STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 27679
5 augustus 2026

Regeling van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 3 juli 2026, houdende regels ten aanzien van de beveiliging van netwerk- en informatiesystemen van essentiële entiteiten in de sector overheid (Cyberbeveiligingsregeling sector overheid) [KetenID WGK027594]

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, handelende in overeenstemming met de Minister van Justitie en Veiligheid,

Gelet op de artikelen 19 en 23, eerste lid, van het Cyberbeveiligingsbesluit;

Besluit:

HOOFDSTUK 1. ALGEMENE BEPALINGEN

Artikel 1 (begripsbepaling)

In deze regeling wordt verstaan onder:
– *besluit:* Cyberbeveiligingsbesluit;
– *cruciaal netwerk- en informatiesysteem:* netwerk- en informatiesysteem als bedoeld in de artikel 4 van deze regeling;
– *NEN:* norm die door de Stichting Koninklijk Nederlands Normalisatie Instituut is uitgegeven;
– *NEN-EN:* NEN die door het Europees Comité voor Normalisatie is vastgesteld;
– *NEN-EN-ISO/IEC:* NEN-EN die door de International Organization for Standardization en de International Electrotechnical Commission is vastgesteld;
– *VIR-BI:* Besluit voorschrift informatiebeveiliging rijksdienst bijzondere informatie 2025.

Artikel 2 (reikwijdte)

Deze regeling is van toepassing op essentiële entiteiten in de sector overheid, bedoeld in bijlage 1 bij de wet, met uitzondering van de waterschappen.

HOOFDSTUK 2. ZORGPLICHT

Paragraaf 1 (managementsystematiek)

Artikel 3 (ISO 27001)

De essentiële entiteit past de NEN-EN-ISO/IEC 27001:2023 toe op het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsystematiek voor de beveiliging van netwerk- en informatiesystemen, als bedoeld in artikel 6, vierde lid, van het besluit, en op het vaststellen van het toepassingsgebied van deze managementsystematiek.

Artikel 4 (identificeren cruciale netwerk- en informatiesystemen)

1. De essentiële entiteit houdt als onderdeel van haar managementsystematiek voor de beveiliging van de netwerk- en informatiesystemen, bedoeld in artikel 6, vierde lid, van het besluit, een overzicht bij van haar cruciale netwerk- en informatiesystemen.

2. Een netwerk- en informatiesysteem van een essentiële entiteit in de subsector centrale overheden is cruciaal indien het systeem een te beschermen belang op niveau 1, 2 of 3 van de tabel in bijlage 1 bij deze regeling heeft.

3. Een netwerk- en informatiesysteem van een essentiële entiteit in de subsector decentrale overheden is cruciaal indien het systeem impactniveau ‘hoog’ of ‘zeer hoog’ van de tabel in bijlage 2 bij deze regeling heeft.

Paragraaf 2 (beveiligingsmaatregelen)

Artikel 5 (ISO 27002 en BIO2)

1. De essentiële entiteit gebruikt ten minste de beheersmaatregelen van de NEN-EN-ISO/IEC 27002:2022 voor het formuleren van passende en evenredige maatregelen voor de beveiliging van netwerk- en informatiesystemen als bedoeld in artikel 21, eerste lid, van de wet, met uitzondering van de beheersmaatregelen 5.32 en 5.34.De passende en evenredige maatregelen omvatten ten minste de voor haar relevante overheidsmaatregelen van de Baseline Informatiebeveiliging Overheid 2, versie 1.3 (Stct. 2026, 7416), met uitzondering van de overheidsmaatregelen 5.32.01 tot en met 5.34.01.

2. In afwijking van het eerste lid kunnen bij het formuleren van passende en evenredige maatregelen de beheersmaatregelen van de NEN-EN-ISO/IEC 27002:2022 en de overheidsmaatregelen van de Baseline Informatiebeveiliging Overheid 2, versie 1.3 (Stct. 2026, 7416), voor zover dat noodzakelijk is, worden vervangen door of gecombineerd met beheersmaatregelen uit andere normenkaders die een beveiligingsniveau bieden dat ten minste gelijkwaardig is aan het niveau van de voornoemde beheers- en overheidsmaatregelen.

3. De essentiële entiteit zorgt ervoor dat de opzet, het bestaan en de werking van de passende en evenredige maatregelen aantoonbaar zijn. Indien de entiteit bij het formuleren van passende en evenredige maatregelen gebruik heeft gemaakt van beheersmaatregelen uit andere normenkaders als omschreven in het tweede lid, zorgt zij er ook voor dat de noodzakelijkheid van het gebruik van die andere passende en evenredige maatregelen en de gelijkwaardigheid van het beveiligingsniveau daarvan aantoonbaar zijn.

HOOFDSTUK 3. MELDPLICHT

Artikel 6 (drempelwaarden meldplicht)

1. Een incident in de subsector centrale overheden is een significant incident als het leidt of kan leiden tot:
   a. uitval van de dienstverlening van de essentiële entiteit van ten minste vier uur;
   b. financiële schade voor de staat of de samenleving van meer dan € 500.000.000;
   c. de ernstige verwonding of de dood van ten minste één natuurlijke persoon;
   d. misbruik van bedrijfsinformatie met financiële schade van meer dan € 5.000.000; of
   e. de kennisname door onbevoegden van vertrouwelijke informatie op ten minste het niveau Staatsgeheim CONFIDENTIEEL, bedoeld in artikel 4, tweede lid, onder c, van het VIR-BI, het niveau NATO CONFIDENTIAL bedoeld in de bijlagen B, paragraaf 5.5 en E, paragraaf 6, van de NATO Security Policy (Security Within the North Atlantic Treaty Organization, CM(2002)49-REV1) of het niveau EU CONFIDENTIAL, bedoeld in artikel 2 van het Besluit 2013/488/EU van de Raad van 23 september 2013 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie.

2. Een incident in de subsector decentrale overheden is een significant incident als het leidt of kan leiden tot:
   a. uitval van de dienstverlening van de essentiële entiteit voor ten minste vier uur;
   b. financiële gevolgen die niet kunnen worden opgevangen in de begroting; of
   c. de ernstige verwonding of de dood van ten minste één natuurlijke persoon.

3. In afwijking van het eerste lid, onderdeel a, en het tweede lid, onderdeel a, is een geplande dienstonderbreking of een ander gepland gevolg van onderhoudswerkzaamheden die door of namens de essentiële entiteit worden uitgevoerd, geen significant incident.

HOOFDSTUK 4. SLOTBEPALINGEN

Artikel 7 (inwerkingtreding)

Indien het bij koninklijke boodschap van 2 juni 2025 ingediende voorstel van wet houdende regels ter implementatie van 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 (PbEU 2022, L 333) (Cyberbeveiligingswet) (Kamerstukken 36 764) tot wet is of wordt verheven en die wet in werking treedt, treedt deze regeling op hetzelfde tijdstip in werking.

Artikel 8 (citeertitel)

Deze regeling wordt aangehaald als: Cyberbeveiligingsregeling sector overheid.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
E. van der Burg

BIJLAGE 1. TE BESCHERMEN BELANGEN CENTRALE OVERHEDEN

BIJLAGE BIJ ARTIKEL 4, TWEEDE LID

Te beschermen belangen		4	3	2	1
Politieke schade	Geen	Politieke schade voor bewindsper-soon.	Aftreden bewinds-persoon	Aftreden kabinet	Parlementaire crisis
Imagoschade	Geen.	Verlies aan publiek respect	Publieke veront-waardiging	Verlies aan vertrouwen	Structureel verlies aan vertrouwen
Diplomatieke schade	Geen	Te herstellen door ambtelijke opscha-ling	Te herstellen door politieke opschaling	Externe bemidde-ling noodzakelijk	Lange termijn schade ten opzichte van bondgenoten; oorlog
Schade vitale processen in de samenleving	Geen invloed	Verlies van zekerheid van continuïteit	Tijdelijk verlies van continuïteit	Langdurig verlies van continuïteit	Blijvende uitval van processen
Letselschade	Geen	Individuele gewonde	Individuele dode, zeer ernstig gewonde	Meerdere doden, ernstig gewonden	Groepen doden
Betrouwbaarheidseisen IT-systemen (quickscan BIR[1])	ZL, ZL, ZL	t/m H, H, H	Eén van de aspecten ZH	Alle aspecten ZH	
Rubriceringsniveau, als bedoeld in artikel 4 lid 2 VIR-BI[2]		Ongerubriceerd met merking; Dep. V	Stg. CONFIDENTI-EEL	Stg. GEHEIM	Stg. ZEER GEHEIM
NAVO-[3] of EU-rubriceringsniveau[4]		NATO-RESTRICTED Of EU-RESTRICTED	NATO-CONFIDENTIAL of EU-CONFIDENTIAL	NATO SECRET of EU-SECRET	COSMIC TOP SECRET of EU-TOP SECRET
Financiële schade aan de economie of de staat in euro's.	Minder dan 50 mln.	>50 mln.	>500 mln.	>5 mld.	>50 mld.
Financiële schade door misbruik van bedrijfsinfor-matie in euro's.	Minder dan 1 mln.	>1 mln.	>5 mln.	> 500 mln.	>5 mld.

1 Volgens Bijlage 2 in *Stcrt.* 2019, 26526.
2 *Stcrt.* 2025, 30222.
3 Als bedoeld in de bijlagen B, paragraaf 5.5 en bijlage E, paragraaf 6, van de NATO Security Policy (Security Within the North Atlantic Treaty Organization, CM(2002)49-REV1).
4 Als bedoeld in artikel 2 van het Besluit 2013/488/EU van de Raad van 23 september 2013 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie.

BIJLAGE 2. IMPACTNIVEAUS DECENTRALE OVERHEDEN

BIJLAGE BIJ ARTIKEL 4, DERDE LID

Impactniveau	Omschrijving	Zeer laag	Laag	Middel	Hoog	Zeer hoog
Impact op beschikbaarheid (dataverlies – RPO[1]); hoeveel dataverlies is acceptabel	Hoeveel dataverlies is acceptabel?	dataverlies 36 uur	dataverlies 24 uur	dataverlies 12 uur	dataverlies 4 uur	dataverlies 1 uur
Hersteltijd (RTO[2]); hoe lang mag het proces hinder ondervinden van uitval?	Hoe lang mag het proces hinder ondervinden van uitval?	Maximaal 1 week uitval (5 x 8 uur) en hersteltijd 16 uur in 2 werkdagen	Maximaal 2 dagen uitval (2 x 8 uur) en hersteltijd 8 uur in 1 werkdag	Maximaal 1 dag uitval (1 x 8 uur) en herstel in uren	Maximaal 4 uur uitval en herstel in 1 uur	Max 1 uur uitval en minimale (geen) hersteltijd
Impact op belang essentiële entiteit	Wat is de impact voor de essentiële entiteit?	Minimale invloed op kernactiviteiten; weinig invloed op strategische doelstellingen.	Beperkte invloed op sommige kernactiviteiten; enige invloed op strategische doelstellingen.	Duidelijke invloed op meerdere kernactiviteiten; strategie moet mogelijk aangepast worden.	Aanzienlijke invloed op kernactiviteiten; strategische doelstellingen ernstig in gevaar.	Kritieke invloed op de kernactiviteiten; het voortbestaan van de organisatie kan in gevaar komen.
Vervangbaarheid informatie	Is de informatie vervangbaar?	Informatie is gemakkelijk te vervangen zonder noemenswaardige kosten of inspanning.	Informatie is vervangbaar met enige inspanning of kosten.	Vervanging van de informatie is mogelijk, maar vereist aanzienlijke tijd of middelen.	Informatie is moeilijk te vervangen, met hoge kosten of aanzienlijke inspanning.	Informatie is onvervangbaar, verlies zou een onherstelbare impact hebben.
Te beschermen belangen uit de ABDO[3]/ ABRO[4] of vergelijkbaar	Te beschermen belang (TBB)		TBB 4	TBB 4	TBB 3	TBB 2 / TBB 1
Informatieclassificatie beleid	Is de informatie gerubriceerd?	Ongerubriceerd	Dep.V (niveau 1 – standaard) (oud BBN 2 uit de BIO1.04)	Dep.V (niveau 2 – weerstand tegen spionage) (Oud BBN3 uit de BIO 1.04)	Stg.C	Stg.G / Stg.ZG
Schade bij openbaarmaking	Wat is de schade bij openbaarmaking?		Indien kennisname door niet-geautoriseerden nadeel kan toebrengen aan de belangen van één of meerdere afdelingen van de essentiële entiteit	Indien kennisname door niet-geautoriseerden schade kan toebrengen aan de belangen van de essentiële entiteit	Indien kennisname door niet geautoriseerden aanzienlijke schade kan toebrengen aan een van de vitale belangen van de essentiële entiteit	Indien kennisname door niet geautoriseerden ernstige of zeer ernstige schade kan toebrengen aan een van de vitale belangen van de essentiële entiteit
Kennisnemen informatie door onbevoegden	Kennisname is:?		Is ongewenst	Moet zoveel mogelijk worden voorkomen	Moet worden voorkomen	Is onacceptabel
Persoonsgegevens	Bevat persoonsgegevens of bijzondere persoonsgegevens of een grote verzameling		Bevat persoonsgegevens	Bevat bijzondere persoonsgegevens of meerdere collecties van persoonsgegevens.	Bevat meerdere collecties met bijzondere persoonsgegevens	

