Inspectie Leefomgeving en Transport
Ministerie van Infrastructuur en Waterstaat

> Retouradres

Directoraat-Generaal Luchtvaart en Maritieme Zaken
T.a.v. de plv. Directeur-Generaal,
[redacted]

ILT
Omgeving, Dienstverlening en Vergunn.
Netwerken transport

Den Haag

[redacted]

Ons kenmerk
ILT-2024/30257

Datum 26 juni 2024
Betreft HUF - Toets Cyberbeveiligingswet (Cbw)

Geachte mevrouw [redacted]

Op 20 mei 2024 verzocht u mij, namens de Directeur-Generaal Luchtvaart en Maritieme Zaken, de Directeur-Generaal Mobiliteit, de Directeur-Generaal Milieu en Internationaal en de Directeur-Generaal Water en Bodem, een handhaafbaarheids-, uitvoerbaarheids- en fraudebestendigheidstoets (HUF-toets) uit te voeren op de Cyberbeveiligingswet (Cbw). De Cbw strekt tot uitvoering van de Richtlijn (EU) 2022/2555 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie. Deze richtlijn wordt hierna aangeduid als de NIS2-richtlijn. De lidstaten van de Europese Unie moeten uiterlijk op 17 oktober 2024 aan de NIS2-richtlijn voldoen door deze waar nodig in hun nationale regelgeving om te zetten. Deze richtlijn beoogt de verschillen weg te nemen die tussen lidstaten bestaan op het gebied van de cyberbeveiligingseisen die worden gesteld aan entiteiten die economisch belangrijke activiteiten of diensten verrichten.
Gelijktijdig met deze toets, stuur ik u de uitkomsten van de HUF – toets over de wet weerbaarheid kritieke entiteiten (Wke). Voor beiden geldt dat de uitwerking in een algemene maatregel van bestuur (AMvB) belangrijk is voor het creëren van meer duidelijkheid. We blijven hier dan ook graag bij betrokken

Algemeen
Met deze brief informeer ik u over de uitkomst van de HUF-toets. In de huidige vorm bevat de wet nog enkele onduidelijkheden en risico's die nader uit te werken zijn via een AMvB. Daarbij zijn onduidelijk-heden over de hoeveelheid entiteiten die onder het toezicht vallen, welk aantal daarvan essentiële en belangrijke entiteiten zijn, de samenwerkings-afspraken met andere toezichthouders alsmede de toekenning van de extra benodigde capaciteit, punten van aandacht. Hieronder volgt per onderdeel van de HUF – toets een korte toelichting.

Handhaafbaarheid
In zijn algemeenheid ben ik van oordeel dat het wetsvoorstel handhaafbaar is. Een aandachtspunt binnen de Cbw is de verplichte registratie van de onder toezichtstaande. Hoewel artikel 45 essentiële en belangrijke entiteiten verplicht om informatie aan te leveren voor het nationale register, betekent dit niet automatisch dat deze entiteiten zich correct zullen registreren. Als ze dit niet doen

of zich verkeerd categoriseren, kunnen ze theoretisch langere tijd buiten het zicht van toezicht blijven. Daarnaast bevat de Cbw regels voor de zorgplicht en meldplicht van significante incidenten, met een gedelegeerde bevoegdheid voor sectorspecifieke regels via een AMvB. De uitwerking hiervan is van belang om deze zorg- en meldplicht goed te regelen.

Uitvoerbaarheid
Het wetsvoorstel is, op enkele kanttekeningen na, uitvoerbaar. De implementatie van de Cbw vraagt om een uitbreiding van toezichtcapaciteit om de kwaliteitsmaatstaven te waarborgen. Het aantal sectoren neemt toe en daardoor ook het aantal entiteiten onder toezicht. Hierdoor is een toename van het aantal inspecteurs en middelen nodig, evenals extra afstemming met andere toezichthouders. Op basis van het relatief lage aantal entiteiten die onder de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni) vallen, voldoen momenteel de gebruikelijke systemen van de ILT voor de informatieverwerking. Door de forse toename van het aantal entiteiten moet de ILT een systeem ontwikkelen voor de verwerking van geclassificeerde informatie van circa 1800 entiteiten, passend binnen de bestaande systemen en nieuwe rapportage-verplichtingen. Dit samen resulteert in een geschatte behoefte aan 36fte inspecteurs en 10fte aan ondersteunend personeel, met een totaal van 46 fte. Er wordt uitgegaan van een ingroeimodel voor NIS-2 van 20% in 2025, oplopend naar 100% vanaf 2029. Het hiervoor toegekende budget betreft vanaf 2029 een structurele toezegging van
€ 7.585.400, = voor de uitvoering van het toezicht op de Cbw.

Verder is er een aantal risico's te benoemen, die van invloed zullen zijn op de uitvoering van het toezicht. Ik noem de belangrijkste:

- ex ante toezicht op kritieke entiteiten is in beginsel proactief en risico-gestuurd. Ex post toezicht op belangrijke entiteiten zal plaatsvinden als daar bijvoorbeeld als gevolg van incidenten reden voor is. Met de groei van het aantal entiteiten, zal de kans op incidenten toenemen en dit zal impact hebben op de beschikbare capaciteit voor zowel regulier als incident gedreven toezicht;
- het aantal handhavingsverzoeken aan en van buitenlandse autoriteiten kan niet goed worden ingeschat;
- de arbeidsmarkt voor medewerkers met expertise op dit voor ILT deels nieuwe vakgebied, maar ook voor bijvoorbeeld de benodigde IT-specialisten, is uiterst gespannen. Het is onzeker of de ILT tijdig de expertise en capaciteit daadwerkelijk kan werven;
- het is onzeker welke aanpassingen nodig zijn in de informatiesystemen en wat de kosten hiervan zullen zijn;
- de mate van naleving is onzeker en de noodzaak tot sanctionering ook. De ervaring met verscherpt toezicht onder de Wbni leert dat dergelijke trajecten arbeidsintensief zijn, waardoor er minder tijd beschikbaar blijft voor reguliere inspecties;
- het aantal entiteiten dat onder de Cbw wordt aangewezen, kan in de toekomst nog wijzigen, evenals het toevoegen van andere vitale sectoren.

Gezien de grote opgave die de ILT hierdoor kent, zal het toezicht geleidelijk aan moeten worden doorontwikkeld. Dit betekent dat ook na de inwerkingtreding de inrichting en doorontwikkeling van het toezicht nog zal doorlopen.

Gelet op deze en andere onzekerheden stel ik daarom voor om twee jaar na inwerkingtreding van de Cbw een evaluatie te houden waarin aandacht wordt besteed aan genoemde implementatievraagstukken en risico's. Aan de hand van deze evaluatie kan nader bepaald worden in hoeverre de beschikbare middelen ook op langere termijn voldoende zijn.

Fraudebestendigheid
Het wetsvoorstel is in beginsel fraudebestendig. Entiteiten kunnen in het geval van incidenten terecht bij een meldpunt opgezet door de NCTV/NCSC. Een Information Security Management System (ISMS) moet controles omvatten om fraude zoveel mogelijk te voorkomen, zoals controle van certificaten, administratief (keten) toezicht, toepassing van de Wet BIBOB, en raadpleging van openbare registers voor controle van derden gegevens. Hierbij is een duidelijke uitwerking in de AMvB van belang voor een goed werkend systeem.

Voor een nadere onderbouwing en gedetailleerd commentaar verwijs ik u naar de bijlagen.
Graag verneem ik uw reactie op deze HUF-toets alsmede de definitieve tekst van de regelgeving en de datum van inwerkingtreding.

BIJLAGE 1: CHECKLIST HUF – TOETS

ILT
Omgeving, Dienstverlening en Vergunn.
Netwerken transport

Datum
18 juni 2024

CHECKLIST HUF-TOETS

Toetsonderwerpen HUF-toetsen

De onderstaande onderwerpen komen aan de orde bij het uitvoeren van een toets. Om wet- en regelgeving te kunnen handhaven is een aantal zaken essentieel:

- Er moet een toezichthouder zijn aangesteld;
- Er moeten heldere en eenduidige normen zijn;
- Het moet duidelijk zijn tot wie deze normen zijn gericht;
- De toezichthouder moet over een adequaat handhavingsinstrumentarium beschikken.

