1 Opmerkingen/ review commentaar Memorie Van Toelichting

1.1 Algemeen

001) Kan van een organisatie één legal entity van toepassing zijn en anderen niet? Waar ligt de grens en is top management van de hele organisatie dan essentieel?
002) Wanneer is er meer duidelijkheid over de toezichthouders per sector?
003) Hoe dient een multinational om te gaan met wisselende implementatie richtlijnen per member state?
004) Is er een klachtenprotocol over de (dienstverlening/ handen) van de bevoegde autoriteit
005) in welke mate kunnen ketens gevrijwaard worden van kwaadwillende besmettingen?
006) Welke vrijwaring is naar ontvangers van diensten te geven over te nemen maatregelen c.q. van ketenpartners te vragen?

1.2 Paragraaf 2.4

007) Wat is een bijna incident in relatie tot een natuurramp?

1.3 Paragraaf 4.8 / 5.5.1: Dubbele meldplicht

008) Op welke wijze zal het CSIRT en de toezichthoudende instantie samenwerken om te voorkomen dat er meerdere handelingen nodig zijn voor de entiteit?
009) Op welke wijze zal er internationaal samenwerking gezocht worden om eenzelfde efficiëntie te behalen voor multinationals?

1.4 Paragraaf 5.2.3

010) Welke toets dient de vakminister te maken om te kiezen voor een aanwijzing bij besluit?

1.5 Paragaaf 5.3.3

011) Tot welke mate kan de omvang van een entiteit of haar financiële capaciteit invloed hebben op de keuze van te nemen maatregelen?

1.6 Paragraaf 5.3.4

012) Wanneer heb je voldaan aan je plicht om (toe)leveranciers te checken? Wat is redelijk en hoe wordt dat beoordeeld?

1.7 Paragraaf 5.3.5

013) In memorie van toelichting staat dat het zou kunnen dat het minimum lijstje uitgebreid gaat worden met meer. Hoe sluit dit aan bij ambitie om geen nationale verschillen te krijgen?

1.8 Paragraaf 5.5.1: Significante incidenten

014) Is er meer richting (guidance) beschikbaar voor de termen ernstige operationele verstoring en aanzienlijke materiële of immateriële schade?
015) Incidenten beperken zich vaak niet tot landsgrenzen. Hoe gaat de Nederlandse overheid zorgen voor voldoende samenwerking met andere lidstaten om efficiëntie te krijgen/ administratieve rompslomp te voorkomen rondom het melden in verschillende landen?

1.9 Paragraaf 5.5.2

016) Wat moet de ernst of onomkeerbaarheid zijn van de nadelige invloed die kan plaatsvinden bij een significant incident?

1.10 Paragraaf 5.6.4

017) waarom staat er “geacht”? Is dit niet op een andere manier te waarborgen?

1.11 Paragraaf 5.7.5

018) hoe verhoudt zich urgentie tot het aanstellen van een controlefunctionaris in relatie tot het open staan van bezwaar, beroep en hoger beroep?

1.12 Paragraaf 5.7.12:

019) Bij een organisatie die bestaat uit meerdere legal entiteiten en suborganisaties, welk bestuur is hier bedoeld?

020) Wie valt er onder bestuur bij aansprakelijkheid, is dat ook de RvC?

1.13 Paragraaf 5.8 Meldplicht & registratieplicht

021) Hoe dient registratie en melding plaats te vinden bij een multinational die acteert in verschillende sectoren, wie moet wat in welke member state en waar melden/ registreren?

2 Review commentaar Cyberbeveiligingswet

2.1 Definities/ begripsbepaling

022) **Artikel 1:**
Als een organisatie bestaat uit een NV structuur en verschillende BVs, zijn de onderliggende BVs dan (ook) een entiteit? Dit punt raakt namelijk overweging 16 van de NIS2 richtlijn, waarbij entiteiten die onafhankelijk zijn van haar partneronderneming of verbonden onderneming wat netwerk- en informatiesystemen betreft niet als KMO hoeft te worden beschouwd en hierdoor buiten het toepassingsgebied van de NIS2 richtlijn vallen.

023) **Artikel 45:** moeten alle BVs van een organisatie als een separate entiteit worden geregistreerd? Moeten joint ventures waarin een organisatie participeert ook als entiteit worden geregistreerd?