Impactniveau	Omschrijving	Zeer laag	Laag	Middel	Hoog	Zeer hoog
Politieke schade	Beleidsmatige gevolg classificatie	Geen politieke aandacht of risico. De situatie heeft geen invloed op bestuurders of vertegenwoordigend orgaan, en blijft binnen de organisatie.	Beperkte politieke gevoeligheid. Mogelijk bestuurlijke notitie of korte interne afstemming, maar geen publieke aandacht of aandacht van het vertegenwoordigend orgaan.	Matige politieke impact. Er is kans op vragen uit het vertegenwoordigend orgaan of lokale media-aandacht. Bestuurders moeten intern of in het vertegenwoordigend orgaan toelichten wat er is gebeurd.	Duidelijke politieke gevolgen. De kwestie leidt tot publieke discussie of mediabelangstelling, politieke druk of reputatieschade. Bestuurders worden ter verantwoording geroepen en moeten zich verantwoorden naar aanleiding van verantwoordingsvragen (vragen in het vertegenwoordigend lichaam gesteld). Er wordt een (lokaal) parlementair onderzoek ingesteld.	Ernstige politieke impact. De kwestie veroorzaakt grote politieke en publieke ophef, mogelijk moties van wantrouwen of aftreden van bestuurders. Vertrouwen in bestuurders of vertegenwoordigers komt ernstig onder druk te staan. Er is sprake van een enquête.
Diplomatieke schade	Is er diplomatieke schade te verwachten?	• Geen diplomatieke schade. De relaties met andere landen zijn stabiel en goed onderhouden, zonder enige negatieve impact. • Effect op burgergerichte processen: Geen impact. Burgers merken geen verandering in de dienstverlening, internationale samenwerking of toegang tot buitenlandse diensten.	• Klein verlies aan diplomatieke goodwill. Er zijn lichte spanningen, maar deze worden snel en efficiënt opgelost zonder grote gevolgen. • Effect op burgergerichte processen: Minimale invloed op internationale samenwerking, bijvoorbeeld lichte vertragingen bij grensoverschrijdende diensten of minder vloeiende samenwerking met buitenlandse partners. Burgers merken nauwelijks iets van de situatie.	• Merkbare diplomatieke schade. Relaties met andere landen verslechteren tot een punt waarop samenwerking in bepaalde gebieden moeilijker wordt. Dit kan bijvoorbeeld leiden tot vertragingen in internationale handel, samenwerking of informatie-uitwisseling. • Effect op burgergerichte processen: Burgers kunnen langere wachttijden ondervinden bij grensoverschrijdende diensten zoals visa-aanvragen, internationale handel of hulp in het buitenland. Er kunnen ook meer bureaucratische hindernissen ontstaan bij internationale procedures.	• Aanzienlijke diplomatieke schade. De relaties met belangrijke diplomatieke partners verslechteren aanzienlijk, wat leidt tot vertragingen of beperkingen in internationale samenwerking, en tot verlies van toegang tot strategische informatie of samenwerkingsovereenkomsten. • Effect op burgergerichte processen: Burgers ondervinden duidelijke problemen, zoals een aanzienlijke afname in toegang tot consulaire diensten in het buitenland, problemen bij internationale reis- of handelsregelingen, en moeilijkheden in grensoverschrijdende communicatie en samenwerking. Er is sprake van toenemende ontevredenheid.	• Ernstige diplomatieke schade. De diplomatieke relaties met andere landen zijn ernstig verstoord of verbroken, wat kan leiden tot sancties, reisbeperkingen, en ernstige verstoringen in internationale samenwerkingen en handelsrelaties. • Effect op burgergerichte processen: Burgers worden geconfronteerd met grote problemen, zoals reisverboden, verlies van consulaire steun in het buitenland, beperkte toegang tot internationale diensten en ernstige verstoringen in de handel. Dit kan leiden tot wijdverspreide ontevredenheid en ernstige gevolgen voor de economie en de toegang tot buitenlandse diensten.
Financiële impact	Hoeveel budget is gemoeid met het risico?	Op te vangen binnen de begroting van de afdeling	Niet meer op te vangen binnen de begroting van de afdeling	Niet meer op te vangen binnen de begroting van de directie	Niet meer op te vangen binnen de begroting van de essentiële entiteit	Niet meer op te vangen binnen de begroting van de essentiële entiteit; leidt tot financieel toezicht

Impactniveau	Omschrijving	Zeer laag	Laag	Middel	Hoog	Zeer hoog
Directe imagoschade	Verlies van publiek respect of organisatie-brede negatieve publiciteit	• Geen imagoschade. De reputatie van de organisatie of overheid blijft ongeschonden. Er is geen negatieve publiciteit of perceptie van het publiek. • Effect: Geen invloed op de reputatie. De essentiële entiteit wordt nog steeds als betrouwbaar, efficiënt en positief gezien.	• Verlies van publiek respect - Lichte imago-schade. Er is sprake van een klein incident of negatieve publiciteit, maar dit blijft beperkt en is snel te herstellen. • Effect: Kortdurende negatieve perceptie bij een beperkt publiek, zonder langdu-rige gevolgen. Vertrouwen wordt snel hersteld door adequate communicatie en acties.	• Publieke verontwaardiging - Merkbare imagoschade. Een incident of reeks incidenten leidt tot bredere negatieve aandacht in de media en onder het publiek. Het vertrouwen in de essentiële entiteit wordt aangetast, en er is kritiek op het beleid of handelen. • Effect: Zichtbare impact op de reputatie, met een afname van vertrouwen en geloofwaardigheid bij een groot deel van het publiek. Herstel vereist actieve maatrege-len en verbeterde communicatie.	• Verlies aan vertrouwen - Aanzienlijke imagoschade. Een grote misser of reeks van schandalen leidt tot wijdverspreide negatieve berichtge-ving en publieke verontwaardiging. Het herstel van het vertrouwen vergt aanzienlijke inspanningen en tijd. • Effect: Het vertrouwen in de essentiële entiteit wordt ernstig geschaad. Het publiek en de media blijven kritisch, en de negatieve impact houdt lange tijd aan. Grootschalige herziening van beleid of manage-ment is nodig om het imago te herstellen.	• Structureel verlies aan vertrouwen - Ernstige imago-schade. Een crisis of schandaal leidt tot langdurige en diepgaande reputatieschade, mogelijk op internationaal niveau. Het imago van de organisatie is ernstig en mogelijk onherstelbaar beschadigd. • Effect: Het vertrou-wen in de essentiële entiteit is volledig verloren, met blijvende gevolgen voor de geloofwaar-digheid en het functioneren. Mogelijk verlies van steun vanuit het publiek, partners of andere stakeholders. Drastische maatrege-len zijn nodig, en volledig herstel kan jaren duren of nooit volledig worden bereikt.
Verlies van publiek respect of vertrouwen	Wat is het effect op het vertrouwen van burgers, bedrijven of maatschappe-lijke organisa-ties in het bestuur of de organisatie?	• Nauwelijks merkbaar verlies van vertrouwen; beperkt tot individuen of kleine groepen. • Voorbeelden: Klacht over wachttijd bij loket, inciden-tele negatieve reacties op sociale media.	• Lokaal verlies van vertrouwen binnen een wijk of doelgroep; beperkt media-aandacht. • Voorbeelden: Onvrede over wijkontwikke-ling, beperkte protesten of petities.	• Breder verlies van vertrouwen; meerdere doelgroepen; lokale media-aandacht. • Voorbeelden: Foutieve belasting-aanslagen, langdurige ICT-storing, onduidelijke communicatie.	• Aanzienlijk verlies van vertrouwen; landelijke media-aandacht. • Voorbeelden: Onrechtmatige uitkeringen, datalek, bestuurlijke onrust.	• Structureel verlies van vertrouwen; langdurige reputatie-schade; mogelijk landelijke of juridische gevolgen. • Voorbeelden: Fraude, corruptie, ernstige schending van burgerrechten, bestuurlijke crisis.
Organisatie-brede negatieve publiciteit	Wat is het effect van organisatie-brede negatieve publiciteit op het imago, het vertrouwen van inwoners en partners, en op de bestuurlijke stabiliteit?	• Interne of zeer beperkte externe aandacht; geen blijvende schade. • Voorbeeld: Kritiek in een bewonersbrief of kleine online discussie.	• Lokale media-aandacht of social media-ophef; beperkt tot één onderwerp of wijk. • Voorbeeld: Artikel in lokale krant over fout in vergunningverle-ning of afvalinza-meling.	• Entiteitbrede aandacht; meerdere afdelingen betrokken; reputatieschade binnen de grenzen van de essentiële entiteit. • Voorbeeld: Nieuwsitem over falende dienstverle-ning, datalek, of onduidelijke communicatie.	• Landelijke media-aandacht; langdurige negatieve beeldvorming; bestuurlijke verantwoording vereist. • Voorbeeld: Nieuwsuur-item over mismanagement, integriteitskwestie of fraude.	• Structurele reputatieschade; landelijke of internationale aandacht; mogelijk juridische of politieke gevolgen. • Voorbeeld: Onderzoek door toezichthouder, parlementaire vragen, of interna-tionale media-aandacht.

Impactniveau	Omschrijving	Zeer laag	Laag	Middel	Hoog	Zeer hoog
Significant verlies van motivatie medewerkers	Wat is het effect op de motivatie van de medewerkers?	• Geen waarneembaar effect op de burgergerichte processen. De dienstverlening blijft op het verwachte niveau zonder vertragingen of fouten. • Effect op burgergerichte processen: Geen merkbare invloed op de kwaliteit van de dienstverlening. Burgers ervaren dezelfde efficiëntie en betrouwbaarheid.	• Een lichte afname in motivatie die minimale gevolgen heeft voor de prestaties. Mogelijk kleine vertragingen of minder efficiëntie, maar zonder significante verstoring van de processen. • Effect op burgergerichte processen: Kleine vertragingen of incidentele fouten in de dienstverlening, maar geen structurele problemen. Burgers merken mogelijk een lichte afname in de respons of efficiëntie.	• Merkbare daling in motivatie wat leidt tot verminderde productiviteit. Dit kan leiden tot vertragingen in besluitvorming, langere doorlooptijden en mogelijk meer fouten. • Effect op burgergerichte processen: Verlengde wachttijden voor burgers, fouten in de afhandeling van aanvragen, en lagere kwaliteit van dienstverlening. Burgers kunnen ontevreden raken over de snelheid en kwaliteit van de overheidsdiensten.	• Aanzienlijk verlies van motivatie, resulterend in frequente fouten, lange vertragingen en verminderd vermogen om op vragen of klachten van burgers te reageren. • Effect op burgergerichte processen: Veel voorkomende vertragingen en kwaliteitsproblemen, waardoor burgers regelmatig problemen ondervinden bij het verkrijgen van diensten. Dit kan leiden tot een afname van het vertrouwen in de overheid.	• Extreme demotivatie die leidt tot ernstige verstoringen in de dienstverlening, inclusief aanzienlijke fouten, langdurige vertragingen en mogelijk ook hogere niveaus van verloop onder medewerkers. • Effect op burgergerichte processen: Ernstige verstoringen in de burgergerichte processen. Burgers ervaren langdurige wachttijden, fouten in administratieve processen, en een drastische afname in de kwaliteit van dienstverlening, wat resulteert in grote publieke ontevredenheid en mogelijk een vertrouwenscrisis in de overheid.
Belangrijk verlies van management control	Kan de organisatie haar processen nog effectief en efficiënt uitvoeren?	• Geen verlies van management control. Processen verlopen zoals gepland, met duidelijke sturing en toezicht. • Effect op burgergerichte processen: Geen impact. De overheid blijft effectief in het leveren van consistente en betrouwbare diensten aan burgers.	• Klein verlies van management control. Er zijn lichte inefficiënties, maar deze worden snel opgemerkt en opgelost zonder grote verstoringen. • Effect op burgergerichte processen: Sporadische kleine inefficiënties in de dienstverlening, zoals lichte vertragingen of communicatiemisverstanden. Burgers ervaren incidenteel minder optimale processen, maar dit leidt niet tot serieuze klachten.	• Merkbaar verlies van management control. Er ontstaan significante inefficiënties en miscommunicatie tussen verschillende afdelingen, wat resulteert in trager besluitvormingsproces en problemen met het naleven van vastgestelde procedures. • Effect op burgergerichte processen: Burgers ondervinden langere wachttijden, inconsistenties in informatieverstrekking of behandeling van aanvragen. Er is een duidelijke afname in de kwaliteit en voorspelbaarheid van overheidsdiensten, wat tot verhoogde frustratie kan leiden.	• Aanzienlijk verlies van management control. Het gebrek aan sturing leidt tot fouten in kritieke processen, langdurige vertragingen, en het niet volgen van protocollen. Management reageert langzaam of inadequaat op problemen. • Effect op burgergerichte processen: Burgers ervaren systematische vertragingen, onvolledige of foutieve dienstverlening, en gebrek aan adequate opvolging van aanvragen of klachten. Het vertrouwen in de efficiëntie en betrouwbaarheid van de overheid neemt merkbaar af.	• Extreem verlies van management control. Het management is vrijwel niet in staat om de operationele processen te beheersen. Er is sprake van een chaotische situatie met frequente fouten, gebrek aan samenhang en ernstige vertragingen. • Effect op burgergerichte processen: Ernstige verstoringen in de dienstverlening aan burgers. Diensten worden slecht uitgevoerd of komen zelfs geheel tot stilstand. Burgers ervaren langdurige vertragingen, administratieve chaos en aanzienlijke fouten in hun aanvragen of diensten, wat resulteert in een groot verlies van vertrouwen in de overheidsinstellingen.
Schade vitale processen	Is er impact op de vitale/kritieke processen van de organisatie?	Geen verstoring van vitale processen.	Beperkte verstoring van vitale processen; processen kunnen snel worden hervat.	Duidelijke verstoring; vitale processen worden tijdelijk gehinderd.	Aanzienlijke verstoring; vitale processen worden ernstig gehinderd.	Catastrofale verstoring; vitale processen worden onwerkbaar of volledig stilgelegd.

Impactniveau	Omschrijving	Zeer laag	Laag	Middel	Hoog	Zeer hoog
Maatschappelijke impact	Incidenten die mogelijk negatieve publiciteit veroorzaken of het vertrouwen van burgers in publieke instellingen beïnvloeden.	Geen of nauwelijks merkbare impact voor de samenleving. De verstoring is beperkt tot een kleine groep mensen of heeft nauwelijks effect op het dagelijks leven van burgers.	Enige impact op een beperkte groep mensen of specifieke gemeenschap. Het dagelijks leven van burgers wordt licht verstoord, maar er zijn alternatieven beschikbaar of de verstoring is kortdurend.	Duidelijke impact op meerdere gemeenschappen of een significante groep mensen. Het dagelijks leven van deze mensen wordt merkbaar beïnvloed, bijvoorbeeld door verstoring van een publieke dienst gedurende meerdere dagen.	Aanzienlijke impact op de samenleving als geheel of op een groot deel van de bevolking. Diensten of voorzieningen die essentieel zijn voor burgers worden onderbroken, wat leidt tot verstoringen op sociaal, economisch of fysiek gebied.	Ernstige impact die de hele samenleving raakt. Essentiële diensten vallen langdurig uit of falen, wat mogelijk leidt tot onrust, massale verstoring van dagelijks leven, en maatschappelijke ontwrichting.
Letsel		Geen of minimale fysieke of psychische schade.	Lichte verwondingen of stress die zonder blijvende gevolgen zijn.	Ernstige verwondingen of stress met tijdelijke gevolgen.	Zeer ernstige verwondingen of blijvende psychische schade.	Dodelijke verwondingen of onherstelbare psychische schade.
Inbreuk op persoonlijke levenssfeer		Geen of minimale inbreuk op privacy, geen impact op betrokkenen.	Beperkte inbreuk op privacy; gering risico voor betrokkenen.	Duidelijke inbreuk op privacy; aanzienlijke impact op betrokkenen.	Aanzienlijke inbreuk op privacy; ernstige impact en grote impact voor betrokkenen en verlies van vertrouwen.	Catastrofale inbreuk op privacy; ernstige gevolgen voor betrokkenen, mogelijk juridische gevolgen.

[1] Recovery Point Objective: De herstelpuntdoelstelling, die weergeeft wat het maximaal toegestane dataverlies is voor de organisatie. Deze hoeveelheid is gemeten in tijd, namelijk de periode tussen de laatste succesvolle data back-up en de verstorende gebeurtenis.
[2] Recovery Time Objective: De hersteltijddoelstelling, die weergeeft wat de maximaal toegestane tijd is dat een systeem of proces offline kan zijn na een incident zonder dat dit gevolgen heeft voor de bedrijfsvoering.
[3] Algemene Beveiligingseisen voor Defensieopdrachten.
[4] Algemene Beveiligingseisen Rijksoverheidsopdrachten.