Dit toetskader is voor het onderdeel Uitvoerbaarheid gebaseerd op SCOPAFIJTH (Security, Communicatie, Organisatie, Personeel, Administratieve organisatie, Financiën, Informatievoorziening, Juridisch, Technologie en Huisvesting)

Informatie

Onderhavige regelgeving	Cyberbeveiligingswet (Cbw)
Beoordelaar(s)	[redacted]
Deadline	Gezien dit implementatiewetgeving van Europese regelgeving betreft die een groot aantal sectoren omvat, ontvangt Plv. Directeur-Generaal Luchtvaart en Maritieme Zaken, B.C.M. Gijsbers ons advies graag uiterlijk maandag 1 juli 2024, gelijktijdig met de sluiting van de internetconsultatie.
Extra info	De Cbw HUF toets is gelijktijdig uitgevoerd met de HUF-toets op de Wet Weerbaarheid Kritieke Entiteiten (Wet Wke). Op grond van het voorstel voor de Wet Wke aangewezen kritieke entiteiten, zijn ook essentiële entiteiten als bedoeld in het onderhavige wetsvoorstel. Gelet daarop is het ten eerste relevant dat in de Wet Wke ook de subsector openbaar vervoer is opgenomen, met onze minister als bevoegde autoriteit. Ten tweede is relevant dat het voornemen bestaat om op basis van artikel 7a, Wet Wke, het reeds vitale proces keren en beheren waterkwantiteit en grootschalige vervaardiging, productie en distributie, (in het verzoek aangehaald als: productie, verwerking en/of opslag) (petro)chemische stoffen aan te wijzen als sector onder deze wetgeving waardoor deze ook onder de werking van de Cbw komen te vallen als Essentieel. De Plv. Directeur-Generaal Luchtvaart en Maritieme Zaken, Mw. B.C.M. Gijsbers heeft het verzoek voor deze HUF toets(en) mede ingediend namens de Directeur-Generaal Luchtvaart en Maritieme Zaken, de Directeur-Generaal Mobiliteit, de Directeur-Generaal Milieu en Internationaal, en de Directeur-Generaal Water en Bodem.
Korte samenvatting regelgeving	De Cbw strekt tot de uitvoering van de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148.1 Deze richtlijn wordt hierna aangeduid als de NIS2-richtlijn. De lidstaten van de Europese Unie (hierna: lidstaten) moeten uiterlijk op

	17 oktober 2024 aan de NIS2-richtlijn voldoen door deze richtlijn waar nodig in hun nationale regelgeving om te zetten. De NIS2-richtlijn is de opvolger van de zogeheten NIS1-richtlijn. Het doel van de richtlijn is om, ter ondersteuning van het functioneren van onze samenleving en economie, eenheid en samenhang te brengen in Europees beleid voor netwerk- en informatiebeveiliging, door de digitale paraatheid te vergroten en de gevolgen van cyberincidenten te verkleinen. De NIS1-richtlijn laat veel discretionaire ruimte over aan lidstaten bij de uitvoering van de richtlijn. Door die geboden ruimte zijn er tussen lidstaten aanzienlijke verschillen ten aanzien van de implementatie van de richtlijn in de lidstaten. Zo zijn er aanzienlijke verschillen op het gebied van de afbakening van het toepassingsgebied van de richtlijn. Dat verschil betekent concreet dat een aanbieder in de ene lidstaat wel onder de werking van de richtlijn valt, terwijl een nagenoeg identieke aanbieder (dezelfde sector, met een soortgelijke dienstverlening, werkzaam in een soortgelijke context) uit een andere lidstaat niet onder de werking van de richtlijn valt. Ook bestaan er aanzienlijke verschillen ten aanzien van de uitvoering van de verplichtingen op nationaal niveau, zoals het soort cyberbeveiligingseisen en de mate van gedetailleerdheid, en het toezicht op de naleving van de verplichtingen die uit de richtlijn volgen. Deze verschillen kunnen nadelige effecten hebben op de werking van de interne markt en kunnen sommige lidstaten meer kwetsbaar maken voor cyberdreigingen, met mogelijke overloopeffecten in de hele Europese Unie. Daarom wordt de NIS1-richtlijn ingetrokken en vervangen door de NIS2-richtlijn. Daarmee wordt beoogd om de hiervoor benoemde verschillen weg te nemen. De NIS2-richtlijn heeft tot doel om een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie te bereiken, teneinde de werking van de interne markt te verbeteren. Deze richtlijn beoogt dit doel te bereiken door de verschillen weg te nemen die tussen lidstaten bestaan op het gebied van de cyberbeveiligingseisen die worden gesteld aan entiteiten die economisch belangrijke activiteiten of diensten verrichten. De richtlijn tracht dit doel te bereiken door onder meer regels vast te stellen over entiteiten die van rechtswege, zonder tussenkomst van een lidstaat, onder het toepassingsbereik van de richtlijn komen te vallen, en door te voorzien in doeltreffende voorzieningen ten aanzien van de cyberbeveiligingseisen waar entiteiten aan moeten voldoen en het toezicht op de naleving van de verplichtingen die voortvloeien uit de richtlijn.4 De NIS2-richtlijn gaat uit van minimumharmonisatie. De richtlijn belet de lidstaten daarom niet om bepalingen vast te stellen of te handhaven die een hoger cyberbeveiligingsniveau waarborgen, mits dergelijke bepalingen stroken met de in het Unierecht vastgelegde verplichtingen van de lidstaten.
Verantwoordelijk afdelingshoofd	[redacted]

1 Handhaafbaarheid

Het aspect handhaafbaarheid richt zich op de vraag of de wetgeving voldoende handvatten biedt om te kunnen handhaven op de normen die in de wetgeving zijn opgenomen. Dit aspect wordt vanuit drie invalshoeken beoordeeld: de wetgeving

zelf, de naleving door de Normadressaat en de handhaving door de toezichthouder(s).

