCB kan, mits motivering, de inspectiedienst of de sectorale overheid ook aanbevelen om de aanbieder van essentiële diensten of digitaaldienstverlener in gebreke te stellen. § 2. Als de inspectiedienst vaststelt dat de aanbieder van essentiële diensten of digitaaldienstverlener geen gevolg geeft aan de ingebrekestelling binnen de gestelde termijn, worden de feiten vastgesteld in een proces-verbaal door de beëdigde leden van de inspectiedienst of de sectorale overheid. § 3. Het feit dat iemand de uitvoering van een controle door de leden van de inspectiedienst vrijwillig verhindert of belemmert, de informatie die hem gevraagd wordt naar aanleiding van deze controle weigert mee te delen, of opzettelijk foutieve of onvolledige informatie meedeelt, wordt vastgesteld in een proces-verbaal door de beëdigde leden van de inspectiedienst of de sectorale overheid. § 4. De paragrafen 1 en 2 zijn ook van toepassing op de potentiële aanbieder van essentiële diensten die de in de	Art. 24 § 1er. Lorsqu'un rapport d'inspection ou un rapport d'audit externe démontre qu'une infraction a été commise à l'encontre de la présente loi ou de ses actes d'exécution, le service d'inspection ou l'autorité sectorielle peuvent mettre en demeure l'opérateur de services essentiels ou le fournisseur de service numérique concerné de se conformer, dans un délai qu'il ou elle fixe, aux obligations qui lui incombent. Le délai est déterminé en tenant compte des conditions de fonctionnement de l'opérateur de services essentiels ou du fournisseur de service numérique et des mesures à mettre en œuvre. Le CCB peut également, de manière motivée, recommander au service d'inspection ou à l'autorité sectorielle de mettre en demeure l'opérateur de services essentiels ou le fournisseur de service numérique. § 2. Lorsque le service d'inspection constate que l'opérateur de services essentiels ou le fournisseur de service numérique n'a pas respecté, dans le délai fixé, la mise en demeure, les faits sont constatés dans un procès-verbal rédigé par les membres assermentés du service d'inspection ou de l'autorité sectorielle. § 3. Le fait pour quiconque d'empêcher ou entraver volontairement l'exécution d'un contrôle effectué par les membres du service d'inspection, de refuser de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle, ou de communiquer sciemment des informations inexactes ou incomplètes est constaté par les membres assermentés du service d'inspection ou de l'autorité sectorielle dans un procès-verbal.

artikelen 11 en 12 bedoelde informatieverplichtingen niet nakomt. § 5. De processen-verbaal opgesteld door de beëdigde leden van de inspectiedienst of de sectorale overheid hebben bewijskracht tot het tegendeel is bewezen.	§ 4. Les paragraphes 1 et 2 sont également applicables à l'opérateur de services essentiels potentiel qui ne se conforme pas aux obligations d'information visées aux articles 11 et 12. § 5. Les procès-verbaux rédigés par les membres assermentés du service d'inspection ou de l'autorité sectorielle font foi jusqu'à preuve du contraire.
Art. 25. De inbreuken op de bepalingen van deze wet of de uitvoeringsbesluiten ervan kunnen het voorwerp uitmaken hetzij van strafrechtelijke sancties, hetzij van administratieve sancties.	Art. 25. Les infractions à la présente loi ou à ses actes d'exécution peuvent faire l'objet soit de sanctions pénales, soit de sanctions administratives.
Afdeling 2. Strafrechtelijke sancties	Section 2. Sanctions pénales
Art. 26. § 1. Wordt gestraft met een gevangenisstraf van acht dagen tot een jaar en een geldboete van 26 euro tot 50 000 euro of een van die straffen alleen, de overtreder die de verplichtingen opgelegd door of krachtens deze wet of de uitvoeringsbesluiten ervan niet naleeft. In geval van herhaling van dezelfde feiten binnen een termijn van drie jaar wordt de geldboete verdubbeld en de overtreder bestraft met een gevangenisstraf van vijftien dagen tot drie jaar. § 2. Wordt gestraft met een gevangenisstraf van acht dagen tot een maand en een geldboete van 26 euro tot 10 000 euro of een van die straffen alleen, hij die de uitvoering van de controle door de leden van de inspectiedienst vrijwillig verhindert of belemmert, de informatie die hem gevraagd is naar aanleiding van deze controle weigert mee te delen, of opzettelijk foutieve of onvolledige informatie meedeelt. In geval van herhaling van dezelfde feiten binnen een termijn van drie jaar wordt de geldboete verdubbeld en de overtreder bestraft met een gevangenisstraf van vijftien dagen tot een jaar. § 3. De bepalingen van Boek 1 van het Strafwetboek, met inbegrip van hoofdstuk VII en artikel 85, zijn van toepassing op voornoemde inbreuken. De artikelen 269 tot 274 en 276 van het Strafwetboek zijn van toepassing op de leden van de inspectiedienst die handelen in de uitoefening van hun functie.	Art. 26. § 1er. Est puni d'une peine d'emprisonnement de huit jours à un an et d'une amende de 26 euros à 50.000 euros ou de l'une de ces peines seulement l'auteur qui ne respecte pas les obligations imposées par ou en vertu de la présente loi ou de ses actes d'exécution. En cas de récidive pour les mêmes faits dans un délai de trois ans, l'amende est doublée et le contrevenant puni d'une peine d'emprisonnement de quinze jours à trois ans. § 2. Est puni d'une peine d'emprisonnement de huit jours à un mois et d'une amende de 26 euros à 10.000 euros ou de l'une de ces peines seulement, quiconque empêche ou entrave volontairement l'exécution du contrôle effectué par les membres du service d'inspection, refuse de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle, ou communique sciemment des informations inexactes ou incomplètes. En cas de récidive pour les mêmes faits dans un délai de trois ans, l'amende est doublée et le contrevenant puni d'une peine d'emprisonnement de quinze jours à un an. § 3. Les dispositions du Livre 1er du Code pénal, en ce compris le chapitre VII et l'article 85, sont applicables auxdites infractions. Les articles 269 à 274 et 276 du Code pénal sont d'application à l'égard des membres du service d'inspection agissant dans l'exercice de leurs fonctions.

§ 4. Inbreuken op artikel 9, paragrafen 2 en 3, van deze wet worden bestraft met de straffen bepaald in artikel 458 van het Strafwetboek.	§ 4. Les infractions à l'article 9, paragraphes 2 et 3 de la présente loi sont punies des peines prévues à l'article 458 du Code pénal.
Afdeling 3. Administratieve sancties	Section 3. Sanctions administratives
Art. 27. § 1. Bij het vaststellen van inbreuken op deze wet of op de uitvoeringsbesluiten ervan kan de overtreder bestraft worden met een administratieve geldboete. § 2. Wordt gestraft met een geldboete van 500 tot 75.000 €, de overtreder die de in de artikelen 16 en 19 bedoelde verplichtingen inzake het melden van incidenten niet nakomt. § 3. Wordt gestraft met een geldboete van 500 tot 100.000 €, de overtreder die de in de artikelen 13 en 18 bedoelde beveiligingsverplichtingen niet nakomt. § 4. Wordt gestraft met een geldboete van 500 tot 125.000 €, de overtreder die de controleverplichtingen bedoeld in de hoofdstukken 1 en 2 van titel 4 niet nakomt. § 5. Wordt gestraft met een geldboete van 500 tot 125.000 €, de overtreder die de in artikel 11 bedoelde informatieverplichtingen niet nakomt.	Art. 27. § 1er. Lors de la constatation d'infractions à la présente loi ou à ses arrêtés d'exécution, une amende administrative peut être infligée à l'auteur de l'infraction. § 2. Est puni d'une amende de 500 à 75.000 € l'auteur de l'infraction qui ne se conforme pas aux obligations de notification d'incidents visées aux articles 16 et 19. § 3. Est puni d'une amende de 500 à 100.000 € l'auteur qui ne se conforme pas aux obligations de sécurité visées aux articles 13 et 18. § 4. Est puni d'une amende de 500 à 125.000 € l'auteur qui ne se conforme pas aux obligations de contrôle visées au chapitre 1er et 2 du titre 4. § 5. Est puni d'une amende de 500 à 125.000 € l'auteur qui ne se conforme pas aux obligations d'information visées à l'article 11.
Art. 28. Het origineel van het proces-verbaal wordt naar de procureur des Konings gestuurd. Tegelijk wordt een kopie van het proces-verbaal naar de overtreder gestuurd.	Art. 28. L'original du procès-verbal est envoyé au procureur du Roi. Une copie du procès-verbal est dans le même temps envoyée à l'auteur.
Art. 29. De procureur des Konings beschikt over een termijn van twee maanden, te rekenen vanaf de dag van ontvangst van het proces-verbaal, om de overtreder in te lichten dat strafrechtelijke vervolging is ingesteld. De sectorale overheid mag de procedure voor het opleggen van een administratieve geldboete niet opstarten vóór het verstrijken van voormelde termijn, behalve indien de procureur des Konings vooraf meedeelt dat hij geen gevolg aan het feit wenst te geven. Wanneer de procureur des Konings nalaat binnen de gestelde termijn van zijn beslissing kennis te geven of van strafvervolging afziet, kan de sectorale overheid beslissen de administratieve procedure op te starten.	Art. 29. Le procureur du Roi dispose d'un délai de deux mois à compter du jour de la réception du procès-verbal pour informer l'auteur que des poursuites pénales ont été engagées. L'autorité sectorielle ne peut diligenter la procédure pour infliger une amende administrative avant l'échéance du délai précité, sauf communication préalable par le procureur du Roi que celui-ci ne souhaite pas réserver de suite au fait. Dans le cas où le procureur du Roi omet de notifier sa décision dans le délai fixé ou renonce à intenter des poursuites pénales, l'autorité sectorielle peut décider d'entamer la procédure administrative.

Art. 30. § 1. De beslissing om een administratieve geldboete op te leggen wordt gemotiveerd. Ze vermeldt ook het bedrag van de administratieve geldboete en de bedoelde inbreuken. § 2. De sectorale overheid bezorgt de overtreder op voorhand haar gemotiveerd voorstel van administratieve sanctie en laat hem weten dat hij het recht heeft om, binnen de 15 dagen na ontvangst van het voorstel, zijn verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. Het voorstel wordt geacht te zijn ontvangen door de overtreder de vierde werkdag na de verzending ervan door de sectorale overheid. § 3. Rekening houdend met de aangevoerde verweermiddelen binnen de in paragraaf 2 bedoelde termijn en bij gebrek aan een antwoord van de overtreder binnen diezelfde termijn, kan de sectorale overheid een in artikel 25 bedoelde administratieve sanctie opleggen. § 4. De administratieve geldboete staat in verhouding tot de ernst, de duur, de gebruikte middelen, de veroorzaakte schade en de omstandigheden van de feiten. De administratieve geldboete wordt verdubbeld in geval van herhaling van dezelfde feiten binnen een termijn van drie jaar. § 5. De samenloop van meerdere inbreuken kan aanleiding geven tot één enkele administratieve geldboete die in verhouding staat tot de ernst van het geheel van de feiten.	Art. 30. § 1er. La décision d'imposer une amende administrative est motivée. Elle mentionne également le montant de l'amende administrative et les manquements visés. § 2. L'autorité sectorielle informe au préalable l'auteur de sa proposition motivée de sanction administrative et lui fait part de son droit, dans les 15 jours de la réception de la proposition, de formuler par écrit ses moyens de défense ou de solliciter d'être d'entendu. La proposition est présumée reçue par l'auteur le quatrième jour ouvrable suivant son envoi par l'autorité sectorielle. § 3. En tenant compte des moyens de défense invoqués dans le délai visé au paragraphe 2 ou en l'absence de réaction de l'auteur dans ce même délai, l'autorité sectorielle peut adopter une sanction administrative visée à l'article 25. § 4. L'amende administrative est proportionnelle à la gravité, la durée, les moyens utilisés, les dommages causés et les circonstances des faits. L'amende administrative est doublée en cas de récidive pour les mêmes faits dans un délai de trois ans. § 5. Le concours de plusieurs infractions peut donner lieu à une amende administrative unique proportionnelle à la gravité de l'ensemble des faits.
Art. 31. De beslissing wordt bij een ter post aangetekend schrijven ter kennis gebracht van de overtreder. Een verzoek tot betaling van de geldboete binnen een maand wordt bij de beslissing gevoegd.	Art. 31. La décision est notifiée par lettre recommandée à la poste à l'auteur de l'infraction. Une invitation à acquitter l'amende dans un délai d'un mois est jointe.
Art. 32. De overtreder die de beslissing van de sectorale overheid betwist, kan, op straffe van nietigheid die ambtshalve wordt uitgesproken en op straffe van verval, binnen een termijn van zestig dagen vanaf de ontvangst van de kennisgeving van de beslissing, beroep instellen bij ondertekend verzoekschrift dat bij de griffie van het Marktenhof, bedoeld in artikel 101 van het Gerechtelijk Wetboek, wordt ingediend.	Art. 32. L'auteur de l'infraction qui conteste la décision de l'autorité sectorielle peut interjeter appel, à peine de nullité prononcée d'office, par voie de requête signée et déposée au greffe auprès de la Cour des marchés, visée à l'article 101 du Code judiciaire, dans un délai de soixante jours à partir de la réception de la notification de la décision, à peine de déchéance.

Het Marktenhof behandelt de zaak zoals in kort geding overeenkomstig de artikelen 1035 tot 1038, 1040 en 1041 van het Gerechtelijk Wetboek en kan de beslissing herzien. Dit beroep schorst de uitvoering van de beslissing niet.	La Cour des marchés traite l'affaire selon les formes du référé conformément aux articles 1035 à 1038, 1040 et 1041 du Code judiciaire et peut réformer la décision. Ce recours ne suspend pas l'exécution de la décision.
Art. 33. Als de overtreder de administratieve geldboete niet betaalt binnen de gestelde termijn en de in artikel 30 bepaalde beroepsmogelijkheid is uitgeput, is de beslissing om een administratieve geldboete op te leggen rechtstreeks uitvoerbaar en kan de sectorale overheid een dwangbevel uitvaardigen.	Art. 33. Lorsque l'auteur de l'infraction reste en défaut de payer l'amende administrative dans le délai imparti et que la possibilité de recours fixée à l'article 30 est épuisée, la décision d'infliger une amende administrative a force exécutoire et l'autorité sectorielle peut décerner une contrainte.
Art. 34. De sectorale overheid kan geen administratieve geldboete opleggen als een termijn van drie jaar, te rekenen vanaf de dag waarop de feiten vastgesteld worden, verstreken is. De betaling overeenkomstig de administratieve procedure doet ook de mogelijkheid vervallen om strafrechtelijke vervolging in te stellen voor de bedoelde feiten.	Art. 34. L'autorité sectorielle ne peut imposer d'amende administrative à l'échéance d'un délai de trois ans, à compter du jour où le fait est constaté. Le paiement selon la procédure administrative éteint également la possibilité d'engager des poursuites pénales pour les faits visés.
Titel 5. - Slotbepalingen	Titre 5. - Disposition finales
Art. 35 De personen die optreden voor rekening van een aanbieder van essentiële diensten of digitaaldienstverlener mogen geen nadelige gevolgen ondervinden vanwege de aanbieder van essentiële diensten of digitaaldienstverlener ingevolge de uitvoering, te goeder trouw en in het kader van hun functie, van de verplichtingen die voortvloeien uit deze wet.	Art. 35. Les personnes qui agissent pour le compte d'un opérateur de services essentiels ou d'un fournisseur de service numérique ne peuvent subir de conséquences négatives de la part de l'opérateur de services essentiels ou du fournisseur de service numérique en raison de l'exécution, de bonne foi et dans le cadre de leurs fonctions, des obligations découlant de la présente loi.
Hoofdstuk 1. Wijzigingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur	Chapitre 1. Modifications de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques
Art. 36. In artikel 3 van de wet wordt een 13° ingevoegd, luidende: " "CCB": het Centrum voor Cybersecurity België als bedoeld in artikel 6, 1°, van de wet van xx xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid". In artikel 3 van de wet wordt een 14° ingevoegd, luidende: " "beveiliging van netwerk- en informatiesystemen": de beveiliging van netwerk- en informatiesystemen als bedoeld in artikel 6, 8° en 9°, van de wet van xx xx 2018 tot vaststelling van een kader voor	Art. 36. A l'article 3 de la loi, est inséré un 13°, rédigé comme suit : « « CCB » : Centre pour la Cybersécurité Belgique, tel que visé à l'article 6, 1°, de la loi du xx xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ». A l'article 3 de la loi, est inséré un 14°, rédigé comme suit : « « sécurité des réseaux et systèmes d'information » : la sécurité des réseaux et systèmes d'information au sens de l'article 6, 8° et 9° de la loi du xx xx 2018 établissant un cadre pour la sécurité des

de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”.	réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ».
Art. 37. In artikel 5 van de wet wordt een paragraaf 3 toegevoegd, luidende: “§ 3. Tijdens het hele identificatieproces, als bedoeld in deze afdeling, wordt het CCB betrokken bij het door de sectorale overheden en de ADCC gevoerde nationale en internationale overleg voor de identificatie van de kritieke infrastructuur met betrekking tot de beveiliging van netwerk- en informatiesystemen.”.	Art. 37. A l'article 5 de la loi, un paragraphe 3 est ajouté et rédigé comme suit : « § 3. Tout au long du processus d'identification visé à la présente section, le CCB est associé aux concertations nationales et internationales menées par les autorités sectorielles et la DGCC, pour les aspects de l'identification des infrastructures critiques liés à la sécurité des réseaux et systèmes d'information. ».
Art. 38. Op het einde van paragraaf 2 van artikel 14 van de wet worden de volgende woorden toegevoegd: “en, in voorkomend geval, het CCB wat de beveiliging van netwerk- en informatiesystemen betreft.”.	Art. 38. A la fin du paragraphe 2 de l'article 14 de la loi, il est ajouté les mots « et, le cas échéant, le CCB pour ce qui concerne la sécurité des réseaux et systèmes d'information. ».
Art. 39. In artikel 18 van de wet worden de woorden “De ADCC, de politiediensten en het OCAD” vervangen door de woorden “De ADCC, de politiediensten, het OCAD en, in voorkomend geval, het CCB, wat de beveiliging van netwerk- en informatiesystemen betreft.”.	Art. 39. A l'article 18 de la loi, les mots « La DGCC, les services de police et l'OCAM » sont remplacés par « La DGCC, les services de police, l'OCAM et, le cas échéant le CCB pour ce qui concerne la sécurité des réseaux et systèmes d'information, ».
Art. 40. In artikel 19 van de wet worden de woorden “De exploitant, het beveiligingscontactpunt, de sectorale overheid, de ADCC, het OCAD en de politiediensten” vervangen door de woorden “De exploitant, het beveiligingscontactpunt, de sectorale overheid, de ADCC, het OCAD, de politiediensten en, in voorkomend geval, het CCB, wat de beveiliging van netwerk- en informatiesystemen betreft.”.	Art. 40. A l'article 19 de la loi, les mots « L'exploitant, le point de contact pour la sécurité, l'autorité sectorielle, la DGCC, l'OCAM et les services de police » sont remplacés par « L'exploitant, le point de contact pour la sécurité, l'autorité sectorielle, la DGCC, l'OCAM, les services de police et, le cas échéant, le CCB pour ce qui concerne la sécurité des réseaux et systèmes d'information ».
Art. 41. In artikel 22 van de wet worden de woorden “De sectorale overheid, de ADCC, het OCAD en de politiediensten” vervangen door de woorden “De sectorale overheid, de ADCC, het OCAD, de politiediensten en het CCB”.	Art. 41. A l'article 22 de la loi, les mots « L'autorité sectorielle, la DGCC, l'OCAM et les services de police » sont remplacés par : « L'autorité sectorielle, la DGCC, l'OCAM, les services de police et le CCB ».
Art. 42. In artikel 3 van de wet worden de volgende wijzigingen aangebracht: a) 3°, c) wordt gewijzigd als volgt: “voor de sector financiën, met uitzondering van de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU: de Nationale Bank van België (NBB); voor de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuur voor de markten voor	Art. 42. A l'article 3 de la loi, les modifications suivantes sont apportées : a) le 3°, c) est modifié comme suit : « pour le secteur des finances, à l'exception des opérateurs de plate-forme de négociation au sens de l'article 3, 6° de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la directive 2014/65/UE : la Banque nationale de Belgique (BNB) ; pour les opérateurs de plate-forme de négociation au sens de l'article 3, 6° de la loi du 21 novembre

financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU: de Autoriteit voor Financiële Diensten en Markten (FSMA);”; b) een 3°, e) wordt ingevoegd, luidende: “voor de sector van de digitale infrastructuur: het Belgisch Instituut voor postdiensten en telecommunicatie (B.I.P.T.);”; c) een 3°, f) wordt ingevoegd, luidende: “voor de gezondheidssector: de Minister bevoegd voor Volksgezondheid of, bij delegatie van deze laatste, een leidend personeelslid van zijn administratie;”;	2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la directive 2014/65/UE: l'Autorité des services et marchés financiers (FSMA) ; » ; b) un 3°, e) est inséré, rédigé comme suit : « pour le secteur des infrastructures numériques : l'Institut belge des services postaux et des télécommunications (I.B.P.T.) ; » ; c) un 3°, f) est inséré, rédigé comme suit : « pour le secteur de la santé : le Ministre ayant la Santé publique dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration ; » ;
Hoofdstuk 2. Wijzigingen van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.	Chapitre 2. Modifications de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire.
Art. 43. In hoofdstuk III van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle wordt een artikel 15ter ingevoegd, dat als volgt luidt: “Art. 15ter. Het Agentschap wordt aangewezen als inspectiedienst, als bedoeld in artikel 22 van de wet van xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang en is het belast met het controleren van de toepassing van de bepalingen van deze wet en de uitvoeringsbesluiten ervan door de aanbieders van essentiële diensten, die krachtens bovengenoemde wet geïdentificeerd zijn, wat betreft de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit. De Koning bepaalt de controlemodaliteiten”.	Art. 43. Dans le chapitre III de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, il est inséré un article 15ter rédigé comme suit : « Art. 15ter. L'Agence est désignée comme service d'inspection, au sens de l'article 22 de la loi du xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique et est chargée du contrôle de l'application des dispositions de ladite loi et de ses arrêtés d'exécution par les opérateurs de services essentiels, identifiés en vertu de la loi susmentionnée, pour ce qui concerne les éléments d'une installation nucléaire destinée à la production industrielle d'électricité et qui servent au transport de l'électricité. Le Roi fixe les modalités de contrôle ».
Hoofdstuk 3. Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector	Chapitre 3. Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges
Art. 44. Artikel 1/1 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, ingevoegd bij de wet van 10 juli 2012, wordt aangevuld met een lid, luidende:	Art. 44. L'article 1er/1 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, inséré par la loi du 10 juillet 2012, est complété par un alinéa rédigé comme suit :

“Deze wet voorziet in een gedeeltelijke omzetting van richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.”.	« La présente loi transpose partiellement la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. ».
Art. 45. In artikel 14, § 1, eerste lid, van dezelfde wet, gewijzigd bij de wetten van 13 december 2010, 10 juli 2012, 27 maart 2014, 18 april 2017, 5 mei 2017 en 31 juli 2017, worden de volgende wijzigingen aangebracht: 1° de woorden “, met betrekking tot de sector van de digitale infrastructuur en” worden ingevoegd tussen de woorden “radioapparatuur” en de woorden “met betrekking tot”; 2° in de bepaling onder 3° worden de woorden “, van de wet van 1 juli 2011 betreffende de veiligheid en de bescherming van de kritieke infrastructuur, wat de sector van de elektronische communicatie betreft, van de wet [omzetting NIS-wet], wat de sector van de digitale infrastructuur betreft” ingevoegd tussen de woorden “in het tweetalig gebied Brussel-Hoofdstad” en de woorden “en hun uitvoeringsbesluiten”.	Art. 45. Dans l'article 14, § 1er, alinéa 1er, de la même loi, modifié par les lois du 13 décembre 2010, 10 juillet 2012, 27 mars 2014, 18 avril 2017, 5 mai 2017 et 31 juillet 2017, les modifications suivantes sont apportées : 1° les mots « , en ce qui concerne le secteur des infrastructures numériques, » sont insérés entre les mots « équipement hertzien » et les mots « et en ce qui concerne » ; 2° au 3°, les mots « , de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne le secteur des communications électroniques, de la loi [transposition loi NIS], pour ce qui concerne le secteur des infrastructures numériques » sont insérés entre les mots « en région bilingue de Bruxelles-Capitale » et les mots « et de leurs arrêtés d'exécution ».
Art. 46. In artikel 24, eerste lid, van dezelfde wet, gewijzigd door de wet van 27 maart 2014 worden de woorden “, de wet van 1 juli 2011 betreffende de veiligheid en de bescherming van de kritieke infrastructuur, wat de elektronische-communicatiesector betreft, de wet [wet tot omzetting van de NIS-richtlijn], wat de sector van de digitale infrastructuur betreft” ingevoegd tussen de woorden “in het tweetalig gebied Brussel-Hoofdstad” en de woorden “en hun uitvoeringsbesluiten”.	Art. 46. Dans l'article 24, alinéa 1er, de la même loi, modifié par la loi du 27 mars 2014, les mots « , ainsi qu' à la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne le secteur des communications électroniques, et à la loi [loi de transposition de la directive NIS], pour ce qui concerne le secteur des infrastructures numériques, » sont insérés entre les mots « dans la région bilingue de Bruxelles-Capitale » et les mots « et à leurs arrêtés d'exécution ».
Hoofdstuk 4. Wijzigingen van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU en van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten	Chapitre 4. Modifications de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE et de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers
Art. 47. § 1. Artikel 71 van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU wordt aangevuld met de woorden “en van de artikelen 11 en 14, §§ 2 en 3 van de wet van [...] 2018 tot vaststelling van een kader voor de beveiliging van	Art. 47. § 1er. L'article 71 de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE est complété par les mots « et des articles 11 et 14, §§ 2 et 3 de la loi du [...] 2018 établissant un cadre pour la sécurité des réseaux et des systèmes

netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”. § 2. Artikel 79 van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU wordt aangevuld met een paragraaf 4, luidend als volgt: “§ 4. De in dit artikel bedoelde maatregelen mogen ook genomen worden in geval van overtreding van de artikelen 11 en 14, §§ 2 en 3 van de wet van [...] 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”.	d’information d’intérêt général pour la sécurité publique ». § 2. L’article 79 de la loi du 21 novembre 2017 relative aux infrastructures des marchés d’instruments financiers et portant transposition de la Directive 2014/65/UE est complété par un paragraphe 4, rédigé comme suit : « § 4. Les mesures visées au présent article peuvent également être prises en cas de violation des articles 11 et 14, §§ 2 et 3 de la loi du [...] 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique ».
Art. 48. Punt 15° van artikel 75, § 1, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector, opgeheven door de wet van 5 december 2017 houdende diverse financiële bepalingen, wordt hersteld in de volgende lezing: “15° binnen de grenzen van het recht van de Europese Unie, aan het Centrum voor Cybersecurity België en de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken voor de uitvoering van de bepalingen van de wet van ... 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur”.	Art. 48. Le point 15° de l’article 75, § 1 de la loi du 2 août 2002 relative à la surveillance du secteur financier, abrogé par la loi du 5 décembre 2017 portant des dispositions financières diverses, est rétabli dans la rédaction suivante : « 15° dans les limites du droit de l’Union européenne, au Centre pour la Cybersécurité Belgique et à la Direction générale Centre de Crise du Service public fédéral Intérieur pour les besoins de l’exécution des dispositions de la loi du ... 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques».
Hoofdstuk 5. Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België	Chapitre 5. Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique
Art. 49. Artikel 36/14, § 1, van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België wordt aangevuld als volgt: 20° de woorden “aan het Centrum voor Cybersecurity België” worden ingevoegd tussen de woorden “de analyse van de dreiging,” en “en aan de politiediensten”; 24°: “24° binnen de grenzen van het recht van de Europese Unie, aan het Centrum voor Cybersecurity België en de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken voor de uitvoering van de bepalingen van de wet van ... 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.”.	Art. 49. L’article 36/14, §1er de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique est complété comme suit : 20° entre les mots « l’analyse de la menace » et « et aux services de police » sont ajoutés les mots « au Centre pour la Cybersécurité Belgique »; 24°: « 24° dans les limites du droit de l’Union européenne, au Centre pour la Cybersécurité Belgique et à la Direction générale Centre de Crise du Service public fédéral Intérieur pour les besoins de l’exécution des dispositions de la loi du ... 2018. ».

Art. 50 . In dezelfde wet wordt een hoofdstuk IV/4 ingevoegd, bestaande uit één enkel artikel 36/47, luidende: “Hoofdstuk IV/4 Toezicht door de Bank in het kader van de wet van ... 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid. Art. 36/47. De Bank ziet als bevoegde sectorale overheid toe op de naleving door de aanbieders van de sector financiën van de bepalingen van de wet van xx 2018, met uitzondering van de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU. De artikelen 36/19 en 36/20 zijn van toepassing. De Sanctiecommissie oordeelt over het opleggen van de administratieve geldboetes bedoeld in artikel 27 van de wet van ... 2018 [de datum en titel van de NIS-wet invullen]. De artikelen 36/8 tot 36/12/3 en artikel 36/21 zijn van toepassing.”.	Art. 50. Dans la même loi, il est inséré un chapitre IV/4, comportant un seul article 36/47 rédigé comme suit : « Chapitre IV/4 Surveillance par la Banque dans le cadre de la loi du ... 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. Art. 36/47. En tant qu'autorité sectorielle compétente, la Banque contrôle le respect par les opérateurs du secteur des finances, des dispositions de la loi du xx 2018, à l'exception des opérateurs de plate-forme de négociation au sens de l'article 3, 6° de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE. Les articles 36/19 et 36/20 sont applicables. La Commission des sanctions statue sur l'imposition des amendes administratives prévues à l'article 27 de la loi du ... 2018 [compléter par la date et l'intitulé de la loi NIS]. Les articles 36/8 à 36/12/3 et l'article 36/21 sont applicables. ».
Hoofdstuk 6. Inwerkingtreding	Chapitre 6. Entrée en vigueur
Art 51. Deze wet treedt in werking de dag waarop ze in het Belgisch Staatsblad wordt bekendgemaakt.	Art. 51. La présente loi entre en vigueur le jour de sa publication au Moniteur belge.

Bijlage I

Voorschriften en taken van het nationale CSIRT

De voorschriften en taken van het nationale CSIRT omvatten onder meer de volgende elementen:

1) Voorschriften voor het nationale CSIRT

a) Het nationale CSIRT garandeert een hoge mate van beschikbaarheid van zijn communicatiediensten door zwakke punten (single points of failure) te voorkomen, en beschikt over diverse kanalen waarlangs te allen tijde contact met hen kan worden opgenomen en contact met anderen kan worden opgenomen.

De communicatiekanalen moeten voorts duidelijk worden gespecificeerd en bekend zijn bij de gebruikersgroep en de samenwerkingspartners.

b) De lokalen van het nationale CSIRT en zijn ondersteunende informatiesystemen bevinden zich op beveiligde locaties.

c) Bedrijfscontinuïteit:

i) het nationale CSIRT wordt, met het oog op vlote overdrachten, uitgerust met een adequaat systeem voor het beheren en routeren van verzoeken;

ii) het nationale CSIRT krijgt voldoende personeel om een volcontinue beschikbaarheid te garanderen;

iii) het nationale CSIRT doet een beroep op infrastructuur waarvan de continuïteit gewaarborgd is. Hiertoe wordt voorzien in redundante systemen en reservewerkruimten.

d) Het nationale CSIRT neemt deel aan de vergaderingen van het CSIRT-netwerk bedoeld in artikel 12 van de NIS-richtlijn.

2) Taken van het nationale CSIRT

a) De taken van het nationale CSIRT omvatten ten minste het volgende:

i) monitoren van incidenten op nationaal niveau;

ii) ten bate van de betrokken belanghebbende partijen zorgen voor vroegtijdige waarschuwingen, alarmmeldingen, aankondigingen en verspreiding van informatie over risico's en incidenten;

Annexe I

Obligations et tâches du CSIRT national

Les obligations et tâches du CSIRT national comprennent notamment les éléments suivants :

1) Obligations du CSIRT national

a) Le CSIRT national garantit un niveau élevé de disponibilité de ses services de communication en évitant les points uniques de défaillance et dispose de plusieurs moyens pour être contactés et contacter autrui à tout moment.

De plus, ses canaux de communication doivent être clairement précisés et bien connus des partenaires et collaborateurs.

b) Les locaux du CSIRT national et ses systèmes d'information se trouvent sur des sites sécurisés.

c) Continuité des opérations :

i) Le CSIRT national est doté d'un système approprié de gestion et de routage des demandes afin de faciliter les transferts.

ii) Le CSIRT national est doté des effectifs adéquats afin de pouvoir garantir une disponibilité permanente.

iii) Le CSIRT national s'appuie sur une infrastructure dont la continuité est garantie. À cette fin, des systèmes redondants et un espace de travail de secours sont disponibles.

d) Le CSIRT national participe aux réunions du réseau des CSIRT visé à l'article 12 de la directive NIS.

2) Tâches du CSIRT national

a) Les tâches du CSIRT national comprennent au moins les éléments suivants :

i) suivi des incidents au niveau national ;

ii) activation du mécanisme d'alerte précoce, diffusion de messages d'alerte, annonces et diffusion d'informations sur les risques et incidents auprès des parties intéressées ;

iii) reageren op incidenten; iv) zorgen voor een dynamische risico- en incidentanalyse en situatiekennis; v) deelnemen aan het CSIRT-netwerk bedoeld in artikel 12 van de NIS-richtlijn. b) Het nationale CSIRT zorgt voor op samenwerking gerichte contacten met de particuliere sector. c) Ter bevordering van de samenwerking stimuleert het nationale CSIRT de vaststelling en het gebruik van gemeenschappelijke of gestandaardiseerde praktijken op het gebied van: i) procedures voor de behandeling van incidenten en risico's; ii) systemen voor de classificatie van incidenten, risico's en informatie. d) Bij de behandeling van meldingen verwerkt het nationale CSIRT de door de wet opgelegde verplichte meldingen prioritair ten opzichte van vrijwillige meldingen. Vrijwillige meldingen worden enkel verwerkt wanneer die verwerking geen onevenredige of overmatige belasting voor het nationale CSIRT vormt. Voorschriften en taken van het sectorale CSIRT 1) Voorschriften van het sectorale CSIRT a) Het sectorale CSIRT garandeert een hoge mate van beschikbaarheid van zijn communicatiediensten door zwakke punten (single points of failure) te voorkomen, en beschikt over diverse kanalen waarlangs te allen tijde contact met hen kan worden opgenomen en contact met anderen kan worden opgenomen. De communicatiekanalen moeten voorts duidelijk worden gespecificeerd en bekend zijn bij de gebruikersgroep en de samenwerkingspartners. b) De lokalen van het sectorale CSIRT en zijn ondersteunende informatiesystemen moeten zich op beveiligde locaties bevinden. c) Bedrijfscontinuïteit:	iii) intervention en cas d'incident ; iv) analyse dynamique des risques et incidents et conscience situationnelle ; v) participation au réseau des CSIRT visé à l'article 12 de la directive NIS. b) Le CSIRT national établit des relations de coopération avec le secteur privé. c) Pour faciliter la coopération, le CSIRT national promeut l'adoption et l'utilisation de pratiques communes normalisées pour : i) les procédures de gestion des risques et incidents ; ii) les systèmes de classification des incidents, risques et informations. d) Lors du traitement des notifications, le CSIRT national donne la priorité aux notifications obligatoires imposées par la loi par rapport aux notifications volontaires. Les notifications volontaires ne sont traitées que lorsque leur traitement ne fait pas peser de charge disproportionnée ou inutile à charge du CSIRT national. Obligations et tâches du CSIRT sectoriel 1) Obligations du CSIRT sectoriel a) Le CSIRT sectoriel doit veiller à un niveau élevé de disponibilité de ses services de communication en évitant les points uniques de défaillance et dispose de plusieurs moyens pour être contactés et contacter autrui à tout moment. De plus, ses canaux de communication doivent être clairement précisés et bien connus des partenaires et collaborateurs. b) Les locaux du CSIRT sectoriel et ses systèmes d'information doivent se trouver sur des sites sécurisés. c) Continuité des opérations : i) Le CSIRT sectoriel est doté d'un système approprié de gestion et de routage des demandes afin de faciliter les transferts.
--	---

i) het sectorale CSIRT wordt, met het oog op vlotte overdrachten, uitgerust met een adequaat systeem voor het beheren en routeren van verzoeken; ii) het sectorale CSIRT krijgt voldoende personeel om een volcontinue beschikbaarheid te garanderen; iii) het sectorale CSIRT doet een beroep op infrastructuur waarvan de continuïteit gewaarborgd is. Hiertoe wordt voorzien in redundante systemen en reservewerkruimten. d) Het sectorale CSIRT kan, in coördinatie met het CCB, deelnemen aan de vergaderingen van het CSIRT-netwerk bedoeld in artikel 12 van de NIS-richtlijn.	ii) Le CSIRT sectoriel est doté des effectifs adéquats afin de pouvoir garantir une disponibilité permanente. iii) Le CSIRT sectoriel s'appuie sur une infrastructure dont la continuité est garantie. À cette fin, des systèmes redondants et un espace de travail de secours sont disponibles. d) Le CSIRT sectoriel peut, en coordination avec le CCB, participer aux réunions du réseau des CSIRT visé à l'article 12 de la directive NIS.
2) Taken van het sectorale CSIRT a) De taken van het sectorale CSIRT omvatten ten minste het volgende: i) monitoren van sectorale incidenten; ii) ten bate van de betrokken belanghebbende partijen uit de sector zorgen voor vroegtijdige waarschuwingen, alarmmeldingen, aankondigingen en verspreiding van informatie over risico's en incidenten; iii) reageren op sectorale incidenten; iv) zorgen voor een dynamische risico- en incidentanalyse en situatiekennis; v) in coördinatie met het nationale CSIRT kunnen deelnemen aan de vergaderingen van het CSIRT-netwerk bedoeld in artikel 12 van de NIS-richtlijn. b) Het sectorale CSIRT zorgt voor op samenwerking gerichte contacten met de particuliere sector. c) Bij de behandeling van meldingen verwerkt het sectorale CSIRT de door de wet opgelegde verplichte meldingen prioritair ten opzichte van vrijwillige meldingen. Vrijwillige meldingen worden enkel verwerkt wanneer die verwerking geen onevenredige of overmatige belasting voor het sectorale CSIRT vormt.	2) Tâches du CSIRT sectoriel a) Les tâches du CSIRT sectoriel comprennent au moins les éléments suivants : i) suivi des incidents sectoriels ; ii) activation du mécanisme d'alerte précoce, diffusion de messages d'alerte, annonces et diffusion d'informations sur les risques et incidents auprès des parties intéressées du secteur ; iii) intervention en cas d'incident sectoriel ; iv) analyse dynamique des risques et incidents et conscience situationnelle ; v) pouvoir participer, en coordination avec le CSIRT national, aux réunions du réseau des CSIRT visé à l'article 12 de la directive NIS. b) Le CSIRT sectoriel établit des relations de coopération avec le secteur privé. c) Lors du traitement des notifications, le CSIRT sectoriel donne la priorité aux notifications obligatoires imposées par la loi par rapport aux notifications volontaires. Les notifications volontaires ne sont traitées que lorsque leur traitement ne fait pas peser de charge disproportionnée ou inutile à charge du CSIRT sectoriel.