TOELICHTING

ALGEMEEN

1. Inleiding

De Europese Network and Information Security (NIS2)-richtlijn)[1] verplicht tot het implementeren van regels over de beveiliging van netwerk- en informatiesystemen van essentiële en belangrijke entiteiten en de daarvoor benodigde governance binnen de entiteiten. Deze regels zijn omgezet in het voorstel voor de Cyberbeveiligingswet (Cbw) en het Cyberbeveiligingsbesluit (Cbb).
In de Cbw en het Cbb is een aantal grondslagen opgenomen om per ministeriële regeling nadere regels te stellen voor de verschillende essentiële en belangrijke sectoren (en eventueel voor subsectoren en entiteiten). Deze zien onder meer toe op het stellen van nadere regels voor de zorgplicht die organisaties hebben voor het beveiligen van hun netwerk- en informatiesystemen, en het opnemen van sectorspecifieke drempelwaarden voor de meldplicht om te bepalen wanneer zich een significant beveiligingsincident voordoet in een netwerk- en informatiesysteem van een entiteit dat gemeld moet worden aan het Computer Security Incident Response Team (CSIRT) en de toezichthouder.
Met deze regeling zijn voor de sector overheid de nadere regels voor de zorgplicht vastgesteld, alsook de drempelwaarden voor de meldplicht. Deze regeling geldt zowel voor de centrale als de decentrale overheden, met uitzondering van de waterschappen. De waterschappen vallen onder de regeling van de Minister van Infrastructuur en Waterstaat (I&W).
Het is mogelijk dat entiteiten die onder de sector overheid vallen tevens kwalificeren als essentiële of belangrijke entiteiten onder een andere sector. Dan zijn ook de regels die volgen uit de ministeriële regeling voor die betreffende sector van toepassing op de daaronder vallende overheidsinstanties. Tussen de betreffende bevoegde autoriteiten alsmede tussen de betreffende CSIRT's zullen samenwerkingsafspraken worden gemaakt over de samenloop bij toezicht en de ondersteuning door de CSIRT's.

2. Hoofdlijnen

Bij het stellen van nadere regels is het uitgangspunt gehanteerd dat zoveel mogelijk wordt aangesloten bij de bestaande praktijk om daarmee de invoeringslast van deze ministeriële regeling zoveel mogelijk te beperken. Per onderdeel wordt hierop nader ingegaan.

2.1 Zorgplicht

Bij de overheid bestond al de Baseline Informatiebeveiliging Overheid (BIO), als interbestuurlijk convenant met een groot aantal zorgplichtbepalingen. Los daarvan zijn er veel andere informatiebeveiligingseisen of zorgplichtbepalingen die vanuit verschillende interbestuurlijke voorzieningen en informatieprocessen wettelijk zijn verplicht.

De Cbw en het Cbb vestigen een algemene zorgplicht voor een groot aantal maatschappelijke sectoren, waaronder de sector overheid. Naast de grondslag om deze onderwerpen nader uit te werken, biedt de delegatiegrondslag van het Cbb de ruimte om per ministeriële regeling ook zorgplichtbepalingen op te nemen over andere dan de genoemde onderwerpen, zolang die binnen de scope van de NIS2-richtlijn en de Cbw vallen. Met het stellen van nadere regels voor de zorgplicht ontstaat er voor overheidsinstanties, zowel op centraal als decentraal niveau, een algemeen wettelijk uniform en afdwingbaar kader met betrekking tot de zorgplicht voor de beveiliging van netwerk- en informatiesystemen. De noodzaak om deze eisen vanuit andere wet- en regelgeving nogmaals te stellen vervalt daarmee.

De keuze is gemaakt om toepassing van de Baseline Informatiebeveiliging Overheid versie 2 (BIO2)[2], de vernieuwde versie van de BIO die al als verplichtende zelfregulering werd toegepast door overheidsinstanties in deze regeling op te nemen als minimale invulling voor het formuleren van passende en evenredige maatregelen, bedoeld in artikel 21, eerste lid, van de Cbw. Deze keuze is gemaakt om de volgende redenen:

Beperken implementatiedruk van de Cbw bij medeoverheden

Met het aansluiten bij reeds bestaande normenkaders voor informatiebeveiliging van de overheid

[1] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 20 mei 2015 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 (NIS 2-richtlijn).
[2] *Stct.* 2026, 7416.

worden de administratieve lasten van implementatie voor overheidsorganisaties beperkt. Zij dienen immers te voldoen aan normen die zij zichzelf eerder al hebben opgelegd. Bovendien hebben alle koepelorganisaties van medeoverheden in hun consultatiereacties op de Cbw en het Cbb reeds aangegeven graag de BIO te hanteren als invulling van de zorgplicht.

Hanteren van één methodiek binnen de overheid

Het uitgangspunt is om binnen de overheid één werkwijze te hanteren, zodat overheidspartijen eenzelfde uitgangspunt hebben bij het maken van ketenafspraken en dezelfde taal en denkwereld hanteren richting de burger en het bedrijfsleven.

Als instrument voor het terugdringen van administratieve lastendruk

Uit de Werkagenda Waardengedreven Digitaliseren[3] en de Nederlandse Cybersecurity Strategie (NLCS)[4] was de wens naar voren is gekomen om de BIO2 wettelijk te verankeren. Met als reden dat dit de noodzaak verkleint om vanuit verschillende (wettelijke) stelsels, denk bijvoorbeeld aan de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI), eisen te stellen aan de informatiebeveiliging voor overheden. Voorafgaand aan deze regeling was dat niet mogelijk, omdat de BIO2 nog een interbestuurlijk convenant was dat niet dezelfde status heeft als een van de genoemde wettelijke regelingen. Door de verankering van de BIO2 in deze ministeriële regeling is de mogelijkheid gecreeërd om in de toekomst een versimpeling te kunnen aanbrengen in het aantal van toepassing zijnde wettelijke regelingen ten aanzien van informatiebeveiliging, waardoor verantwoordings- en toezichtlasten voor overheden aanzienlijk kunnen worden teruggedrongen. Hierover zal via de bestaande structuren voor de Eenduidige Normatiek Single Information Audit (ENSIA) worden afgestemd.

Verzoek vanuit alle bestuurslagen

Ten slotte is op 23 september 2025 door het Overheidsbreed Beleidsoverleg Digitalisering Overheid (OBDO) akkoord gegeven op de BIO2 en is de Staatssecretaris van Binnenlandse Zaken (BZK) en Koninkrijksrelaties geadviseerd om de BIO2 als normenkader voor de zorgplicht op te nemen in de regelgeving onder de Cbw voor de sector overheid.

De BIO2 blijft daarnaast verplichtende zelfregulering voor de organisaties of onderdelen van organisaties die niet onder de reikwijdte van de Cbw vallen maar de BIO2 wel onderschreven hebben.

Verplichtingen

In de regeling zijn om die reden de volgende verplichtingen opgenomen. De entiteit heeft de verplichting tot het toepassen van de NEN-EN-ISO/IEC 27001 (ISO 27001) op het formuleren van eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsystematiek voor informatiebeveiliging en het vaststellen van het toepassingsgebied van deze managementsystematiek. De beheersmaatregelen van de NEN-EN-ISO/IEC 27002 (ISO 27002) en de verplichte overheidsmaatregelen uit de BIO2 worden toegepast op het formuleren van passende en evenredige maatregelen. Hierbij wordt voor de beheersmaatregelen uit de ISO 27002 rekening gehouden met de omgeving(en) waarin de informatiebeveiligingsrisico's voorkomen, gebaseerd op de scope en de onderkende risico's. De beheers- en overheidsmaatregelen uit de ISO 27002 en de BIO2 kunnen, voor zover dat noodzakelijk is én daarmee een gelijkwaardig beveiligingsniveau wordt gegarandeerd, worden vervangen door of gecombineerd met beheersmaatregelen uit andere normen en richtlijnen, zoals voor zorginformatie NEN 7510 en voor Operationele Technologie (OT) de CSIR en IEC 62443 Industriële cybersecurity. Dat kan bijvoorbeeld wanneer het ingeschatte risico beter afgedekt is met een gelijkwaardige beheersmaatregel vanuit andere, specifiekere normenkaders.

De essentiële entiteit draagt er zorg voor dat de opzet, het bestaan, en de werking van de passende en evenredige maatregelen aantoonbaar zijn. Dit is een specificering van de eis uit artikel 18 van het Cbb om de doeltreffendheid van de genomen maatregelen periodiek te evalueren. De eis sluit aan bij de BIO2 en specificeert wat aangetoond moet worden over de implementatie van de maatregelen.
Als er gebruik is gemaakt van passende en evenredige maatregelen uit andere normenkaders is daarbij ook vereist dat de noodzakelijkheid van het gebruik van die andere normen en de gelijkwaardigheid van het beveiligingsniveau die ze bieden aantoonbaar worden gemaakt in de Verklaring van Toepasselijkheid.

[3] *Kamerstukken II,* 2022/23, 26 643, 640, bijlage 1062267.
[4] *Kamerstukken II,* 2022/23, 26 643, 925, bijlage 1054176.

2.2 Identificeren cruciale netwerk- en informatiesystemen

Daarnaast zijn er bepalingen opgenomen die het identificeren van de cruciale netwerk- en informatiesystemen voor de centrale en decentrale overheden verplicht stelt. Hiervoor is aangesloten op bestaande werkwijzen bij zowel rijksoverheid als gemeenten. Het doel daarvan is meervoudig:

- het helpt organisaties bij het proportioneel beveiligen van hun netwerk- en informatiesystemen. Het is een onderdeel van het risicomanagement en het geeft inzicht bij welke diensten de beveiliging de hoogste mate van zorgvuldigheid vraagt. Het is echter niet zo dat deze verplichting ertoe leidt dat aan de zorgplicht wordt voldaan als er alleen maatregelen worden genomen ter bescherming van deze cruciale systemen;
- het helpt entiteiten bij het voldoen aan de meldplicht. Deze drempelwaarden sluiten aan op de criteria die zijn gebruikt voor het identificeren van de cruciale netwerk- en informatiesystemen. Hierdoor is het bij incidenten op cruciale netwerk- en informatiesystemen aannemelijker dat er gemeld zou moeten worden, bij de inschatting van de netwerk- en informatiesystemen is immers reeds gekeken naar de mogelijke impact die aantasting van deze systemen kunnen hebben.

Voor de inschatting wat cruciale netwerk- en informatiesystemen binnen de sector overheid zijn, is gekeken naar de tabel met te beschermen belangen (TBB's) uit de Leidraad te beschermen belangen en de impacttabel die de Informatiebeveiligingsdienst van VNG Realisatie BV (IBD) bij gemeenten toepast en die ook door enkele provincies wordt gebruikt. Deze tabellen werden al gebruikt door overheidsorganisaties voor het inschatten van belangen of processen voor de organisatie. Hierbij wordt gekeken naar de mogelijke impact die niet-functioneren kan hebben.

De rijksoverheid kent 4 niveaus voor de tabel met TBB's, gemeenten spreken over 5 impactniveaus. Beide modellen gebruiken voor de inschatting van deze niveaus criteria die overeenkomen met de gevolgen van een incident zoals benoemd in de Cbw:

- Schade aan personen, denk aan doden of ernstig gewonden als gevolg van het incident.
- Materiële en immateriële schade, denk aan financieel verlies dat niet binnen de reguliere begroting van de organisatie is op te vangen.
- Integriteit en vertrouwelijkheid, denk aan de openbaarmaking van informatie op het niveau Staatsgeheim Confidentieel of hoger.
- Beschikbaarheid, denk aan uitval van dienstverlening van kernprocessen die een bepaalde tijd voortduurt of herstel dat niet binnen afzienbare tijd mogelijk is.

Voor het bepalen of er sprake is van een cruciaal netwerk- en informatiesysteem kijken entiteiten naar de mogelijke impact die een aantasting van de beschikbaarheid, integriteit en vertrouwelijkheid van dit netwerk- en informatiesysteem kan hebben. Daarvoor gebruiken de essentiële entiteiten van de centrale overheid de tabel als bedoeld in bijlage 1 van deze regeling en decentrale overheden de tabel in bijlage 2. Zij lopen de verschillende categorieën, zoals financiële impact, van deze tabellen langs en bepalen de mogelijke impact van het betreffende netwerk- en informatiesysteem op die categorie. Uiteindelijk bepaalt de hoogst-geclassificeerde categorie op welk niveau het netwerk- en informatiesysteem wordt ingeschaald. Een netwerk- en informatiesysteem is cruciaal indien het systeem een te beschermen belang op niveau 1, 2 of 3 van de tabel in bijlage 1 voor essentiële entiteiten van de centrale overheid, of het systeem impactniveau 'hoog' of 'zeer hoog' van de tabel in bijlage 2 heeft voor essentiële entiteiten van de decentrale overheid.

De IBD heeft reeds gezamenlijk met enkele gemeenten uitgewerkt wat volgens hen kritieke processen zijn. Dat doen zij aan de hand van de impacttabel die gelijk is aan de tabel in bijlage 2 van deze regeling.[5] Deze uniforme uitwerking is gemaakt om lasten voor individuele gemeenten te beperken, veel gemeenten kennen immers dezelfde processen. Gemeenten kunnen deze uitwerking gebruiken om voor hun eigen organisatie te toetsen welke netwerk- en informatiesystemen als cruciaal moeten worden ingeschaald.

2.3 Meldplicht

De Cbw maakt onderscheid tussen een 'incident' en een 'significant incident'.
Volgens artikel 1 van de Cbw is een incident een gebeurtenis die de beschikbaarheid, integriteit, vertrouwelijkheid of authenticiteit van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt. Een gebeurtenis hoeft niet per definitie plaats te vinden in het cyberdomein. De Cbw kent namelijk een benadering die alle gevaren omvat (*all hazard*) en heeft tot doel om netwerk- en informatiesystemen en de fysieke omgeving daarvan te beschermen tegen gebeurtenissen die de

[5] BIO2 kritieke processen gemeenten, december 2025 (versie 1.1), gepubliceerd op: https://www.informatiebeveiligingsdienst.nl/product/bio2-kritieke-processen-gemeenten/.

beveiliging van die systemen kunnen aantasten. Het gaat ook om de bescherming van die systemen tegen andersoortige gebeurtenissen, zoals natuurrampen of branden.
In artikel 25, tweede lid, van de Cbw wordt aan de hand van drie parameters beschreven wanneer er sprake is van een significant incident, namelijk wanneer een incident:

a. een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of
b. andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

Een significant incident moet overeenkomstig de artikelen 26 tot en met 29 van de Cbw door de getroffen essentiële entiteit gemeld worden bij de toezichthouder en het CSIRT.
In de praktijk is voorzien om deze tweeledige melding in te vullen via het meld- en registratieportaal, dat gebeurt via het MijnNCSC-portaal. Entiteiten hoeven dan slechts eenmalig melding te maken van een incident, die wordt gerouteerd naar zowel het ondersteunend CSIRT als de toezichthouder (aangewezen door de bevoegde autoriteit). Artikel 27, eerste lid, van de Cbw bepaalt dat de entiteit onverwijld of, indien dit niet mogelijk is, binnen 72 uur, nadat zij kennis heeft gekregen van het significante incident een melding daarvan doet bij het CSIRT en de bevoegde autoriteit. Deze melding wordt voorafgegaan door een vroegtijdige waarschuwing die zo snel mogelijk, maar in ieder geval binnen 24 uur wordt afgegeven. De tijdsperiode voor beide meldingen begint te lopen zodra de entiteit kennis heeft genomen van het feit dat een incident ook een significant incident is. Het is dus aan de entiteit om zo snel mogelijk te onderzoeken en vast te stellen of de gestelde drempelwaarden overschreden worden of kunnen worden en te melden indien nodig.
In artikel 23, eerste lid, van het Cbb is een delegatiegrondslag opgenomen om bij ministeriële regeling per sector invulling te geven aan de criteria voor het bepalen wanneer sprake is van een significant incident door daarvoor drempelwaarden op te stellen. In deze regeling worden de drempelwaarden voor significante incidenten uit de Cbw verder uitgewerkt voor essentiële entiteiten binnen de sector overheid. Zij geven de betreffende entiteiten en de toezichthouder handvatten om te beoordelen of een incident als significant moet worden aangemerkt en dus meldingsplichtig is. De drempelwaarden moeten in samenhang met artikel 25 Cbw worden gelezen: alleen als een incident aan ten minste één van deze drempelwaarden voldoet, is sprake van een significant incident en geldt de meldplicht. Daarnaast worden entiteiten nadrukkelijk uitgenodigd vrijwillig melding te maken van niet-significante incidenten of bijna-incidenten.
Bij het opstellen van de drempelwaarden voor zowel de subsector centrale als decentrale overheden is afstemming gezocht met diverse experts vanuit verschillende bestuurslagen, andere ministeries en betrokken toezichthouders. Deze uitwerking had als doel de drempelwaarden goed te laten aansluiten op de praktijk en bestaande kaders, om de uitvoerbaarheid en handhaafbaarheid te borgen en regeldruk voor entiteiten te beperken. Tegelijkertijd dient voorkomen te worden dat relevante meldingen niet als significant worden aangemerkt en daardoor niet worden gemeld bij het CSIRT en de toezichthouder. Tevens is in ogenschouw genomen dat de Cbw vereist dat meldingen kort na ontdekking van een incident moeten worden gedaan. Tijd om een (complexe) analyse te maken van de mogelijke gevolgen van het incident – terwijl het incident ook moet worden beheerst – is er vaak niet. Daarom is ervoor gekozen entiteiten zoveel mogelijk in staat te stellen deze analyse op voorhand te maken, bij de uitvoering van het risicomanagement in de zorgplicht en het bepalen van de cruciale netwerk- en informatiesystemen. Dat doen zij mede door te kijken naar de impact die mogelijke uitval van deze systemen kunnen hebben. Door de drempelwaarden te baseren op een aantal van die criteria, kunnen zij ten tijde van een incident sneller vaststellen of een incident significant is en gemeld zou moeten worden.

