

## Reacties van de inzagepartijen op de conceptrapportage *Beveiliging van meldkamersystemen*. Wederhoortabel 1/2

Nr.	Inzagepartij	Hoofdstuk/ paragraaf	Te corrigeren tekst (eerste...laatste woord)	Argumentatie/onderbouwing van uw reactie	Reactie Inspectie JenV
1	JenV	1.2	<i>Het Strategisch Meldkamer Beraad (SMB) is verantwoordelijk voor het aansturen van de LMS op het beheer van de risico's in de informatiebeveiliging.</i>	<p>De rol van het SMB wordt niet juist en overeenkomstig de Ministeriële Regeling Hoofdlijnen Beleid en Beheer (MR HBB) weergegeven in het rapport.</p> <p>Het SMB is niet verantwoordelijk voor de aansturing van de LMS, maar bewaakt de uitvoering van het beleids- en bestedingsplan van de meldkamers. Zie artikel 4. lid 5 HBB: Het SMB draagt zorg voor het opstellen van het beleids- en bestedingsplan en de jaarverantwoording op landelijk niveau; beslist binnen de kaders van het beleids- en bestedingsplan over de uitvoering van beleid en beheer; bewaakt de uitvoering van het beleids- en bestedingsplan;</p> <p>LMS fungeert als secretaris van het SMB en draagt zorg voor het opstellen van de agenda.</p>	<p>De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.</p> <p>Het SMB is op grond van artt. 2 en 4 lid 1 van de <i>Regeling Hoofdlijnen beleid en beheer meldkamers verantwoordelijk</i> voor de aansturing van de LMS. Het SMB is daarmee verantwoordelijk voor het beheer van de risico's in de informatiebeveiliging.</p> <p>Art. 4 lid 5 van de regeling beschrijft hoe het SMB deze aansturing moet uitvoeren: Het Strategisch Meldkamer Beraad verzamelt de inbreng voor het beleids- en bestedingsplan; draagt zorg voor het opstellen van het beleids- en bestedingsplan en de jaarverantwoording op landelijk niveau; beslist binnen de kaders van het beleids- en bestedingsplan over de uitvoering van beleid en beheer; bewaakt de uitvoering van het beleids- en bestedingsplan; doet voorstellen voor de agenda van het Bestuurlijk Meldkamer Beraad; adviseert het Bestuurlijk Meldkamer Beraad; kan hulpstructuren instellen, die bijdragen aan het realiseren van de</p>

					vastgestelde kaders voor beleid en beheer.
2	JenV	1.2	<i>In 2021 bleek opnieuw dat de continuïteit van de meldkamers nog niet goed geborgd is 2.</i>	<p>Deze constatering “opnieuw” wekt de indruk dat dit “opnieuw” gebaseerd is op onderzoek bij meldkamers. Dit is niet het geval.</p> <p>De Inspectie heeft in 2019 gekeken met een onderzoek naar de continuïteit meldkamers. In 2021 heeft zij een observatie gedaan.</p>	<p>De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.</p> <p>Uw mening hierover is bij de Inspectie bekend, zoals verwoord in <i>Reactie opvolging aanbevelingen onderzoek continuïteit meldkamers</i> van 4 juni 2021. De Inspectie heeft verschillende middelen om tot vaststelling te komen. De annotatie verwijst naar de documenten waarin de vaststelling is beschreven.</p>
3	JenV	1.2, blz5	<i>De systemen van de meldkamers worden beveiligd door de Landelijkemeldkamersamenwerking (LMS).</i>	<p>De LMS is verantwoordelijk voor het Beheer van de meldkamersystemen en de beveiliging van het Beheer. De beveiliging van het gebruik ligt bij de disciplines.</p> <p>De disciplines blijven zelf verantwoordelijk voor het eigen IB beleid en de invulling daarvan.</p> <p>In de regeling hoofdlijnen beleid en Beheer staat: artikel 2 lid 2b de informatieveiligheid van de meldkamers en meldkamerfuncties voldoet aan de wettelijke kaders en aan de van toepassing zijnde normen van de partijen.</p>	<p>De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.</p> <p>Artikel 2 lid 2 onder b beoogt dat de LMS de zogeheten meldkamervoorzieningen beheert, hierin gestuurd door het SMB middels het Beleids- en bestedingsplan. Tot deze meldkamervoorzieningen behoren de meldkamersystemen zoals bedoeld in deze rapportage. Deze voorzieningen faciliteren de meldkamerfuncties. Het wettelijk kader en de voornaamste normen voor informatiebeveiliging van de partijen maken deel uit van het toetsingskader van dit onderzoek. Het wettelijk kader en de normen gaan terug op de norm ISO/IEC 27001 en 27002 en</p>