1.1 Wetgeving

1. Is de regeling duidelijk en specifiek geformuleerd?	Ja. De regelging is duidelijk en specifiek geformuleerd aanzien van handhaafbaarheid. Er wordt onderscheid gemaakt in Essentiële en Belangrijke entiteiten waarbij voor beiden specifieke voorschriften duidelijk en specifiek zijn geformuleerd en opgenomen.
2. Zijn de begripsomschrijvingen duidelijk en specifiek geformuleerd en in overeenstemming met begripsomschrijvingen in gerelateerde regelgeving?	Ja. De Europese Commissie heeft, als onderdeel van de Digital Decade, een aantal verordeningen en richtlijnen opgesteld, waarvan de Cbw een uitwerking is van de NIS2 als één van deze in samenhang opgestelde Europese standaarden, formats en aanvullende wetgeving op het gebied van digitalisering. De hierin opgenomen termen zijn voor ingewijden duidelijk. In de NIS2 is ook een directe link aangebracht tussen de NIS2 en de Cybersecurity Act (CSA). Er kan een verplichting worden opgelegd aan NIS2 entiteiten om CSA gecertificeerde producten en diensten te gebruiken. Daarnaast gaan verschillende CSA gecertificeerde entiteiten ook onder de NIS2 vallen. Ook de Cyber Resilience Act (CRA) legt een nadrukkelijke link met de NIS2 via producten, ingedeeld in risicoklassen, die door NIS2-entiteiten worden gebruikt. Artikel 5 van de NIS2-richtlijn biedt lidstaten de ruimte om bepalingen vast te stellen die een hoger cyberbeveiligingsniveau waarborgen. In de AMvB wordt naar verwachting gebruik gemaakt van deze ruimte uit de richtlijn om maatregelen vast te stellen die een hoger cyberbeveiligingsniveau waarborgen. Daarnaast biedt deze delegatiegrondslag ook de mogelijkheid om aan essentiële en belangrijke entiteiten op te leggen dat zij bepaalde ICT-producten, ICT-diensten en ICT-processen gebruiken die zijn gecertificeerd op grond van artikel 49 van de Cyberbeveiligingsverordening (EU) 2019/881 (Cybersecurity Act (CSA)). Dit ter implementatie van artikel 24, eerste lid van NIS2. In de AMvB wordt voorzien in een delegatiegrondslag om bij ministeriële regeling van de vakminister sectorspecifieke regels te kunnen stellen over de te nemen maatregelen in het kader van de zorgplicht. De IenW sectoren waarvoor de Cbw gaat gelden kennen daarnaast ook hun eigen sectorspecifieke wetgeving. In artikel 4 NIS2-richtlijn is bepaald dat als sectorspecifieke rechtshandelingen van de EU voorschrijven dat essentiële entiteiten of belangrijke entiteiten risicobeheersmaatregelen op het gebied van cyberbeveiliging moeten nemen of significante incidenten moeten melden, en als deze eisen ten minste gelijkwaardig zijn aan de in de NIS2-richtlijn vastgestelde verplichtingen, de relevante bepalingen van de NIS2-richtlijn dan niet van toepassing zijn op die entiteiten. Meer concreet gaat het hierbij om de zorgplicht en de meldplicht. De andere bepalingen uit dit wetsvoorstel zijn dus wel van toepassing op die entiteiten. Artikel 4 NIS2-richtlijn is geïmplementeerd in de artikelen 24 en 33 van dit wetsvoorstel. Op dit moment zijn deze sectorspecifieke bepalingen voor de IenW sectoren, echter nog niet zover ontwikkeld dat hier een lex specialis voor zou gelden. Welke bepalingen er in sectorspecifieke regelgeving (denk aan bijvoorbeeld PART-IS voor de luchtvaart of ISPS voor de Havenbeveiligingswet en de Scheepvaartverkeersbegeleiding) wel overeenkomen met bepalingen die voortvloeien uit de zorgplicht en/of meldplicht van de Cbw dienen deze in samenwerking met toezichthouders die op deze bepalingen toezicht uitvoeren te worden afgestemd.

	Voor een leek zijn er wel veel termen die door elkaar worden gebruikt, Vitaal/Kritiek (Wet Wwke) en Essentieel en Belangrijk onder de Cbw. Voor een leek is dat geen begrijpelijke taal (richtlijn 2019/882EU). Als een toezichthouder dit naar normadressaten moet verwoorden kan onduidelijkheid ontstaan. De begripsbepalingen zijn echter in de Wet duidelijk omschreven.
3. Zijn de normen waar het in de regeling om gaat duidelijk?	De normen waarop het toezicht zich zal gaan richten zijn duidelijk omschreven. In artikel 23 wordt de zorgplicht omschreven waarbij in lid 4 van dit artikel is opgenomen dat bij of krachtens algemene maatregel van bestuur regels worden gesteld over de in het eerste lid bedoelde maatregelen, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren en type entiteiten. Hiermee wordt de handhaafbaarheid van het wetsvoorstel deels afhankelijk van het nog op te stellen besluit en de daarin op te nemen sectorspecifieke regels over de te nemen maatregelen in het kader van de zorgplicht. De nog op te stellen AMvB zal echter ook voor een HUF-toets aan de ILT worden voorgelegd waarmee dan ook de nadere uitwerking van de zorgplicht is geborgd. Verdere uitwerking van de zorgplicht in de AMvB en eventueel de Ministeriele regeling is ook noodzakelijk om in lijn te blijven met EU en andere lidstaten. Zo is in de internetconsultatie al opgemerkt dat de zorgplicht per lidstaat anders wordt ingevuld waardoor verschillen in bijvoorbeeld de uitwerking van een risico gebaseerde aanpak dreigen. Het verdient aanbeveling om daar waar mogelijk zoveel mogelijk aansluiting te zoeken bij standaarden die door bijvoorbeeld ENISA zijn ontwikkeld. In hoofdstuk 9 is de meldplicht van significante incidenten, incidenten, bijna-incidenten, significante cyberdreigingen, cyberdreigingen en kwetsbaarheden opgenomen. (Artikel 27 meldplicht significante incidenten). Indien significante incidenten niet worden gemeld conform de voorgeschreven wijze, staat het instrumentarium van Toezicht en Handhaving zoals omschreven in hoofdstuk 16 ter beschikking.
4. Zijn de verantwoordelijkheden en bevoegdheden duidelijk vastgelegd?	In de motie van toelichting is het verschil in duiding bevoegd gezag duidelijk uitgewerkt. In de Cbw is in artikel 16 tevens opgenomen waarvoor Onze Minister bevoegd gezag is. In combinatie met Mandaat en Aanwijzing voor de ILT als toezichthouder is hierdoor de scope van het toezicht duidelijk. De bevoegde autoriteit heeft daarmee de volgende taken: a. Het zorgen voor de bestuursrechtelijke handhaving van het bepaalde bij of krachtens deze wet door essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen; en b. De overige in deze wet genoemde taken. Het toe te passen instrumentarium voor Toezicht en Handhaving is in Hoofdstuk 16 van de Cbw duidelijk omschreven en vastgelegd.

1.2 Naleving door Normadressaat

1. Is duidelijk tot wie de norm is gericht? (Normadressaat), is de doelgroep duidelijk afgebakend?	De normadressaten voor wie de gegeven normen gelden worden per sector aangeduid. In de Cbw is in artikel 16 opgenomen waarvoor Onze Minister de bevoegde autoriteit is voor de entiteiten in de sectoren en subsectoren, genoemd in bijlage 1 en bijlage 2 van deze wet. Dit is duidelijk omschreven. Volgens artikel 22 (nationaal register van entiteiten) lid 1, beheert de Minister (JenV) een nationaal register van entiteiten die bij of krachtens

	deze wet essentiële entiteit of belangrijke entiteit zijn of als zodanig zijn aangewezen, en van entiteiten die domeinnaamregistratiediensten verlenen. In artikel 45 van dit wetsvoorstel is opgenomen welke informatie entiteiten moeten aanleveren bij de Minister van Justitie en Veiligheid ten behoeve van dat register. De delegatiegrondslag in artikel 45, eerste lid, onderdeel e, van dit wetsvoorstel biedt de mogelijkheid om de opsomming van de verplicht te verstrekken informatie uit te breiden, bijvoorbeeld als in de toekomst blijkt dat er meer informatie nodig is om de taken uit de wet goed uit te kunnen voeren. Dit geeft vertrouwen voor aanvullingen op de Handhaafbaarheid in de toekomst. In artikel 45 is weliswaar de verplichting opgenomen voor een essentiële of belangrijke entiteit en een entiteit die domeinnaamregistratiediensten verleent om ten behoeve van het in artikel 22 bedoelde nationale register informatie aan te leveren, dat wil nog niet automatisch zeggen dat deze entiteiten zich ook daadwerkelijk of correct zullen registeren middels het daarvoor opgezette mechanisme. Als de entiteit dat vervolgens niet doet of zichzelf in een verkeerde categorie indeelt kan deze langere tijd uit het zicht blijven van het toezicht op de werking van de Cbw. Dit is een gevoelig punt. In artikel 26 staan Governance verplichtingen voor het bestuur. Het is niet duidelijk wie daarmee wordt bedoeld. Gaat het om commissarissen, algemeen- of dagelijks bestuur? En wat als bestuur de verplichtingen niet navolgt? Is dan de entiteit of de bestuurder in overtreding? Dit dient nader te worden uitgewerkt.
2. Is de norm uitvoerbaar (haalbaar/realistisch) voor de Normadressaat?	Ja. Op grond van dit wetsvoorstel moeten essentiële entiteiten en belangrijke entiteiten, zich registeren, dient deze ieder significant incident te melden overeenkomstig de artikelen 28 tot en met 31 en conform artikel 23 passende en evenredige technische, operationele en organisatorische maatregelen te nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen te beheersen. Afhankelijk van de in te schatten risico's en/of de grote van de normadressaat, kan het basisniveau van de veiligheidseisen in evenredigheid verschillen waardoor de uitvoerbaarheid haalbaar en realistisch is op elk schaalniveau.
3. Is duidelijk hoe de norm moet worden nageleefd?	Ja. In artikel 23 wordt de zorgplicht omschreven. Lid 1: Iedere essentiële entiteit en belangrijke entiteit neemt passende en evenredige technische, operationele en organisatorische maatregelen om de risico's voor de beveiliging van de netwerk- en informatiesystemen, die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruikt, te beheersen. Ook neemt zij deze maatregelen om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van haar diensten en voor andere diensten te beperken. Lid2: De in het eerste lid bedoelde maatregelen zorgen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de in het eerste lid bedoelde risico's. Bij het nemen van de maatregelen houdt de entiteit in ieder geval rekening met de stand van de techniek, de uitvoeringskosten en, indien van toepassing, de desbetreffende Europese en internationale normen. Ten aanzien van de evenredigheid van de in het eerste lid bedoelde maatregelen houdt de entiteit naar behoren rekening met de mate waarin zij aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met