Voor essentiële entiteiten in de subsector centrale overheden zijn de drempelcriteria opgenomen in artikel 6, eerste lid, van deze regeling die zijn gebaseerd op de tabel met TBB's in bijlage 1. Er is gekeken naar criteria die voor de entiteit goed vast te stellen zijn, vanwege het feit dat ze tot meetbare resultaten leiden, zoals een bepaald bedrag of een bepaalde tijdsduur. Andere categorieën uit bijlage 1, zoals diplomatieke schade of politieke schade, zijn wel van invloed op het aanmerken van systemen als cruciaal, maar lenen zich minder goed als drempelwaarde voor het melden van een incident.

Voor essentiële entiteiten in de subsector decentrale overheden zijn de drempelcriteria opgenomen in artikel 6 tweede lid. Deze zijn gebaseerd op niveau 'hoog' uit de tabel met impactcriteria in bijlage 2. Ook voor de meldplicht voor decentrale overheden geldt dat er verschillende drempelwaarden zijn overgenomen uit de tabel in bijlage 2, die een duidelijk vast te stellen impact met zich meebrengen, zodat essentiële entiteiten gemakkelijk vast kunnen stellen of er sprake is van een significant incident. De overige categorieën die van invloed zijn op het identificeren van cruciale netwerk- en informatie-systemen als onderdeel van de zorgplicht, doen veelal ook het vermoeden rijzen dat een incident op een dergelijk netwerk- en informatiesysteem de genoemde impactniveaus in artikel 6, tweede lid kunnen bereiken.

Er is geen sprake van een significant incident indien de dienstverlening op een vooraf gepland moment wordt onderbroken als gevolg van geplande onderhoudswerkzaamheden die door of namens

de essentiële of belangrijke entiteit worden uitgevoerd. Onderhoudswerkzaamheden zijn noodzakelijk voor het correct functioneren van de netwerk- en informatiesystemen. Ook geplande onderbrekingen van de dienstverlening als gevolg van vooraf vastgestelde contractuele afspraken tussen partijen worden niet als een significant incident beschouwd. Deze bepaling geldt uitsluitend ten aanzien van de geplande gevolgen van de onderhoudswerkzaamheden. Indien tijdens of als gevolg van de geplande onderhoudswerkzaamheden ongeplande gevolgen ontstaan geldt deze bepaling niet. Zo kan bijvoorbeeld een incorrecte systeemupdate leiden tot een niet-voorziene uitval van netwerk- en informatiesystemen, met gevolgen voor de dienstverlening van de essentiële entiteit. In dat geval is sprake van een significant incident, indien tevens aan één of meer criteria van deze regeling wordt voldaan.

3. Gevolgen

De regeling codificeert de bestaande praktijk op veel vlakken. Op zichzelf geeft dat weinig directe gevolgen. Anders dan voorheen wordt het nu echter een wettelijke verplichting waarop ook toezicht en handhaving uitgevoerd kan worden. Dat betekent dat organisaties die voorheen minder aandacht hadden voor informatiebeveiliging en hierdoor mogelijk 'achterstallig onderhoud' hebben, een extra prikkel krijgen om de beveiliging in lijn te brengen met wat van een overheidsorganisatie verwacht mocht en mag worden. In de onderstaande subparagrafen wordt specifieker ingegaan op de verschillende verplichtingen die voor de entiteiten uit deze regeling volgen.

3.1 Zorgplicht

In de situatie voorafgaand aan de inwerkingtreding van deze regeling hadden alle overheidslagen (rijksoverheid, provincies, gemeenten en waterschappen) zich vanaf 2018 gecommitteerd aan de BIO. Het effect dat de BIO vervolgens heeft gehad is afhankelijk van de aard van de netwerk- en informatiesystemen in de verschillende overheidsorganisaties, omdat met de BIO risicomanagement als uitgangspunt werd genomen.
De eerdergenoemde ISO-standaarden die op informatiebeveiliging toezien, staan sinds 2008 op de Pas-toe-of-leg-uit lijst van het Forum Standaardisatie.[6] Deze standaarden zijn toegepast in de verschillende baselines die voorafgaand aan de vaststelling van de eerste versie van de BIO al per bestuurslaag waren opgesteld en zijn dus al geruime tijd in gebruik bij de verschillende overheidsentiteiten.
Voor de inschatting wat cruciale netwerk- en informatiesystemen binnen de sector overheid zijn, is de tabel met TBB's uit de Leidraad te beschermen belangen en de impacttabel die de IBD bij gemeenten toepast en die ook door enkele provincies worden gebruikt, als uitgangspunt genomen. Deze tabellen werden voorheen al gebruikt door overheidsorganisaties voor het inschatten van het belang van de systemen voor de organisatie op basis van de mogelijke impact die het niet-functioneren van een van deze systemen kan hebben.
Uit het voorgaande blijkt dat de gevolgen van de voorgeschreven verplichtingen uit de zorgplicht aldus beperkt zijn, omdat de entiteiten in de sector overheid de voorgeschreven instrumenten al toepasten. Met de Cbw en de lagere regelgeving worden wel enkele accenten aangebracht, maar deze vormen geen grote uitbreiding van de verplichtingen. Zo krijgen de bedrijfscontinuïteit, crisis(beheer) en de (toeleverings)keten meer aandacht dan in de voorgaande situatie. Daarnaast moeten beveiligde spraak-/tekst- en videoverbindingen en beveiligde noodcommunicatiesystemen worden ingezet wanneer gepast.[7] Samen met overheidsorganisaties wordt gekeken op welke manier zij ondersteuning nodig hebben op deze terreinen.

3.2 Meldplicht

De meldplicht is met name voor decentrale overheidsorganisaties nieuw. Organisaties van de rijksoverheid kenden over het algemeen reeds een meldplicht op basis van de Wet beveiliging netwerk- en informatiesystemen. Niettemin hebben alle overheidsorganisaties ook voorheen al te maken gehad met een meldplicht bij datalekken waar persoonsgegevens in het geding zijn. Tevens bevatte de BIO, waaraan overheidsorganisaties zichzelf reeds hadden gebonden, ook een paragraaf over incidentbeheer met een set maatregelen. In de drempelwaarden voor de meldplicht is om gevolgen voor overheidsorganisaties te beperken, zoveel mogelijk aangesloten bij de bekende systematieken binnen de rijksoverheid en bij gemeenten, die ze ook moeten gebruiken voor het inschatten van de cruciale netwerk- en informatiesystemen.

---

6 *Verkennend onderzoek NEN-ISO/IEC 27001 en 27002*, Forum Standaardisatie, 2014
7 *Mapping NIS2 en ISO 27002:2022/BIO2*, biooverheid.nl, 2024

3.3 Ondersteuning entiteiten

Bij het proces van totstandkoming van de Cbw en onderliggende regelgeving is er regelmatig contact geweest met alle overheidslagen, met als doel om wensen en knelpunten vanuit medeoverheden al in een vroeg stadium van het wetgevingsproces te betrekken. Dat is onder meer gebeurd via reguliere overleggen met de koepelvertegenwoordigers van de medeoverheden, vanuit het proces van de Uitvoerbaarheidstoets Decentrale Overheden (UDO) en de BIO governance. Zo is zoveel mogelijk aan de voorkant al gewaarborgd dat het wettelijk kader van de Cbw goed aansluit op de bestaande praktijk en het tot zo min mogelijk ongewenste gevolgen leidt.

Daarnaast ondersteunt BZK de medeoverheden met het voldoen aan deze verplichtingen via verschillende wegen. Zo biedt BZK aan alle overheidsorganisatie ondersteuning bij alle aspecten van informatiebeveiliging door middel van kennisdeling. Dit gebeurt met name via het Centrum Informatiebeveiliging en Privacy (CIP), die kennisproducten maakt en ter beschikking stelt. Voorbeelden zijn handreikingen die helpen bij de implementatie van de BIO of webinars en themabijeenkomsten over dit onderwerp. Ook organiseert BZK jaarlijks een overheidsbrede cyberoefening die organisaties helpt bij het organiseren van hun eigen incident- en crisisbeheer.

3.4 Bijdrage aan vermindering regeldruk in de toekomst

Reeds voorafgaand aan de onderhandelingen over de NIS2-richtlijn heeft het Ministerie van BZK met de verschillende bestuurslagen vanaf het voorjaar van 2019 ambtelijk overleg gevoerd om wetgeving voor te bereiden ter zake van de informatieveiligheid van de overheid.[8] Deze wetgeving moest een eerste stap zijn om een veelheid aan interbestuurlijke informatiebeveiligingseisen en toezicht daarop bij de medeoverheden te vereenvoudigen. Deze vereenvoudiging heeft als doel om de lastendruk en nalevingskosten bij medeoverheden, die zich nu vooral voordoen bij gemeenten, te verlagen. Het ENSIA-initiatief[9] is een goede illustratie van het verlagen van de lastendruk en wordt al een aantal jaar door gemeenten gebruikt voor hun geharmoniseerde verantwoording over informatiebeveiliging. Het verder brengen van deze harmonisering is bovendien als ambitie opgenomen in de Werkagenda Waardengedreven Digitalisering.[10] Bij het toezicht en de verantwoording over de Cbw is zoveel mogelijk aangesloten bij bestaande verantwoordingsmechanismen. Voor de gemeenten is dat, zoals hiervoor al aangegeven is, ENSIA. Daarnaast verkent het Ministerie van BZK of de ENSIA-methodiek in de toekomst ook in te zetten is voor verantwoording over de Cbw voor de andere bestuurslagen van de overheid.

De NIS2-richtlijn gaf de mogelijkheid om de eerste stap van deze ambitie versneld te realiseren. Hierover zijn de verschillende bestuurslagen formeel per brief geïnformeerd op 20 november 2023.[11] Bij het opstellen van lagere regelgeving onder de Cbw was, met het oog op het beperken van de lastendruk, het voornemen om voor medeoverheden maximaal gebruik te maken van bestaande verplichtingen. Voor de nadere invulling van de zorgplicht voor de overheid is daarom gebruikgemaakt van de herziene versie van de BIO, namelijk de BIO2, waaraan alle overheidslagen zich eerder hebben gecommitteerd.[12] De totstandkoming van de BIO2 heeft plaatsgevonden onder coördinatie van het Ministerie van BZK in samenwerking met alle bestuurslagen en is vervolgens vastgesteld in het OBDO van september 2025. Als onderdeel van deze vaststelling is aan het Ministerie van BZK het advies gegeven de BIO2 onderdeel te maken van de nadere regelgeving met betrekking tot de zorgplicht onder de Cbw. Volgende iteraties van de BIO2 zullen ook steeds opnieuw in afstemming met alle bestuurslagen onder coördinatie van BZK worden vormgegeven.

4. Toezicht en handhaving

De Rijksinspectie Digitale Infrastructuur (RDI) is, namens de Minister van BZK, de toezichthouder op de Cbw voor ministeries, gemeenten, provincies, gemeenschappelijke regelingen en zelfstandige bestuursorganen. Deze laatste twee categorieën voor zover zij voldoen aan de criteria voor overheidsinstanties uit de Cbw. Waterschappen vallen onder verantwoordelijkheid van het Ministerie van I&W en het toezicht van de ILT.

---

[8] Wetgeving werd al genoemd als mogelijk instrument in de *Eindrapportage Taskforce Bestuur & Informatieveiligheid Dienstverlening*, februari 2015.

[9] ENSIA is een initiatief van gemeenten, het Ministerie van BZK en Ministerie van Sociale Zaken en Werkgelegenheid. ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatiebeveiliging en informatiekwaliteit. Meer informatie is terug te vinden op www.ensia.nl.

[10] *Kamerstukken II* 2022/23, 26 643, nr. 940, bijlage 1062267, paragraaf 2.4.

[11] *NIS2 bij de overheid,* https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/nis2-bij-de-overheid-kamerbrief/.

[12] *Stcrt.* 2019, 26526.

Het toezicht heeft als doel te waarborgen dat overheidsorganisaties laten zien dat zij op basis van hun risicoprofiel voldoende weerbaar zijn tegen dreigingen en kwetsbaarheden. Dit is van belang omdat overheidsorganisaties een essentiële rol hebben in het maatschappelijk verkeer en in grote mate met gegevens van burgers omgaan. Het toezicht van de RDI gaat uit van maximale effectiviteit en een minimale toezichtslast voor organisaties. Om die reden sluit het toezicht aan op bestaande verantwoording van overheidsorganisaties, zowel de structuren, processen en rapportages die hiervoor bestaan. De RDI gebruikt informatie en data uit deze bestaande rapportages als basis voor haar beeldvorming van het verantwoordingsproces en de kwaliteit en volwassenheid van de digitale weerbaarheid van overheidsorganisaties. Op basis van die analyse kan de RDI zo nodig onderzoeken verrichten of eventueel gerichte nalevingsinspecties bij overheidsorganisaties doen. De RDI zet in op effectief toezicht met als doel om de kwaliteit en volwassenheid van de digitale weerbaarheid van de Nederlandse overheid te vergroten. De RDI heeft daarvoor een breed palet aan instrumenten om in te zetten, naast de wettelijke bevoegdheden, zoals het geven van voorlichting en guidance, het voeren van gesprekken met organisaties en ook signalering en bestuurlijke escalatie. Daarnaast beschikt de RDI ook over alle toezichts- en handhavingsbevoegdheden uit de Cbw, zie paragraaf 5.6 van de memorie van toelichting bij de Cbw voor een nadere uitwerking daarvan.

Voor de toezichtstaak is er bij de RDI een capaciteit van 15,65 fte beschikbaar. De jaarlijkse kosten worden ingeschat op 5 miljoen euro. Deze kosten worden gedragen door het Ministerie van BZK en worden gedekt vanuit artikel 6.2 van de rijksbegroting van BZK.