					<p>27005. <i>De Baseline informatiebeveiliging overheid (BIO)</i> baseert zich op de uitgangspunten van de voornoemde ISO-normen.</p> <p>Het is bij de Inspectie bekend dat de disciplines zelfstandig informatiebeveiliging toepassen. Het betreft hier systemen die binnen het meldkamerdomein tot de meldkamerfunctie worden gerekend. Deze worden in het meldkamerdomein los gezien van de meldkamersystemen die de LMS als meldkamervoorziening beheert. De informatiebeveiliging van deze meldkamerfuncties valt buiten de scope van dit onderzoek, zoals beschreven in paragraaf 1.4.</p>
4	JenV	Voetnoot9, blz 6	<i>Het ministerie JenV hanteert een driehoeksturingmodel waarin wordt gesproken over eigenaar, opdrachtgever en opdrachtnemer. In dit driehoeksturingmodel is de Secretaris-generaal eigenaar van de systemen C2000, GMS, NL-Alert en WAS</i>	De staat der Nederlanden, minister van JenV is eigenaar van de systemen C2000, GMS, NL-Alert, WAS en NCV. Op basis van welke bron constateert de Inspectie dat sprake is van een driehoeksturingmodel?	De Inspectie neemt uw voorstel over in de rapportage. Formulering van deze voetnoot is aangepast.
5	JenV	1.4	<i>Anderzijds biedt het inzicht in de aansturing van het SMB als verantwoordelijke voor het beheer van de risico's in de informatiebeveiliging.</i>	Het SMB is niet verantwoordelijk voor de aansturing van de LMS, maar bewaakt de uitvoering van het beleids- en bestedingsplan van de meldkamers. Zie artikel 4. lid 5 HBB: Het SMB draagt zorg voor het opstellen van het beleids- en	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.
					De minister van JenV heeft de taken ten behoeve van de landelijke strategische sturing op het beleid en beheer aan het SMB

				bestedingsplan en de jaarverantwoording op landelijk niveau; beslist binnen de kaders van het beleids- en bestedingsplan over de uitvoering van beleid en beheer; bewaakt de uitvoering van het beleids- en bestedingsplan;	opgedragen. Zie de opmerkingen bij 1 en 3.
6	Vz SMB	1.4 pag5	<i>Dit onderzoek..... de Regeling hoofdlijnen beleid en beheer meldkamers, het Voorschrift informatiebeveiliging rijksdienst, de Baseline informatiebeveiliging overheid (BIO) en de standaarden ISO/IEC 27001, 27002 en 27005.</i>	Dit is breder dan het wettelijk kader in de regeling beleid en beheer. Daar staat: 'de informatieveiligheid van de meldkamers en meldkamerfuncties voldoet aan de wettelijke kaders en aan de van toepassing zijnde normen van de partijen;' (artikel 2.2.lidb).	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage. Het betreft hier het wettelijk kader. De formulering van de passage is ter verduidelijking aangepast.
7	Vz SMB	1.4,pg 6	<i>SMB als verantwoordelijke voor hetbeheer van de risico's in de informatiebeveiliging.</i>	Dit wijkt af/is breder met wat in 1.2 staat: SMB als verantwoordelijke voor het aansturen van de LMS op het beheer van de risico's in de informatiebeveiliging	De Inspectie neemt uw voorstel over in de rapportage. Formulering is aangepast.
8	Vz SMB	1.5 pag7	<i>De bevindingen .... de directeur/lidvan het SMB... herkend</i>	De directeur LMS is geen lid van het SMB (zie regeling beleid en beheer), de directeur treedt op als adviseur	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.  De Inspectie neemt kennis van uw uitleg van de <i>Regeling hoofdlijnen beleid en beheer meldkamers</i> , maar vindt in de Regeling geen redelijke onderbouwing voor een voorbehoud voor de directeur LMS als adviseur van het SMB. Temeer omdat de directeur LMS en de plv. directeur LMS op de website van de LMS in het overzicht 'aansturing en overlegorganen' zonder voorbehoud als