	inbegrip van de maatschappelijke en economische gevolgen. De norm is daarmee op hoofdlijnen beschreven en geeft de normadressaat veel ruimte om dit op zijn eigen wijze in te vullen. Lid 3 vermeld dat de in het eerste lid bedoelde maatregelen zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen. Waarbij in lid 4 van dit artikel is opgenomen dat bij of krachtens algemene maatregel van bestuur regels worden gesteld over de in het eerste lid bedoelde maatregelen, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren en type entiteiten. Hoe de norm vervolgens moet worden nageleefd is daarmee deels afhankelijk van het nog op te stellen besluit en de daarin op te nemen sectorspecifieke regels over de te nemen maatregelen in het kader van de zorgplicht.
4. Is overschrijding van de norm eenvoudig en eenduidig door de Normadressaat vast te stellen?	Op hoofdlijnen. De regels gesteld bij of krachtens algemene maatregel van bestuur over de in het eerste lid bedoelde maatregelen zal hier meer duiding aan geven.
5. Zijn de lasten voor de Normadressaat duidelijk?	De lasten kunnen verschillen per normadressaat en sector. Afhankelijk van de in te schatten risico's en/of de grote van de normadressaat, kan het basisniveau van de veiligheidseisen en daaraan gekoppelde lasten in evenredigheid verschillen.
6. Zijn er ontwijkingsmogelijkheden voor de naleving van de norm?	Ja en nee. In artikel 45 is de verplichting opgenomen voor een essentiële of belangrijke entiteit en een entiteit die domeinnaamregistratiediensten verleent om ten behoeve van het in artikel 22 bedoelde nationale register informatie aan te leveren. Dat wil nog niet automatisch zeggen dat deze entiteiten zich ook daadwerkelijk of correct zullen registeren middels het daarvoor opgezette mechanisme. Als de entiteit dat vervolgens niet doet of zichzelf in een verkeerde categorie indeelt kan deze langere tijd uit het zicht blijven van het toezicht op de werking van de Cbw. Dit is een gevoelig punt. Ook is hier niet geregeld dat als een onderneming kleiner wordt dat hij zich weer moet uitschrijven. Verder is niet duidelijk of- en hoe je kunt optreden als hij zich onvolledig of onjuist registreert. Dit moet in de AMvB worden opgenomen. Indien de normadressaat zich conformeert en correct registreert zijn er daarna in principe geen ontwijkingsmogelijkheden voor de naleving van de gestelde normen.

1.3 Handhaving door de toezichthouder

1. Is duidelijk welke organisaties de ontwerp-regelgeving zullen uitvoeren/handhaven?	Zie hiervoor ook punt 1.1 onder 4. Er doet zich wel een onduidelijkheid voor indien er sprake is van overlap en een normadressaat onder verschillende sectoren valt. De normadressaat kan dan onder verschillende Ministers en daarmee toezichthouders vallen. In de Wet wordt geen primaat toegekend voor bijvoorbeeld het toezicht in een onderverdeling in prioritaire sectoren. Dat betekent dat in voorkomende gevallen er nadere samenwerkingsafspraken dienen te worden gemaakt tussen de onderlinge toezichthouders en Ministeries. Bijvoorbeeld bij het toezicht op bedrijven die eerder onder het Besluit Risico's Zware Ongevallen (BRZO) vallen en nu als SEVESO-inrichting onder de nieuwe Omgevingswet, is de Provincie het bevoegd gezag. De samenwerking met de zes Omgevingsdiensten, die met het toezicht hierop namens de provincies zijn belast, willen de ILT zo veel

	mogelijk langs bestaande lijnen inregelen. Hiervoor zijn inmiddels de eerste contacten gelegd. De intentie is om als ITL aan te sluiten bij het bestaande BRZO+-overleg.
2. Is de norm uitvoerbaar/handhaafbaar?	Ja. De ILT is op dit moment één van de toezichthouders voor de Wbni en wel voor de sectoren vervoer en drinkwater. De ILT zal voor deze sectoren ook de toezichthouder worden voor de Cyberbeveiligingswet. De sectoren Openbaar vervoer, Chemie, Afvalstoffenbeheer en Afvalwater worden ingevolgde de Cbw aan het toezicht toegevoegd. Op grond van het voorstel voor de Wet Wke aangewezen kritieke entiteiten, zijn ook essentiële entiteiten als bedoeld in het onderhavige wetsvoorstel. Gelet daarop is het ten eerste relevant dat in de Wet Wke ook de subsector openbaar vervoer is opgenomen, met onze minister als bevoegde autoriteit. Ten tweede is relevant dat het voornemen bestaat om op basis van artikel 7a, Wet Wke, het reeds vitale proces keren en beheren waterkwantiteit en grootschalige vervaardiging, productie en distributie, (in het verzoek aangehaald als: productie, verwerking en/of opslag) (petro)chemische stoffen aan te wijzen als sector onder deze wetgeving waardoor deze ook onder de werking van de Cbw komen te vallen als Essentieel. Essentiële entiteiten komen in de Cyberbeveiligingswet onder proactief toezicht te vallen. Dit wil zeggen dat er risicogericht toezicht gehouden wordt op het naleven van de verplichtingen, ook wanneer er geen sprake is van eventuele incidenten. Voor belangrijke entiteiten geldt dat toezicht achteraf plaatsvindt, bijvoorbeeld als er signalen zijn voor het niet naleven van de wet, of als er een incident heeft plaatsgevonden. Zowel belangrijke als essentiële aanbieders krijgen te maken met een zorgplicht, meldplicht, registratieplicht en toezicht. In de Cbw is sprake van ‘open normen’. Dat wil zeggen dat de wet wel het doel voorschrijft, maar niet hoe een bedrijf dat doel moet bereiken. Bij een algemene maatregel van bestuur dienen dan ook regels te worden gesteld over de bedoelde maatregelen, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren en type entiteiten. Hiermee wordt de handhaafbaarheid van het wetsvoorstel deels afhankelijk van het nog op te stellen besluit en de daarin op te nemen sectorspecifieke regels over de te nemen maatregelen in het kader van de zorgplicht. De handhaafbaarheid hangt tevens samen met een forse toename in het aantal toezichthouders. Dit punt wordt verder uitgewerkt bij het hoofdstuk Uitvoerbaarheid van deze HUF-toets.
3. Is overschrijding van de norm eenvoudig en eenduidig door de toezichthouder(s) vast te stellen?	Ja. Discussie kan tot het minimum worden beperkt door uitwerking in voornoemde algemene maatregel van bestuur van de te nemen maatregelen in het kader van de zorgplicht. De norm dient vervolgens verder te worden gespecificeerd in de Ministeriële Regeling en het ILT-toezichtskader.
4. Is duidelijk hoe de handhaving van de norm moet plaatsvinden? Beschikt de toezichthouder over een toereikend instrumentarium (binnen het Interventiekader) om te kunnen handhaven?	Ja. De ILT is op dit moment een van de toezichthouders voor de Wbni en zal voor de diverse sectoren ook toezichthouder worden voor de Cyberbeveiligingswet. Essentiële entiteiten komen in de Cyberbeveiligingswet onder proactief toezicht te vallen. Het toe te passen instrumentarium voor Toezicht en Handhaving is in Hoofdstuk 16 van de Cbw duidelijk omschreven en vastgelegd. Het toezicht zelf wordt uitgevoerd met gebruikmaking van de Awb. Het risico-gestuurd toezicht door de ILT als onafhankelijke toezichthouder zal zoveel mogelijk aansluiten bij de bestaande Wbni-systematiek en