024) **Artikel 2, lid f**: hoe is een "bijna-incident" gedefinieerd? Voorstel is een definitie op te nemen onder Artikel 1 (begripsbepaling). In Artikel 2 van NIS2 richtlijn: "*bijna-incident": een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar had kunnen brengen, maar die met succes is voorkomen of zich niet heeft voorgedaan.*"

025) **Artikel 27, lid 2:** definitie van een significant incident is niet duidelijk. Ieder incident kan immers leiden tot financiële verliezen. In Artikel 6 van NIS2 richtlijn komt de definitie "significant incident" overigens ook niet voor. In Artikel 6 van NIS2 richtlijn is wel sprake van "incident" en "grootschalig cyberbeveiligingsincident ". Voorstel is in Artikel 1 (begripsbepaling) aan te sluiten bij definities uit NIS2, om een andere interpretatie in Europese lidstaten te voorkomen.

026) **Artikel 35:** De voorwaarden en implicaties van vrijwillige meldingen van incidenten zijn mogelijk niet duidelijk, wat kan leiden tot aarzeling bij het melden van potentiële cyberdreigingen of bijna-incidenten.

027) **Artikel 16, lid 5, artikel 42 lid 1 en 2:**
de wet "weerbaarheid kritieke entiteiten" is niet nader gespecifieerd/ geen nadere referentie. Voorstel om dit op te nemen in de begripsbepaling (artikel 1): "Regels ter implementatie van Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (PbEU 2022, L 333) (Wet weerbaarheid kritieke entiteiten)"

028) **Artikel 17, lid 7:** het is niet nader gespecificeerd waar "taxonomieën" betrekking op hebben. Voorstel is een definitie op te nemen onder Artikel 1 (begripsbepaling)

029) **Artikel 79, lid 1:** het is niet duidelijk wat met een beveiligingsscan bedoeld wordt. Heeft dit betrekking op controle van organisatorische maatregelen? Of dienen hiervoor sensors in het interne netwerk te worden geplaatst?

2.2 Registratie

030) **Artikel 22, lid 2:** als het nationale register per 17 januari 2025 tot stand komt, betekent dit dan dat bedrijven zich al eerder hebben moeten registreren of is registratie per die datum?

031) **Artikel 22, lid 2:** welke voorwaarden worden gesteld aan de functionaris die namens een bedrijf de registratie opvoert?

032) **Artikel 59, lid 3:** hoe weet de bevoegde autoriteit waar de bevoegde toezichthoudende autoriteit vanuit AVG is gevestigd? Is dit onderdeel van registratieproces?

2.3 CSIRT

033) **Artikel 17, lid 7:** wordt invoering en gebruik van gemeenschappelijke of gestandaardiseerde praktijken, classificatieschema's en taxonomieën door CSIRT een verplichting voor bedrijven?

034) **Artikel 19:** is/ wordt het nationaal plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons openbaar?

035) **Artikel 28, lid 1:** wie is namens een entiteit gemandateerd om melding te doen van een significant incident aan CSIRT?

036) **Artikel 28, lid 1:** Een bedrijf dat in meerdere EU-lidstaten opereert kan gehinderd worden bij het coördineren van incidentrespons en naleving van verschillende nationale wetgevingen. Moet een (multi-nationaal) bedrijf dat in meerdere Europese lidstaten actief is een vroegtijdige melding doen bij alle nationale CSIRTs of volstaat een melding bij de lidstaat waar het hoofdkwartier is gevestigd?

037) **Artikel 29, lid 1d:** het indienen van een melding met alle beschikbare informatie om het CSIRT in staat te stellen eventuele grensoverschrijdende gevolgen van het incident te bepalen is te ruim gedefinieerd. Hierin zou minimaal vermeld moeten zijn welke informatie wordt verwacht.

038) **Artikel 30:** hoe vaak kunnen bedrijven verzoeken van het CSIRT verwachten voor een tussentijds verslag? Is dit enkel gedurende de eerste 72 uur?

039) **Artikel 31, lid 1:** ik zou ook een relatie verwachten naar een beheersmaatregel die heeft gefaald of (nog) niet is gerealiseerd. Tevens zou ik verwachten welke lessons learned/ verbeteringen worden toegepast ter voorkoming.

040) **Artikel 38, lid 2:** is aanvullende technische ondersteuning door CSIRT kosteloos? Dienen hier van te voren afspraken over te worden gemaakt?

041) **Artikel 41, lid 2:** op welke wijze beschermt het centrale contactpunt de beveiligingsbelangen, privacy en commerciële belangen van de entiteit en de vertrouwelijkheid van de informatie?

042) **Artikel 55:** De interactie en informatie-uitwisseling met CSIRTs en bevoegde autoriteiten in derde landen kan complex zijn, vooral gezien de verschillende juridische kaders en nalevingsvereisten. Hoe wordt naleving getoetst en geborgd?