					onderdeel van het SMB staan beschreven. De samenstelling van het SMB zoals gepubliceerd in overzicht 'Aansturing en overlegorganen' is niet transparant en lijkt niet compliant met art. 4 lid 2 van de <i>Regeling hoofdlijnen beleid en beheer meldkamers</i> .
9	Veiligheidsregio's	2.1 pg.8	<i>De uitwerking van de beveiligingsafspraken is in handen van de Werkgroep Informatiebeveiliging Meldkamers die is samengesteld uit, .... en de LMS.</i>	De werkgroep stelt alleen kaders en houdt toezicht op de voortgang van activiteiten. De uitwerking vindt plaats in 'oplosgroepen'.	De Inspectie neemt uw voorstel over in de rapportage. Formulering is aangepast.
10	Vz SMS	2.1, pg 9	<i>De Inspectie concludeert dat het SMB de beveiliging van de meldkamersystemen ten tijde van het onderzoek nog niet aanstuurt op basis van risicomanagement.</i>	Dit is onjuist. Vier maandelijks is de landelijke continuïteitsmonitor besproken, waarin risico's benoemd en geduid zijn. Deze monitor is op 2 februari en 7 juli besproken  Deze conclusie verhoudt zich niet tot de taak, zoals deze is beschreven in 1.2 HBB. Het SMB is verantwoordelijk voor het aansturen van de LMS op het beheer van de risico's. Het sturen op de beveiliging van de meldkamersystemen is een zaak van de organisatie LMS en niet van het SMB. Het SMB beperkt zich tot het bewaken of er sprake is van een werkend risicomanagementsysteem bij de LMS. ISO/IEC 270055 gaat uit van een organisatie als actor. De opstellers van het rapport zien	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.  De Inspectie waardeert het dat het SMB een landelijke continuïteitsmonitor hanteert. Het probleem is echter dat deze monitor niet/onvoldoende is gebaseerd op risicomanagement dat tot stand is gekomen zoals bedoeld in de ISO/IEC 27005. Het SMB loopt hiermee een te groot risico door te sturen op een onvolledig beeld van de informatieveiligheid van de meldkamersystemen. Dit is een te groot risico omdat de meldkamersystemen onderdeel zijn van de landelijke vitale infrastructuur en de dreiging van het opzettelijk verstoren van systemen toeneemt zoals beschreven in paragraaf 1.1. Zie ook 10 wederhoortabel Politie.