Bijlage II

Soorten aanbieders van essentiële diensten bedoeld in artikel 11, § 1

Sector	Deelsector	Soort entiteit
1. Energie	a) Elektriciteit	Elektriciteitsbedrijven in de zin van artikel 2, 15° ter, van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt.
		Distributienetbeheerders in de zin van artikel 2, 11°, van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt.
		Netbeheerders in de zin van artikel 2, 8°, van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt.
	b) Aardolie	Exploitanten van oliepijpleidingen.
		Exploitanten van installaties voor de productie, raffinage, verwerking, opslag en het vervoer van aardolie.
	c) Gas	Aardgasondernemingen in de zin van artikel 1, 5° bis, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.
		Distributienetbeheerders in de zin van artikel 1, 13°, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.
		Beheerders van het aardgasvervoersnet in de zin van artikel 1, 31°, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.
		Beheerders van de opslag in de zin van artikel 1, 33°, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.
		Beheerders van de LNG-installatie in de zin van artikel 1, 35°, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.
		Exploitanten van raffinage- en verwerkingsinstallaties van aardgas.
2. Vervoer	a) Luchtvervoer	Luchtvaartmaatschappijen in de zin van artikel 3, punt 4) van de verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart en tot intrekking van verordening (EG) nr. 2320/2002.
		Luchthavenbeheerders in de zin van in artikel 2, punt 2), van het KB van 6 november 2010 betreffende de toegang tot de grondafhandelingsmarkt op de luchthaven Brussel-Nationaal, luchthavens in de zin van artikel 2, punt 1), van richtlijn 2009/12/EG van het Europees Parlement en de Raad, met inbegrip van de luchthavens die tot het kernnetwerk behoren, opgesomd in bijlage II, afdeling 2, van verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad,

		alsook entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden.
		Luchtvaartnavigatiediensten in de zin van artikel 2, punt 4), van de verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot vaststelling van het kader voor de totstandbrenging van het gemeenschappelijke Europese luchtruim ("de kaderverordening").
		De netwerkbeheerder in de zin van artikel 2, punt 22), van de verordening (EU) nr. 677/2011 van de Commissie van 7 juli 2011 tot vaststelling van nadere regels ter uitvoering van de netwerkfuncties voor luchtverkeersbeheer en tot wijziging van Verordening (EU) nr. 691/2010.
	b) Spoorvervoer	Infrastructuurbeheerders in de zin van artikel 3, 29°, van de Spoorcodex.
		Spoorwegondernemingen in de zin van artikel 3, 27°, van de Spoorcodex.
	c) Vervoer over water	Bedrijven voor land-, zee- en kustvervoer van passagiers en goederen in de zin van bijlage I van de verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad, behalve schepen die individueel worden geëxploiteerd door die bedrijven.
		Beheerders van havens in de zin van artikel 5, punt 7), van de wet van 5 februari 2007 betreffende de maritieme beveiliging, met inbegrip van hun havenfaciliteiten in de zin van artikel 2, punt 11), van verordening (EG) nr. 725/2004, alsook entiteiten die werken en uitrusting in havens beheren.
		Exploitanten van verkeersbegeleidingssystemen (VBS) in de zin van artikel 1, punt 12), van het KB van 17 september 2005 tot omzetting van richtlijn 2002/59/EG van 27 juni 2002.
	d) Vervoer over de weg	Wegenautoriteiten in de zin van artikel 2, punt 12), van de gedelegeerde verordening (EU) 2015/962 van de Commissie van 18 december 2014 ter aanvulling van Richtlijn 2010/40/EU van het Europees Parlement en de Raad wat de verlening van EU-wijde realtimeverkeersinformatiediensten betreft, belast met de verkeerbeheerscontrole.
		Exploitanten van intelligente vervoerssystemen in de zin van artikel 3, punt 1), van de wet van 17 augustus 2013 tot creatie van het kader voor het invoeren van intelligente vervoerssystemen en tot wijziging van de wet van 10 april 1990 tot regeling van de private en bijzondere veiligheid (geciteerd als "ITS-kaderwet").
3. Financiën	a) Financiële instellingen	Kredietinstellingen in de zin van artikel 4, punt 1), van de verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende prudentiële vereisten voor kredietinstellingen en beleggingsondernemingen en tot wijziging van verordening (EU) nr. 648/2012.
		Centrale tegenpartijen in de zin van artikel 2, punt 1), van de verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters.
		Financiële instellingen (andere dan de kredietinstellingen en de centrale tegenpartijen) die onderworpen zijn aan het toezicht van de Nationale Bank van België, krachtens de artikelen 8 en 12bis van de wet van 22

		februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België.
	b) Financiële handelsplatformen	Exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.
4. Gezondheidszorg	Zorginstellingen (waaronder ziekenhuizen en privéklinieken)	Zorgverleners in de zin van artikel 3, punt g), van de richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg.
5. Levering en distributie van drinkwater		Leveranciers en distributeurs van water bestemd voor menselijke consumptie in de zin van artikel 2, punt 1) a), van de richtlijn 98/83/EG van de Raad van 3 november 1998 betreffende de kwaliteit van voor menselijke consumptie bestemd water, behalve de distributeurs voor wie de distributie van water bestemd voor menselijke consumptie slechts een deel is van hun algemene distributieactiviteit van andere producten en goederen die niet worden beschouwd als essentiële diensten.
6. Digitale infrastructuur		IXP.
		Leveranciers van DNS-diensten.
		Registers van topleveldomeinnamen.

Annexe II

Types d'opérateurs de services essentiels visés à l'article 11, § 1er

Secteur	Sous-secteur	Type d'entités
1. Énergie	a) Électricité	Entreprises d'électricité au sens de l'article 2, 15° ter de la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité.
		Gestionnaires de réseau de distribution au sens de l'article 2, 11° de la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité.
		Gestionnaires de réseau au sens de l'article 2, 8° de la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité.
	b) Pétrole	Exploitants d'oléoducs.
		Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole.
	c) Gaz	Entreprises de gaz naturel au sens de l'article 1, 5° bis de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations.
		Gestionnaires de réseau de distribution au sens de l'article 1, 13° de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations.
		Gestionnaires du réseau de transport de gaz naturel au sens de l'article 1, 31° de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations.
		Gestionnaires de stockage au sens de l'article 1, 33° de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations.
		Gestionnaires d'installation de GNL au sens de l'article 1, 35° de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations.
2. Transports	a) Transport aérien	Exploitants d'installations de raffinage et de traitement de gaz naturel.
		Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) n°300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n°2320/2002.
		Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de l'AR du 6 Novembre 2010 réglementant l'accès au marché de l'assistance en escale à l'aéroport de Bruxelles-National, aéroports au sens de l'article 2, point 1), de la directive 2009/12/CE du Parlement européen et du Conseil, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n°1315/2013 du Parlement européen et du Conseil, et entités exploitant les installations annexes se trouvant dans les aéroports.
		Services de navigation aérienne au sens de l'article 2, point 4), du règlement (CE) n°549/2004 du Parlement européen et du Conseil du 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen («règlement-cadre»).

		Le gestionnaire de réseau au sens de l'article 2, point 22), du règlement (UE) n° 677/2011 de la Commission du 7 juillet 2011 établissant les modalités d'exécution des fonctions de réseau de la gestion du trafic aérien et modifiant le règlement (UE) n° 691/2010.
	b) Transport ferroviaire	Gestionnaires de l'infrastructure au sens de l'article 3, 29° du Code ferroviaire.
		Entreprises ferroviaires au sens de l'article 3, 27° du Code ferroviaire.
	c) Transport par voie d'eau	Sociétés de transport terrestre, maritime et côtier de passagers et de fret au sens de l'annexe I du règlement (CE) n° 725/2004 du Parlement européen et du Conseil, à l'exclusion des navires exploités à titre individuel par ces sociétés.
		Entités gestionnaires des ports au sens de l'article 5 point 7) de la loi du 5 février 2007 relative à la sûreté maritime, y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) n° 725/2004, ainsi que les entités exploitant des ateliers et des équipements à l'intérieur des ports.
		Exploitants de services de trafic maritime (STM) au sens de l'article 1 ^{er} , point 12), de l'AR du 17 septembre 2005 transposant la directive 2002/59/CE du 27 juin 2002.
	d) Transport routier	Autorités routières au sens de l'article 2, point 12), du règlement délégué (UE) 2015/962 de la Commission du 18 décembre 2014 complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne la mise à disposition, dans l'ensemble de l'Union, de services d'informations en temps réel sur la circulation, chargées du contrôle de gestion du trafic.
		Exploitants de systèmes de transport intelligents au sens de l'article 3, point 1), de la loi du 17 août 2013 portant création du cadre pour le déploiement de systèmes de transport intelligents et modifiant la loi du 10 avril 1990 réglementant la sécurité privée et particulière (dénommée : " loi-cadre STI ").
3. Finances	a) Etablissements financiers	Établissements de crédit au sens de l'article 4, point 1), du règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012.
		Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux.
		Etablissements financiers (autres que les établissements de crédit et les contreparties centrales) soumis au contrôle de la Banque nationale de Belgique, en vertu des articles 8 et 12bis de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique.
	b) Plates-formes de négociation financière	Opérateurs de plate-forme de négociation au sens de l'article 3, 6° de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE.
4. Secteur de la santé	Établissements de soins de santé (y compris les	Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers.

	hôpitaux et les cliniques privées)	
5. Fourniture et distribution d'eau potable		Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la directive 98/83/CE du Conseil du 3 novembre 1998 relative à la qualité des eaux destinées à la consommation humaine, à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine ne constitue qu'une partie de leur activité générale de distribution d'autres produits et biens qui ne sont pas considérés comme des services essentiels.
6. Infrastructures numériques		IXP.
		Fournisseurs de services DNS.
		Registres de noms de domaines de haut niveau.

Bijlage III Soorten digitale diensten 1. Onlinemarktplaats 2. Onlinezoekmachines 3. Cloudcomputerdiensten	Annexe III Types de services numériques 1. Place de marché en ligne 2. Moteurs de recherche en ligne 3. Service d'informatique en nuage
---	---

Bijlage IV	Annexe IV
De sectorale overheden aangewezen voor de in bijlage II bedoelde sectoren	Les autorités sectorielles désignées pour les secteurs visés à l'annexe II
a) voor de energiesector: de federale Minister bevoegd voor Energie of, bij delegatie van deze laatste, een leidend personeelslid van zijn/haar administratie; b) voor de transportsector: de federale Minister bevoegd voor Vervoer of, bij delegatie van deze laatste, een leidend personeelslid van zijn/haar administratie; c) voor de sector financiën, met uitzondering van de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU: de Nationale Bank van België (NBB) als bedoeld in de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België; d) voor exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU: de Autoriteit voor Financiële Diensten en Markten (FSMA) als bedoeld in de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten; e) voor de gezondheidssector: de federale Minister bevoegd voor Volksgezondheid of, bij delegatie van deze laatste, een leidend personeelslid van zijn/haar administratie; f) voor de sector van de digitale infrastructuur: het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT) als bedoeld in de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.	a) pour le secteur de l'énergie: le Ministre fédéral ayant l'Energie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration ; b) pour le secteur des transports : le Ministre fédéral ayant les Transports dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration ; c) pour le secteur des finances, à l'exception des opérateurs de plate-forme de négociation au sens de l'article 3, 6° de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE : la Banque nationale de Belgique (BNB) visée par la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique ; d) pour les opérateurs de plate-forme de négociation au sens de l'article 3, 6° de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la directive 2014/65/UE : l'Autorité des services et marchés financiers (FSMA) visée par la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers ; e) pour le secteur de la santé : le Ministre fédéral ayant la Santé publique dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration ; f) pour le secteur des infrastructures numériques : l'Institut belge des services postaux et des télécommunications (IBPT) visé par la loi du 17 janvier 2003 relative au

De sectorale overheden aangewezen voor de digitaaldienstverleners bedoeld in bijlage III voor de sector van de digitaaldienstverleners: de federale Minister bevoegd voor Economie of, bij delegatie van deze laatste, een leidend personeelslid van zijn/haar administratie;	statut du régulateur des secteurs des postes et des télécommunications belges. Les autorités sectorielles désignées pour les fournisseurs de service numérique visés à l'annexe III pour le secteur des fournisseurs de service numériques : le Ministre fédéral ayant l'Economie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration ;
--	--

MEMORIE VAN TOELICHTING

MEVROUWEN, MIJNE HEREN,

ALGEMENE BESCHOUWINGEN

Dit wetsontwerp beoogt met name de omzetting van de Europese richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, hierna "NIS-richtlijn" genoemd.

Netwerk- en informatiesystemen spelen een cruciale rol in onze moderne maatschappij. Een groot deel van de entiteiten die essentiële diensten verlenen voor het behoud van kritieke maatschappelijke of economische activiteiten in België zijn afhankelijk van netwerk- en informatiesystemen. De verstoring van de in de wet bedoelde digitale diensten kan ook verhinderen dat diezelfde essentiële diensten worden verleend. Ook tal van overheden gebruiken de in de wet bedoelde digitale diensten in het kader van hun opdrachten van algemeen belang.

De verplichtingen vervat in de NIS-richtlijn gelden voor entiteiten die, in geval van een incident dat de beveiliging van hun netwerk- en informatiesystemen aantast, de verlening van essentiële diensten voor het behoud van kritieke maatschappelijke of economische activiteiten aanzienlijk kunnen verstoren. De NIS-richtlijn bepaalt ook dat bij de beoordeling van het belang van het verstorende effect van een incident met name rekening moet worden gehouden met de gevolgen ervan voor economische of maatschappelijke activiteiten of voor de openbare veiligheid.

De NIS-richtlijn heeft tot doel ervoor te zorgen dat technische en organisatorische beveiligingsmaatregelen worden genomen door de aanbieders van essentiële diensten om incidenten te voorkomen of de impact ervan te beperken, teneinde de continuïteit van essentiële diensten te waarborgen. In dezelfde geest heeft de in de richtlijn vervatte meldingsplicht van incidenten betrekking op incidenten die een aanzienlijke impact hebben op de verleende essentiële diensten.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

CONSIDÉRATIONS GÉNÉRALES

Ce projet de loi vise notamment à transposer la Directive européenne (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, ci-après dénommée la "Directive NIS".

Les réseaux et systèmes d'information jouent un rôle crucial dans nos sociétés modernes. Une grande partie des entités fournissant des services essentiels au maintien d'activités sociétales ou économiques critiques en Belgique sont tributaires de réseaux et systèmes d'information. La perturbation des services numériques visés par la loi est également susceptible d'empêcher la fourniture de ces mêmes services essentiels. De même, de nombreuses autorités publiques utilisent les services numériques visés par la loi, dans le cadre de leurs missions d'intérêt général.

Les destinataires des obligations de la directive NIS sont les entités susceptibles, en cas d'incident affectant la sécurité de leurs réseaux et systèmes d'information, de perturber de manière importante la fourniture de services essentiels au maintien d'activités sociétales ou économiques critiques. La directive NIS précise également que l'importance de l'effet perturbateur d'un incident doit s'apprécier notamment au regard de ses conséquences sur les fonctions économiques ou sociétales ou sur la sûreté publique.

L'objectif de la directive NIS est d'assurer la prise de mesures de sécurité techniques et organisationnelles par les opérateurs de services essentiels pour prévenir les incidents ou en limiter l'impact, en vue d'assurer la continuité des services essentiels. Dans le même esprit, les obligations de notification des incidents contenues dans la directive portent sur les incidents qui ont un impact significatif sur les services essentiels fournis.

De omvang, de frequentie en de gevolgen van incidenten die netwerk- en informatiesystemen aantasten, nemen almaar toe en vormen een grote bedreiging voor de goede werking van de essentiële diensten ervan. De informatiesystemen kunnen met name een doelwit worden van opzettelijke schadelijke acties die bedoeld zijn om de werking van de systemen te verstoren of te onderbreken.

De bescherming, de beveiliging en de betrouwbaarheid van de netwerk- en informatiesystemen van aanbieders van essentiële diensten en van sommige digitaaldienstverleners zijn voortaan overwegingen van algemeen belang voor de bescherming van de bevolking en de ondernemingen van ons land. De beveiligingsvoorschriften voor hun netwerk- en informatiesystemen vallen bijgevolg onder de openbare orde en veiligheid in ruime zin.

In het licht van deze beschouwingen moeten eisen inzake beveiliging en melding van incidenten van toepassing zijn op aanbieders van essentiële diensten en sommige digitaaldienstverleners om een cultuur van risicobeheer te bevorderen en ervoor te zorgen dat de ernstigste incidenten worden gemeld.

Bovendien blijkt het noodzakelijk om een nationale strategie te ontwikkelen waarin passende strategische en reglementaire doelstellingen worden bepaald met het oog op het tot stand brengen van een hoog beveiligingsniveau van netwerk- en informatiesystemen, ten minste voor de aanbieders van essentiële diensten en digitaaldienstverleners bedoeld in de NIS-richtlijn die actief zijn in België.

Momenteel voorziet het Belgische wetgevende kader enkel in algemene beveiligingsverplichtingen, die ook gelden voor netwerk- en informatiesystemen, voor de exploitanten van zogenaamde "kritieke" infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur, die voorziet in de omzetting van richtlijn 2008/114/EG van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuur, de aanmerking van infrastructuur als Europese kritieke infrastructuur en de beoordeling van de

L'ampleur, la fréquence et l'impact des incidents affectant les réseaux et les systèmes d'information ne cessent de croître et représentent une menace considérable pour le bon fonctionnement de ses services essentiels. Les systèmes d'information peuvent notamment devenir des cibles pour des actions intentionnelles malveillantes qui visent à la détérioration ou à l'interruption de leur fonctionnement.

La protection, la sécurité et la fiabilité des réseaux et systèmes d'information des opérateurs fournissant des services essentiels et de certains fournisseurs de service numérique sont désormais des considérations d'intérêt général pour la protection de la population et des entreprises du pays. Les règles de sécurité de leurs réseaux et systèmes d'information relèvent dès lors de l'ordre et de la sécurité publique au sens large.

Ces considérations imposent donc de soumettre les opérateurs de services essentiels et certains fournisseurs de service numérique à des exigences en matière de sécurité et de notification des incidents, afin de promouvoir une culture de gestion des risques et de faire en sorte que les incidents les plus graves soient signalés.