	bestaande bevoegdheden en instrumenten van sectorale toezichthouders om waar mogelijk de samenhang te van de diverse sectorale wetgevingsverplichtingen te stroomlijnen met het toezicht van de Cbw en de Wet Wke. Daarbij is het streven om stapelingen van toezicht te voorkomen. Een aandachtspunt is de verplichte audit vermeld onder artikel 70 (gerichte beveiligingsaudit) en artikel 70a (ad hoc beveiligingsaudit). Deze artikelen zijn niet in lijn met de NIS2 en kennen veel overlap. Zoals in artikel 70a staat geformuleerd kan een verplichte audit alleen plaatsvinden na aanleiding (incident o.i.d.) in de NIS2 staan hiervoor geen voorwaarden. Beide artikelen overlappen elkaar nu deels terwijl in artikel 70 de kosten voor de entiteit zijn en in artikel 70a dit niet staat vermeld waardoor onduidelijkheid kan ontstaan over de kosten.
5a. Over welke persoonsgegevens moet de ILT kunnen beschikken en moet de ILT vastleggen? 5b. Voorziet de wetgeving in de bevoegdheid deze gegevens uit te wisselen en/of vast te leggen? Denk bijvoorbeeld aan de Algemene Verordening Gegevensbescherming (AVG)	De normadressaten voor wie de gegeven normen gelden worden per sector aangeduid. In de Cbw is in artikel 16 opgenomen waarvoor Onze Minister de bevoegde autoriteit is voor de entiteiten in de sectoren en sub sectoren, genoemd in bijlage 1 en bijlage 2 van deze wet. Dit is duidelijk omschreven. Volgens artikel 22 (nationaal register van entiteiten) lid 1, beheert de Minister (JenV) een nationaal register van entiteiten die bij of krachtens deze wet essentiële entiteit of belangrijke entiteit zijn of als zodanig zijn aangewezen, en van entiteiten die domeinnaamregistratiediensten verlenen. In artikel 45 van dit wetsvoorstel is opgenomen welke informatie entiteiten moeten aanleveren bij de Minister van Justitie en Veiligheid ten behoeve van dat register. Op dit moment gaat het om a. De naam van de entiteit; b. Het adres en de actuele contactgegevens van de entiteit, met inbegrip van e-mailadressen, IP-bereiken en telefoonnummers; c. Indien van toepassing, de sectoren en subsectoren, bedoeld in bijlage 1 of 2 van deze wet, waartoe de entiteit behoort; d. Indien van toepassing, een vermelding van de lidstaten van de Europese Unie waar de entiteit zijn diensten als bedoeld in bijlage 1 of bijlage 2 van deze wet verleent; en e. e. indien van toepassing, de andere bij of krachtens algemene maatregel van bestuur genoemde gegevens. De delegatiegrondslag in artikel 45, eerste lid, onderdeel e, van dit wetsvoorstel biedt de mogelijkheid om de opsomming van de verplicht te verstrekken informatie uit te breiden, bijvoorbeeld als in de toekomst blijkt dat er meer informatie nodig is om de taken uit de wet goed uit te kunnen voeren. 5b. Conform artikel 52 is er een grond voor samenwerking en informatie-uitwisseling tussen de betrokken instanties. 1. De bevoegde autoriteiten, de CSIRT's en het centrale contactpunt werken met elkaar samen voor de doeltreffende en doelmatige uitvoering van hun taken uit hoofde van deze wet en wisselen daartoe onderling alle daarvoor benodigde gegevens uit, waaronder persoonsgegevens. 2. De bevoegde autoriteit, het CSIRT en het centrale contactpunt werken voor de doeltreffende en doelmatige uitvoering van hun taken uit hoofde van deze wet samen met de volgende instanties

	in Nederland en wisselen daartoe onderling alle daarvoor benodigde gegevens uit, waaronder persoonsgegevens: a. De bij of krachtens algemene maatregel van bestuur aangewezen rechtshandhavingsautoriteiten; b. De Autoriteit persoonsgegevens; c. De nationale bevoegde autoriteiten als bedoeld in de Verordening (EG) nr. 300/2008 en Verordening (EU) 2018/1139; d. Onze Minister van Economische Zaken en Klimaat uit hoofde van Verordening (EU) nr. 910/2014 e. De bevoegde autoriteiten uit hoofde van Verordening (EU) 2022/2554; f. Onze Minister van Economische Zaken en Klimaat uit hoofde van Richtlijn (EU) 2018/1972; g. De bevoegde autoriteiten, bedoeld in artikel 8 van de Wet weerbaarheid kritieke entiteiten; h. De bij of krachtens algemene maatregel van bestuur aangewezen bevoegde autoriteiten uit hoofde van andere sectorspecifieke rechtshandelingen van de Europese Unie. Voor de AVG geldt het zogenaamde doelbindingsbeginsel. De WOO Artikel 65, derde lid, kent een bijzondere openbaarheidsregeling voor vertrouwelijke gegevens. De bijzondere regeling geldt niet alleen zolang die gegevens bij de in het eerste en tweede lid genoemde overheidsinstanties berusten, maar ook nadat zij zijn verstrekt. De Wbni kende in relatie tot de Woo eenzelfde bijzondere openbaarmakingsregeling. Daardoor vallen onder andere incidentgegevens en ten behoeve van het toezicht verkregen onderzoeksgegevens volledig onder de uitzondering en hoeven zij dus niet openbaar te worden gemaakt.
6. Is de ingangsdatum van de regeling zodanig vastgesteld dat de voorbereidingstijd voor handhavende organisaties voldoende is?	De ingangsdatum van de Cbw is nog niet duidelijk maar zal pas in 2025 plaatsvinden. De ILT heeft zich met een zogenaamd ingroeipad voorbereid op de ingang van deze wet en is derhalve tijdig voorbereid op de uitvoering.

Conclusie handhaafbaarheid: Samenvattend	De regelgeving is helder geformuleerd voor handhaafbaarheid en maakt onderscheid tussen Essentiële en Belangrijke entiteiten met specifieke voorschriften. De Cyberbeveiligingswet (Cbw) is een uitwerking van de NIS2-richtlijn, onderdeel van de Europese Digital Decade, en heeft een directe link met de Cybersecurity Act (CSA) en Cyber Resilience Act (CRA). De Cbw bevat regels voor de zorgplicht en meldplicht van significante incidenten, met een gedelegeerde bevoegdheid voor sectorspecifieke regels via een algemene maatregel van bestuur (AMvB). De Minister van Justitie en Veiligheid beheert een nationaal register van entiteiten die onder deze wet vallen, waarbij essentiële en belangrijke entiteiten verplicht zijn zich te registreren en informatie aan te leveren. Handhaving en toezicht zal worden uitgevoerd door de Inspectie Leefomgeving en Transport (ILT), die proactief toezicht houdt op essentiële entiteiten en reactief op belangrijke entiteiten. Een risico-gestuurd toezichtkader en samenwerkingsafspraken moet worden opgesteld tussen de

	verschillende toezichthouders. Het is echter ook aan de ministeries om met elkaar in overleg te treden om de overlap van sectoren te bespreken. Bij het toezicht op bedrijven die nu eerder onder het Besluit Risico's Zware Ongevallen (BRZO) vallen en nu als SEVESO-inrichting onder de nieuwe Omgevingswet, is de Provincie het bevoegd gezag. De samenwerking met de zes Omgevingsdiensten die hiermee namens de provincies zijn belast, willen we zo veel mogelijk langs bestaande lijnen inregelen. De regelgeving moet nog verder worden uitgewerkt in een aanvullend besluit en een ministeriële regeling. De ingangsdatum van de Cbw is gepland voor 2025, daarmee is voldoende tijd voor de te maken voorbereidingen door de ILT om de wetgeving effectief te implementeren en daarna te handhaven. Een aandachtspunt is de verplichte registratie. Hoewel artikel 45 essentiële en belangrijke entiteiten verplicht om informatie aan te leveren voor het nationale register, betekent dit niet automatisch dat deze entiteiten zich correct zullen registreren. Als ze dit niet doen of zich verkeerd categoriseren, kunnen ze theoretisch langere tijd buiten het toezicht van de Cyberbeveiligingswet (Cbw) blijven.