				<p>vervolgens het SMB als organisatie en verbinden daar conclusies aan. Het SMB is geen organisatie en kan als zodanig niet gezien worden als actor.</p> <p>In de verwachting pg.8 staat dat de verwachting is dat het SMB toeziet dat de meldkamer-systemen zijn beveiligd op basis van het risicomanagement en de LMS daarop aanstuurt. De conclusie haalt deze rollen door elkaar. Hiervoor is al aangegeven dat het SMB wel degelijk toezicht houdt; zie de voorbeelden en dat zij aanstuurt op basis van risicomanagement.</p>	<p>Het SMB is bij <i>Regeling Hoofdlijnen beleid en beheer</i>, art. 4 lid 1 ingesteld als bestuursorgaan, met de taak om te sturen op het beleid en beheer. Uw argument dat het SMB niet als actor kan worden gezien is daarmee niet valide.</p>
11	JenV	2.2. blz11	<p><i>Het directoraat-generaal Politie en Veiligheidsregio's van het ministerie van JenV neemt het standpunt in dat de verantwoordelijkheden voor het beheer van de voorzieningen juist welhelder zijn vastgelegd in de Wijzigingswet meldkamers, de Regeling hoofdlijnen beleid en beheermeldkamers (2020) en de Ministeriële regeling C2000 (concept).</i></p>	<p>Het gaat hier om een verschil in inzicht in de interpretatie van de taak van de LMS op basis van de regeling hoofdlijnen beleid en beheer meldkamers. JenV vindt dat de LMS op basis van deze regeling Toelichting onder 2 van de Hoofdlijnen Beleid en Beheer meldkamers. Hier staat: De Landelijke Meldkamer Samenwerking ondersteunt de partijen en neemt daarbij initiatief om de samenwerking te stimuleren, zodat de betrokken partijen gezamenlijk komen tot goed ingerichte en functionerende meldkamers waar de partijen hun meldkamerfunctie kunnen uitoefenen.</p> <p>Op basis hiervan verwacht JenV een regiefunctie voor de LMS op</p>	<p>De Inspectie neemt uw voorstel over in de rapportage.</p>

				het gebied van informatiebeveiliging.	
12	JenV	2.2	<i>Het ministerie gaf in het gesprek aan dat het hierover met de LMS in gesprek wil. Het ministerie biedt aan om hen bij te staan in het maken van de vertaalslag.</i>	Deze tekst suggereert dat de LMS en JenV hierover geen contact/gesprek hebben, terwijl dit bijvoorbeeld onderwerp van gesprek is in de werkgroep IB. Tekstvoorstel: Het ministerie is hierover in gesprek met de LMS.	De Inspectie neemt uw voorstel over in de rapportage. Formulering is aangepast.  De Inspectie beschrijft hier een open en oplossingsgerichte gesprekshouding van JenV naar de LMS. De Inspectie waardeert het dat JenV en de LMS hierover (inmiddels) in gesprek zijn.
13	MinJenV	2.2	<i>Conclusie</i>	De conclusie van de inspectie over het toepassen en borgen van risicomanagement is uitsluitend beschreven vanuit het niet volledig doorlopen van processtappen.  De Inspectie gaat niet in op hoe het ontstaan is vanuit het verleden. Een feit is dat het risicomanagement al geruime tijd niet op orde is, op zowel operationeel, tactisch als strategisch niveau. Een voorbeeld voor C2000 is dat tijdens de Vernieuwing alleen de technische infrastructuur is vervangen.  Een conclusie die nog niet benoemd is door de inspectie is dat processen inclusief risicomanagement voor IB reeds beschikbaar hadden moeten zijn en ingezet moeten worden voor de herziening van IB risico's.	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.  De Inspectie waardeert de opstelling van het ministerie van JenV dat het erkent dat risicomanagement al geruime tijd niet op orde is, op zowel operationeel, tactisch als strategisch niveau.  De Inspectie ondersteunt uw bevinding dat processen inclusief risicomanagement voor de informatiebeveiliging reeds beschikbaar hadden moeten zijn en ingezet moeten worden voor de herziening van risico's op het gebied van informatiebeveiliging.  Het doel van dit onderzoek is het bespreekbaar maken van de informatieveiligheid van de meldkamersystemen en daarmee aan de continuïteit van de meldkamers. Het rapport beschrijft