De plus, il s'avère nécessaire de développer une stratégie nationale qui définit les objectifs stratégiques et réglementaires appropriées en vue de parvenir à un niveau élevé de sécurité des réseaux et des systèmes d'information, au moins pour les opérateurs de services essentiels et les fournisseurs de services numériques visés par la directive NIS et opérant en Belgique.

Actuellement, le cadre législatif belge prévoit seulement des obligations générales de sécurité, en ce compris des réseaux et systèmes d'information, aux exploitants d'infrastructures dites "critiques" au sens de la loi du 1 juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, qui transpose la directive 2008/114/CE du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.

noodzaak de bescherming van dergelijke infrastructuren te verbeteren.

Zoals bepaald in de NIS-richtlijn, wil dit wetsontwerp een gemeenschappelijke aanpak van de door de verschillende soorten aanbieders toegepaste beveiligingsmaatregelen ontwikkelen, de doelgroep van de beveiligingsverplichtingen uitbreiden, de definities herzien en verplichtingen invoeren voor het melden van beveiligingsincidenten.

Tot op heden beschikte ons land niet over een volledig arsenaal aan wetgeving over de beveiliging van netwerk- en informatiesystemen. Dit ontwerp heeft ook tot doel om deze leemte op te vullen, op een gebied waarvan het strategische belang almaar toeneemt.

Het wetsontwerp doet geen afbreuk aan de bepalingen inzake de bescherming van persoonsgegevens vervat in de Europese verordening nr. 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit. Hierbij wordt evenwel opgemerkt dat dit wetsontwerp een aanpak van het beheer van beveiligingsrisico's wil bevorderen die aansluit bij voormelde wetgevingen.

Vanuit institutioneel oogpunt zullen de verschillende ingestelde of bestaande autoriteiten die door dit wetsontwerp gemachtigd worden, een essentiële rol moeten vervullen bij de uitvoering van de wet. Het wetsontwerp beoogt hen daartoe de nodige bevoegdheden en middelen te verschaffen.

De inhoud van de verplichtingen vervat in de NIS-richtlijn heeft betrekking op het beveiligingsniveau van de netwerk- en informatiesystemen van entiteiten die diensten van algemeen belang verlenen voor de bevolking en de ondernemingen, of kritiek zijn voor het economisch potentieel van ons land. De omzetting van de bepalingen ervan in Belgisch recht behoort bijgevolg tot de residuaire bevoegdheden van de federale wetgever inzake de bescherming uitgeoefend op het vlak van openbare veiligheid.

Comme le prévoit de la directive NIS, le présent projet de loi entend mettre en œuvre une approche commune des mesures de sécurité appliquées par les différents types d'opérateurs, élargir les destinataires des obligations de sécurité, revoir les définitions et prévoir des obligations de notification des incidents de sécurité.

Notre pays ne s'était jusqu'à présent pas doté d'un arsenal législatif complet sur la sécurité des réseaux et des systèmes d'information. Le présent projet vise aussi à combler cette lacune, dans un domaine qui devient de plus en plus stratégique.

Le projet de loi est sans préjudice des dispositions en matière de protection des données à caractère personnel prévues par le Règlement européen n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données. Il faut toutefois souligner que le présent projet tend à promouvoir une approche de la gestion des risques de sécurité qui soit en harmonie avec les législations précitées.

D'un point de vue institutionnel, les différentes autorités instituées ou existantes habilitées par le présent projet de loi auront un rôle essentiel à jouer dans la mise en œuvre de la loi. Le projet de loi vise à les investir des compétences et des moyens nécessaires à cette fin.

Le contenu des obligations de la directive NIS porte sur le niveau de sécurité des réseaux et des systèmes d'information des entités fournissant des services d'intérêt général pour la population et les entreprises, ou critiques pour le potentiel économique du pays. La transposition de ses dispositions relève dès lors, en droit belge, des compétences résiduelles du législateur fédéral en matière de protection exercée dans le domaine de la sécurité publique.

Naar analogie van de bepalingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren bepaalt de wet niettemin dat de deelgebieden worden geraadpleegd wanneer sommige aanbieders van essentiële diensten (publiekrechtelijke of privaatrechtelijke personen) of digitaaldienstverleners voor andere aspecten van hun activiteiten onderworpen zouden zijn aan gewestelijke of gemeenschapsregels.

Tot slot blijft de uitoefening van de federale bevoegdheid in het wetsontwerp in elk geval in verhouding en heeft ze niet tot gevolg dat het voor de gewesten of gemeenschappen onmogelijk of bovenmatig moeilijk zou zijn om hun bevoegdheden op de werkterreinen van sommige betrokken aanbieders van essentiële diensten of digitaaldienstverleners gewoon uit te oefenen.

A l'instar des dispositions de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, il est néanmoins prévu dans la loi de consulter les entités fédérées lorsque certains opérateurs de services essentiels (personnes publiques ou privées) ou fournisseurs de services numériques seraient, pour d'autres aspects de leurs activités, soumis à des règles régionales ou communautaires.

Enfin, l'exercice de la compétence fédérale dans le projet de loi reste, en tout état de cause, proportionné et n'a pas pour conséquence de rendre impossible ou exagérément difficile l'exercice normal des compétences régionales ou communautaires dans les domaines d'activités de certains opérateurs de services essentiels ou fournisseurs de services numériques concernés.

ARTIKELSGEWIJZE BESPREKING

TITEL 1

Definities en algemene bepalingen

HOOFDSTUK 1

Onderwerp en toepassingsgebied

Artikel 1

Dit artikel bevat de grondwettelijke grondslag van de wet.

Artikel 2

Dit artikel vermeldt de richtlijn die door de wet wordt omgezet.

Artikel 3

Dit artikel verduidelijkt het territoriale toepassingsgebied van de wet.

De wet is van toepassing op aanbieders van essentiële diensten die minstens één vestiging hebben op Belgisch grondgebied en daadwerkelijk een activiteit uitoefenen die betrekking heeft op de verlening van minstens één essentiële dienst op Belgisch grondgebied.

COMMENTAIRE DES ARTICLES

TITRE 1^{er}

Définitions et dispositions générales

CHAPITRE 1^{er}

Objet et champ d'application

Article 1^{er}

Cet article précise le fondement constitutionnel de la loi.

Article 2

Cet article précise la directive transposée par la loi.

Article 3

Cet article précise le champ d'application territorial de la loi.

La loi s'applique aux opérateurs de services essentiels ayant au moins un établissement sur le territoire belge et exerçant effectivement une activité liée à la fourniture d'au moins un service essentiel sur le territoire belge.

Het begrip “vestiging” wordt gedefinieerd overeenkomstig het recht van de Europese Unie. De rechtsvorm van deze vestiging, of het nu om een bijkantoor of om een dochteronderneming met rechtspersoonlijkheid gaat, is daarbij niet doorslaggevend.

Deze wet is van toepassing op digitaaldienstverleners die hun hoofdvestiging in België hebben. Een digitaaldienstverlener wordt geacht zijn hoofdvestiging in België te hebben als zijn hoofdkantoor zich daar bevindt.

Wanneer een digitaaldienstverlener niet in de Europese Unie gevestigd is maar binnen de Europese Unie diensten verleent zoals bedoeld in bijlage III van de wet, moet deze dienstverlener een vertegenwoordiger aanwijzen in de Europese Unie. De vertegenwoordiger moet gevestigd zijn in een van de lidstaten waar de diensten worden verleend. Krachtens deze wet valt de digitaaldienstverlener onder de bevoegdheid van de Belgische overheid wanneer zijn vertegenwoordiger in België gevestigd is.

Artikel 4

Dit artikel heeft betrekking op het toepassingsgebied van de wet. Het verduidelijkt dat sommige aanbieders afwijken van de bepalingen van de wet zodat, overeenkomstig de richtlijn, andere specifieke Europese en Belgische wetgeving volledig of gedeeltelijk op hen van toepassing is.

De door de richtlijn opgelegde beveiligings- en meldingseisen zijn niet van toepassing op ondernemingen die onderworpen zijn aan de eisen van de artikelen 13 bis en 13 ter van richtlijn 2002/21/EG van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten, omgezet in Belgisch recht door de artikelen 114 en 114/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Deze uitzondering geldt vanzelfsprekend enkel voor de activiteiten van deze ondernemingen die werkelijk onderworpen zijn aan de artikelen 114 en 114/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, namelijk deze in verband met het aanbieden van openbare

Cette notion d'établissement est définie conformément au droit de l'Union européenne. La forme juridique retenue pour un tel établissement, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard.

La présente loi s'applique aux fournisseurs de service numérique dont l'établissement principal est situé en Belgique. Un fournisseur de service numérique est réputé avoir son établissement principal en Belgique lorsque son siège social s'y trouve.

Lorsqu'un fournisseur de service numérique n'est pas établi dans l'Union européenne mais fournit des services visés à l'annexe III de la loi à l'intérieur de l'Union européenne, ce fournisseur doit désigner un représentant dans l'Union européenne. Le représentant doit être établi dans l'un des États membres dans lesquels les services sont fournis. Le fournisseur de service numérique relève de la compétence des autorités belges en vertu de la présente loi lorsque son représentant est établi en Belgique.

Article 4

L'article porte sur le champ d'application de la loi. Il précise certains opérateurs qui dérogent aux dispositions de la loi pour se voir appliquer entièrement ou partiellement d'autres législations européennes et belges spécifiques, conformément à la directive.

Les exigences en matière de sécurité et de notification prévues par la directive ne s'appliquent pas aux entreprises soumises aux exigences énoncées aux articles 13 bis et 13 ter de la directive 2002/21/CE du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, transposée en droit belge par les articles 114 et 114/1 de la loi du 13 juin 2005 relative aux communications électroniques.

Cette exception ne vaut, bien entendu, que pour les activités de ces entreprises qui sont effectivement soumises aux articles 114 et 114/1 de la loi du 13 juin 2005 relative aux communications électroniques, à savoir celles de fourniture de réseaux publics de

elektronische-communicatienetwerken of communications électroniques ou de services de openbare elektronische-communicatiediensten. communications électroniques accessibles au public.

Wanneer een onderneming zowel diensten aanbiedt als bedoeld in de wet van 13 juni 2005 als andere diensten (bijvoorbeeld digitale diensten als bedoeld in bijlage III van de wet of digitale infrastructuurdiensten als bedoeld in bijlage II van de wet), is zij onderworpen aan de bepalingen van deze wet voor deze andere diensten.

Lorsqu'une entreprise fournit à la fois des services visés par la loi du 13 juin 2005 et d'autres services (par exemple, des services numériques visés à l'annexe III de la loi ou des services d'infrastructures numériques visés à l'annexe II de la loi), celle-ci est soumise aux dispositions de la présente loi pour ces autres services.

Hetzelfde geldt voor de verleners van vertrouwensdiensten die onderworpen zijn aan de eisen vervat in artikel 19 van de Europese verordening (EU) nr. 910/2014 van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

Il en va de même pour les prestataires de services de confiance soumis aux exigences énoncées à l'article 19 du règlement européen (UE) n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

De aanbieders van essentiële diensten die deel uitmaken van de financiële sector vallen enkel onder sommige bepalingen van deze wet. Ze blijven onderworpen aan de bepalingen van Europese en Belgische wetgeving die minstens feitelijk gelijkwaardig zijn aan de beveiligings- en meldingsverplichtingen van de wet.

Les opérateurs de services essentiels appartenant au secteur des finances ne se voient appliquer que certaines des dispositions de la présente loi. Ils demeurent soumis aux dispositions des législations européennes et belges qui ont un effet au moins équivalent à celui des obligations de sécurité et de notification prévues par la loi.

Overeenkomstig de richtlijn zijn de bepalingen van Titel I van de wet (toepassingsgebied, definities, samenwerking op nationaal niveau, informatie-uitwisseling en nationale strategie), van hoofdstuk 1 van Titel II (identificatie van de aanbieders van essentiële diensten) en van de paragrafen 2 en 3 van artikel 16 (melding van incidenten) echter wel van toepassing op de aanbieders van essentiële diensten die deel uitmaken van de financiële sector.

Conformément à la directive, les dispositions du Titre I de la loi (le champ d'application, les définitions, la coopération au niveau national, l'échange d'informations et la stratégie nationale), du chapitre 1 du Titre II (identification des opérateurs de services essentiels) et des paragraphes 2 et 3 de l'article 16 (notification des incidents) sont néanmoins applicables aux opérateurs de services essentiels appartenant au secteur des finances.

Artikel 17 is volledig van toepassing op de exploitanten van een handelsplatform omdat zij nog niet onder een wettelijke verplichting voor het melden van incidenten vallen. Voor aanbieders van essentiële diensten die deel uitmaken van de financiële sector, is niettemin voorzien in een specifiek mechanisme voor het melden van beveiligingsincidenten aan de Nationale Bank van België, die de melding vervolgens onverwijld aan het CCB en de ADCC bezorgt.

L'article 17 s'applique complètement aux opérateurs de plate-forme de négociation car ceux-ci ne sont pas encore couverts par une obligation légale de notification des incidents. Pour les opérateurs de services essentiels appartenant au secteur des finances, il est prévu néanmoins un mécanisme de notification spécifique des incidents de sécurité à la Banque nationale de Belgique, qui transmet ensuite la notification, sans retard injustifié, au CCB et à la DGCC.

Tot slot blijven de controles ten aanzien van aanbieders van essentiële diensten die deel uitmaken van de financiële sector onderworpen aan specifieke sectorale wetgeving. Titel IV van de wet is dus op hen niet van toepassing voor de

Enfin, les contrôles des opérateurs de services essentiels appartenant au secteur des finances demeurent régis par les législations sectorielles spécifiques. Le Titre IV de la loi ne leur est donc pas applicable, à l'exception de l'article 27 pour les

aanbieders van de financiën sector, met uitzondering van artikel 27 voor de aanbieders van de financiën sector andere dan exploitanten van een handelsplatform.

Artikel 5

Dit artikel verduidelijkt dat de bepalingen van deze wet geen afbreuk doen aan de toepassing van sommige andere wettelijke bepalingen, waaronder de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur, de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen en de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle

HOOFDSTUK 2

Definities

Artikel 6

Dit artikel bevat de definities zoals die vooraf zijn vastgesteld door de NIS-richtlijn, alsook sommige aspecten die specifiek betrekking hebben op het Belgische wetgevende kader.

De sectorale overheden die, voor hun respectievelijke sector, belast zijn met het toezicht op de uitvoering van de bepalingen van de wet, worden aangewezen door de wet in bijlage IV of door de Koning bij in Ministerraad overlegd besluit.

De mogelijkheid tot aanwijzing door de Koning laat toe rekening te houden met de eventuele toevoeging van nieuwe sectoren of deelsectoren en sectorale overheden op te richten, bestaande uit vertegenwoordigers van de Gemeenschappen en Gewesten, op basis van artikel 92 *ter* van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.

Er wordt bijvoorbeeld overwogen om de Koning een Nationaal Comité voor de beveiliging van netwerk- en informatiesystemen voor de levering en distributie van drinkwater te laten oprichten, dat zou zijn samengesteld uit vertegenwoordigers van de Federale Staat, het Vlaams Gewest, het

opérateurs du secteur financier autres que les opérateurs de plate-forme de négociation.

Article 5

L'article précise que les dispositions de la présente loi sont sans préjudice de l'application de certaines autres dispositions légales, dont la loi du 1^{er} juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité et de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire.

CHAPITRE 2

Définitions

Article 6

Cet article reprend les définitions telles que préalablement établies par la directive NIS ainsi que certains éléments spécifiques au cadre législatif belge.

Les autorités sectorielles chargées, pour leur secteur respectif, de veiller à la mise en œuvre des dispositions de la loi sont désignées par la loi à l'annexe IV, ou désignées par le Roi, par arrêté délibéré en conseil des Ministres.

La faculté de désignation par le Roi permet de pouvoir tenir compte de l'ajout éventuel de nouveaux secteurs ou sous-secteurs et de créer des autorités sectorielles, composées de représentants des Communautés et des Régions, sur base de l'article 92 *ter* de la loi spéciale du 8 août 1980 de réformes institutionnelles.

Il est envisagé, par exemple, la création par le Roi d'un Comité national de sécurité des systèmes et réseaux de l'information pour la fourniture et de la distribution d'eau potable, lequel serait composé de représentant

Brussels Hoofdstedelijk Gewest en het Waals Gewest.

Het begrip “sectoraal CSIRT” is met name eigen aan de Belgische omzetting van de richtlijn en omvat niet alle bevoegdheden die in de richtlijn en de bijlagen ervan aan het CSIRT worden toegekend. Het betreft een dienst van de sectorale overheid die voor zijn sector de taken van een CSIRT vervult, maar in coördinatie met en met inachtneming van de bevoegdheden van het nationale CSIRT (CCB).

Om alle twijfel weg te nemen over de draagwijdte van het begrip “netwerk- en informatiesysteem”, wordt de definitie ervan verduidelijkt in punt 8, b), om er onder meer uitdrukkelijk de permanent of tijdelijk gekoppelde netwerken en de digitale, elektronische of mechanische componenten van een apparaat in op te nemen die met name de automatisering van het operationele proces, de controle op afstand, of het verkrijgen van gegevens inzake de werking in real time mogelijk maken.

Het is de bedoeling om te verduidelijken dat het begrip “apparaat dat digitale gegevens verwerkt” onder meer de digitale, elektronische of mechanische componenten van met name SCADA-systemen bevat (van het Engels “Supervisory Control And Data Acquisition”), alsook permanent of tijdelijk gekoppelde apparaten.

de l’Etat fédéral, de la Région flamande, de la Région de Bruxelles-Capitale et de la Région wallonne.

Le CSIRT sectoriel est notamment une notion propre à la transposition belge de la directive, qui ne reprend pas toutes les compétences attribuées au CSIRT par la directive et ses annexes. Il s’agit d’un service de l’autorité sectorielle qui exerce pour son secteur les tâches d’un CSIRT mais en coordination et dans le respect des compétences du CSIRT national (CCB).

Afin de lever les doutes quant à l’étendue de la notion de réseau et système d’information, sa définition est précisée au point 8, b) pour inclure explicitement, entre autres choses, les réseaux interconnectés de manière permanente ou temporaire et les composants numériques, électroniques ou mécaniques d’un dispositif permettant notamment l’automatisation de processus opérationnel, le contrôle à distance, ou l’obtention de données de fonctionnement en temps réel.

Il s’agit de préciser que la notion de dispositif traitant des données numériques comprend entre autre chose les composants numériques, électroniques ou mécaniques notamment de systèmes d’acquisition et de contrôle de données industriels (en anglais “Supervisory Control And Data Acquisition”, en abrégé “SCADA”), ainsi que les dispositifs interconnectés de manière permanente ou temporaire.

HOOFDSTUK 3

Bevoegde overheden, samenwerking op nationaal en internationaal niveau

Afdeling 1

Bevoegde overheden

Artikel 7

Dit artikel wijst de overheden aan die bevoegd zijn voor de uitvoering van de wet.

Overeenkomstig het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België wordt het CCB aangewezen als nationale autoriteit belast met de opvolging en coördinatie van de wet, en dit voor alle aanbieders van essentiële diensten en digitaaldienstverleners.

CHAPITRE 3

Autorités compétentes, coopération au niveau national et international.