In het Besluit aanwijzing toezichthouders en verlening mandaat en machtiging Cyberbeveiligingswet is geregeld dat de RDI kan handhaven, welke ambtenaren daartoe bevoegd zijn en over welke bevoegdheden ze daarvoor beschikt.

5. Financiële gevolgen

Overheidsorganisaties zijn heel verschillend, om die reden is het zeer complex een inschatting te maken van kosten die met deze verplichtingen gepaard gaan. De ene organisatie zal vanwege zijn aard meer en/of andere maatregelen hebben getroffen dan de ander. De overheid kent reeds lang het uitgangspunt van risicogestuurd beveiligen: afhankelijk van het te beschermen belang en de dreiging wordt een afweging gemaakt welke maatregelen noodzakelijk zijn. Deze aanpak voorkomt te hoog ingeschatte kosten waar deze eigenlijk niet nodig zijn, maar ook te lage kosteninschattingen die niet toereikend blijken. Uitkomst van deze aanpak is dat organisaties zelf de kosten dragen voor beveiliging van hun systemen.

Een algemene inschatting van de kosten voor decentrale overheden is niet te maken. Kosten gerelateerd aan taken, diensten en voorzieningen bestaan voor ongeveer 85% uit taken in medebewind[13] waarvoor telkens eigen financiering is georganiseerd, ook voor de beveiliging ervan. Het kan voorkomen dat overheidsorganisaties niet voldoen aan bestaande verplichtingen die straks onder de Cbw gaan vallen, maar dat is generiek niet in te schatten. Ook worden de kosten om aan bestaande verplichtingen te voldoen niet betrokken, omdat men zich immers al aan die regels moest houden.

6. Advies en consultatie

Een ontwerp van deze regeling is tussen 11 november 2025 en 21 januari 2026 in consultatie geweest en in dat kader voorgelegd aan de Vereniging Nederlandse Gemeenten (VNG), het Interprovinciaal Overleg (IPO) en het Adviescollege Toetsing Regeldruk (ATR). Daarnaast heeft de RDI een uitvoerings- en handhavingstoets gedaan. Tot slot heeft in de periode van 11 november tot en met 23 december internetconsultatie plaatsgevonden. In deze paragraaf wordt ingegaan op een aantal aandachtspunten en wordt aangegeven hoe deze, waar mogelijk, zijn verwerkt in de regeling of de toelichting daarbij. Hiertoe is een onderverdeling gemaakt op basis van de verschillende onderwerpen.

6.1 Consultatie

6.1.1 Zorgplicht

Ten aanzien van de zorgplicht is zowel in de internetconsultatie als door de VNG en de IPO gevraagd om meer duidelijkheid te verschaffen over hoe de zorgplichtbepalingen in de artikelen 3 en 5 m.b.t. de ISO-standaarden en de BIO2 moeten worden toegepast, om die reden zijn er een aantal aanpassingen aangebracht in de artikelen 3 en 5 en de artikelsgewijze toelichting bij die artikelen, zodat het voor de essentiële entiteiten duidelijker wordt waar ze aan moeten voldoen.

[13] Zie bijvoorbeeld: *Lokale autonomie verder onder druk*, Binnenlands Bestuur, 2010.

Daarnaast is in een internetconsultatiereactie gevraagd om meer duidelijkheid over de verhouding tussen de ISO 27002 en de BIO. Meer specifiek gaat het om de vraag of de ISO 27002 voorgaat op de BIO2. Hiervan is geen sprake, de beide normen zijn complementair aan elkaar. De ISO 27002 geeft een aantal beheersmaatregelen, die moeten worden geoperationaliseerd in de organisatie. Voor een aantal van die beheersmaatregelen geeft de BIO2 vervolgens een verplichte invulling. Om die reden is er geen sprake van conflicten tussen beide normen en geldt geen eventuele voorrang van de ISO 27002 ten opzichte van de BIO2.

Vanuit Forum Standaardisatie is gevraagd om te verduidelijken dat het opnemen van beveiligingseisen in de afspraken met leveranciers, niet betekent dat de leveranciers dan ook alle normen die volgen uit de twee ISO-standaarden en de BIO2 verplicht moeten toepassen of zich daarvoor moeten certificeren. Entiteiten kennen inderdaad vanuit de BIO2 de verplichting om dit risicogedreven toe te passen. Er is daarmee geen verplichting om alle eisen die gelden voor de betreffende entiteit door te zetten naar de leverancier. Het gaat hierbij alleen om de eisen die relevant en nodig zijn om te komen tot passende en evenredige maatregelen voor het beheersen van het risico. Ook is er geen de facto verplichting tot het uitvragen van een certificering.

Ook zijn er verschillende reacties gekomen, onder meer vanuit de gemeente 's-Hertogenbosch en de G4-gemeenten, over de verplichting om de opzet, het bestaan en de werking van maatregelen aan te tonen. Dit kan voor sommige organisaties een uitdaging zijn, maar het is van groot belang om deze verplichting in stand te houden. Het toetsen van opzet, bestaan en werking van maatregelen geeft invulling aan het cyclisch proces van informatiebeveiliging, waarbij gevraagd wordt om de genomen maatregelen te beoordelen in het licht van de risicoanalyse van organisatie, en de maatregelen aan de hand daarvan zo nodig aan te passen. Bovendien volgt deze verplichting reeds vanuit het Cbb met betrekking tot de evaluatie van de doeltreffendheid van de maatregelen. Tot slot sluit deze benadering ook aan bij de BIO2. In dit licht is in de reacties ook gevraagd om het voorschrijven van een zeker assurance niveau. Het wordt op dit moment echter niet wenselijk geacht om een zeker assurance niveau te specificeren, gelet op het feit dat de implementatie van deze eis risicogedreven moet worden opgepakt.
Tevens wordt in een consultatiereactie het belang meegegeven dat opzet, bestaan en werking aantoonbaar zijn in het beheer van cyberrisico's. Dit volgt reeds uit artikel 21 van de Cbw waarin entiteiten worden gevraagd passende en evenredige maatregelen te nemen ten aanzien van de risico's voor hun netwerk- en informatiesystemen. Daarnaast vragen diverse artikelen uit het Cbb om het aantoonbaar toepassen van maatregelen en geeft artikel 18 van het Cbb de verplichting om maatregelen te evalueren.

Daarnaast is door de VNG gevraagd om een overheidsbrede norm voor rubricering van informatie. Hoewel het Ministerie van BZK de behoefte naar voren gebracht door de VNG onderschrijft, ziet zij hiertoe op dit moment niet de mogelijkheid onder de Cbw. Deze richt zich immers primair op de beveiliging van netwerk- en informatiesystemen en niet ook op de bescherming van 'papieren' informatie, terwijl dit voor een eenduidige classificatie en rubricering van informatie wel van belang is. Om die reden is een dergelijke wijziging niet doorgevoerd in deze regeling.

6.1.2 Meldplicht en inschatten cruciale netwerk- en informatiesystemen

Er zijn enkele vragen gesteld over de nadere definitie van 'essentiële diensten'. Zo was er enige verwarring over wat er bedoeld werd met deze definitie, vooral ook omdat het associaties oproept met het begrip kritieke dienst in de Wet weerbaarheid kritieke entiteiten (Wwke). Daarnaast bleek dat het inschatten op het niveau van diensten tot aanzienlijke uitvoeringslasten zou leiden, omdat de essentiële entiteiten hun eerdere inventarisaties met name op proces- en systeemniveau hadden uitgevoerd, wat tot gevolg zou hebben dat dergelijke inventarisaties opnieuw zouden moeten worden uitgevoerd voor deze regeling. Als reactie hierop is het begrip 'essentiële dienst' vervangen door 'cruciaal netwerk- en informatiesysteem'. Met het vervangen van het begrip 'essentieel' door 'cruciaal' wordt voorkomen dat er verwarring kan overstaan door overlap met begrippen uit andere wet- en regelgeving op het gebied van (digitale) weerbaarheid. Terwijl het begrip 'netwerk- en informatiesystemen' niet alleen beter aansluit op de terminologie van de Cbw en Cbb, maar tegelijkertijd ook op de eerder gemaakte inventarisaties door de betreffende essentiële entiteiten.

Ook zijn enkele vragen gesteld, onder meer vanuit de G4-gemeenten over de toepassing van de tabellen voor de meldplicht. Zo zouden enkele punten uit de impacttabel, opgenomen in bijlage 2 bij deze regeling, niet toepasbaar zijn voor decentrale overheden. De meldplichtsystematiek is daarop aangepast en bestaat nu louter uit drempelwaarden, gebaseerd op de tabel in bijlage 2, die kunnen worden toegepast door gemeenten. De tabel blijft echter wel van toepassing voor het identificeren van de cruciale netwerk- en informatiesystemen, waardoor ze nu louter een hulpmiddel zijn voor de inschatting van het belang van de netwerk- en informatiesystemen, in plaats van een meetbare drempelwaarde voor de meldplicht.

Daarnaast geeft de G4 aan voorkeur te hebben voor het aansluiten bij de eenduidige definities en terminologie, zoals die zijn opgenomen in de tabel voor de centrale overheid in bijlage 1. Omwille van het beperken van de regeldruk is ervoor gekozen om zoveel mogelijk bestaande methodieken bij overheidsorganisaties te gebruiken. Op termijn ligt het voor de hand om de samenhang tussen de criteria voor de centrale overheid en decentrale overheden te vergroten.

In de internetconsultatie is ook de vraag gesteld of deze ministeriële regeling een beperktere scope heeft dan de Cbw met betrekking tot de meldplicht voor incidenten die alleen potentieel en niet feitelijk de drempelwaarden kunnen overschrijden. Dit is niet het geval. De formulering 'leidt of kan leiden' in artikel 6, eerste en tweede lid, benadrukt dat het ook gaat om incidenten die potentieel, maar niet feitelijk, de drempelwaarden konden overschrijden.

Verder is in de internetconsultatie verzocht om bij de toepassing van de niveaus in de impacttabel consistent uit te gaan van de formulering 'ten minste hoog', zodat dit duidelijk is voor de entiteiten die een inschatting moeten maken van het impactniveau. De terminologie in artikel 4 en de artikelsgewijze toelichting is hierop aangepast, zodat de bepaling duidelijker maakt welke impactniveaus het betreft.

In de internetconsultatie is door de gemeente Gouda gevraagd of het onderscheid in de meldplicht tussen cruciale en niet-cruciale diensten ertoe kan leiden dat hetzelfde incident in de ene gemeente wel meldplichtig is en voor de andere niet. Naar aanleiding van de consultatie is er gekozen voor het opnemen van een integrale set aan meldplichtcriteria in artikel 6 van deze regeling. Toch blijft het wel het geval dat het ene incident in de ene gemeente wel tot een meldplichtig incident leidt, terwijl dat in de andere gemeente niet het geval is. Het kan namelijk voorkomen dat een incident op een netwerk- en informatiesysteem voor dienstverlening van de ene gemeente van cruciaal belang is, terwijl hetzelfde incident nauwelijks impact heeft op de andere gemeente.

Tevens zijn door de VNG enkele vragen gesteld over de impacttabel voor de drempelwaarden. Zo is verzocht om de impacttabel niet op te nemen in de regeling, maar om direct te verwijzen naar de brondocumentatie. Deze reactie is niet overgenomen, omdat er bij rechtstreekse verwijzing niet voldoende waarborgen zijn om de beschikbaarheid en de inhoud van de tabel te kunnen garanderen. Dit is onwenselijk in het kader van rechtszekerheid voor entiteiten. Bovendien geldt de inhoud van deze tabel niet alleen meer voor de gemeenten, maar voor alle decentrale overheden. Om die reden zijn er ten opzichte van de oorspronkelijke tabel enkele kleine aanpassingen gedaan zodat deze ook voor andere decentrale overheden toepasbaar is. Dit laat onverlet dat de tabel in de regeling gewijzigd kan worden als dat nodig blijkt te zijn.
Daarnaast is vanuit de VNG het verzoek gekomen om een gewijzigde versie van de impacttabel als bijlage 2 op te nemen, omdat de tabel die eerst in de regeling stond niet actueel meer was. Als reactie hierop is de nieuwe versie van de tabel alsnog opgenomen in deze regeling.

De gemeente 's Hertogenbosch heeft gevraagd om een gezamenlijke lijst met cruciale netwerk- en informatiesystemen voor gemeenten op te stellen aan de hand van de tabellen in de bijlage. Er is al een lijst met relevante processen beschikbaar. Deze lijst is opgesteld door de IBD en kan behulpzaam zijn bij het vaststellen van de cruciale netwerk- en informatiesystemen. In paragraaf 2.2 van de toelichting bij deze regeling wordt hier specifiek naar verwezen.

Het IPO heeft verzocht om nader toe te lichten vanaf welk moment de 72-uurstermijn voor het melden van significante incidenten gaat lopen. Deze termijn gaat lopen vanaf het moment dat het voor de essentiële entiteit duidelijk is dat een incident een significant incident is. Op basis hiervan is paragraaf 2.2 van de toelichting bij deze regeling aangevuld.

De VNG heeft daarnaast gevraagd om nader toe te lichten hoe de meldplicht werkt bij grootschalige incidenten en gaf hierbij aan dat coördinatie tussen CSIRT's, toezichthouders en ketenpartners nodig is. Entiteiten zijn verplicht om significante incidenten op hun netwerk- en informatiesystemen te melden. Deze meldingen komen terecht bij de CSIRT's en toezichthouders. Zowel de CSIRT's onderling, als de CSIRT's en toezichthouders hebben samenwerkingsafspraken om onderlinge samenwerking af te stemmen.

Door de gemeente 's-Hertogenbosch is aangegeven dat niet alle onderdelen van de drempelwaarden voor niet-cruciale diensten bekend zijn bij decentrale overheden, zoals drempelwaarde d) voor gerubriceerde informatie. Dit is correct, deze drempelwaarde is om die reden verwijderd uit artikel 6, tweede lid, van deze regeling.

6.1.3 Aanwijzing CSIRT

Enkele consultatiereacties, bijvoorbeeld van de G4-gemeenten, hebben gevraagd om nadere eisen te stellen voor het CSIRT zoals dit ook in de regelingen van andere sectoren wordt gedaan. De Minister

van Justitie en Veiligheid (J&V), in de praktijk het Nationaal Cyber Security Centrum (NCSC), zal het CSIRT zijn voor de sector overheid, waarvoor de aanwijzing en een aantal eisen daarbij al zijn vastgesteld in het Cbb met de mogelijkheid om bij lagere regelgeving nadere eisen te stellen. Op dit moment is dat vanuit specifiek de sector overheid niet nodig geacht.

Daarnaast werd gevraagd om in deze regeling ook de aanwijzing van de Minister van J&V als CSIRT voor de overige overheidsorganisaties te regelen. Deze aanwijzing is echter reeds gedaan in artikel 2, eerste lid, van het Cbb. Alleen het aanwijzen van een ander CSIRT dan de Minister van J&V kan per ministeriële regeling worden geregeld. Om dit verder te verduidelijken zijn enkele passages in de toelichting op de regeling aangevuld.

Door de G4-gemeenten is ook aangegeven dat als gemeenten zouden moeten aansluiten bij meerdere CSIRT's, dit interne gevolgen heeft, als er dan ook meerdere registraties nodig zijn en dus beheerd moeten worden. In reactie daarop kan worden aangegeven dat de registratie van de essentiële entiteit, ook al valt die onder meerdere CSIRT's, uniek en eenmalig is.