2.4 Bestuur van een entiteit

043) **Artikel 26, lid 1**: het bestuur van een essentiële entiteit of belangrijke entiteit is niet eenduidig. Wellicht verwijzing opnemen naar Artikel 129 uit het Burgerlijk Wetboek 2 (bestuurstaken en verantwoordelijkheden in NV) en Artikel 239 uit het Burgerlijk Wetboek 2 (bestuurstaken en verantwoordelijkheden in BV). Een MKB bedrijf is vaak georganiseerd als een BV.

044) **Artikel 26, lid 1**: in theorie zou een BV dat onderdeel uitmaakt van een NV verschillende bestuurders kunnen hebben. Wie is in dat geval aansprakelijk in het kader van eventuele boetes?

045) **Artikel 26, lid 6:** wanneer worden via Algemene maatregel van bestuur regels gesteld aan de training (duur, niveau), zoals te volgen door bestuurders?

046) **Artikel 28, lid 2c:** welke eisen worden gesteld aan de functionaris die verantwoordelijk is voor de melding? Wordt met "de melding" de melding aan het CSIRT bedoeld, of wordt de melding bedoeld intern een entiteit?

047) **Artikel 84 lid 3:** als sprake is van een boete, kan een entiteit dan in verschillende lidstaten beboet worden als sprake is van eenzelfde overtreding in meerdere lidstaten?

2.5 Generieke vragen

048) **Artikel 42, lid 1:** het is vreemd om in deze wet een verwijzing te maken naar de bevoegde autoriteit zoals gedefinieerd in artikel 8 van de Wet weerbaarheid kritieke entiteiten. Wellicht beter om hier te verwijzen naar artikel 16 van Cyberbeveiligingswet?

049) **Artikel 44:** waarom wordt in Nederland enkel een vertegenwoordiger aangewezen als een entiteit in Nederland wel diensten aanbiedt en nog geen vertegenwoordiger in een andere Europese lidstaat heeft aangeboden? Dat lijkt rechtsongelijkheid ten opzichte van essentiële of belangrijke entiteiten die in lidstaten zijn gevestigd en in al deze landen een registratieplicht hebben.

050) **Artikel 24:** Voor sectoren waarin een entiteit actief is, kunnen er sectorspecifieke rechtshandelingen van toepassing zijn die gelijkwaardige beveiligingsmaatregelen vereisen. Het is belangrijk om duidelijkheid te krijgen over welke sectorspecifieke regels van toepassing zijn en hoe deze zich verhouden tot de NIS2-verplichtingen.

2.6 Verwerking Persoonsgegevens

051) **Artikel 52, 53, 55, 56:** in het kader van informatie uitwisseling tussen CSIRTS, hoe wordt invulling gegeven aan waarborgen persoonsgegevens? Hoe vindt toetsing plaats of systemen voldoen aan het noodzakelijke beveiligingsniveau? Over welke persoonsgegevens gaat het op dat moment?

052) **Artikel 55:** uitwisseling van persoonsgegevens kan ook plaatsvinden met een derde land, waar landen buiten de EU mee bedoeld worden. Op welke wijze wordt invulling gegeven aan rechtmatige verwerking van persoonsgegevens conform AVG in deze derde landen?

053) **Artikel 64:** in het artikel is vermeld dat verwerkingsverantwoordelijken (controllers) betrekking hebben op de bevoegde autoriteit, het centrale contactpunt, het CSIRT en Onze Minister voor de taken die zij op grond van cyberbeveiligingswet uitvoeren. Voorstel is om een samenvatting van deze taken als onderdeel van het wetsartikel op te nemen.

054) **Artikel 65, lid 1**: in de voorwaarden voor het verstrekken van vertrouwelijke gegevens zijn persoonsgegevens niet expliciet vermeld. Voorstel is om dit alsnog expliciet te maken.

2.7 Cyberbeveiligingswet <> Wet weerbaarheid kritieke entiteiten

055) In **bijlage** 1 en bijlage 2 worden **essentiële** en **belangrijke** entiteiten vermeld. In de bijlage van de Wet weerbaarheid **kritieke** entiteiten zijn bijna dezelfde sectoren en subsectoren vermeld, maar is sprake van verschillen. In Wet weerbaarheid kritieke entiteiten is bijv. sector vervoer, subsector Openbaar vervoer vermeld, maar deze ontbreekt in Cyberbeveiligingswet. Voorstel is om dezelfde sectoren en subsectoren te hanteren in de verschillende bijlagen van beide wetteksten.

2.8 Spelfoutjes

056) **Artikel** 54: spelfout (NIS@)

057) **Artikel** 61, lid 3: na *de* ontvangst.

058) **Artikel** 82: gevenom

059) **Artikel** 83: terhandhaving