Section 1

Autorités compétentes

Article 7

Cet article désigne les autorités compétentes pour la mise en œuvre de la loi.

Conformément à l’arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, le CCB est désigné comme autorité nationale chargée du suivi et de la coordination de la loi, pour tous les opérateurs de services essentiels et les

Het CCB vervult een algemene coördinerende rol op nationaal en internationaal niveau. Het is nauw betrokken bij het identificatieproces van de aanbieders van essentiële diensten. Het kan zich steeds een kopie laten overmaken door de sectorale overheid van de controle- en auditverslagen opgelegd door of krachtens de wet. Het kan de sectorale overheid ook steeds aanbevelen om controles uit te voeren.

De sectorale overheden worden aangewezen als nationale autoriteiten die voor hun respectievelijke sector belast zijn met het toezicht op de uitvoering van de bepalingen van deze wet. Ze voeren de door de wet voorgeschreven opdrachten uit in het kader van hun bevoegdheden, met name de identificatie van de aanbieders van essentiële diensten en het toezicht op de naleving van de beveiligingseisen opgelegd aan de aanbieders en digitaaldienstverleners, in samenwerking met het CCB.

Het nationale contactpunt is een nieuwigheid ingevoerd door de NIS-richtlijn. Het gaat om een verbindingfunctie die moet zorgen voor samenwerking tussen de autoriteiten van de lidstaten van de Europese Unie en met de betrokken autoriteiten van de andere lidstaten, de Samenwerkingsgroep bedoeld in artikel 11 en het CSIRT-netwerk bedoeld in artikel 12 van de NIS-richtlijn. Overeenkomstig zijn opdrachten bepaald in het koninklijk besluit van 10 oktober 2014, wordt het Centrum voor Cybersecurity België ("CCB") aangewezen als uniek nationaal contactpunt en coördineert het de vertegenwoordiging van België binnen het CSIRT-netwerk en de Samenwerkingsgroep.

Het CCB oefent de functie van nationaal CSIRT uit om meldingen van incidenten door aanbieders van essentiële diensten en digitaaldienstverleners te ontvangen.

Dit artikel wijst het CCB aan als nationaal CSIRT dat ermee belast is meldingen van incidenten door aanbieders van essentiële diensten en digitaaldienstverleners te ontvangen. Het ontvangt ook meldingen van incidenten in andere landen.

Dit artikel bepaalt ook dat elke sectorale overheid ervoor kan kiezen om een sectoraal CSIRT uit te bouwen ter ondersteuning van het nationale CSIRT.

fournisseurs de services numériques. Le CCB a un rôle général de coordination au niveau national et international. Il est étroitement associé au processus d'identification des opérateurs de services essentiels. Il peut toujours se faire remettre par l'autorité sectorielle copie des rapports de contrôle et des rapports d'audit qui sont imposés par ou en vertu de la loi. De même, il peut toujours recommander à l'autorité sectorielle d'effectuer des contrôles.

Les autorités sectorielles sont désignées comme autorités nationales chargées, pour leur secteur respectif, de veiller à la mise en œuvre des dispositions de la présente loi. Elles exécutent les missions prévues par la loi dans le cadre de leurs compétences, notamment l'identification des opérateurs de services essentiels et le contrôle du respect des exigences de sécurité imposées aux opérateurs et fournisseurs de service numérique, en collaboration avec le CCB.

Le point de contact national est une nouvelle figure introduite par la directive NIS. Il s'agit d'une fonction de liaison afin d'assurer une coopération entre les autorités des Etats membres de l'Union européenne, ainsi qu'avec les autorités concernées des autres Etats membres, le groupe de coopération visé à l'article 11 et le réseau des CSIRT visé à l'article 12 de la directive NIS. Conformément à ses missions prévues dans l'arrêté royal du 10 octobre 2014, le Centre pour la Cybersécurité Belgique ("CCB") est désigné comme étant le point de contact national unique et coordonne la représentation de la Belgique au sein du réseau des CSIRT et du Groupe de coopération.

Le CCB exerce la fonction de CSIRT national afin de recevoir les notifications d'incidents des opérateurs de services essentiels et des fournisseurs de service numérique.

Cet article désigne le CCB comme CSIRT national chargé de recevoir les notifications d'incidents des opérateurs de services essentiels et des fournisseurs de service numérique, ainsi que notifications d'incidents d'autres Etats.

Cet article précise également que chaque autorité sectorielle peut choisir de développer une équipe d'intervention sectorielle, en appui du CSIRT national.

Samenwerking op nationaal niveau**Artikel 8**

Dit artikel voorziet in samenwerking op nationaal niveau, namelijk dat het CCB, de ADCC en de sectorale overheden nauw samenwerken om de in deze wet vastgestelde verplichtingen te vervullen, zoals bepaald in de richtlijn.

Naargelang de behoeften en overeenkomstig de toepasselijke wettelijke bepalingen werken bovengenoemde overheden ook samen met, onder meer, de diensten van het Openbaar Ministerie, de politie en de Gegevensbeschermingsautoriteit.

HOOFDSTUK 4**Informatie-uitwisseling****Artikel 9**

Dit artikel bepaalt dat de informatie-uitwisseling met de autoriteiten van de Europese Unie en met buitenlandse of nationale autoriteiten noodzakelijk moet zijn voor de toepassing van de wet en in overeenstemming moet zijn met de wettelijke bepalingen die de vertrouwelijkheid van de informatie m.b.t. de wezenlijke belangen van de openbare veiligheid waarborgen. Deze bepaling heeft met name tot doel om de toepassing van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen te waarborgen.

Om deze informatie-uitwisseling mogelijk te maken, blijkt het evenwel noodzakelijk om, in sommige gevallen en behoudens de informatie m.b.t. de wezenlijke belangen van de openbare veiligheid, af te wijken van andere wetgeving die verplichtingen inzake beroepsgeheim oplegt.

Dit artikel voorziet bijgevolg in een beperking van de toegang tot de door de aanbieder van essentiële diensten en de digitaledienstverlener toevertrouwde informatie en in een beperking van de inhoud van de uitgewisselde informatie.

Coopération au niveau national**Article 8**

Cet article prévoit la coopération au niveau national, à savoir que le CCB, la DGCC et les autorités sectorielles coopèrent étroitement aux fins du respect des obligations énoncées dans la présente loi, comme le prévoit la directive.

En fonction des besoins et conformément aux dispositions légales applicables, les autorités précitées coopèrent également, entre autres, avec les services du Ministère public, de la police et de l'Autorité de protection des données.

CHAPITRE 4**Echanges d'information****Article 9**

L'article prévoit que l'échange d'information avec des autorités de l'Union européenne, avec des autorités étrangères ou nationales, doit être nécessaire à l'application de la loi et respecter les dispositions légales garantissant la confidentialité des informations liées aux intérêts essentiels de la sécurité publique. Cette disposition vise à garantir notamment l'application de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

Pour permettre cet échange d'informations, il s'avère toutefois nécessaire de déroger, dans certains cas et en dehors des informations liées aux intérêts essentiels de la sécurité publique, à d'autres législations imposant des obligations de secret professionnel.

L'article prévoit, par voie de conséquence, une limitation de l'accès aux informations confiées par l'opérateur de services essentiels ou le fournisseur de service numérique et une limitation du contenu des informations échangées.

L'autorité sectorielle, le CCB et la DGCC limitent l'accès aux informations visées aux titres 2 et 3 et aux informations qui leur sont confiées par l'opérateur de services essentiels ou le fournisseur de service

De sectorale overheid, het CCB en de ADCC beperken de toegang tot de in de titels 2 en 3 bedoelde informatie en tot de informatie die hen wordt toevertrouwd door aanbieders van essentiële diensten of digitaledienstverleners, tot de personen die er de kennis van nodig hebben of er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met deze wet.

Onverminderd andere strengere wettelijke bepalingen mogen de aanbieder van essentiële diensten, zijn medewerkers en onderaannemers enkel toegang geven tot de inhoud van de maatregelen in het beveiligingsbeleid voor de netwerk- en informatiesystemen (hierna "I.B.B." genoemd) aan personen die er de kennis van nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met deze wet. Ze zijn gebonden aan het beroepsgeheim wat deze informatie betreft.

Het artikel bepaalt verder dat de aanbieder van essentiële diensten, de digitaledienstverlener, het CCB, de sectorale overheid en de ADCC te allen tijde moeten samenwerken door een adequate informatie-uitwisseling betreffende de beveiliging van de netwerk- en informatiesystemen.

Tot slot wordt opgemerkt dat de persoonsgegevens uitgewisseld in het kader van de wet moeten worden verwerkt overeenkomstig de toepasselijke wetgeving betreffende de verwerking van persoonsgegevens.

HOOFDSTUK 5

Nationale strategie voor de beveiliging van netwerk- en informatiesystemen

Artikel 10

Dit artikel bepaalt dat de Koning, bij in Ministerraad overlegd besluit, de nationale strategie voor de beveiliging van netwerk- en informatiesystemen goedkeurt, na raadpleging van het CCB, de ADCC en de sectorale overheden en van de Gegevensbeschermingsautoriteit.

Concreet zal het CCB, na raadpleging van de betrokken overheden, een voorstel formuleren voor de Ministerraad.

numérique, aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec la présente la loi.

Sans préjudice d'autres dispositions légales plus contraignantes, l'opérateur de services essentiels, ses agents et ses sous-traitants ne peuvent donner accès au contenu des mesures figurant dans la politique de sécurité des systèmes et réseaux d'information (ci-après dénommé « P.S.I. ») qu'aux personnes qui ont besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec la présente la loi. Ils sont tenus au secret professionnel en ce qui concerne ces informations.

L'article prévoit encore que l'opérateur de services essentiels, le fournisseur de service numérique, le CCB, l'autorité sectorielle et la DGCC doivent collaborer en tout temps, par un échange adéquat d'informations concernant la sécurité des systèmes et réseaux d'informations.

Enfin, il convient de préciser que les données à caractère personnel échangées dans le cadre la loi devront être traitées conformément aux législations applicables en matière de traitement des données à caractère personnel.

CHAPITRE 5

Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information

Article 10

Cet article prévoit que le Roi adopte, par arrêté délibéré en Conseil des ministres, la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, après consultation du CCB, de la DGCC, des autorités sectorielles et de l'Autorité de protection des données.

Concrètement, le CCB formulera, après consultation des autorités concernées, une proposition au Conseil des Ministres.

In de nationale strategie worden de strategische doelstellingen en passende beleids- en regelgevingsmaatregelen bepaald om een hoog beveiligingsniveau van de netwerk- en informatiesystemen te bereiken en te handhaven, en waarin ten minste de in bijlage III van de wet genoemde sectoren aan bod komen.

Het artikel somt ook de punten op waarop de nationale strategie betrekking heeft.

Die punten omvatten een risicobeoordelingsplan om risico's te identificeren. Dat plan zal worden gecoördineerd in nauwe samenwerking met het Crisiscentrum, rekening houdend met de opdrachten van dit centrum wat de analyse van de nationale risico's betreft.

TITEL 2

Netwerk- en informatiesystemen van de aanbieders van essentiële diensten

HOOFDSTUK 1

Identificatie van de aanbieders van essentiële diensten

Artikel 11

Het identificatieproces van de aanbieders van essentiële diensten en van de door hen verleende essentiële diensten is beschreven in artikel 11.

Volgens deze bepaling identificeert de sectorale overheid de aanbieders van essentiële diensten in overleg met het CCB en de ADCC, binnen de grenzen van hun respectievelijke bevoegdheden.

De wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur bepaalt immers dat de sectorale overheid de kritieke infrastructuur identificeert in overleg met de ADCC.

Om deze beide identificatieprocessen en de rationalisatie van de middelen te optimaliseren, werkt het CCB nauw samen met de ADCC.

De sectorale overheid raadpleegt ook de gewesten en gemeenschappen en, indien ze dit nuttig acht, de vertegenwoordigers van de sector en van de potentiële aanbieders van essentiële diensten.

La stratégie nationale définit les objectifs stratégiques et les mesures politiques et réglementaires appropriées permettant d'atteindre un niveau élevé de sécurité des réseaux et des systèmes d'information et de le maintenir, et de couvrir au moins les secteurs visés à l'annexe III de la loi.

L'article énumère également les points sur lesquels porte la stratégie nationale.

Parmi ces points, figure un plan d'évaluation des risques permettant d'identifier les risques. La coordination de ce plan se fera en collaboration étroite avec le Centre de crise, compte tenu de ses missions en matière d'analyse des risques nationaux.

TITRE 2

Réseaux et systèmes d'information des opérateurs de services essentiels

CHAPITRE 1

Identification des opérateurs de services essentiels

Article 11

Le processus d'identification des opérateurs de services essentiels et des services essentiels qu'ils fournissent est décrit à l'article 11.

Cette disposition prévoit que l'autorité sectorielle identifie les opérateurs de services essentiels, en concertation avec le CCB et la DGCC, chacun dans les limites de leurs compétences respectives.

La loi du 1^{er} juillet 2011 relative à la sécurité et à la protection des infrastructures critiques prévoit que l'autorité sectorielle identifie, en effet, les infrastructures critiques, en concertation avec la DGCC.

Afin d'optimiser ces deux processus d'identification et la rationalisation des ressources, le CCB et la DGCC travailleront en étroite collaboration.

L'autorité sectorielle consultera aussi les régions et communautés, et si elle l'estime utile, les représentants du secteur et des opérateurs de services essentiels potentiels.

Volgens paragraaf 2 moet, om een aanbieder van essentiële diensten te identificeren, de definitie van deze term worden toegepast en vervolgens de vastgestelde criteria, drempelwaarden of weerslagniveau's. De wet bepaalt dat de identificatie plaatsvindt zodra de drempelwaarde of het weerslagniveau van een criterium, ongeacht of het sectoraal of intersectoraal is, vervuld is.

Om de sectorale overheid toe te laten de aanbieders van essentiële diensten die actief zijn in haar sector zo goed mogelijk te identificeren, moet zij minstens rekening houden met de soorten aanbieders in bijlage II van de wet, maar kan zij ook andere soorten aanbieders identificeren die tot haar sector behoren.

In een eerste identificatiefase bepaalt de sectorale overheid, wat de diensten betreft die verleend worden door de entiteiten van haar sector en minstens door deze bedoeld in bijlage II van de wet, welke dienst of diensten van essentieel belang zijn voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten.

In een tweede identificatiefase wordt bepaald of de als essentieel beschouwde dienst afhankelijk is van netwerk- en informatiesystemen, wat overeenstemt met de tweede voorwaarde van de definitie van aanbieder van essentiële diensten.

Rekening houdend met het feit dat de informatie- en communicatietechnologie voortaan aan de basis ligt van bijna alle economische systemen en de moderne samenleving, werd beslist ervan uit te gaan dat de verlening van de geïdentificeerde essentiële diensten afhankelijk is van deze systemen.

Aangezien dit vermoeden niet onweerlegbaar is, blijft het steeds mogelijk om het te weerleggen door het bewijs van het tegendeel te leveren.

Zo zal een potentiële aanbieder van essentiële diensten die dit vermoeden wenst te weerleggen, de objectieve redenen hiervoor moeten toelichten aan de sectorale overheid. Deze zal, in samenwerking met het CCB en de ADCC, de ingeroepen argumenten onderzoeken en beslissen over dit verzoek, aangezien zij, krachtens artikel 11, § 1, de aanbieders van essentiële diensten die tot haar sector behoren dient te identificeren.

Le paragraphe 2 précise que pour identifier un opérateur de services essentiels, il y a lieu d'appliquer la définition de ce terme, puis d'appliquer les critères, les seuils ou les niveaux d'incidence fixés. La loi précise que l'identification aura lieu dès que le seuil ou le niveau d'incidence d'un critère, qu'il soit sectoriel ou intersectoriel, est rempli.

Afin de permettre à l'autorité sectorielle d'identifier aux mieux les opérateurs de services essentiels actifs dans son secteur, celle-ci doit prendre en compte au minimum les types d'opérateurs qui figurent à l'annexe II de la loi mais elle peut aussi identifier d'autres types d'opérateurs relevant de son secteur.

La première étape de l'identification sera la détermination par l'autorité sectorielle, parmi les services fournis par les entités de son secteur au moins visées à l'annexe II de la loi, du ou des services qui sont essentiels au maintien d'activités sociétales et/ou économiques critiques.

La seconde étape de l'identification sera de déterminer la dépendance aux réseaux et systèmes d'information du service considéré comme essentiel, ce qui correspond à la deuxième condition de la définition d'un opérateur de services essentiels.

Compte tenu du fait que les technologies de l'information et des communications se trouvent désormais à la base de pratiquement tous les systèmes économiques et sociétés modernes, il a été décidé de présumer que la fourniture des services essentiels identifiés est dépendante de ces systèmes.

Cette présomption étant non irréfutable, il demeure toujours possible de la renverser en apportant la preuve du contraire.

Ainsi, dans le cas où un opérateur de service essentiel potentiel souhaite renverser cette présomption, il lui appartiendra d'en expliquer les raisons objectives à l'autorité sectorielle. Celle-ci, en collaboration avec le CCB et la DGCC, examinera les arguments invoqués et statuera sur cette demande, puisque c'est à elle qu'il revient, en vertu de l'article 11, § 1^{er} d'identifier les opérateurs de services essentiels relevant de son secteur.

In een derde fase worden de entiteiten bepaald voor wie een incident betreffende de beveiliging van netwerk- en informatiesystemen aanzienlijke verstorende effecten kan hebben voor de verlening van hun essentiële dienst.

Om het belang van een in het vorige lid bedoeld verstorend effect te bepalen, stelt de sectorale overheid (sectorale of intersectorale) criteria, weerslagniveau's en drempelwaarden vast. Dit gebeurt in samenwerking met het CCB en de ADCC en, desgevallend, met de betrokken gewesten en gemeenschappen.

Tijdens deze fase overlegt het CCB met de ADCC om voor de nodige coherentie te zorgen tussen de verschillende sectoren en de andere lidstaten van de Europese Unie.

De sectorale overheid raadpleegt ook de gewesten of gemeenschappen wanneer potentiële aanbieders van essentiële diensten onder hun bevoegdheden vallen voor andere aspecten dan de openbare veiligheid van informatiesystemen.

Paragraaf 5 bevat een niet-limitatieve opsomming van een aantal intersectorale criteria bedoeld in artikel 6.1. van de richtlijn.

Verduidelijkt wordt dat de richtlijn de term "sectoroverschrijdende factoren" gebruikt, terwijl deze wet naar de term "intersectorale criteria" verwijst die gebruikt wordt in de wet op de kritieke infrastructuur aangezien beide termen hetzelfde doel nastreven, en om in dit verband te zorgen voor de nodige samenhang in de nationale wetgeving.

Krachtens paragraaf 6 moet de potentiële aanbieder van essentiële diensten alle nuttige informatie bezorgen over zijn eventuele identificatie als aanbieder van essentiële diensten.

Deze informatie moet de sectorale overheid toelaten om, in samenwerking met het CCB en de ADCC, na te gaan of de voorwaarden voor de identificatie van de aanbieder al dan niet vervuld zijn.

Ze kan te allen tijde ook door de sectorale overheid worden gevraagd, op eigen initiatief of op verzoek van het CCB of de ADCC, zelfs indien er geen betwisting is, bijvoorbeeld om te objectiveren of de verlening van de essentiële dienst al dan niet

La troisième étape consiste à déterminer les entités pour lesquelles un incident relatif à la sécurité des réseaux et des systèmes d'information pourrait avoir un effet perturbateur important sur la fourniture de leur service essentiel.