				<p>Dit wordt onderbouwd door het overzicht Geraadpleegde documenten: uit dit overzicht en dan vooral de jaartallen van de documenten blijkt dat informatiebeveiliging en de daarvoor vereiste beleid en risicoanalyses al geruime tijd blijven liggen, op niveau van LMS, SMB en Min JenV.</p>	<p>daarom de noodzaak en de actualiteit om de meldkamersystemen op de voorgeschreven wijze te beveiligen, en dat deze noodzaak ook langer bekend is.</p>
14	MinJenV	2.4	<p><i>"Van het SMB wordt verwacht dat het maatregelen kiest voor risicobeperking, dat het deze maatregelen vaststelt en dat het de LMS aanstuurt op het uitvoeren van deze maatregelen."</i></p>	<p>De inspectie zegt hier dat door het SMB moet worden uitgevoerd:</p> <ul style="list-style-type: none"> <li>- Het inrichten en borgen van risicomangement</li> <li>- Het beoordelen van de risico's</li> <li>- Het kiezen en vaststellen van risicobeperkende maatregelen</li> <li>- Het vaststellen en aanvaarden van restrisico's</li> </ul> <p>Alleen de uitvoering van de maatregelen en beheer van restrisico's liggen dan formeel bij LMS.</p> <p>Deze aanbeveling verhoudt zich niet tot de rol van het SMB zoals vastgelegd in regeling HBB zie ook eerder opmerkingen zoals opmerking 5.</p>	<p>De Inspectie neemt uw argument en onderbouwing ten dele over in de rapportage. Formulering is aangepast.</p> <p>Sturing op de inrichting en borging van de informatiebeveiliging behoort tot de hoofdtaak van het SMB, zoals beoogd in de Regeling Hoofdlijnen beleid en beheer. (Zie hiervoor de opmerkingen bij 1 en 3 en 5.) Daar hoort ook bij dat het SMB maatregelen kiest voor risicobeperking, dat het deze maatregelen vaststelt en dat het de LMS aanstuurt op het uitvoeren van deze maatregelen.</p> <p>Het kiezen van maatregelen dient door het SMB te worden ingevuld door het sturen op het kiezen van maatregelen voor risicobeperking en het beheer van de restrisico's. Zaak is dat het SMB zijn verantwoordelijkheid blijft nemen op de aansturing zoals bedoeld in art 4 lid 1 en 5 van de Regeling Hoofdlijnen beleid en beheer. De uitvoering van de</p>



					maatregelen en beheer van rest-risico's liggen formeel bij LMS, maar het betreft hier een uitvoeringsverantwoordelijkheid.
15		Bijlage pag 22	<i>Het Strategisch Meldkamer Beraad (SMB) vervult een centrale rol in de aansturing van de samenwerkende meldkamers<sup>28</sup>.</i>	De bijlage is een onjuiste vertaling van de governancestructuur zoals vastgelegd in de HBB. Het SMB heeft geen verantwoordelijkheid in de aansturing van de samenwerkende meldkamers. Het SMB vervult een centrale rol in de beleidsvorming voor het landelijk beleid en beheer van de meldkamers en houdt toezicht op de Uitvoering van het beleid- en bestedingsplan en adviseert het BMB.	De Inspectie neemt uw voorstel ten dele over in de rapportage. Formulering aangepast.  Het SMB vervult een centrale rol in landelijke strategische sturing op het beleid en beheer van de meldkamers. Het SMB verzamelt de inbreng voor het beleids- en bestedingsplan; draagt zorg voor het opstellen van het beleids- en bestedingsplan en de jaarverantwoording op landelijk niveau; beslist binnen de kaders van het beleids- en bestedingsplan over de uitvoering van beleid en beheer; bewaakt de uitvoering van het beleids- en bestedingsplan; doet voorstellen voor de agenda van het Bestuurlijk Meldkamer Beraad; adviseert het Bestuurlijk Meldkamer Beraad; en kan hulpstructuren instellen, die bijdragen aan het realiseren van de vastgestelde kaders voor beleid en beheer.
16		Bijlage 2	<i>Aansturing van de LMS:</i>	In de bijlage II wordt de aansturing beschreven obv een vertaling van de regeling HBB. Is dit stukergens vastgesteld dat de aansturing van de LMS zo verloopt? Obv dit stuk worden de verwachtingen geformuleerd: 2.1 verwachting Het SMB werkt....	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.  Deze tekst is in de bijlage opgenomen om lezers buiten het meldkamerdomein op hoofdlijnen inzicht te geven in de aansturing van de meldkamers, met het doel om beter inzicht te krijgen

In HBB Artikel 2 lid 3 staat echter: De Landelijke Meldkamer Samenwerking voert het beheer\* van de meldkamers uit volgens de in de [artikelen 3, 4 en 5](#) opgenomen multidisciplinaire sturingslijnen met inachtneming van de in dit artikel opgenomen beleidsdoelen en beleidskaders.