2 Uitvoerbaarheid

De uitvoerbaarheid van beleid of van wet- en regelgeving behelst de vraag of het *toezicht* praktisch uitvoerbaar is. Dit betekent dat de ILT duidelijk en concreet moet hebben op welke wijze de ILT-invulling kan geven aan die nieuwe of gewijzigde taak. N.B. Hier wordt dus niet gedoeld op de uitvoerbaarheid door de Normadressaat; deze wordt beoordeeld onder 1.2.2.

1. Vindt er met de Normadressaat toereikende communicatie plaats over de nieuwe wet- en regelgeving? Moet de ILT aanvullende communicatie inzetten om de Normadressaat te bereiken over de handhaving van de wet- en regelgeving?	Ja de programma's van beleid/DG's per sector en vanuit de regie JenV/NCSC/DTC/NCTV ontvangt de normadressaat toereikende communicatie over de nieuwe wet- en regelgeving. Dit is voldoende mits overdracht vanuit het Ministerie op de juiste wijze aan de toezichthouder plaatsvindt en over deze overdracht ook wordt gecommuniceerd aan de normadressaat. Aanvullend wordt door de ILT ook gecommuniceerd op onze website en geven wij presentaties over de nieuwe wetgeving op symposia van de diverse sectoren om hen voor de Cbw voor te bereiden.
2. Leidt de nieuwe wet- en regelgeving tot veranderingen in de organisatorische inrichting van de ILT? Denk hierbij niet alleen aan het 'harkje', maar ook aan verantwoordelijkheden en bevoegdheden, takenpakket en bemensing van afdelingen.	De ILT is op dit moment een van de toezichthouders voor de Wbni en zal voor de diverse sectoren ook toezichthouder worden voor de Cyberbeveiligingswet. Per 1 Oktober 2022 is de huidige afdeling van programma naar reguliere lijn activiteit omgevormd naar 1 van de 6 afdelingen van Toezicht en Opsporing. De implementatie van de Cbw betekend een groei met ca. 46 Fte in 5 jaar. De Cbw betekend voor de ILT een forse uitbreiding in het aantal sectoren en het aantal entiteiten. De entiteiten vallen automatisch onder de Cbw. Het toezicht gaat met deze wet van ca 36 entiteiten naar ca 1852. Voor de uitvoerbaarheid is dan ook een groei in het aantal toezichthouders en de benodigde middelen voorzien. Buiten de afdeling kan dit echter ook voor extra afstemmingsbehoefte leiden met andere toezichthouders op sectorale wetgeving. Deze afstemmingsbehoefte komt dan ook deels voor andere sectorspecifieke afdelingen binnen de ILT maar ook daarbuiten.

3. Heeft de nieuwe wet- en regelgeving gevolgen voor de personele bezetting, zowel in kwantitatief en kwalitatief opzicht? Welke kennis en vaardigheden zijn benodigd en hoe moet hierin worden voorzien (werving nieuwe medewerkers, opleiden bestaande medewerkers, verplaatsing bestaande medewerkers)? Moeten er tijdelijk medewerkers worden ingehuurd om aanloopproblemen te ondervangen?	Om het toezicht met de juiste kwaliteitsmaatstaven op te kunnen zetten, is een uitbreiding van het toezicht nodig. Het aantal aanbieders waar toezicht op zal moeten worden gehouden zal fors toenemen, wat zorgt voor een noodzaak voor aanvullende toezicht capaciteit. IenW gaat uit van een noodzaak tot toezicht op 1852 aanbieders. Het proactieve toezicht op essentiële entiteiten is risico-gestuurd op basis van beschikbare informatie. Hierbij wordt uitgegaan dat een koppel inspecteurs in een jaar 20 aanbieders kan inspecteren. Het voornemen is om iedere aanbieder waar ex ante toezicht noodzakelijk is eenmaal per 3 jaar te inspecteren. Het voornemen is tevens om op basis van meldingen en incidenten bij ongeveer de helft van de aanbieders ex post te inspecteren. Deze toezicht ambitie leidt tot een behoefte aan 36 fte aan inspecteurs, uitgerust met de noodzakelijke specialistische apparatuur, en teamleiders. Daarnaast geldt een groeiend capaciteitsbeslag in de vorm van analisten, juristen en ondersteuning van 10 fte. De groei van totaal 46 fte wordt realistisch en inpasbaar geacht. Het gaat hier voornamelijk om het aantrekken van nieuwe medewerkers met specifieke competenties voor het uitvoeren van het toezicht op de Cbw. De ILT heeft ingestemd met een ingroeipad voor NIS-2 van 20% in 2025, oplopend naar 100% vanaf 2029. Het hiervoor toegekende budget betreft vanaf 2029 een structurele toezegging van € 7.585.400, = voor de uitvoering van het toezicht op de Cbw.
4. Heeft de nieuwe wet- en regelgeving gevolgen voor de procesinrichting binnen de ILT? Passen de nieuwe taken binnen de bestaande uniforme kaders of moeten deze worden aangepast/uitgebreid? Moeten er aanvullende werkinstructies worden opgesteld? Moeten bestaande kwaliteitsmanagementsystemen worden aangepast?	De afdeling toezicht cybersecurity is al ingebed in de huidige organisatie. (Zie hier ook punt 2.2) Wat nog verder moet worden opgepakt is de afstemming binnen sectoren met de andere toezichthouders om een samenwerking op te zetten t.b.v. efficiëntie en het voorkomen van extra toezichtlast voor de normadressaten. Kaders die nu bestaan moet worden aangepast c.q. uitgebreid. Onder andere het Wbni toezichtskader dient te worden aangepast en is voorzien.
5. De extra financiële lasten voor de ILT als gevolg van nieuwe taken moeten worden gedekt door tariefstelling derden (in geval van nieuwe taken op het gebied van vergunningverlening) en/of een hogere agentschapsbijdrage (in het geval van toezicht, of in het geval van vergunningverlening waar de tariefopbrengst niet dekkend zal zijn (art. 24 Hoofdstuk XII Rijksbegroting). De investeringen die de ILT moet doen om de	De Cbw voorziet niet in vergunningverlening maar wel in toezicht en handhaving. Voor het uitvoeren van het toezicht op de Cbw heeft de ILT ingestemd met een ingroeipad voor budget van 20% in 2025, oplopend naar 100% vanaf 2029. Het hiervoor toegekende budget betreft op termijn een structurele toezegging van € 7.585.400, = voor de uitvoering van het toezicht op de Cbw.