Afin de déterminer l'importance de l'effet perturbateur visé à l'alinéa précédent, l'autorité sectorielle établira des critères (sectoriels ou intersectoriels), des niveaux d'incidence et des seuils. Ceux-ci seront fixés, en collaboration avec le CCB et la DGCC, et si nécessaire, les régions et les communautés concernées.

Cette étape se fera en concertation, avec le CCB et la DGCC, afin d'assurer une cohérence entre les différents secteurs et les autres Etats membres de l'Union européenne.

L'autorité sectorielle consultera également les régions ou communautés lorsque des opérateurs de services essentiels potentiels relèveront de leurs compétences pour d'autres éléments que la sécurité publique des systèmes d'informations.

Le paragraphe 5 énumère de manière non exhaustive une série de critères intersectoriels, visés à l'article 6.1. de la Directive.

Il convient de préciser que la Directive utilise les termes de « facteurs transsectoriels » alors que la présente loi se réfère à la terminologie de « critères intersectoriels » utilisée dans la loi sur les infrastructures critiques dès lors que la finalité de ces deux terminologies sont identiques, et pour s'assurer d'une cohérence à cet égard en droit interne.

En vertu du paragraphe 6, l'opérateur de services essentiels potentiel est tenu de transmettre toutes les informations utiles quant à son éventuelle identification en tant qu'opérateur de services essentiels.

Ces informations doivent permettre à l'autorité sectorielle, en collaboration avec le CCB et la DGCC, de vérifier la réunion des conditions d'identification ou non de l'opérateur.

Elles peuvent également être sollicitées par l'autorité sectorielle, d'initiative ou à la demande du CCB ou de la DGCC, en tous temps, même en l'absence de contestation, en vue, par exemple, d'objectiver la dépendance ou non de la fourniture du service essentiel aux réseaux et systèmes de l'information.

afhankelijk is van netwerk- en informatiesystemen.

Paragraaf 7 verduidelijkt dat de sectorale overheid een voorstel van lijst van potentiële aanbieders van essentiële diensten, samen met haar motivering, aan het CCB en de ADCC moet bezorgen.

Vervolgens brengen het CCB en de ADCC, binnen de grenzen van hun respectievelijke bevoegdheden, samen advies uit over het gemotiveerde voorstel van lijst, in voorkomend geval na raadpleging van de gewesten en gemeenschappen.

Paragraaf 8 bepaalt dat, wanneer de sectorale overheid vaststelt dat de aanbieder een of meer essentiële diensten in minstens één andere lidstaat van de Europese Unie verleent, ze het CCB en de ADCC daarvan op de hoogte moet brengen. Deze laatste en de betrokken sectorale overheden zijn, in voorkomend geval in samenwerking met de betrokken gewesten of gemeenschappen, ermee belast besprekingen te voeren met de bevoegde buitenlandse nationale autoriteit of autoriteiten.

Volgens paragraaf 9 moet de sectorale overheid vervolgens, op beveiligde wijze, de administratieve beslissingen betreffende de aanwijzing van de aanbieders van essentiële diensten, samen met de motivering ervan, aan het CCB, de ADCC en, in voorkomend geval, aan de gewesten en gemeenschappen bezorgen.

Paragraaf 10 verduidelijkt dat de aanbieder van essentiële diensten de sectorale overheid binnen de drie maanden na zijn aanwijzing een beschrijving bezorgt van de netwerk- en informatiesystemen waarvan de verlening van een of meer betrokken essentiële diensten afhankelijk is.

De sectorale overheid heeft dit soort informatie immers nodig om na te gaan of de aanbieder de beveiligingseisen naleeft waartoe hij gehouden is krachtens deze wet.

Voor het overige kan deze informatie, in voorkomend geval, het identificatieproces een zekere coherentie en objectiviteit verlenen en de evaluatie van de opgestelde lijst vergemakkelijken

Le paragraphe 7 précise qu'il appartient ensuite à l'autorité sectorielle de communiquer une proposition de liste des opérateurs de services essentiels potentiels, accompagnée de sa motivation, au CCB et à la DGCC.

Ensuite, le CCB et la DGCC, dans les limites de leurs compétences respectives, rendent ensemble un avis sur la proposition motivée de liste, le cas échéant après consultation des régions et des communautés.

En vertu du paragraphe 8, lorsque l'autorité sectorielle constate que l'opérateur fournit un ou des services essentiels dans au moins un autre Etat membre de l'Union européenne, elle en informe le CCB et la DGCC. Ces derniers sont chargés avec les autorités sectorielles concernées et le cas échéant, en collaboration avec les régions ou communautés concernées, de mener des discussions avec la ou les autorités nationales étrangères compétentes.

Le paragraphe 9 précise qu'il appartient ensuite à l'autorité sectorielle de communiquer, de manière sécurisée, les décisions administratives de désignation des opérateurs de services essentiels, accompagnées de leur motivation, au CCB, à la DGCC, et le cas échéant, aux régions et communautés.

Le paragraphe 10 précise que dans les trois mois de sa désignation, l'opérateur de services essentiels transmet à l'autorité sectorielle un descriptif des réseaux et systèmes d'information dont la fourniture du ou des services essentiels concernés est tributaire.

Ce type d'informations est en effet nécessaire pour permettre à l'autorité sectorielle de vérifier si l'opérateur respecte les exigences de sécurité qui lui incombent en vertu de la présente loi.

Cela permet, pour le surplus, d'apporter le cas échéant, une certaine cohérence et objectivité au processus d'identification et de faciliter le travail de

die moet plaatsvinden overeenkomstig paragraaf 11.

De eerste identificatiefase van de aanbieders van essentiële diensten die gevestigd zijn op Belgisch grondgebied zal eind 2018 voltooid zijn.

Artikel 12

In afwijking van artikel 11 is voorzien in een vereenvoudigd systeem voor de aanwijzing van exploitanten van kritieke infrastructuur. Zij worden als dusdanig aangewezen overeenkomstig de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur.

Zij worden door de sectorale overheid aangewezen als aanbieders van essentiële diensten, in overleg met het CCB en de ADCC, binnen hun respectievelijke bevoegdheidsgebieden, wanneer de verlening van hun kritieke diensten afhankelijk is van netwerk- en informatiesystemen. Deze afhankelijkheid wordt vermoed naar het voorbeeld van wat bepaald is voor de aanbieders van essentiële diensten die geen exploitanten van kritieke infrastructuur zijn.

Deze identificatie onder de geïdentificeerde kritieke infrastructuur zal deel uitmaken van de eerste identificatiefase van de aanbieders van essentiële diensten, die eind 2018 zal voltooid zijn.

Artikel 13

Dit artikel machtigt de Koning om de verplichte identificatie van aanbieders van essentiële diensten eventueel uit te breiden tot andere soorten aanbieders of andere sectoren.

HOOFDSTUK 2 Beveiligingsmaatregelen

Artikel 14

Paragraaf 1 van deze bepaling voorziet in een algemene verplichting voor de aanbieder van essentiële diensten om passende en evenredige technische en organisatorische maatregelen te nemen voor de beveiliging van de netwerk- en

réexamen de la liste établie, qui doit intervenir, conformément au paragraphe 11.

La première phase d'identification des opérateurs de service essentiels établis sur le territoire belge sera réalisée pour la fin de l'année 2018.

Article 12

Par dérogation à l'article 11, il est prévu un système de désignation simplifié pour les exploitants d'infrastructures critiques désignées comme telles en application de la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

Ceux-ci sont désignés par l'autorité sectorielle comme opérateurs de services essentiels, en concertation avec le CCB et la DGCC dans les limites de leurs compétences respectives, lorsque la fourniture des services critiques qu'ils délivrent est tributaire de réseaux et des systèmes d'information. Il est entendu que cette dépendance est présumée, à l'instar de ce qui est prévu pour les opérateurs de services essentiels qui ne sont pas des exploitants d'infrastructures critiques.

Cette identification parmi les infrastructures critiques identifiées fera partie de la première phase d'identification des opérateurs de services essentiels, qui sera accomplie pour la fin de l'année 2018.

Article 13

Cet article permet au Roi d'étendre éventuellement l'identification obligatoire d'opérateurs de services essentiels à d'autres types d'opérateurs ou à d'autres secteurs.

CHAPITRE 2 Mesures de sécurité

Article 14

Cette disposition prévoit, dans son paragraphe 1^{er}, l'obligation générale pour l'opérateur de services essentiels de prendre les mesures techniques et organisationnelles nécessaires et proportionnées de sécurité des réseaux et des systèmes d'information

informatiesystemen waarvan de door hem verleende essentiële diensten afhankelijk zijn.

De doelstellingen en maatregelen zijn opgenomen in een document genaamd "beveiligingsbeleid voor de netwerk- en informatiesystemen" (I.B.B.).

Naast de algemene beveiligingsverplichting is bepaald dat de Koning bepaalde beveiligingsmaatregelen kan opleggen aan de aanbieders van essentiële diensten van verschillende sectoren. Doel is, in voorkomend geval, bepaalde minimale en specifieke beveiligingsmaatregelen verplicht te maken voor de aanbieders van essentiële diensten van verschillende sectoren.

Na overleg met het CCB kan de sectorale overheid ook bepaalde bijkomende beveiligingsmaatregelen opleggen aan de aanbieders van essentiële diensten die tot haar sector of deelsectoren behoren.

Om de uitwerking van het I.B.B. voor de exploitanten van kritieke infrastructuren te vergemakkelijken, worden de maatregelen voor de fysieke en logische beveiliging van netwerk- en informatiesystemen die reeds vervat zijn in hun beveiligingsplan van de exploitant gelijkgesteld met het I.B.B. wanneer deze maatregelen aan de verplichte inhoud van het I.B.B. voldoen.

Wanneer de aanbieder van essentiële diensten een beroep doet op een onderaannemer, moet hij zich ervan vergewissen dat deze de beveiligingsmaatregelen waartoe hij gehouden is werkelijk toepast.

Tot slot wordt verduidelijkt dat deze wet in dit stadium niet op alle mogelijke situaties betrekking heeft, op het vlak van specifieke cyberbeveiligingsmaatregelen, met name waar het risico-objecten betreft die zouden worden geïdentificeerd door de ADCC voor de kritieke infrastructuur en waarvoor zij een beroep zou doen op het CCB, met het oog op het nemen van die maatregelen.

Artikel 15

Om de uitvoering van de algemene beveiligingsverplichting te vergemakkelijken, bepaalt dit artikel dat aanbieders die erkende technische normen hanteren, zoals de norm ISO/IEC 27001, het vermoeden genieten dat de inhoud van hun

dont sont tributaires les services essentiels qu'il fournit.

Les objectifs et les mesures sont reprises dans un document dénommé politique de sécurité des systèmes et réseaux d'information (P.S.I.).

Outre l'obligation générale de sécurité, il est précisé que le Roi peut imposer certaines mesures de sécurité applicables aux opérateurs de services essentiels de plusieurs secteurs. L'objectif est de rendre obligatoire, le cas échéant, certaines mesures minimales et précises de sécurité pour les opérateurs de services essentiels de plusieurs secteurs.

Après concertation avec le CCB, l'autorité sectorielle peut également imposer certaines mesures complémentaires de sécurité aux opérateurs de services essentiels relevant de son secteur ou de ses sous-secteurs.

Afin de faciliter l'élaboration de la P.S.I. pour les exploitants d'infrastructures critiques, les mesures de sécurité physique et logique des réseaux et systèmes d'information déjà contenues dans leur plan de sécurité de l'exploitant sont assimilées à la P.S.I. lorsque celles-ci répondent au contenu exigé pour celle-ci.

Lorsqu'il fait appel à un sous-traitant, l'opérateur de services essentiels doit s'assurer que son sous-traitant applique effectivement les mesures de sécurité qui lui incombent.

Enfin, il convient de préciser que la présente loi ne vise à ce stade pas la totalité des situations susceptibles d'arriver, en terme de prise de mesures spécifiques de cybersécurité, notamment dans le chef des objets de risque qui seraient identifiés par la DGCC pour les infrastructures critiques, et pour lesquelles elle ferait appel au CCB, en vue de la mise en place de ces mesures.

Article 15

Afin de faciliter la mise en œuvre de l'obligation générale de sécurité, cet article énonce que les opérateurs utilisant des standards techniques

I.B.B. conform is, wanneer voldaan is aan de eisen van deze norm of aan een nationale, buitenlandse of internationale norm die door de Koning als gelijkwaardig wordt erkend.

Het conformiteit vermoeden heeft enkel betrekking op de inhoud van het I.B.B., d.w.z. op de doelstellingen inzake beveiligingsbeheer die in dat document moeten staan, en niet op het afdoende karakter van de toegepaste beveiligingsmaatregelen. De beveiligingsmaatregelen kunnen immers door de Koning of de sectorale overheid worden aangevuld en moeten het voorwerp uitmaken van een controle door een externe auditeur of de inspectiedienst van de sectorale overheid.

In de wet wordt rechtstreeks verwezen naar de norm ISO/IEC 27001 om voor alle aanbieders een duidelijke en concrete richting aan te geven, wat de minimale maatregelen voor het beveiligingsbeheer van hun systemen betreft, zodat zij kunnen voldoen aan de eisen van artikel 14, zonder een latere tussenkomst van de Koning of van de sectorale overheden af te wachten.

De norm ISO/IEC 27001 is immers de internationaal erkende technische norm die de algemene en gestructureerde aanpak bepaalt voor het beveiligingsbeheer van eender welk informatiesysteem. Het betreft dus een basisnorm die de algemene beginselen bepaalt voor de uitvoering van elke beveiligingsmaatregel voor informatiesystemen en die van toepassing is in alle sectoren. Bij deze norm wordt geen datum vermeld zodat steeds de meest recente versie ervan kan worden toegepast.

Tegelijk krijgen de sectorale overheden de mogelijkheid om hun in de wet bepaalde opdrachten zowel op een effectieve als een doeltreffende manier uit te voeren, doordat ze over een duidelijk referentiekader inzake minimale beveiligingsmaatregelen beschikken. Dit kader is evenwel niet verplicht omdat ook rekening moet worden gehouden met de specifieke kenmerken van elke sector of betrokken aanbieder.

Niettemin is voorzien in de mogelijkheid dat de Koning de gelijkwaardigheid van andere technische normen erkent om de houders van een certificaat op basis van eventueel vergelijkbaar of verdergaande technische beveiligingsnormen niet te benadelen. In hun advies aan de Koning zullen

reconnus, comme la norme ISO/IEC 27001, pourront bénéficier d'une présomption de conformité du contenu de leur P.S.I. lorsque celle-ci répond aux exigences de cette norme - ou à une norme nationale, étrangère ou internationale reconnue équivalente par le Roi.

La présomption porte uniquement sur le contenu de la P.S.I., c'est-à-dire sur les objectifs de gestion de la sécurité qui doivent figurer dans ce document, et non sur le caractère suffisant des mesures de sécurité appliquées. En effet, les mesures de sécurité peuvent être complétées par le Roi ou l'autorité sectorielle et elles doivent faire l'objet d'un contrôle par un auditeur externe ou le service d'inspection de l'autorité sectorielle.

Le choix de la référence directe dans la loi à la norme ISO/IEC 27001 vise à donner une direction claire et prévisible à l'ensemble des opérateurs, en ce qui concerne les mesures minimales de gestion de la sécurité de leurs systèmes, afin de se conformer aux exigences de l'article 14, sans attendre une intervention ultérieure du Roi ou des autorités sectorielles.

La norme ISO/IEC 27001 est, en effet, la norme technique internationalement reconnue qui fixe l'approche générale et structurée à adopter pour disposer d'une gestion de la sécurité de n'importe quel système d'informations. Il s'agit donc d'une norme de base fixant les principes généraux pour la mise en œuvre de toute mesure de sécurité d'un système d'information et est applicable dans tous les secteurs. Celle-ci est reprise sans indication de date afin de permettre d'appliquer toujours sa version la plus récente.

En même temps, il s'agit de permettre aux autorités sectorielles d'exercer leur missions prévues par la loi de façon effective tout autant qu'efficace, en disposant d'un cadre de référence clair en matière de mesures minimales de sécurité, sans que ce cadre possède un caractère obligatoire pour autant car il convient aussi de tenir compte des particularités propres à chaque secteur ou opérateur concerné.

La reconnaissance de l'équivalence d'autres normes techniques par le Roi est néanmoins prévue pour ne pas pénaliser les détenteurs d'un certificat obtenu selon des normes techniques de sécurité comparables ou éventuellement plus poussées. Dans leur avis au

de sectorale overheid en het CCB hun analyse van de eventuele gelijkwaardigheid tussen beide technische normen uiteenzetten. BELAC, de accreditatie-instelling van de instellingen voor de conformiteitsbeoordeling in België, zal advies uitbrengen over de accrediteerbaarheid van de als gelijkwaardig voorgestelde norm, met inbegrip van het bestaan van een technisch schema dat een accreditatie mogelijk maakt.

Aanbieders die wensen dat dit vermoeden van overeenstemming voor hen zou gelden, moeten een certificaat verkrijgen van een instelling voor de conformiteitsbeoordeling die op basis van de norm ISO/IEC 17021 (certificatie van managementsysteem) of ISO/IEC 17065 (certificatie van producten) geaccrediteerd is. De normen ISO/IEC 17021 en ISO/IEC 17065 zijn technische basisnormen die het technische schema bepalen dat moet worden gebruikt om certificaten te kunnen uitreiken voor alle soorten specifieke technische normen, waaronder, maar niet uitsluitend, de norm ISO/IEC 27001.

Dit certificaat moet uiteraard tot het certificeringsdomein behoren waarvoor de instelling geaccrediteerd is. Zo moet de instelling voor de conformiteitsbeoordeling die certificaten uitreikt aan een aanbieder van essentiële diensten geaccrediteerd zijn door BELAC of een andere erkende instelling die de erkenningsakkoorden van de "European Cooperation for Accreditation" medeondertekend heeft.

De accreditatie door BELAC volgens de norm ISO/IEC 17021 of ISO/IEC 17065 laat toe na te gaan of de instellingen voor de conformiteitsbeoordeling bij de uitreiking van een certificaat algemene regels inzake onafhankelijkheid, onpartijdigheid, vertrouwelijkheid en constante kwaliteit hebben nageleefd.

Artikel 16

De aanwijzing van een contactpunt voor de beveiliging van netwerk- en informatiesystemen laat de bevoegde sectorale overheid, het CCB en de ADCC toe om gemakkelijk met de geïdentificeerde aanbieders te communiceren in geval van incidenten of deze te informeren over eventuele dreigingen.

HOOFDSTUK 3

Roi, l'autorité sectorielle et le CCB exposeront leur analyse de l'équivalence éventuelle entre les deux normes techniques. De son côté, BELAC, qui est l'organisme d'accréditation des organismes d'évaluation de la conformité en Belgique, donnera un avis sur l'accréditabilité de la norme proposée à l'équivalence, en ce compris l'existence d'un schéma technique permettant d'effectuer une accréditation.

Les opérateurs qui souhaitent bénéficier de cette présomption de conformité devront obtenir un certificat délivré par un organisme d'évaluation de la conformité accrédité sur base de la norme ISO/IEC 17021 (certification système de gestion) ou ISO/IEC 17065 (certification produits). Les normes ISO/IEC 17021 et ISO/IEC 17065 sont des normes techniques de base qui déterminent le schéma technique à utiliser pour pouvoir délivrer des certificats pour tous types de normes techniques spécifiques, dont entre autres la norme ISO/IEC 27001 mais pas seulement.