Artikel 4 lid 1: Er is een Strategisch Meldkamer Beraad ten behoeve van de landelijke strategischesturing op het beleid en beheer van de meldkamers.

Obv aangereikt beleid en kaders (B&B) voert LMS beheer uit (tactisch en operationeel) en daarmee stuurt het SMB dit aan strategisch aan; worden doelen behaald, welke maatregelen worden genomen etc.

De vertaling van de zienswijze zoals nu in bijlage II staat beschreven lees je door het hele document terug en daarmee wordt de bevinding niet op het juiste niveau geadresseerd.

\*beheer: facilitaire dienstverlening, huisvesting, inrichting, onderhoud en ontwikkeling van gemeenschappelijke ICT-voorzieningen ten behoeve van de meldkamers en het ICT-beheer ten behoeve van de meldkamerfuncties;

in de problemen bij het inrichten en borgen van de informatiebeveiliging.

De formulering was ontleend aan het overzicht 'Aansturing en overlegorganen' gepubliceerd op de website van de LMS, zoals vermeld op de website van de LMS ten tijde van het onderzoek. De voetnoot verwijst naar dit overzicht. Zie ook 1.

17	Veiligheidsregio's	Bijlage 2, pg.22	<i>De meldkamers worden bestuurd, ...Brandweer Nederland en de Nationale Politie.</i>	<p>De brandweer is onderdeel van de veiligheidsregio's, derhalve kan Brandweer Nederland worden verwijderd.</p> <p>De meldkamers worden niet bestuurd. Meldkamers zijn volgens artikel 25a Politiewet fysieke plaatsen; daar is geen sprake van besturing. De meldkamerfuncties in een meldkamer worden bestuurd door directieteams (hoofdlijnen beleid en beheer, artikel 5). De disciplines zijn verantwoordelijk voor de meldkamerfunctie in hun verzorgingsgebied; de LMS voor het goed functioneren van de meldkamer en ICT.</p>	<p>De Inspectie neemt uw voorstel over in de rapportage. Formulering is aangepast.</p> <p>Voor de disciplines en de meldkamerfunctie verwijst ik u naar de opmerking bij 3.</p>
18	Vz SMB	Bijlage 2	<i>In zijn geheel</i>	<p>Uit deze bijlage blijkt niet hoe de LMS aangestuurd wordt. De LMS komt in de hele tekst niet voor en in deze bijlage ontbreekt de verhouding van de LMS tot de Nationale Politie (waaronder MDC).</p>	<p>De Inspectie neemt uw voorstel ten dele over.</p> <p>Zie 16 en 17. Uit de gesprekken met medewerkers van het MDC blijkt dat MDC bijdraagt aan de beveiliging van de meldkamersystemen. Functioneel zijn de medewerkers onderdeel van de LMS. Zowel MDC als LMS maken deel uit van de Nationale politie. Het doel van deze rapportage is om de borging en de inrichting van de meldkamersystemen bespreekbaar te maken. Het vermelden van deze details is niet dienstbaar om lezers buiten het meldkamerdomein inzicht te geven, temeer omdat de</p>