6.1.4 Toezicht en handhaving

Het IPO heeft verzocht om in deze regeling expliciet op te nemen dat de RDI de toezichthouder wordt en niet de ILT. Voor de sector overheid zal inderdaad de RDI, middels een aanwijzingsbesluit, worden aangewezen als toezichthouder voor de Cbw. Dit laat echter onverlet dat een essentiële entiteit vanuit de Cbw ook onder een andere sector kan vallen, met daarbij een eigen bevoegd gezag. Om die reden kan de betreffende vakminister ook een andere toezichthouder aanwijzen. Om dubbele lasten te voorkomen, zullen er op basis van artikel 55 van de Cbw afspraken worden gemaakt tussen de beide toezichthouders om dubbele toezichtslasten zo veel mogelijk te voorkomen.

De VNG heeft daarnaast enkele aandachtspunten genoemd bij de aanwijzing van een controlefunctionaris als mogelijk instrument dat door de toezichthouder kan worden gebruikt. Zo zou rekening moeten worden gehouden met kosten die hierdoor bij de essentiële entiteit terecht komen. Het instellen van een controlefunctionaris is een van de verschillende toezicht- en handhavingsinstrumenten die door de toezichthouder kan worden gebruikt. Uiteindelijk is het aan de toezichthouder om te bepalen in welke gevallen welk instrument passend is. Het is goed voorstelbaar dat ook de consequenties die deze handhavingsinstrumenten hebben voor de essentiële entiteit zelf, in deze afweging worden meegenomen.
Ook verzoekt de VNG om het toezicht op de gemeenten onder de Cbw en Wwke zoveel mogelijk te harmoniseren. De bedoeling is dat er door de verschillende toezichthouders samenwerkingsprotocollen worden opgesteld die ook expliciet het doel hebben om samenloop van toezicht, zowel met betrekking tot de verschillende sectoren onder de Cbw alsmede tussen de Cbw en de Wwke, zoveel mogelijk wordt voorkomen.

6.1.5 Overige punten uit de consultatie

Door onder meer de VNG is aandacht gevraagd voor de samenhang in regelgeving tussen verschillende sectoren. In de nadere uitwerking voor verplichtingen vanuit de Cbw is hier waar mogelijk rekening mee gehouden, zo is uitgebreid afgestemd tussen de Ministeries van BZK, I&W en Volksgezondheid Welzijn en Sport (VWS) om de betreffende regelingen zo veel mogelijk op elkaar aan te sluiten en conflicterende regels te voorkomen. Tegelijkertijd was het met het oog op beperken van de regeldruk door zoveel mogelijk aan te sluiten bij reeds bekende systematieken, zoals bijvoorbeeld de BIO2, onvermijdelijk dat er sectorale verschillen zouden ontstaan.

Ook geeft de VNG aan dat er behoefte is aan meer helderheid over hoe de verplichtingen in de praktijk samenkomen Om nader inzicht te krijgen in deze behoefte is door het CIP een uitvraag gedaan bij overheidsorganisaties. Op basis van de inzichten die hieruit voortkomen wordt samen met de bestuurslagen gekeken hoe hieraan invulling kan worden gegeven.

Door de VNG en IPO is ook gevraagd naar een ruime implementatietermijn voor het invoeren van verplichtingen om te voorkomen dat medeoverheden met sancties worden geconfronteerd. Als reactie hierop wordt het volgende aangegeven, in de praktijk zijn veel verplichtingen uit de Cbw reeds van toepassing op de overheid. Gemeenten gebruiken de BIO2 bijvoorbeeld ook al een langere tijd als richtinggevend kader. Daarnaast maken overheidsorganisaties onderdeel uit van verschillende bestuurlijke ketens, zowel met andere sectoren als met de centrale overheid, waarvoor geen mogelijkheid bestaat tot het kiezen voor een andere implementatietermijn. Omwille van de duidelijkheid geldt om die reden voor de gehele overheid hetzelfde moment van inwerkingtreding, gelijktijdig met de inwerkingtreding van de Cbw.

De VNG en het IPO geven aan bezorgd te zijn over de kosten die zij moeten maken om te voldoen aan

de Cbw. Volgens hen zouden extra uitvoeringskosten die zij moeten maken, moeten worden gedekt door de rijksoverheid in lijn met artikel 2 van de Financiële-verhoudingswet. Omwille van dit punt is in hoofdstuk 6, over de financiële gevolgen, nadere toelichting gegeven.

In de internetconsultatie is ook aangegeven dat de tabel in bijlage 1 op dit moment geen drempelwaarde kent voor het in bulk verwerken van persoonsgegevens en het verzoek daarbij is om dit alsnog op te nemen. Het uitgangspunt bij de keuze voor deze tabel ten behoeve van het vaststellen van de cruciale netwerk- en informatiesystemen is geweest om aan te sluiten bij bestaande instrumenten die zijn afgestemd met en worden gebruikt door de entiteiten die onder deze wet komen te vallen. Een eenzijdige wijziging daarvan in deze regeling, zonder een zorgvuldig afstemmingsproces, zou dat te niet doen. Wel is het zo dat een incident waarbij een dergelijke bulk aan persoonsgegevens zou uitlekken naar alle waarschijnlijkheid ook zou voldoen aan een van de andere criteria uit de tabel in bijlage 1.

6.1.6. Consultatiereacties die toezien op de Cbw of Cbb

In de consultatie van deze regeling zijn bovendien enkele opmerkingen geplaatst die strikt genomen niet toezien op deze regeling, maar waar in deze paragraaf kort op wordt gereageerd.

Door de VNG is de vraag gesteld om voor essentiële entiteiten in de sector overheid expliciet vast te leggen wie de normadressaat is van sancties, zoals de bestuurlijke boete. In de Cbw is steeds de essentiële of belangrijke entiteit de normadressaat van verplichtingen. Dat wil zeggen dat de verplichtingen rusten op de entiteit. Handhavend optreden zal zich dan ook in beginsel richten tot een entiteit. Voor een bestuurlijke boete is dan ook in artikel 80, eerste lid, Cbw neergelegd dat deze kan worden opgelegd aan een essentiële entiteit. Voor de handhaving van de Cbw gelden ook de algemene bepalingen over handhaving uit de Awb. Uit artikel 5:1, derde lid, Awb, gelezen in verbinding met artikel 51, tweede en derde lid, van het Wetboek van Strafrecht, volgt dat handhavend optreden zich ook kan richten tot degenen die tot de door de entiteit begane overtreding opdracht hebben gegeven en tegen degenen die feitelijke leiding hebben gegeven aan de verboden gedraging. Het kan hierbij gaan om bestuurders van de entiteit, maar ook om andere personen. Het enkele feit dat iemand bestuurder is van de entiteit, is onvoldoende om diegene als opdrachtgever of feitelijke leidinggevende (en dus als overtreder) aan te kunnen merken. In de rechtspraak is nadere invulling gegeven aan deze begrippen. Te verwachten valt dat slechts in uitzonderlijke gevallen gebruik zal worden gemaakt van de bevoegdheid om een handhavingsbesluit (ook) te richten tot een opdrachtgever of feitelijke leidinggevende. Een uitzondering op het voorgaande vormen de in artikel 24, tweede tot en met zesde lid, Cbw neergelegde verplichtingen om te beschikken over voldoende kennis en vaardigheden en om deel te nemen aan een training. Bij deze verplichtingen zijn de individuele leden van het bestuur de normadressaten. Handhavend optreden bij het niet nakomen van die verplichtingen zal zich dan ook richten tot de individuele bestuurder. Dit is ook neergelegd in de artikelen 92 en 93 Cbw.

De VNG heeft ook de opmerking gemaakt dat het onwenselijk is dat bestuurlijke boetes onverkort gelden bij de inwerkingtreding, aangezien gemeenten tijd nodig hebben om te kunnen voldoen aan de verplichtingen uit de Cbw. Hiermee bestaat volgens hen het risico dat zij reeds beboet worden terwijl zij nog bezig zijn met het implementeren van verplichtingen. Deze boeteverplichting geldt voor alle entiteiten die onder de Cbw vallen. Die hebben te maken met dezelfde implementatietermijn als overheidsinstanties. Het zou om die reden onwenselijk zijn om onderscheid te maken tussen verschillende sectoren. Bovendien gebruiken de toezichthouders het toezicht met als doel ervoor te zorgen dat organisaties weerbaarder worden. Sancties zijn hierin geen doel op zich.

Eveneens wordt door onder meer de VNG en IPO de oproep gedaan om vanuit het Ministerie van BZK een coördinerende rol te pakken met betrekking tot de wildgroei van trainingen die zijn ontstaan met deze verplichting in de Cbw. Naar aanleiding van dit verzoek lopen gesprekken tussen het Ministerie van BZK en de verschillende bestuurslagen. Het voornemen is om gezamenlijk te kijken naar een invulling voor de training. Overheidsorganisaties staat het vervolgens vrij om aan de hand van deze informatie zelf de opleiding aan te bieden, de Cbw en het Cbb laten hier immers de ruimte toe, of de opleiding extern in te kopen.

6.2 Advies ATR

Het ATR heeft op 18 december 2025 haar advies uitgebracht ten aanzien van deze regeling. Het ATR geeft in haar advies het dictum ‘vaststellen nadat met de adviespunten rekening is gehouden’. In deze deelparagraaf wordt nader toegelicht hoe is omgegaan met de genoemde adviespunten.

Het ATR adviseert ten eerste om de afweging van beleidsalternatieven, bijvoorbeeld om lichtere of gefaseerde maatregelen voor kleinere overheidsorganisaties, of differentiatie naar risico of omvang en benutting van bestaande structuren te hanteren.

De differentiatie naar risico waar het ATR in haar advies naar verwijst, is expliciet onderdeel van de Cbw en onderliggende regelgeving, waaronder deze regeling. Organisaties dienen passende en evenredige maatregelen te nemen om de gelopen risico's voor hun informatiebeveiliging af te dekken. Het bepalen welke maatregelen passend en evenredig zijn, is afhankelijk van de risico-inschatting van de organisatie zelf. Dat betekent dat organisaties die minder risico's lopen, bijvoorbeeld omdat hun dreigingsniveau lager ligt of dat zij vanwege hun grootte minder belangrijke netwerk- en informatiesystemen hebben, minder ingrijpende maatregelen hoeven te nemen. Organisaties die grotere belangen hebben om te beschermen, of te maken hebben met grotere dreigingen, zullen dientengevolge meer maatregelen moeten nemen.

In lijn met het advies van het ATR, is bij de nadere uitwerking van de zorgplicht zoveel mogelijk aangesloten bij reeds bestaande structuren, instrumenten en kaders, zoals de BIO2 en de ISO 27001 en ISO 27002. Dit om de lasten voor overheidsorganisaties zoveel mogelijk te beperken. Dit is nader uitgewerkt in paragraaf 2.1 van deze toelichting.

Wat betreft de suggestie om in kaart te brengen of lichtere of gefaseerde maatregelen voor kleinere overheidsorganisaties mogelijk zouden zijn, kan worden aangegeven dat de BIO2 bewust één benadering voor de gehele overheid hanteert. Overheidsorganisaties wisselen immers in hoge mate onderling gegevens uit. Door één kader te hanteren met een minimaal niveau of ondergrens aan beveiligingsmaatregelen kan beter binnen ketens van overheden worden afgestemd. Bovendien zorgt dit voor administratieve lastenverlichting bij overheid en bedrijven, zowel afnemers als leveranciers, doordat er voorspelbare en uniforme beveiligingsvoorschriften bij de overheid gelden.

Het ATR adviseert ten tweede toe te lichten welke onderdelen rechtstreeks uit Europese verplichtingen komen en welke nationaal zijn ingevuld. Daarbij dient gemotiveerd te worden dat geen sprake is van nationale koppen.
In deze ministeriële regeling worden de volgende Europese verplichtingen uitgewerkt: het voorschrijven van passende en evenredige maatregelen voor de beveiliging van netwerk- en informatiesystemen (artikel 21 van de NIS2-richtlijn) en het vaststellen van criteria voor de meldplicht van significante incidenten (artikel 23 van de NIS2-richtlijn). Hierbij is geen sprake van nationale koppen, omdat het niet meer vormt dan een nadere uitwerking van de verplichtingen uit de NIS2-richtlijn. Door dit nader uit te werken, wordt meer duidelijkheid geboden aan de sector over wat er van ze wordt verwacht. Daarnaast sluiten we daarmee zoveel mogelijk aan bij bestaande instrumenten die in samenspraak met de betreffende overheidsentiteiten zijn vastgesteld en waarvan al gebruik wordt gemaakt. Dat gaat onder meer over de invulling van de zorgplicht via de BIO.

Het ATR adviseert ten derde om inzichtelijk te maken welke alternatieven er zijn overwogen in de informatie-uitvraag aan leveranciers. Zij stellen vragen over hoe de hoe de informatie-uitvraag aan leveranciers wordt ingericht, hoe uniformiteit wordt geborgd en welke organisatorische en technische lasten hierbij voor leveranciers wordt verwacht.
Vanuit de NIS2-richtlijn en de implementatie daarvan in de Cbw is de primaire verantwoordelijkheid voor het afdichten van risico's voor de netwerk- en informatiesystemen bij de entiteit gelegd. Dat geld ook voor de risico's die zich vanuit de leverancierskete bij de entiteit bevinden. Het is aan de entiteit om de afweging te maken om bepaalde taken of diensten van de entiteit al dan niet uit te besteden en onder welke condities dit gebeurt. Het is vervolgens aan leveranciers om te bepalen of zij in willen gaan op de condities die door de entiteit worden gesteld. Het is ook mogelijk dat ondanks genomen maatregelen bij leveranciers een restrisico overblijft voor de entiteit. De entiteit is uiteindelijk verantwoordelijk voor het besluit of dit overgebleven restrisico aanvaardbaar is, deze is immers verantwoordelijk voor de genomen maatregelen. De nadere invulling van de Cbw laat geen ruimte om anders om te gaan met deze verplichting voor entiteiten ten opzichte van hun leveranciers.
In de nadere uitwerking van deze verplichting in deze regeling is bewust gekozen voor aansluiting bij bestaande instrumenten die reeds door de overheid worden gehanteerd richting hun leveranciers zoals de ISO 27001, ISO 27002 en de BIO2. Dit zorgt voor zo veel mogelijk duidelijkheid en consistentie voor de betreffende leveranciers. Ook het hanteren van één kader zoals de BIO2 voor zowel afnemers als leveranciers binnen de overheid en het bedrijfsleven draagt bij aan die voorspelbaarheid en uniformiteit van beveiligingsnormen voor leveranciers.

Het ATR adviseert tot slot de regeldruk in kaart te brengen volgens de Rijksbrede methodiek, specifiek ziet dat op de eisen die via de implementatie bij overheidsorganisaties gevolgen hebben voor de leveranciers. Zoals in de alinea hiervoor aangegeven, is gekozen voor het aansluiten bij bestaande instrumenten die al door overheidsorganisaties werden gehanteerd richting hun leveranciers. Om die reden is de verwachting niet dat dit tot aanvullende regeldruk voor leveranciers leidt. Entiteiten kunnen desondanks besluiten om op basis van hun eigen risico-inschatting aanvullende eisen richting hun leveranciers te stellen. De regeldruk die hiermee gepaard gaat, is afhankelijk van de implementatie door entiteiten zelf en om die reden is er op basis van de Rijksbrede methodiek geen eenduidige uitwerking van te maken.