Ce certificat devra bien entendu faire partie du domaine de certification pour lequel l'organisme est accrédité. L'organisme d'évaluation de la conformité délivrant les certificats à un opérateur de services essentiels devra ainsi disposer d'une accréditation par BELAC ou par une autre institution reconnue et donc cosignataire des accords de reconnaissance du «European Cooperation for Accreditation».

L'accréditation par BELAC selon la norme ISO/IEC 17021 ou ISO/IEC 17065 permet de s'assurer du respect par les organismes d'évaluation de la conformité, lors de la délivrance d'un certificat, de règles générales d'indépendance, d'impartialité, de confidentialité et de qualité continue.

Article 16

La désignation d'un point de contact pour la sécurité des systèmes et réseaux d'information permettra à l'autorité sectorielle compétente, au CCB et à la DGCC de communiquer facilement avec les opérateurs identifiés en cas d'incidents ou de les informer de menaces éventuelles.

CHAPITRE 3

Melding van incidenten

Artikel 17

Dit artikel is gewijd aan de verplichting om incidenten te melden die een aanzienlijke impact hebben op de bevoegde overheden en regelt een aantal aspecten in verband met deze meldingen. De vraag of een incident een aanzienlijke impact heeft, moet worden beoordeeld rekening houdend met de gevolgen ervan voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de informatiesystemen waarvan de door de aanbieder verleende essentiële diensten afhankelijk zijn.

Voor de verplichte melding moet in de eerste plaats rekening worden gehouden met de impact van een incident op alle elementen vervat in de definitie van de beveiliging van netwerk- en informatiesystemen, vermeld in de richtlijn, zonder zich te beperken tot de impact op de continuïteit van de verleende essentiële diensten. Een incident dat een impact heeft op de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van informatiesystemen voor het verlenen van een essentiële dienst vormt immers een gebeurtenis die aan de bevoegde overheden moet worden meegedeeld en een belangrijk risico kan vormen voor de beveiliging van de aanbieder van essentiële diensten. De continuïteit van een verleende essentiële dienst is slechts één aspect van de beveiliging van informatiesystemen waarvan een aanbieder van essentiële diensten afhankelijk kan zijn. Een cyberaanval verloopt evenwel vaak in verschillende fasen met diverse verstorende effecten en veroorzaakt pas op het einde problemen voor de continuïteit van de diensten.

De aanbieder van essentiële diensten moet niet wachten tot hij over alle relevante informatie over een incident beschikt om het te melden. Wanneer hij uit de hem ter beschikking staande informatie reeds kan afleiden dat het incident een aanzienlijke impact heeft, moet hij het melden.

In eerste instantie is ervoor gekozen om de aanbieders te laten beoordelen of een incident een aanzienlijke impact kan hebben op de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de door hen verleende essentiële diensten. De wet bepaalt dus geen criteria maar machtigt de Koning, na advies van het

Notification d'incidents

Article 17

Cet article consacre l'obligation de notifier les incidents ayant un impact significatif aux autorités compétentes et règlemente plusieurs questions liées à ces notifications. Le caractère significatif de l'impact d'un incident doit être évalué au regard de son effet sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des systèmes d'information dont sont tributaires les services essentiels fournis par l'opérateur.

Tout d'abord, il s'agit de prendre en compte, pour l'obligation de notification, de l'impact d'un incident sur l'ensemble des éléments inclus dans la définition donnée par la directive de la sécurité des réseaux et systèmes d'information, sans se limiter au seul impact sur la continuité des services essentiels fournis. En effet, un incident ayant un impact sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité de systèmes d'information liés à la fourniture d'un service essentiel constitue un événement qui mérite d'être communiqué aux autorités compétentes et qui peut constituer potentiellement un risque important pour la sécurité de l'opérateur de services essentiels. La continuité de la fourniture d'un service essentiel n'est qu'un élément de la sécurité des systèmes d'information dont peut être tributaire un opérateur de services essentiels. Cependant, une attaque cyber est souvent menée en plusieurs phases avec des effets perturbateurs divers et ne se manifeste par un problème de continuité des services qu'en bout de course.

L'opérateur de services essentiels ne doit pas attendre de disposer de toutes les informations pertinentes sur un incident pour procéder à la notification. Lorsque les informations à sa disposition lui permette déjà de savoir qu'il s'agit d'un incident ayant un impact significatif, il convient qu'il le notifie.

Le choix a été fait, dans un premier temps, de laisser les opérateurs apprécier si l'incident est de nature à avoir un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des services essentiels qu'ils fournissent. La loi ne fixe donc pas de critères mais habilite le Roi, après avis du CCB, de la DGCC et des autorités sectorielles ainsi que,

CCB, de ADCC en de sectorale overheden, alsook, in voorkomend geval, van de deelgebieden, om, per sector of deelsector, de weerslagniveaus of drempelwaarden te bepalen die noodzakelijkerwijs een aanzienlijke impact hebben.

Deze in paragraaf 7 vermelde mogelijkheid waarover de Koning beschikt, heeft tot doel om de aanbieders van essentiële diensten, indien nodig, meer rechtszekerheid te bieden wat de gevallen betreft waarin wordt aangenomen dat een incident noodzakelijkerwijs een aanzienlijke impact heeft. In afwachting van deze weerslagniveaus of drempelwaarden worden de aanbieders verzocht rekening te houden met alle gebeurtenissen die een impact hebben op de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de informatiesystemen voor het verlenen van een essentiële dienst.

Doel van deze meldingen is het incidentbeheer te verbeteren, waarbij de wet de aanbieders ertoe verplicht om, samen met de melding, alle informatie te verstrekken die toelaat de aard van het incident te bepalen en de impact ervan te beoordelen, alsook de grensoverschrijdende impact ervan.

Zoals hierboven aangegeven is deze verplichte melding bovendien van toepassing op de aanbieders van essentiële diensten die bedoeld worden door de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten. De aanbieders van essentiële diensten die tot de financiële sector, moeten beveiligingsincidenten melden aan de Nationale Bank van België, die ze vervolgens aan het CCB en de ADCC bezorgt.

In principe moet deze melding tegelijk gebeuren bij drie afzonderlijke overheden, namelijk het CCB, de sectorale overheid of haar sectorale CSIRT en de ADCC. Paragraaf 4 bepaalt evenwel dat de Koning belast is met de oprichting van een gemeenschappelijk meldingsplatform om de uitvoering en verwerking van de verplichte meldingen door aanbieders van essentiële diensten en digitaaldienstverleners te vergemakkelijken, zodat in de praktijk slechts één enkele melding nodig is via dit unieke platform.

Na beslissing door de Koning en advies van de Gegevensbeschermingsautoriteit kan dit platform

le cas échéant, des entités fédérées, à établir des niveaux d'incidence ou des seuils, par secteur ou sous-secteur, constituant nécessairement un impact significatif.

Cette faculté laissée au Roi au paragraphe 7 vise à offrir si besoin une plus grande sécurité juridique aux opérateurs de services essentiels quant aux hypothèses dans lesquelles un incident doit nécessairement être considéré comme ayant un impact significatif. Dans l'attente de tels niveaux d'incidence ou de seuils, les opérateurs seront invités à prendre en compte tous les événements ayant un effet sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des systèmes d'information liés à la fourniture d'un service essentiel.

L'objectif de ces notifications est de permettre une meilleure gestion des incidents, de sorte que la loi oblige les opérateurs à fournir avec la notification toutes les informations permettant de caractériser l'incident et d'en évaluer l'impact y compris au niveau transfrontalier.

Par ailleurs, comme indiqué ci-avant, cette obligation de notification s'applique aux opérateurs de services essentiels visés par la loi du 21 novembre 2017 relative aux infrastructures de marchés d'instruments financiers ; quant aux autres opérateurs de services essentiels relevant du secteur des finances, ils doivent notifier les incidents de sécurité à la Banque Nationale de Belgique, qui se charge de les transmettre ensuite au CCB et à la DGCC.

Dans son principe, cette notification doit se faire, en même temps, à trois autorités distinctes, à savoir le CCB, l'autorité sectorielle ou à son CSIRT sectoriel, et à la DGCC. Toutefois, il est prévu, au paragraphe 4, que le Roi est chargé de créer une plateforme commune de notification pour faciliter la mise en œuvre et le traitement des notifications imposées aux opérateurs de services essentiels et aux fournisseurs de service numérique de sorte que ces derniers pourront réaliser en pratique une seule démarche de notification via cette plateforme unique.

Cette plateforme pourrait servir également, après décision du Roi et avis de l'Autorité de protection des

ook worden gebruikt voor verplichte meldingen door aanbieders van essentiële diensten en digitaaldienstverleners krachtens Verordening EU 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

Om het beheer en de verwerking van meldingen efficiënt te laten verlopen, verduidelijkt paragraaf 5 dat de Koning specifieke modaliteiten voor de melding en rapportering van incidenten kan bepalen.

Tot slot is het steeds mogelijk voor de aanbieders van essentiële diensten om het risico op incidenten of incidenten die geen aanzienlijke impact hebben in de zin van dit artikel vrijwillig te melden via het gemeenschappelijke meldingsplatform.

TITEL 3

Netwerk- en informatiesystemen van de digitaaldienstverleners

Artikel 18

Dit artikel vormt slechts de omzetting van de NIS-richtlijn en behoeft geen verdere commentaar.

HOOFDSTUK 1 De beveiligingseisen

Artikel 19

Dit artikel verplicht digitaaldienstverleners om de risico's voor de beveiliging van netwerk- en informatiesystemen te identificeren die gebruikt worden voor het verlenen, in de Europese Unie, van digitale diensten bedoeld in de NIS-richtlijn, alsook om passende en evenredige technische en organisatorische beveiligingsmaatregelen te nemen om deze risico's te beheer, naar het voorbeeld van wat bepaald is voor de aanbieders van essentiële diensten. Het artikel is grotendeels een omzetting van de richtlijn.

De digitaaldienstverleners moeten ook een contactpunt aanwijzen, om dezelfde redenen als de aanbieders van essentiële diensten.

données, pour les notifications imposés aux opérateurs de service essentiels et aux fournisseurs de service numérique, en vertu du Règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Afin de permettre la gestion et le traitement efficace des notifications, il est prévu au paragraphe 5 que le Roi peut fixer des modalités particulières de notification et de rapportage des incidents.

Enfin, il est toujours possible pour les opérateurs de services essentiels de notifier volontairement via la plateforme de notification commune des risques d'incidents ou des incidents n'ayant pas un impact significatif au sens du présent article.

TITRE 3

Réseaux et systèmes d'information des fournisseurs de service numérique

Article 18

Cet article constitue une simple transposition de la directive NIS et n'appelle pas de commentaires particuliers.

CHAPITRE 1 Les exigences de sécurité

Article 19

Cet article impose aux fournisseurs de service numérique d'identifier les risques menaçant la sécurité des réseaux et systèmes d'information utilisés pour fournir dans l'Union européenne de services numériques visés par la directive NIS, et de prendre les mesures techniques et organisationnelles de sécurité nécessaires et proportionnées pour les gérer, de façon similaire à ce qui est prévu pour les opérateurs de services essentiels. L'article constitue largement une transposition de la directive.

Les fournisseurs de service numérique doivent également désigner un point de contact, pour les mêmes raisons que les opérateurs de services essentiels.

HOOFDSTUK 2 Melding van incidenten

Artikel 20

Dit artikel voorziet in de verplichting om bepaalde incidenten te melden aan de bevoegde overheden en regelt een aantal aspecten in verband met deze meldingen, naar het voorbeeld van wat bepaald is voor de aanbieders van essentiële diensten.

De digitaaldienstverleners moeten incidenten melden die een aanzienlijke impact hebben op de verlening van de in de wet bedoelde en in de Europese Unie aangeboden dienst.

De melding gebeurt overeenkomstig de bepalingen van de uitvoeringsverordening (EU) 2018/151 van de Europese Commissie van 30 januari 2018 tot vaststelling van toepassingsbepalingen voor Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad wat betreft de nadere specificatie van de door digitaaldienstverleners in aanmerking te nemen elementen voor het beheer van de risico's in verband met de beveiliging van netwerk- en informatiesystemen en van de parameters om te bepalen of een incident aanzienlijke gevolgen heeft.

Overeenkomstig de richtlijn bevestigt de wet bovendien dat de dienstverlener een incident enkel moet melden indien hij toegang heeft tot de informatie die nodig is om de impact te beoordelen en dat, indien het incident dat de digitale dienst aantast een aanzienlijke impact heeft op de continuïteit van diensten die van essentieel belang zijn voor de instandhouding van kritieke maatschappelijke en economische activiteiten, de aanbieder van essentiële diensten die afhankelijk is van deze digitale dienst voor de verlening van zijn essentiële diensten, deze melding moet doen.

De digitaaldienstverlener moet niet wachten tot hij over alle relevante informatie over een incident beschikt om het te melden. Wanneer hij uit de hem ter beschikking staande informatie reeds kan afleiden dat het incident een aanzienlijke impact heeft, moet hij het melden.

Het artikel bevestigt verder de rol van het CCB op het gebied van grensoverschrijdende

CHAPITRE 2 Notification d'incidents

Article 20

Cet article consacre l'obligation de notifier certains incidents aux autorités compétentes et règlemente plusieurs questions liées à ces notifications, de façon analogue à ce qui est prévu pour les opérateurs de services essentiels.

Les fournisseurs de services numériques doivent notifier les incidents ayant un impact significatif sur la fourniture du service visé par la loi et offert dans l'Union européenne.

La notification se fait conformément aux dispositions du règlement d'exécution de la Commission européenne du 30 janvier 2018 (UE) 2018/151 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.

La loi confirme par ailleurs, ce qui résulte de la directive, que le fournisseur ne doit notifier un incident que s'il a accès aux informations nécessaires pour évaluer l'impact, et que si l'incident affectant le service numérique a un impact significatif sur la continuité de services essentiels au maintien de fonctions sociétales et économiques critiques, il incombe à l'opérateur de services essentiels qui s'appuie sur ce service numérique pour la prestation de ses services essentiels, d'effectuer la notification.

Le fournisseur de services numériques ne doit pas attendre de disposer de toutes les informations pertinentes sur un incident pour procéder à la notification. Lorsque les informations à sa disposition lui permette déjà de savoir qu'il s'agit d'un incident ayant un impact significatif, il convient qu'il le notifie.

L'article confirme encore le rôle de coopération du CCB sur le plan transfrontalier dans le partage d'informations avec d'autres États membres et dans

samenwerking bij het delen van informatie met andere lidstaten en bij het informeren van het publiek indien dit nodig is of in het algemeen belang is.

Tot slot kunnen digitaal dienstverleners risico's op incidenten of incidenten die geen aanzienlijke impact hebben op de verlening van hun digitale dienst, in de zin van dit artikel, ook vrijwillig melden via het gemeenschappelijke meldingsplatform.

TITEL 4

Toezicht en sancties

HOOFDSTUK 1

Toezicht op de aanbieders van essentiële diensten

Afdeling 1 Audits

Artikel 21

Dit artikel bepaalt dat aanbieders van essentiële diensten jaarlijks een interne audit en minstens om de drie jaar een externe audit moeten uitvoeren.

De interne audit kan worden uitgevoerd door de aanbieder van essentiële diensten zelf, door een andere aanbieder van de sector (collegiale toetsing) of door een externe dienstverlener.

Gezien de snelle evolutie van de informatie- en communicatietechnologie blijkt het noodzakelijk om aanbieders van essentiële diensten te verplichten minstens om de drie jaar een externe audit van de netwerk- en informatiesystemen uit te voeren. De termijn van drie jaar is een redelijk compromis tussen de kostprijs van een externe audit voor de aanbieder en deze constante evolutie van de technologie.

Het gebruik van geaccrediteerde externe auditinstellingen waarborgt een hoog gemeenschappelijk expertiseniveau tussen de verschillende sectoren voor de regelmatige controles van de aanbieders. Dit mechanisme is ook een hulpmiddel voor de inspectiediensten in het kader van hun controleopdrachten en laat toe de noodzakelijke budgettaire kosten voor de goede werking van voormelde diensten te beheersen.

l'information du public en cas de nécessité ou dans l'intérêt public.

Enfin, il est également possible pour les fournisseurs de services numériques de notifier volontairement, via la plateforme de notification commune, des risques d'incidents ou des incidents n'ayant pas un impact significatif sur la fourniture de leur service numérique, au sens du présent article.

TITRE 4

Contrôle et sanctions

CHAPITRE 1^{er}

Les contrôles des opérateurs de services essentiels

Section 1 Audits

Article 21

Cet article impose aux opérateurs de services essentiels de réaliser annuellement un audit interne, et au moins tous les trois ans un audit externe.

L'audit interne peut être réalisé par l'opérateur de services essentiels lui-même, par un autre opérateur du secteur (évaluation par ses pairs) ou par un prestataire extérieur.

Vu l'évolution rapide des technologies de l'information et de la communication, il s'avère nécessaire d'imposer au moins tous les trois ans la réalisation d'un audit externe des réseaux et des systèmes des opérateurs de services essentiels. Le délai de trois ans est un compromis raisonnable entre le coût pour l'opérateur de faire réaliser un audit externe et cette évolution constante des technologies.

Le recours à des organismes d'audit externe accrédités assure un niveau commun et élevé d'expertise entre les différents secteurs pour réaliser les contrôles réguliers des opérateurs. Ce mécanisme permet également d'aider les services d'inspection dans leur missions de contrôle et de maîtriser les coûts budgétaires nécessaires au bon fonctionnement des services précités.

Om de kosten betreffende de tussenkomst van een externe en geaccrediteerde instelling voor de conformiteitsbeoordeling te verdelen, kunnen verschillende aanbieders overeenkomen om samen een beroep te doen op dezelfde dienstverlener en voordelige prijsvoorwaarden te bedingen. Ook kunnen verschillende aanbieders van een sector of deelsector de oprichting van een sectorspecifieke instelling voor de conformiteitsbeoordeling aanmoedigen, die zich door BELAC zal laten accrediteren en voor de aanbieders van deze sector lagere tarieven zal hanteren.

Overeenkomstig de beginselen van onafhankelijkheid en autonomie mag de geaccrediteerde externe instelling voor de conformiteitsbeoordeling geen sectorale overheid zijn en evenmin een entiteit bestaande uit vertegenwoordigers van de sectorale overheid of uit de aanbieders van essentiële diensten die betrokken zijn bij de externe audits.

Indien de aanbieder heeft geopteerd voor certificering en het in artikel 15 van de wet bedoelde vermoeden geniet, kunnen de certificeringsaudits of de interne audits uitgevoerd in het kader van de certificering worden gelijkgesteld met de verplichte interne audit bedoeld in artikel 21. Aldus wordt het gebruik van gestandaardiseerde technische normen aangemoedigd, zonder verplicht te worden gesteld.

Ook worden, met hetzelfde doel, de certificeringsaudits conform artikel 15 gelijkgesteld met de externe audit die artikel 21 om de drie jaar oplegt. Zo belooft de wet het gebruik van erkende technische normen en voorkomt ze een opeenstapeling van soortgelijke audits.