nieuwe taken te kunnen uitvoeren moeten in kaart zijn gebracht en er moet een waarborg zijn dat deze lasten voldoende gewaarborgd zijn. Daarbij moet met name worden gedacht aan:		
5.a	Personele kosten (incidenteel/structureel)	De toezichtsambitie vereist een behoefte van 36 fte voor inspecteurs (uitgerust met de noodzakelijke specialistische apparatuur) en teamleiders. Daarnaast is er een toenemende behoefte aan capaciteit voor analisten, juristen en ondersteunend personeel, wat neerkomt op 10 fte. De groei van totaal 46 fte wordt realistisch en inpasbaar geacht. Het hiervoor toegekende budget betreft vanaf 2029 een structurele toezegging van € 7.585.400, = voor de uitvoering van het toezicht op de Cbw. De kosten voor een FTE bedragen €164.900 en omvatten salariskosten, overhead (€ 141.600, --, bron: HAFIR 2022) en bijkomende kosten vanwege de Dep V en expertise/certificering, zoals opleiding, certificering, screening, huisvesting, IT en communicatie (€ 23.300, --).
5.b	Kosten van eventuele aanvullende bedrijfsmiddelen (meetapparatuur e.d.) (structureel)	Zie boven
5.c	Kosten van aanpassingen aan bestaande/ investeringen in nieuwe informatiesystemen (incidenteel (ontwikkeling)/structureel (beheer)	Zie boven
5.d	Kosten van implementatie (bijvoorbeeld communicatie) (incidenteel)	Zie boven
5.e	Kosten van huisvesting, voor zover niet opgenomen in de vaste FTE-opslag (incidenteel, bijvoorbeeld verhuiskosten of specifieke aanpassingen aan een pand)	Zie boven
6. Heeft de nieuwe wet- en regelgeving gevolgen voor de informatievoorziening? Denk hierbij aan:		De ILT is op dit moment een van de toezichthouders voor de Wbni en zal voor de diverse sectoren ook toezichthouder worden voor de Cyberbeveiligingswet. In de huidige informatieverwerking is met de bij de ILT gebruikelijke systemen voorzien. Met het oog op inwerkingtreding 2025 heeft de ILT een systeem nodig dat gekwalificeerde informatie kan beheren van ca 1852 entiteiten. In de nog beschikbare voorbereidingstijd zullen de nodige aanpassingen worden toegepast. De afdeling Data&Analyse is hierbij nodig voor:

			- Het ontsluiten van data (registratieportaal en evt. andere bron voor het risicoframework); - Het meedenken over de juiste vragen in dossiervorming t.b.v. toekomstig informatiebeeld; - Analyses op risico's, meldingen en dossiers.
6.a	Dient er over de uitvoering van de wet- en regelgeving te worden gerapporteerd en kunnen deze rapportages worden verzorgd door de bestaande informatiesystemen?		Uit de Cbw volgen voor de ILT op het moment geen rapportageverplichting. Bestaande en in te voeren systemen voor het toezicht in de toekomst, zullen naar alle waarschijnlijk wel in nog nader te definiëren rapportageverplichtingen kunnen voorzien.
6.b	Leiden aanpassingen aan de procesinrichting (zie 4) tot wijzigingen in bestaande informatiesystemen of de ontwikkeling/aanschaf van nieuwe informatiesystemen?		Ja en nee. In de huidige informatieverwerking is met de bij de ILT gebruikelijke systemen voorzien. In de nog beschikbare voorbereidingstijd zal ook de toepassing van een beveiligde omgeving voor geclassificeerde informatie nader worden verkend. Middelen zijn er maar moet nog worden omgezet in een plan en worden gerealiseerd. Hier punt Richard
6.c	Moeten er afspraken over de archivering van gegevens worden gemaakt?		Ja zie punt 6b
6.d	Gegevensuitwisseling tussen organisaties:		In de Cbw bestaan er voor de normadressaat verplichten voor het registreren, de zorgplicht en de meldplicht van significante incidenten. Een en ander wordt opgezet onder regie van de NCTV. Het meldt en registratieportaal is momenteel in ontwikkeling. Bij de kwalificaties van dit portaal heeft de ILT op dit moment inspraak. Meldingen gaan bijvoorbeeld via DCC en bestaande beleidsafpraken. Een verdere professionalisering van het registratie en meldproces is momenteel bezig. De uit te wisselen gegevens zijn duidelijk. Het is belangrijk om hier als ILT maar ook als beleidsdepartement goed bij aan te sluiten. Momenteel gebeurd de uitwisseling via mail. Een te ontwikkelen systeem met een convertor tussen NCTV en een systeem van de ILT is daarbij denkbaar. De NCSC bouwt het portaal, ILT moet ervoor zorgen dat die meldingen binnengehaald en verwerkt kunnen worden. Specificaties zijn nog onbekend, medio november volgt hierover meer nieuws.
		i Als uitvoering en toezicht bij meerdere organisaties is belegd, is dan voorzien in laagdrempelige gegevensuitwisseling tussen deze organisaties?	
		ii Als de Normadressaat gegevens moet leveren aan de uitvoeringsorganisatie of de handhavingsorganisatie, is dan voorzien in laagdrempelige gegevensuitwisseling?	
		iii Is duidelijk welke gegevens moeten worden uitgewisseld?	
		iv Zijn deze gegevens eenduidig gedefinieerd?	
		v Is duidelijk op welke wijze de gegevens moeten worden uitgewisseld?	

	vi	Voorziet de wetgeving in de bevoegdheid deze gegevens uit te wisselen en vast te leggen? Denk bijvoorbeeld aan de Algemene Verordening Gegevensbescherming (AVG)	Voor de AVG geldt het zogenaamde doelbindingsbeginsel. De WOO Artikel 65, derde lid, kent een bijzondere openbaarmakingsregeling voor vertrouwelijke gegevens. De bijzondere regeling geldt niet alleen zolang die gegevens bij de in het eerste en tweede lid genoemde overheidsinstanties berusten, maar ook nadat zij daarin verstrekt. De Wbni kende in relatie tot de Woo eenzelfde bijzondere openbaarmakingsregeling. Daardoor vallen onder andere incidentgegevens en ten behoeve van het toezicht verkregen onderzoeksgegevens volledig onder de uitzondering en hoeven zij dus niet openbaar te worden gemaakt. Artikel 59, tweede lid, van dit wetsvoorstel gaat over overtredingen van de zorgplicht en van de meldplicht die een inbreuk in verband met persoonsgegevens kunnen inhouden. Hierin is bepaald dat wanneer de bevoegde autoriteit bij toezicht of handhaving er kennis van krijgt dat een overtreding van de zorgplicht of van de meldplicht een inbreuk in verband met persoonsgegevens kan inhouden die op grond van artikel 33 AVG gemeld zou moeten worden, zij de bevoegde toezichthoudende autoriteiten als bedoeld in de artikelen 55 en 56 van de AVG onverwijld daarvan in kennis moet stellen.
7. Zijn de gevolgen van de nieuwe wet- en regelgeving voor de organisatiestructuur voldoende wettelijk verankerd in het Mandaatbesluit , mandaatregisters e.d. en zijn deze zaken tijdig met de Ondernemingsraad besproken?			Het mandaatbesluit moet nog worden opgesteld. Deze wordt gecoördineerd uitgevoerd door de gezamenlijke DG's. Bij het formuleren van het mandaatbesluit heeft de ILT ook inspraakmogelijkheden via bestaande overleggen. Indien noodzakelijk zal indien van toepassing ook de OR worden betrokken. Dit wordt tot op heden nog niet voorzien.
8. Zijn er aanvullende technische hulpmiddelen nodig om de nieuwe wet- en regelgeving te kunnen uitvoeren/handhaven? Denk hierbij aan meetapparatuur, beschermingsmiddelen, specifieke werkplek- en communicatieapparatuur, transportmiddelen.			Ja. Voor de uitvoering is specifieke kennis aar ook uitrusting noodzakelijk. Zie hiervoor vraag 5a.
9. Wat zijn de gevolgen van de nieuwe wet- en regelgeving voor de huisvesting van de ILT? Voldoen de bestaande locaties of zijn er uitbreidingen/verhuizingen nodig? Dienen er specifieke aanpassingen aan een gebouw te worden gemaakt om de nieuwe taken te kunnen uitvoeren?			Zie 5a.
10. Zijn er specifieke eisen op het gebied van beveiliging die voortvloeien uit de nieuwe taken? Denk hierbij aan de reeds genoemde aanpassingen aan			Zie 5a.

gebouwen maar ook aan aanvullende eisen op het gebied van autorisaties voor en versleuteling van informatiesystemen?	
11. Leidt de nieuwe wet- en regelgeving tot specifieke aandachtspunten op het gebied van integriteit?	Ja. Screening vereist hetgeen is geborgd. Zie 5a.
12. Zijn er eventuele andere aandachtspunten uit bijvoorbeeld het kabinetsbeleid, het Meerjarenplan ILT of de IBRA die door de nieuwe wet- en regelgeving worden geraakt? Denk bijvoorbeeld aan gevolgen voor de gezondheid, kans op ongelukken (fysieke schade) of economische en financiële gevolgen voor derden, waaronder voor burgers (niet zijde de normadressaat) en/of effecten op de leefomgeving/het milieu.	Ja. Betreft vitale infrastructuur. Niet naleven leidt onmiddellijk tot ernstige schade. Samenhang en afstemming met andere cyber gerelateerde wetgeving, maar ook met toezichthouders op sectorspecifieke regelgeving die wordt ontwikkeld is noodzakelijk en moet nader worden verkend. Met de geclassificeerde informatie moet omzichtig worden omgegaan waarbij afstemming met andere beleidsterreinen en toezichthouders is vereist.