6.3 Toezichts- en handhavingstoets RDI

De RDI heeft in december 2025 een uitvoerbaarheids- en handhaafbaarheidstoets (UHT) uitgevoerd op het concept van deze regeling. In deze UHT geven zij aan het conceptvoorstel uitvoerbaar, handhaafbaar en fraudebestendig te achten, mits genoemde aandachtspunten nader worden verduidelijkt dan wel aangepast in deze regeling. In deze deelparagraaf wordt nader toegelicht hoe is omgegaan met de aandachtspunten die in de UHT naar voren zijn gebracht door de RDI.

Als eerste aandachtspunt vraagt de RDI om een verduidelijking van de relatie tussen de voorgeschreven ISO-standaarden en de BIO2 in verhouding tot de Cbw en de Cbb. Het gaat hier om de vraag of het toepassen van de beide normenkaders volstaat om te voldoen aan de zorgplicht in de Cbw en Cbb. De maatregelen uit de ISO standaarden en BIO2 geven een nadere uitwerking van de zorgplichtvereisten uit de Cbw en Cbb. Zij dekken in principe alle onderwerpen af die benoemd zijn in de Cbw en het Cbb. Wel wordt benadrukt dat het eenmalig implementeren van deze maatregelen niet altijd voldoende is om te voldoen aan de zorgplicht. De zorgplicht vereist namelijk ook dat entiteiten deze maatregelen continu aanpassen aan hun risico's, die kunnen wijzigen door bijvoorbeeld veranderingen in het dreigingslandschap of de organisatiecontext. Het is aan de entiteit om zich hierover te kunnen verantwoorden richting de toezichthouder. Deze verhouding is nader verduidelijkt in de artikelsgewijze toelichting bij artikel 5 van deze regeling.

Als tweede aandachtspunt vraagt de RDI of met de verwijzing naar de NEN-EN-ISO/IEC 27001:2023 en NEN-EN-ISO/IEC 27002:2022 ook verwezen wordt naar eventuele aanvullingen of nieuwere versies van deze norm of dat het gaat om een verwijzing naar een specifieke versie. Volgens hen bestaat door dat laatste het risico dat hierdoor de invulling van de zorgplicht achterloopt ten opzichte van de actualiteiten.
De verwijzingen naar de beide ISO-standaarden en naar de BIO2 betreffen statische verwijzingen naar een specifieke versie. Dat betekent dat een wijziging van de ISO-standaarden en de BIO2 niet automatisch leidt tot een verplichting van nieuwe versies of aanvullingen. In plaats daarvan zal er altijd een wijziging moeten worden aangebracht in deze regeling om die nieuwe versie van toepassing te laten zijn. Zo wordt gegarandeerd dat een wijziging van de inhoud van deze regeling altijd plaatsvindt nadat hier een weloverwogen besluit over is genomen. Wanneer een nieuwe versie van de ISO-standaard beschikbaar is, waar deze regeling nog niet op is aangepast en een essentiële entiteit wil deze nieuwe versie gaan toepassen is dat toegestaan, zolang dit niet leidt tot een lager beveiligingsniveau. Dit is nader verduidelijkt in de artikelsgewijze toelichting bij artikel 5 van deze regeling.

Als derde aandachtspunt geeft de RDI aan dat mogelijk interpretatieverschillen kunnen ontstaan door de formulering in artikel 3 van deze regeling, omdat de formulering van deze regeling en de NEN-EN-ISO/IEC 27001:2023 ten aanzien van de managementsystematiek van elkaar zouden verschillen.
Er is echter geen verschil van interpretatie of formulering tussen de twee onderdelen. Deze regeling geeft de verplichting om de NEN-EN-ISO/IEC 27001:2023 toe te passen op het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsystematiek voor de beveiliging van netwerk- en informatiesystemen, in de norm ISMS genoemd. NEN-EN-ISO/IEC 27001:2023 geeft weer welke eisen gesteld kunnen worden aan deze managementsystematiek. Het blijft voor organisaties mogelijk om aanvullend op de NEN-EN-ISO/IEC 27001:2023 organisatiespecifieke eisen op te nemen in de managementsystematiek.

Als vierde aandachtspunt geeft de RDI aan dat met het dwingend voorschrijven van de NEN-EN-ISO/IEC 27001:2023 de suggestie kan worden gewekt dat een certificering voldoende is om aan deze verplichting te voldoen.
Het afgeven van een certificering kan een indicatie zijn voor de toezichthouder over de volwassenheid van de informatiebeveiliging van de entiteit, bijvoorbeeld ten aanzien van de inrichting van hun managementsystematiek. Tegelijkertijd geldt vaak voor certificering dat deze op basis van een momentopname wordt gegeven. Zoals eerder in deze paragraaf aangegeven, dienen entiteiten passende en evenredige maatregelen te nemen. Dat doen zij op basis van een risico-inschatting die kan wijzigen, bijvoorbeeld als gevolg van veranderingen in het dreigingslandschap of de organisatiecontext. Een certificering voor deze ISO-norm hoeft dus niet te betekenen dat daarmee aangetoond is dat het beveiligingsniveau voldoende is.

Als vijfde aandachtspunt geeft de RDI aan het niet duidelijk is hoe de tekst van artikel 5, eerste lid, van deze regeling – die de ISO 27002 en de BIO2 dwingend voorschrijft – zich verhoudt tot de tekst die toestaat om de beheersmaatregelen van de ISO 27002 en de BIO2 door andere normen te vervangen. Deze reactie is overgenomen en verwerkt in de artikel 5, waarin nu expliciet is opgenomen dat waar dat noodzakelijk is en het beveiligingsniveau gelijkwaardig blijft, gebruik mag worden gemaakt van andere normenkaders voor informatiebeveiliging.

Als zesde aandachtspunt vraagt de RDI om kosteloze beschikbaarstelling van de beide voorgeschre-

ven ISO-standaarden. Voor deze ISO-standaarden geldt dat ze rijksbreed worden ingekocht en zodoende voor de essentiële entiteiten die onder de sector overheid vallen vrij beschikbaar zijn.

Met betrekking tot het identificeren van de cruciale netwerk- en informatiesystemen wordt door de RDI in haar aandachtspunt aangegeven dat hierdoor het risico ontstaat dat de essentiële entiteiten zich bij het nemen van maatregelen om te voldoen aan de zorgplicht zullen beperken tot enkel deze cruciale netwerk- en informatiesystemen, terwijl dat niet de bedoeling is van de zorgplicht.
Het is inderdaad niet de bedoeling dat de essentiële entiteiten alleen maatregelen nemen voor de geïdentificeerde cruciale netwerk- en informatiesystemen. Het identificeren van deze netwerk- en informatiesystemen is in plaats daarvan juist bedoeld om een goede inschatting te kunnen maken van de risico's voor deze systemen. Als een netwerk- en informatiesysteem niet cruciaal blijkt te zijn, kan dat dus gevolgen hebben voor de mate van beveiliging die daarvoor benodigd is, maar dat betekent niet dat er geen maatregelen hoeven te worden genomen voor niet-cruciale netwerk- en informatiesystemen voor het voldoen aan de zorgplicht. Dit is nader uitgewerkt in paragraaf 2.2 van deze toelichting.

Als achtste aandachtspunt geeft de RDI aan dat de delegatiegrondslag in het Cbb voor het vaststellen van de criteria voor het melden van significante incidenten geen ruimte biedt voor het verplichten van het bijhouden van een overzicht van cruciale netwerk- en informatiesystemen.
Het is inderdaad het geval dat artikel 23, eerste lid, van het Cbb geen grondslag biedt voor het verplichten van het bijhouden van een overzicht van cruciale netwerk- en informatiesystemen. Dit vormt echter een nadere invulling van de verplichting om een managementsystematiek voor de beveiliging van netwerk- en informatiesysteem te hebben, waarvan het inschatten van de risico's voor de netwerk- en informatiesystemen, door middel van een risicoanalyse, deel uitmaakt.
De impactcriteria van de tabellen in de beide bijlagen bij deze regeling, op basis waarvan wordt ingeschat wat een cruciaal netwerk- en informatiesysteem is, kunnen daarentegen wel gezien worden als drempelwaarden voor het bepalen of een incident als significant te gelden heeft.

Als negende aandachtspunt wordt gevraagd of de meldplichtcriteria die genoemd staan in artikel 6 van deze regeling uitputtend zijn.
Dat is inderdaad het geval en naar aanleiding van deze reactie is dat verduidelijkt in de artikelsgewijze toelichting bij dat artikel.

Als tiende aandachtspunt geeft de RDI aan dat het niet voor alle TBB's duidelijk is hoe deze onder de definitie van een significant incident vallen.
Op basis van de consultatie is een nieuwe versie gemaakt van de meldplichtbepaling met een kortere lijst aan drempelwaarden die voldoen aan de criteria voor het vaststellen van een significant incident, bedoeld in artikel 25, tweede lid, van de Cbw.

De RDI geeft in haar elfde aandachtspunt aan dat artikel 25, eerste lid, van de Cbw heeft bedoeld om ook incidenten als significant aan te wijzen wanneer deze ook daadwerkelijk tot de genoemde schade leiden. De RDI ziet graag dat ook die incidenten worden toegevoegd aan artikel 6, eerste en tweede lid, van deze regeling om in lijn te blijven met de bepaling uit de Cbw.
De laatste versie van de meldplichtbepaling is daarop in lijn gebracht met de criteria uit artikel 25, tweede lid, van de Cbw.

Het laatste aandachtspunt van de RDI ziet op de artikel 6, derde lid, van deze regeling, waarin een uitzondering op de meldplicht is opgenomen als het gaat om geplande onderbrekingen van de dienst of geplande onderhoudswerkzaamheden. De RDI verzoekt om deze bepaling te beperken tot verwachte gevolgen van dergelijke onderbrekingen en onderhoudswerkzaamheden. Per abuis was deze bepaling inderdaad niet beperkt tot de door de essentiële entiteit verwachte gevolgen van geplande onderbrekingen van de dienst of geplande onderhoudswerkzaamheden. Het is heel wel mogelijk dat een dergelijke geplande onderbreking alsnog kan leiden tot onverwachte gevolgen die een significant incident kunnen vormen. Om die reden is dat in artikel 6, derde lid, alsnog aangevuld.

7. Inwerkingtreding

Deze regeling geeft nadere regels onder de Cbw en de Cbb. Om die reden treedt deze regeling op hetzelfde moment als de Cbw en Cbb in werking.

ARTIKELSGEWIJZE TOELICHTING

Artikel 1

Op grond van artikel 1 van de Cbw en artikel 1 van het Cbb zijn de in die artikelen genoemde begrips-

bepalingen ook van toepassing op deze regeling. In artikel 1 van deze regeling wordt een aantal begrippen omschreven, die specifiek voor deze regeling van belang zijn.

Artikel 2

Deze bepaling beperkt de reikwijdte van deze regeling tot de essentiële entiteiten die vallen onder de sector overheid, bedoeld in bijlage 1 bij de Cbw, met uitzondering van de waterschappen, waarvoor de Minister van I&W de bevoegde autoriteit is.

Artikel 3

Dit artikel verplicht de essentiële entiteit om de ISO 27001:2023 toe te passen op het formuleren van eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsystematiek voor beveiliging van informatie in netwerk- en informatiesystemen. Hiermee wordt bedoeld dat de managementsystematiek van de essentiële entiteit moet voldoen aan de eisen uit deze standaard. Ook moet deze standaard worden toegepast op het vaststellen van het toepassingsgebied van de managementsystematiek. Doorgaans zal een dergelijk managementsystematiek ook zien op beveiliging van informatie buiten netwerk- en informatiesystemen, gelet op de scope van de Cbw en lagere regelgeving, beperkt dat zich in deze regeling tot netwerk- en informatiesystemen.

De verwijzing naar deze ISO-standaard betreft een statische verwijzing naar een specifieke versie. Dat betekent dat een wijziging van deze standaard niet automatisch leidt tot het verplicht worden van de nieuwe versie onder deze regeling. In plaats daarvan zal er altijd een wijziging moeten worden aangebracht in deze regeling om die nieuwe versie van toepassing te laten zijn. Zo wordt gegarandeerd dat een wijziging van de inhoud van deze regeling altijd plaatsvindt nadat hier een weloverwogen besluit over is genomen. Indien een nieuwe versie van de ISO-standaard beschikbaar is, maar deze regeling hierop nog niet is aangepast en een essentiële entiteit wil deze nieuwe versie toepassen, dan is het gebruik daarvan mogelijk, mits dit niet leidt tot een lager beveiligingsniveau dan de in deze regeling voorgeschreven versie.

Artikel 4

Deze bepaling verplicht essentiële entiteiten om hun cruciale netwerk- en informatiesystemen te identificeren en daarvan een overzicht bij te houden als onderdeel van de managementsystematiek voor de beveiliging van netwerk- en informatiesystemen, bedoeld in artikel 6, vierde lid, van het Cbb.

In het tweede en derde lid wordt onderscheid gemaakt tussen essentiële entiteiten van de centrale overheid en de decentrale overheid met betrekking tot wat onder een cruciaal netwerk- en informatiesysteem wordt verstaan. Hierbij wordt gebruikgemaakt van tabellen die zijn opgenomen als bijlage 1 en bijlage 2 bij deze regeling. Deze tabellen zijn gebaseerd op de tabel die is opgenomen in de Leidraad te beschermen belangen (subsector centrale overheid), respectievelijk de impacttabel die is uitgegeven door de IBD (subsector decentrale overheden).
Daarmee kan worden bepaald wat de verwachte gevolgen zijn bij een incident dat betrekking heeft op het betreffende netwerk- en informatiesysteem.

De essentiële entiteiten in de subsector centrale overheden inventariseren hun cruciale netwerk- en informatiesystemen op basis van het tweede lid, aan de hand van de tabel opgenomen in bijlage 1. Deze tabel geeft in de eerste rij een aantal categorieën met gevolgen, zoals politieke schade of schade aan staat en samenleving. Vervolgens wordt per kolom een niveau aangegeven waaronder een bepaalde waarde, bijvoorbeeld een bepaald bedrag of een rubriceringsniveau, per categorie gevolgen wordt gehangen. Daarvoor zijn vijf kolommen opgenomen: geen niveau en TBB 4 tot en met 1. Hoe lager het getal van het TBB-niveau is, des te groter is het te beschermen belang van een dergelijk netwerk- en informatiesysteem.
Een netwerk- en informatiesysteem van een essentiële entiteit in de subsector centrale overheden is cruciaal als die binnen ten minste één van de categorieën, bijvoorbeeld ‘schade aan vitale belangen van de staat of de samenleving’, voldoet aan een drempelwaarde van ten minste niveau TBB 3 (d.w.z. TBB 3, TBB 2 of TBB 1). Als bijvoorbeeld in de categorie letselschade sprake is van het voldoen aan TBB 3 en in de rest van de categorieën gaat het om TBB 4, dan is er niettemin sprake van een cruciaal systeem, omdat in ieder geval in één categorie gevolgen de drempelwaarden overschreden wordt. Als er sprake is van schades op verschillende niveaus geldt dat dus uitgegaan dient te worden van de categorie gevolgen die de hoogste impact heeft.