Een aanbieder van essentiële diensten kan beslissen om jaarlijks een externe audit uit te voeren, maar zal dit minstens om de drie jaar moeten doen. Externe audits moeten steeds worden uitgevoerd door een geaccrediteerde of erkende instelling. Deze accreditering is gebaseerd op een accreditatie van de certificeringsinstelling door Belac of door een instelling die de erkenningsakkoorden van de "European Cooperation for Accreditation" medeondertekend heeft en die aan de minimumeisen van de ISO/IEC 17021 of ISO/IEC 17065 of een andere

Afin de mutualiser des coûts liés à l'intervention d'un organisme d'évaluation de la conformité externe et accrédité, plusieurs opérateurs peuvent s'entendre pour faire appel ensemble à un même prestataire en négociant avec lui des conditions avantageuses de prix. De même, plusieurs opérateurs d'un secteur ou d'un sous-secteur peuvent encourager la création d'un organisme d'évaluation de la conformité spécifique au secteur qui se fera accréditer par BELAC et proposera des tarifs réduits pour les opérateurs de ce secteur.

Afin de respecter les principes d'indépendance et d'autonomie, l'organisme d'évaluation de la conformité externe accrédité ne pourra être ni une autorité sectorielle ni une entité composée de représentants de l'autorité sectorielle ou des opérateurs de services essentiels concernés par les audits externes.

Si l'opérateur a opté pour la certification et bénéficie de la présomption visée à l'article 15 de la loi, les audits de certification ou les audits internes réalisés dans le cadre de la certification peuvent être assimilés à l'audit interne obligatoire prévu à l'article 21. Le recours à des normes techniques standardisées sont ainsi encouragées, sans être rendues obligatoires.

De même, et toujours dans le même but, les audits de certification réalisés auprès des opérateurs de services essentiels bénéficiant de la présomption visée à l'article 15 de la loi peuvent être assimilés à l'audit externe obligatoire imposé tous les trois ans. De la sorte, la loi encourage l'utilisation de normes techniques reconnues et évite la multiplication des audits similaires.

Un opérateur de services essentiels pourrait décider d'effectuer annuellement un audit externe mais devra au minimum effectuer cet exercice tous les trois ans. Les audits externes devront toujours être effectués par un organisme accrédité ou agréé. Cette accréditation de l'organisme de certification est effectuée par Belac ou par une institution qui est co-signataire des accords de reconnaissance du « European Cooperation for Accreditation » répondant aux exigences minimales de l'ISO/IEC 17021 ou

gedefinieerde norm voldoet, alsook op de naleving van eventuele bijkomende eisen die de bevoegde overheid voor de betrokken sector bepaalt, zoals bijvoorbeeld het feit over een veiligheidsmachtiging van een bepaald niveau te beschikken.

In een aantal gevallen kan een beroep worden gedaan op een instelling die enkel door de sectorale overheid is erkend, volgens de door de Koning bepaalde voorwaarden en modaliteiten.

De uitvoering van een externe audit door een instelling voor de conformiteitsbeoordeling betekent niet noodzakelijk dat een volledig auditproces moet worden overgedaan indien de aanbieder reeds onderworpen werd aan een extern auditmechanisme krachtens sectorale of buitenlandse regels (indien de informatiesystemen zich in het buitenland bevinden).

De instelling voor de conformiteitsbeoordeling kan immers reeds gecontroleerde elementen of door andere auditurs opgestelde auditverslagen eventueel erkennen, gebruiken en als relevant beschouwen.

Om een accreditering te bekomen voor het uitvoeren van de in paragraaf 3 bedoelde externe audits, moet de externe instelling via een accreditering het bewijs leveren dat ze de algemene beginselen opgelegd aan een instelling voor de conformiteitsbeoordeling naleeft en over de nodige bevoegdheden beschikt om na te gaan of de eisen voor de beveiliging van informatiesystemen worden nageleefd. De bevoegde overheid kan de externe instelling ook bijkomende eisen opleggen voor het bekomen van een accreditering.

Opgemerkt wordt dat de inhoud van de in deze wet bedoelde technische normen ISO/IEC gratis kan worden geraadpleegd bij het Bureau voor Normalisatie (NBN), bedoeld in artikel VIII.3 van het Wetboek van economisch recht, dat gevestigd is in Brussel.

Gezien het belang om over nuttige informatie te beschikken om de beveiliging van netwerk- en informatiesystemen te beoordelen, kan het CCB zich steeds een kopie laten overmaken van de auditverslagen.

De aanbieder van essentiële diensten zal een eerste interne audit uitvoeren uiterlijk binnen de

ISO/IEC 17065 ou autre norme définie par le Roi. En outre, cette accréditation peut inclure d'éventuelles exigences supplémentaires fixées par l'autorité compétente pour le secteur visé, comme par exemple, le fait de disposer d'une habilitation de sécurité d'un certain niveau.

Dans certains cas, il est possible de faire appel à un organisme seulement agréé par l'autorité sectorielle, selon les conditions et les modalités définies par le Roi.

La réalisation d'un audit externe par un organisme d'évaluation de la conformité ne signifie pas qu'il faille nécessairement recommencer tout un processus complet d'audit si l'opérateur a déjà été soumis à un mécanisme d'audit externe en vertu de règles sectorielles ou étrangères (si les systèmes d'information sont situés à l'étranger).

En effet, l'organisme d'évaluation de la conformité pourra éventuellement reconnaître, utiliser et juger pertinent des éléments déjà contrôlés ou des rapports d'audits réalisés par d'autres auditurs.

Afin d'obtenir une accréditation pour effectuer les audits externes visés au paragraphe 3, l'organisme externe doit apporter la preuve, par une accréditation, qu'il respecte les principes généraux imposés à un organisme de contrôle de la conformité et qu'il possède les compétences nécessaires pour évaluer le respect des exigences en matière de sécurité des systèmes d'information. L'autorité compétente peut également fixer des exigences supplémentaires à l'organisme externe pour qu'il obtienne une accréditation.

Il convient de préciser que le contenu des normes techniques ISO/IEC visées dans la présente loi peut être consulté gratuitement sur place au Bureau de Normalisation (NBN), visé à l'article VIII.3 du Code de droit économique et situé à Bruxelles.

Dans l'intérêt de disposer d'informations utiles pour évaluer la sécurité des réseaux et systèmes d'information, le CCB peut toujours se faire communiquer une copie des rapports d'audits.

L'opérateur de services essentiels réalisera pour la première fois un audit interne au plus tard dans les

drie maanden na de uitwerking van zijn I.B.B., dat, zoals bepaald in artikel 14, § 3, van de wet, moet worden aangenomen binnen een termijn van twaalf maanden na de kennisgeving van zijn aanwijzing door de sectorale overheid.

De aanbieder van essentiële diensten zal een eerste externe audit uitvoeren uiterlijk binnen de twee jaar na de uitvoering van zijn eerste interne audit. Bijgevolg vindt de eerste externe audit plaats na de termijn waarover de aanbieder van essentiële diensten volgens artikel 14, § 3, beschikt om de in zijn I.B.B. opgenomen maatregelen te implementeren, namelijk een termijn van uiterlijk vierentwintig maanden na de kennisgeving van zijn aanwijzing door de sectorale overheid.

Afdeling 2 Inspectiedienst

Artikel 22

Dit artikel draagt de Koning op om een bevoegde inspectiedienst aan te wijzen per sector of deelsector en, in voorkomend geval, de praktische modaliteiten voor de organisatie van de inspectiedienst te bepalen.

De inspectiedienst kan reactief of preventief optreden. Hij kan dit doen op eigen initiatief, op basis van een klacht of op verzoek van het CCB of van de sectorale overheid.

De inspectiedienst beschikt over ruime bevoegdheden om grondige controles uit te voeren op de naleving van de beveiligingsmaatregelen en de regels voor het melden van incidenten door de aanbieders van essentiële diensten. Zo mogen de leden van de inspectiedienst met name zonder voorafgaande verwittiging alle lokalen betreden die de aanbieder gebruikt, alsook de bewoonde lokalen mits voorafgaande machtiging van de onderzoeksrechter.

De inspectiedienst kan buitenlandse bevoegde overheden om samenwerking en bijstand verzoeken wanneer hij netwerk- en informatiesystemen van een aanbieder van essentiële diensten die zich buiten het Belgische grondgebied bevinden wenst te laten controleren.

trois mois de l'élaboration de sa P.S.I., laquelle devra être adoptée, comme le prévoit l'article 14, § 3 de la loi, dans un délai de douze mois à dater de la notification de sa désignation par l'autorité sectorielle.

Quant au premier audit externe, l'opérateur de services essentiels réalisera celui-ci au plus tard deux ans après la réalisation de son premier audit interne. Le premier audit externe interviendra donc postérieurement au délai accordé par l'article 14, § 3 à l'opérateur de services essentiels pour mettre en œuvre les mesures contenues dans sa P.S.I., à savoir un délai de vingt-quatre mois au plus tard à dater de la notification de sa désignation par l'autorité sectorielle.

Section 2 Service d'inspection

Article 22

Cet article charge le Roi de désigner un service d'inspection compétent par secteur ou sous-secteur et de fixer le cas échéant les éventuelles modalités sectorielles pratiques du contrôle.

Le service d'inspection peut intervenir de manière réactive ou préventive. Celui-ci peut agir d'initiative, ou sur base d'une plainte, ou à la demande du CCB ou encore de l'autorité sectorielle.

Le service d'inspection dispose de larges pouvoirs afin d'effectuer des contrôles approfondis du respect des mesures de sécurité et des règles de notification des incidents par les opérateurs de services essentiels. Ainsi, les membres du service d'inspection peuvent notamment pénétrer sans avertissement préalable dans tous les locaux utilisés par l'opérateur, et dans les locaux habités moyennant une autorisation préalable du juge d'instruction.

Le service d'inspection peut solliciter la coopération et l'assistance des autorités compétentes étrangères lorsqu'il souhaite faire contrôler des réseaux et systèmes d'information d'un opérateur de services essentiels qui sont situés en dehors du territoire belge.

Het artikel machtigt de Koning ook om jaarlijkse retributies te heffen. Deze retributies zullen door de sectorale overheid worden bepaald op basis van een onderzoek naar de kostprijs van de inspectieprestaties.

HOOFDSTUK 2

Toezicht op de digitaaldienstverleners

Artikel 23

Dit artikel regelt het toezicht op de digitaaldienstverleners. Deze moeten geen audits uitvoeren, maar zijn verplicht om de sectorale overheid alle informatie te verstrekken die nodig is om de beveiliging van de netwerk- en informatiesystemen te beoordelen, en elke niet-inachtneming van de beveiligingseisen en de eisen inzake het melden van incidenten recht te zetten.

De wet staat de sectorale overheid toe om maatregelen te nemen in geval van niet-naleving van voormelde eisen, alsook op grond van een aangifte door een autoriteit van een andere lidstaat.

HOOFDSTUK 3

De sancties

Afdeling 1

Procedure

Artikel 24

Ingevolge de controles van de inspectiedienst kan de sectorale overheid een ingebrekestelling overmaken aan de aanbieders van essentiële diensten en digitaaldienstverleners, met een remediëringstermijn. Bij gebrek aan remediëring na een ingebrekestelling wordt een proces-verbaal opgemaakt door de beëdigde personeelsleden van de inspectiedienst of de sectorale overheid.

Artikel 25

Dit artikel voorziet in de mogelijkheid om administratieve en strafrechtelijke sancties op te leggen.

Afdeling 2

L'article habilite aussi le Roi à établir des rétributions annuelles. Ces rétributions seront déterminées sur base d'un examen du coût de la prestation d'inspection par l'autorité sectorielle.

CHAPITRE 2

Contrôle des fournisseurs de service numérique

Article 23

Cet article règle le contrôle des fournisseurs de service numérique. Ceux-ci ne doivent pas effectuer d'audits, mais ils sont tenus de fournir à l'autorité sectorielle toutes les informations nécessaires pour évaluer la sécurité des réseaux et systèmes d'information, et de corriger tout manquement aux exigences de sécurité et de notification d'incidents.

La loi permet à l'autorité sectorielle d'adopter des mesures en cas de non-respect des exigences précitées, y compris sur dénonciation d'une autorité d'un autre État membre.

CHAPITRE 3

Les sanctions

Section 1

Procédure

Article 24

Suite aux contrôles du service d'inspection, l'autorité sectorielle peut adresser une mise en demeure aux opérateurs de services essentiels et fournisseurs de service numérique, avec un délai de remédiation. A défaut de remédiation suite à une mise en demeure, un procès-verbal sera dressé par les membres du personnel assermentés du service d'inspection ou de l'autorité sectorielle.

Article 25

Cet article prévoit la possibilité de sanctions administratives comme de sanctions pénales.

Section 2

Sanctions pénales

Strafrechtelijke sancties

Artikel 26

Dit artikel bepaalt de straffen in geval van niet-naleving van de verplichtingen opgelegd door de wet of de uitvoeringsbesluiten ervan.

Afdeling 3

Administratieve sancties

Artikel 27

Dit artikel bepaalt het bedrag van de administratieve geldboetes en regelt de tenlasteneming van de eventuele expertisekosten.

Artikel 28

Dit artikel verduidelijkt dat het in artikel 24 bedoelde proces-verbaal naar de procureur des Konings en overtreder wordt gestuurd.

Artikel 29

Volgens dit artikel beschikt de procureur des Konings over een termijn van twee maanden te rekenen vanaf de ontvangst van het proces-verbaal om strafrechtelijke vervolging in te stellen tegen de aanbieder van essentiële diensten, die hierover binnen dezelfde termijn wordt ingelicht. Er mag geen administratieve geldboete worden opgelegd vóór het verstrijken van deze termijn of vóór de beslissing van de procureur des Konings om niet te vervolgen.

Artikel 30

Dit artikel regelt de principes voor het bepalen van het bedrag van de geldboete, de in aanmerking te nemen omstandigheden, de situaties van herhaling en de situatie van samenloop van inbreuken.

Met het oog op de eerbiediging van de rechten van de verdediging is bepaald dat de overtreder kan worden gehoord of zijn verweermiddelen schriftelijk kan indienen binnen een termijn van 15 dagen.

De leden van de inspectiedienst of van de sectorale overheid die hebben deelgenomen aan de betrokken inspecties of controles mogen, in de

Article 26

Cet article prévoit les peines applicables en cas de non-respect des obligations imposées par la loi ou par ses actes d'exécution.

Section 3

Sanctions administratives

Article 27

Cet article prévoit le montant des amendes administratives et règle la prise en charge des frais éventuels d'expertise.

Article 28

Cet article prévoit la communication du procès-verbal visé à l'article 24, au procureur du Roi et à l'auteur de l'infraction.

Article 29

Cet article permet au procureur du Roi de mouvoir l'action pénale dans un délai de deux mois à compter de la réception du procès-verbal, à l'encontre de l'opérateur de services essentiels, qui en sera informé dans le même délai. Avant l'expiration de ce délai ou la décision du procureur du Roi de ne pas poursuivre, une amende administrative ne peut être infligée.

Article 30

Cet article règle les principes de détermination du montant de l'amende, des circonstances à prendre en considération, des situations de récidive et la situation du concours.

Pour assurer le respect des droits de la défense, il est prévu de permettre à l'auteur d'être entendu ou de formuler ses moyens de défense par écrit dans un délai de 15 jours.

Les membres du service d'inspection ou de l'autorité sectorielle ayant participé aux inspections ou aux contrôles concernés veilleront également à s'abstenir,

mate van het mogelijke, ook niet deelnemen aan beraadslagingen van de sectorale overheid betreffende de sanctie voor de aanbieder van essentiële diensten of digitaledienstverlener.

Artikel 31

Dit artikel bepaalt dat de beslissing ter kennis wordt gebracht van de overtreder, de burgerrechtelijk aansprakelijke persoon en de procureur des Konings.

Artikel 32

Dit artikel maakt het mogelijk om de beslissing te betwisten bij verzoekschrift bij het Marktenhof dat de zaak behandelt zoals in kort geding overeenkomstig de artikelen 1035 tot 1038, 1040 en 1041 van het Gerechtelijk Wetboek en dat de beslissing kan herzien.

Het beroep heeft geen schorsende werking.

Artikel 33

Dit artikel bepaalt de voorwaarden waarin de beslissing uitvoerbaar wordt.

Artikel 34

Uit dit artikel blijkt dat de verjaringstermijn voor de administratieve geldboetes drie jaar bedraagt.

TITEL 5 Slotbepalingen

HOOFDSTUK 1 Wijzigingsbepalingen

Artikel 35 en volgende passen de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur aan, om er de rol van het Centrum voor Cybersecurity België in te verankeren.

Aangezien de exploitanten van kritieke infrastructuur als aanbieders van essentiële diensten kunnen worden geïdentificeerd, moet ook het Centrum voor Cybersecurity België worden betrokken bij het identificatieproces van de kritieke infrastructuur, wat de beveiliging van netwerk- en informatiesystemen betreft.

dans la mesure du possible, de participer aux délibérations de l'autorité sectorielle relative à la sanction à infliger à l'opérateur de service essentiels ou au fournisseur de service numérique.

Article 31

Cet article prévoit que la décision est notifiée à l'auteur de l'infraction et à la personne civilement responsable, ainsi qu'au procureur du Roi.

Article 32

Cet article permet de contester la décision par voie de requête auprès de la Cour des marchés qui traite l'affaire selon les formes du référé conformément aux articles 1035 à 1038, 1040 et 1041 du Code judiciaire et qui peut réformer la décision.

Le recours n'est pas suspensif.

Article 33

Cet article prévoit les conditions dans lesquelles la décision devient exécutoire.

Article 34

Cet article prévoit que le délai de prescription est de trois ans pour les amendes administratives.

TITRE 5 Disposition finales

CHAPITRE 1 Dispositions modificatives

L'article 35 et suivants visent à adapter la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques, afin d'y consacrer le rôle du Centre pour la Cybersécurité Belgique.

Compte tenu du fait que les exploitants d'infrastructures critiques peuvent être identifiés comme opérateurs de services essentiels, il est utile d'associer également le Centre pour la Cybersécurité Belgique au processus d'identification des infrastructures critiques, pour ce qui concerne la sécurité des réseaux et systèmes d'information.

Deze artikelen behoeven geen verdere commentaar.

HOOFDSTUK 2 Inwerkingtreding

Artikel 50

Dit artikel behoeft geen verdere commentaar.

BIJLAGE I

Deze bijlage beschrijft de voorschriften en taken van het nationale CSIRT en van de eventuele sectorale CSIRT's.

BIJLAGE II

Deze bijlage bevat de soorten aanbieders van essentiële diensten die minstens in aanmerking moeten worden genomen voor de identificatie-procedure.

BIJLAGE III

Deze bijlage bevat de soorten digitaaldienstverleners.

BIJLAGE IV

Deze bijlage bevat de reeds door de wet aangewezen sectorale overheden.

Les autres articles n'appellent pas de commentaires particuliers.

CHAPITRE 2 Entrée en vigueur

Article 50

Cet article n'appelle pas de commentaire particulier.

ANNEXE I

Cette annexe décrit les obligations et les tâches du CSIRT national et des éventuels CSIRT sectoriels.

ANNEXE II

Cette annexe reprend les types d'opérateurs de services essentiels qui doivent au minimum être pris en compte par la procédure d'identification.

ANNEXE III

Cette annexe reprend les types de fournisseurs de service numérique.

ANNEXE IV

Cette annexe reprend les autorités sectorielles déjà désignées par la loi.