Conclusie uitvoerbaarheid: Samenvattend, hoeveel extra fte en andere financiële middelen heeft de ILT nodig om het toezicht uit te kunnen voeren?	De implementatie van de Cbw vraagt om een uitbreiding van toezichtcapaciteit om de kwaliteitsmaatstaven te waarborgen. Het aantal sectoren neemt toe en daardoor ook het aantal entiteiten onder toezicht. Hierdoor is een toename van het aantal inspecteurs en middelen nodig, evenals extra afstemming met andere toezichthouders. In de huidige informatieverwerking is met de bij de ILT gebruikelijke systemen voorzien. Deze zijn echter gebaseerd op het relatief lage aantal entiteiten die onder de huidige Wbni vallen. Daarom moet de ILT een systeem ontwikkelen voor de verwerking van geclassificeerde informatie van circa 1800 entiteiten, passend binnen de bestaande systemen en nieuwe rapportageverplichtingen. Dit samen resulteert in een geschatte behoefte aan 36 fte inspecteurs en 10 fte aan ondersteunend personeel, met een totaal van 46 fte. De ingangsdatum van de Cbw is gepland voor 2025, daarmee is er tijd voor de te maken voorbereidingen om de wetgeving effectief te implementeren en daarna te handhaven. Echter moet er rekening worden gehouden met arbeidsmarktontwikkelingen als het gaat om gekwalificeerde inspecteurs. Er zijn dan ook een aantal risico's te benoemen, waarvan nu nog niet is te voorzien hoe deze zullen uitpakken maar die van invloed zullen zijn op de uitvoering van het toezicht. Denk daarbij aan: - Ex ante toezicht op kritieke entiteiten is in beginsel proactief en risico-gestuurd. Ex post toezicht op belangrijke entiteiten zal plaatsvinden als daar bijvoorbeeld als gevolg van incidenten reden voor is. Het aantal incidenten laat zich niet

	voorspellen, maar als dat veel groter is dan nu kan worden voorzien, zal dat een negatieve impact hebben op de beschikbare capaciteit voor het reguliere ex post toezicht; - Het aantal handhavingsverzoeken aan en van buitenlandse autoriteiten kan niet goed worden ingeschat; - De arbeidsmarkt voor medewerkers met expertise op dit voor ILT deels nieuwe vakgebied, maar ook voor bijvoorbeeld de benodigde IT-specialisten, is uiterst gespannen. Het is onzeker of de ILT tijdig de expertise en capaciteit daadwerkelijk kan werven; - Onzeker is de mate van naleving en de noodzaak tot sanctionering. De ervaring met verscherpt toezicht onder de Wbni leert dat dergelijke trajecten arbeidsintensief zijn, waardoor er minder tijd beschikbaar blijft voor reguliere inspecties; - Het aantal entiteiten dat onder de Cbw wordt aangewezen, kan in de toekomst nog wijzigen, evenals het toevoegen van andere vitale sectoren. Gelet op al deze en andere onzekerheden lijkt het wenselijk om twee jaar na inwerkingtreding van de Cbw een evaluatie te houden waarin aandacht wordt besteed aan genoemde implementatievraagstukken en risico's. Aan de hand van deze evaluatie kan nader bepaald worden in hoeverre de beschikbare middelen ook op langere termijn voldoende zijn.

3. Fraudebestendigheid

1. Zijn er partijen die (direct of indirect) gegevens verstrekken aan de overheid voor het nemen van een besluit, en die een financieel en/of economisch belang hebben bij het frauderen hiermee (denk ook aan intermediairs en onderlinge beïnvloeding door de partijen)? Zo ja, welke partijen?	Marktpartijen springen in op de opleidingsverplichtingen voor bestuur en op te zetten zogenaamde NIS2 certificatie. Deze zijn nog niet geaccrediteerd en daar is in de wetgeving van de Cbw ook nog niet in voorzien. De op te zetten AMvB gaat hier mogelijk in voorzien maar dat is nog niet duidelijk.
2. Zijn in de regeling maatregelen opgenomen om de fraude te voorkomen/bestrijden? Denk aan het instellen van meldpunten, het verplicht aanleveren van bewijsstukken, zoals certificaten, accountantsverklaringen, diploma's.	Het meldpunt is ingeregeld bij de NCTV/NCSC. Bij toezicht vindt verificatie plaats en reality- checks op inhoud en bewijsmateriaal.
3. Zijn voldoende effectieve sancties benoemd in de regeling of toelichting voor alle betrokken partijen (inclusief intermediairs en certificerende instellingen)?	Ja. Er zijn voldoende effectieve sancties benoemd in de regeling of toelichting voor alle betrokken partijen. Echter, voor de entiteiten die onder het toepassingsbereik van dit wetsvoorstel vallen geldt de verplichting uit artikel 5:20 Awb om alle medewerking te verlenen aan de toezichthouder. Voor het boetemaximum van een bestuurlijke boete voor een overtreding van deze verplichting is gekozen voor het

	bedrag van de tweede categorie, bedoeld in artikel 23, vierde lid, Wetboek van Strafrecht. In de praktijk betekent dit een boetemaximum van €5.000,-. Naar mijn oordeel is dit bedrag te laag om effectief medewerking af te kunnen dwingen.
4. Is duidelijk welke maatregelen door de uitvoeringsorganisatie kunnen worden genomen om fraude zoveel mogelijk tegen te gaan (zoals controle van certificaten, administratief (keten-) toezicht, toepassing Wet BIBOB, raadpleging openbare registers voor controle van derdengegevens)?	Ja. Een ISMS zou een dergelijke check om fraude zoveel mogelijk tegen te gaan (zoals controle van certificaten, administratief (keten-) toezicht, toepassing Wet BIBOB, raadpleging openbare registers voor controle van derdengegevens moeten omvatten. Dit zal nader moeten worden uitgewerkt in de AMvB.

Conclusie fraudebestendigheid: Samenvattend	Ja de Cbw is fraudebestendig. Op het moment anticiperen marktpartijen op de opleidingsverplichtingen voor bestuurders en de te ontwikkelen NIS2-certificatie, hoewel deze nog niet zijn geaccrediteerd en nog niet zijn opgenomen in de Cbw-wetgeving. De aankomende Algemene Maatregel van Bestuur (AMvB) zal hier mogelijk in voorzien, maar dit is nog niet zeker. Het meldpunt voor meldingen is ingericht bij de NCTV/NCSC. Tijdens toezicht worden verificaties en reality-checks uitgevoerd op inhoud en bewijsmateriaal. Er zijn voldoende effectieve sancties genoemd in de regeling of toelichting voor alle betrokken partijen. Een Information Security Management System (ISMS) zou controles moeten omvatten om fraude zoveel mogelijk te voorkomen, zoals controle van certificaten, administratief (keten-)toezicht, toepassing van de Wet BIBOB, en raadpleging van openbare registers voor controle van derden gegevens. Dit zal naar verwachting nader worden uitgewerkt in de AMvB.

Opmerkingen: Definitieve versie 25 juni ’24.