De essentiële entiteiten in de subsector decentrale overheden inventariseren hun cruciale netwerk- en informatiesystemen, op basis van het derde lid, aan de hand van de tabel opgenomen in bijlage 2. Deze tabel geeft in de eerste rij een aantal categorieën met gevolgen, zoals maatschappelijke impact of letsel. Vervolgens wordt per kolom een impactniveau aangegeven waaronder een bepaalde waarde,

bijvoorbeeld een bedrag of een rubriceringsniveau, per categorie gevolgen wordt gehangen. Daarvoor zijn vijf kolommen opgenomen: Zeer laag, Laag, Middel, Hoog en Zeer hoog.
Een netwerk- en informatiesysteem van een essentiële entiteit in de subsector decentrale overheid is cruciaal is indien het systeem impactniveau 'Hoog' of 'Zeer hoog' van de tabel in bijlage 2 bij deze regeling heeft. Als bijvoorbeeld in de categorie financiële impact sprake is van het voldoen aan niveau 'Hoog' en de rest van de categorieën gevolgen betreft het niveau 'Laag', dan is er niettemin sprake van een cruciaal netwerk- en informatiesysteem, omdat de gevolgen van het incident in ten minste één categorie van de impacttabel de drempelwaarde overschrijden. Indien sprake is van schades op verschillende impactniveaus dient dus uitgegaan te worden van de categorie gevolgen die de hoogste impact heeft.
In de categorieën waar ook een passage is opgenomen over het 'effect op burgergerichte processen', bijvoorbeeld de categorie diplomatieke schade of significant verlies van motivatie bij medewerkers, hoeft niet aan beide genoemde situaties voldaan te zijn. Niet alle decentrale overheden zullen immers te maken hebben met burgergerichte processen. Om in die betreffende categorie te vallen is het voldoende dat wordt voldaan aan de eerste alinea van de betreffende categorie.

Artikel 5

Eerste lid

De kern van de zorgplicht is het komen tot een passende set aan maatregelen die de risico's die zijn geïnventariseerd afdoende beheersen. Artikel 5, eerste lid, verplicht essentiële entiteiten tot het gebruikmaken van de beheersmaatregelen van de ISO 27002:2022 voor het formuleren van passende maatregelen voor de beveiliging van netwerk- en informatiesystemen, bedoeld in artikel 21, eerste lid, van de wet. De beheersmaatregelen uit de ISO 27002 moeten risicogedreven toegepast worden, dat volgt uit de verplichting om deze ISO-standaard te gebruiken voor 'het formuleren van passende en evenredige maatregelen'. Dit is waartoe de ISO-standaard zelf ook verplicht. Dat impliceert dat het noodzakelijk is dat een essentiële entiteit aanvullende maatregelen treft als het risico daarom vraagt, om die reden is de verplichting opgenomen dat ze 'ten minste' deze ISO-standaard moeten toepassen. Tegelijkertijd betekent de risicogedreven benadering ook dat toepassing van bepaalde beheersmaatregelen achterwege gelaten kan worden als het risico beperkt is of als de betreffende beheersmaatregel niet relevant is, omdat de essentiële entiteit bijvoorbeeld niet beschikt over bepaalde systemen waar een beheersmaatregel op ziet.
Ingevolge het eerste lid omvatten deze passende en evenredige maatregelen ten minste de relevante overheidsmaatregelen van de Baseline Informatiebeveiliging Overheid 2, versie 1.3 (Stct. 2026, 7416). Deze overheidsmaatregelen uit de BIO2 komen niet "bovenop" de ISO-beheersmaatregelen, maar vormen een gedeeltelijke invulling van de passende en evenredige maatregelen die geformuleerd moeten worden op basis van de ISO 27002. Essentiële entiteiten dienen deze overheidsmaatregelen te implementeren ongeacht het ingeschatte risico. Dit betreft echter wel een minimale invulling, waar het risico groter is, zullen meer passende en evenredige maatregelen moeten worden genomen. Als een BIO2-overheidsmaatregel niet toe te passen is, omdat de essentiële entiteit bijvoorbeeld niet beschikt over een systeem waarop deze maatregel ziet, kan het gebruik van die overheidsmaatregel achterwege worden gelaten. Om die reden is in de tweede zin van het eerste lid de formulering 'de voor haar relevante overheidsmaatregelen' opgenomen.

Met het eerste lid wordt de toepassing van deze standaarden vastgelegd, voor zover zij zien op de beveiliging van netwerk- en informatiesystemen. Deze beperking is noodzakelijk, omdat deze standaarden in principe zien op informatiebeveiliging in bredere zin, inclusief bijvoorbeeld informatie die op papier staat. Dit valt buiten de reikwijdte van de NIS2-richtlijn en daardoor ook van de Cbw en de daarop gebaseerde regelgeving. Toepassing ervan kan dus niet in deze regeling worden verplicht.

Enkele beheersmaatregelen uit de ISO 27002 en overheidsmaatregelen uit de BIO2 vallen buiten de reikwijdte van de Cbw. Toepassing daarvan kan en wordt daarom in deze regeling niet verplicht gesteld. Een voorbeeld hiervan is een beheersmaatregel die ziet op de bescherming van intellectuele-eigendomsrechten. Dit is een onderwerp dat de Cbw niet regelt. Het eerste lid voorziet daarom in een expliciete uitzondering van deze beheers- en overheidsmaatregelen. In de BIO2 is dit voor de uitgezonderde overheidsmaatregelen duidelijk gemaakt door middel van het aanbrengen van een vetgedrukte tekstmarkering. Voor de uitgezonderde beheers- en overheidsmaatregelen blijft wel de verplichtende zelfregulering van toepassing die voor de gehele BIO2 geldt. Deze verplichting staat echter los van de Cbw.

De verwijzingen naar de ISO 27002:2022 en de Baseline Informatiebeveiliging Overheid 2, versie 1.3 (Stct. 2026, 7416) betreffen statische verwijzingen naar een specifieke versie. Dat betekent dat een wijziging niet automatisch leidt tot het verplicht worden van de nieuwe versie onder deze regeling. Om een nieuwe versie van deze standaarden van toepassing te laten zijn, zal eerst een wijziging in deze regeling moeten worden aangebracht. Zo wordt gegarandeerd dat een wijziging van de materiële

eisen die op grond van deze standaarden worden gesteld aan de entiteit altijd plaatsvindt nadat hier een weloverwogen besluit over is genomen. Indien een nieuwe versie van een standaard beschikbaar is, maar deze regeling hierop nog niet is aangepast en een essentiële entiteit wil deze nieuwe versie toepassen, dan is dat mogelijk, zolang dit niet leidt tot een lager beveiligingsniveau.

Tweede lid

Op basis van het tweede lid kunnen de beheersmaatregelen uit de ISO 27002 en de overheidsmaatregelen uit de BIO2 worden vervangen door of gecombineerd met beheersmaatregelen uit andere normenkaders voor informatiebeveiliging. Hierbij kan worden gedacht aan de NEN 7510 voor zorginformatie en de CSIR en IEC 62443 Industriële cybersecurity voor OT. De essentiële entiteit dient wel aannemelijk te maken dat het vervangen door of combineren met andere passende en evenredige maatregelen noodzakelijk is en dat deze maatregelen een gelijkwaardig beveiligingsniveau bieden.

Derde lid

De verplichting in het derde lid voor de essentiële entiteit om te zorgen voor aantoonbaarheid van opzet, bestaan en werking van maatregelen geldt voor alle netwerk- en informatiesystemen. Daarbij is er ruimte om deze aantoonbaarheid risicogedreven vorm te geven als onderdeel van de operationalisering van de beheersmaatregelen. De controle op en aantoonbaarheid van opzet, bestaan en werking van de maatregelen ter bescherming van netwerk- en informatiesystemen die het meest cruciaal zijn of waar de hoogste dreiging voor geldt, dient het strengste te zijn. Voor netwerk- en informatiesystemen met een laag risicoprofiel is het toegestaan deze controle minder uitgebreid in te vullen. De wijze waarop deze controle wordt ingevuld, moet kunnen worden onderbouwd met een risicoafweging. Indien de entiteit gebruik heeft gemaakt van andere passende en evenredige maatregelen, geldt naast de bovenstaande verplichting om de opzet, bestaan en werking aan te tonen, ook de verplichting om de noodzakelijkheid en gelijkwaardigheid van de andere normen en richtlijnen aantoonbaar te maken. Dit wordt aangetoond in de Verklaring van Toepasselijkheid.

Hoe de maatregelen zijn geoperationaliseerd, moet via verwijzingen worden vastgelegd, bijvoorbeeld in een beleids- of ontwerpdocument. Hiermee toont de essentiële entiteit de ‘opzet’ van maatregelen aan. Al dan niet met behulp van externe partijen of via self-assessments, audits, pentesten, redteamtesten en dergelijke toont de essentiële entiteit het ‘bestaan’ en de ‘werking’ van maatregelen aan. Met bestaan wordt bedoeld dat de maatregelen daadwerkelijk zijn geïmplementeerd, met werking wordt bedoeld dat de organisatie aantoont dat de maatregelen effectief zijn.

Artikel 6

Met dit artikel worden de drempelwaarden voor significante incidenten bedoeld in artikel 25, tweede lid van de Cbw geregeld. Door het toetsen van een incident aan de in deze regeling opgenomen criteria voor significante incidenten wordt volledig en uitputtend invulling gegeven aan de parameters die zijn opgenomen in artikel 25, tweede lid, van de Cbw.

Het eerste lid stelt deze drempelwaarden vast met betrekking tot de netwerk- en informatiesystemen van entiteiten in de subsector centrale overheden. Deze zijn gebaseerd op een aantal van de criteria uit de Leidraad te beschermen belangen die zijn opgenomen in bijlage 1 bij deze regeling.

De verplichting tot het melden van incidenten die leiden of kunnen leiden tot de uitval van de dienstverlening van de essentiële entiteit van ten minste vier uur, bedoeld in het eerste lid, onder a, komt ook voort uit deze bestaande methodiek. Onder de quickscan BIR, onderdeel van de tabel in bijlage 1, is uitval van systemen tot vier uur geoorloofd voor systemen die als ‘zeer hoog’ (ZH) worden geclassificeerd. In de tabel is te zien dat bij de categorie betrouwbaarheidseisen quickscan BIR het scoren van ten minste één van de aspecten op ZH, valt onder TBB 3. Daarbij is van belang dat het gaat om uitval van dienstverlening van de entiteit. Ondersteunende werkzaamheden, denk aan de uitval van de website van het bedrijfsrestaurant, zullen naar alle waarschijnlijkheid geen impact hebben op de dienstverlening van de entiteit en vallen zodoende niet onder deze drempelwaarde.

De drempelwaarde voor financiële schade aan de staat of de samenleving, bedoeld in het eerste lid, onder b heeft betrekking op schade die als gevolg van het incident op het betreffende netwerk- en informatiesysteem niet zozeer direct ten laste komt van de eigen begroting, maar wel een vast te stellen impact heeft op de rest van de staat of de samenleving.

De derde drempelwaarde in het eerste lid, onder c, is de ernstige verwonding of de dood van een natuurlijke persoon. Hierbij kan worden gedacht aan een datalek met persoonsgegevens van personeel van de rijksoverheid met een verhoogd veiligheidsrisico, dat tot gevolg heeft of kan hebben dat geweld tegen dat personeel wordt gebruikt. Een dergelijk incident dient gemeld te worden als er

redelijkerwijs vermoed kan worden dat er een causaal verband bestaat tussen het incident en de eventuele verwonding of de dood van een natuurlijke persoon of dat het aannemelijk is dat een incident potentieel zou kunnen leiden tot de betreffende gevolgen.

De drempelwaarde voor misbruik van bedrijfsinformatie in het eerste lid, onder d, ziet toe op financiële schade die direct ten laste komt van de eigen begroting. Voorbeelden daarvan zijn het verlies van persoonsgegevens of het lekken van gevoelige informatie van bedrijven, zoals intellectueel eigendom, waarvoor de essentiële entiteit rechtens aansprakelijk wordt of kan worden gesteld. Met de term misbruik wordt niet alleen kwade opzet bedoeld, maar elk ongeoorloofd gebruik van de informatie op de netwerk- en informatiesystemen.

Met de drempelwaarde in het eerste lid, onder e, wordt de kennisname door onbevoegden van informatie die door de essentiële entiteit is gekwalificeerd op basis van de rubriceringsniveaus van de rijksoverheid, vastgelegd in het VIR-BI, of informatie die wordt gedeeld vanuit de EU of de NAVO en daar al van een rubriceringsniveau is voorzien, gekwalificeerd als een significant incident, als het voldoet aan respectievelijk de niveaus Staatsgeheim CONFIDENTIEEL, EU-CONFIDENTIAL en NATO CONFIDENTIAL of een hoger niveau. Deze niveaus vormen alle drie het op een na laagste niveau van rubricering binnen het eigen stelsel en zijn met name bedoeld voor informatie waarvan de ongeoorloofde kennisname de vitale belangen of *essential interests* van de Nederlandse Staat, de EU of de NAVO kan schaden.

Met het tweede lid worden de drempelwaarden voor significante incidenten bedoeld in artikel 25, tweede lid van de Cbw, uitputtend geregeld voor de subsector decentrale overheden. De specifieke drempelwaarden die hierin zijn opgenomen komen voort uit de impacttabel van gemeenten die is opgenomen als bijlage 2 bij deze regeling.

Een tweetal van deze drempelwaarden, uitval van ten minste vier uur en de ernstige verwonding of de dood van ten minste één natuurlijke persoon (tweede lid onder a en c) komen overeen met de drempelwaarden die gelden voor de centrale overheden en dienen op dezelfde wijze te worden toegepast.

Wat betreft financiële schade, bedoeld in het tweede lid, onder b, is als drempelwaarde opgenomen dat de financiële gevolgen niet meer opgevangen kunnen worden binnen de eigen begroting van de betreffende essentiële entiteit. Die keuze is gemaakt vanwege het feit dat de decentrale overheden in grootte en daarmee ook in financiële capaciteit behoorlijk van elkaar verschillen, zo is de gemeente Amsterdam bijvoorbeeld vele malen groter dan de gemeente Schiermonnikoog. Als gevolg daarvan zou een vast bedrag als drempelwaarde voor de ene entiteit veel te laag zijn en voor de ander juist veel te hoog. Om die reden is uitgegaan van financiële gevolgen die aanpassing van de begroting vereisen, waardoor andere voorgenomen keuzes in de begroting noodgedwongen niet door kunnen gaan. Als de financiële impact van het incident daarentegen gedragen kan worden door bijvoorbeeld een reserve voor onverwachte uitgaven, is er geen sprake van een significant incident.

Met de formulering ‘leidt of kan leiden’, opgenomen in zowel de aanhef van het eerste als tweede lid, wordt bedoeld dat dat het niet alleen gaat om de situatie waarin de gevolgen van het incident zich daadwerkelijk voordoen, maar ook om de situaties waarin die drempelwaarden mogelijk gehaald kunnen worden. De verplichte inschatting of systemen cruciaal zijn of niet, aan de hand van de tabellen uit bijlage 1 en 2, kan voor die laatste situatie behulpzaam zijn. De inschatting van het systeem als cruciaal op basis van gelijksoortige criteria geeft immers aanleiding om ervan uit te gaan dat een incident dezelfde mogelijke impact heeft.

Het derde lid zondert geplande gevolgen, zoals bij gepland onderhoud of testen, uit van de meldplicht. Zie voor een nadere toelichting paragraaf 2.2 van deze toelichting.

Artikel 7

Dit artikel regelt de inwerkingtreding van deze regeling. De regeling treedt tegelijkertijd met de Cbw en het Cbb in werking.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
E. van der Burg