					LMS deze details ook in het gepubliceerde overzicht 'Aansturing en overlegorganen' op haar website achterwege laat.
19	Vz SMB	Bijlage 2	<i>De meldkamers ....Nationale politie</i>	Dit is onjuist. Meldkamers zijn volgens artikel 25a Politiewet fysieke plaatsen; daar is geen sprake van besturing. Daarnaast: de meldkamersfuncties in een meldkamer worden bestuurd door directieteams, zie regeling beleid en beheer, artikel 5. De disciplines zijn verantwoordelijk voor de meldkamerfunctie in hun verzorgingsgebied; de LMS voor het goed functioneren van de meldkamer en ICT.	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.  Zie 3 en 16. Dit onderzoek richt zich op het inrichten en borgen van de informatiebeveiliging van de meldkamersystemen als onderdeel van de meldkamervoorzieningen. De meldkamerfuncties en -systemen vallen buiten de scope van dit onderzoek en hierdoor niet benoemd, zoals beschreven in paragraaf 1.4.
20	Veiligheidsregio's	Bijlage 2, pg.22	<i>Het Bestuurlijk Meldkamer Beraad (BMB) neemt op het hoogste niveaubesluiten over beleidskeuzes, de besteding en uitvoering van de meldkamers.</i>	Het BMB gaat alleen over het beheer van de meldkamers en adviseert de minister over beleids- en bestedingsplan. De minister stelt deze vast. Aan het BMB worden dus meer verantwoordelijkheden toegeschreven dat dat zij conform de wettelijke regeling Hoofdpijnen van beleid en beheer hebben.	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage. Zie 16.
21	Veiligheidsregio's	Bijlage 2, pg.22	<i>Het SMB vervult een centrale rol in de aansturing van de samenwerkende meldkamers.</i>	Het SMB heeft conform de wettelijke regeling Hoofdpijnen van beleid en beheer geen rol in de aansturing en ook geen doorzettingsmacht. Het SMB stuurt op de uitvoering van het beleids- en bestedingsplan van de meldkamers.	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.  Sturing is de taak van het SMB. Zie 1 en 16.

22	Veiligheidsregio's	Bijlage 2, pg.22	<i>Daarnaast is een regionaal kwartiermaker aangesteld die een verdere samenwerking voorbereidt door een samenvoeging van 13 naar 10 meldkamerlocaties</i>	Er zijn nog twee regionale kwartiermakers, die zich bezighouden met de samenvoeging van meldkamers in het betreffende gebied voorbereiden. Per toekomstige samengevoegde meldkamer is dus één regionaal kwartiermaker aangesteld.	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage. Formulering is aangepast.
23	Vz SMB en veiligheidsregio's	Bijlage 3	<i>De directeur LMS, lid van het Strategisch meldkamerberaad...meldkamers.</i>	De directeur LMS is geen lid van het SMB (zie regeling beleid en beheer), de directeur treedt op als adviseur	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage. Zie 8.
24	MinJenV	Bijlage 3	<i>Geraadpleegde documenten</i>	De geldende Beleidsregels informatiebeveiligingsbeleid uit 2012 is niet geraadpleegd. Hierin staat ook een passage -weliswaar zeer beperkt - over risicomanagement en de verantwoordelijkheden. Ook de vigerende Beheerovereenkomst C2000 periode 2014 - 2017 (tussen MinJenV en Politie) is niet geraadpleegd.	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.  De Inspectie is bekend met de Beleidsregels informatiebeveiligingsbeleid mbt C2000 en de beheerovereenkomst, maar heeft in het onderzoek accent gelegd op de lopende actualisering van de beleidsregels met de toepassing van risicomanagement en het centraal stellen van de BIO.

## Wederhoortabel 2/2

Nr.	Inzagepartij	Hoofdstuk/ paragraaf	Te corrigeren tekst (eerste...laatste woord)	Argumentatie/onderbouwing van uw reactie	Reactie Inspectie JenV
1	Politie	1.2	<p>[Dat is een organisatieonderdeel van de Nationale Politie.]</p> <p>Suggestie toevoegen: dat is een <i>bijzonder</i> onderdeel van de Nationale Politie. <i>Bijzonder, omdat de functionele sturing op de LMS gebeurt vanuit Multi Governance: veiligheidsregio's, ambulancezorg- organisaties, politie en KMar sturen samen op de prioriteiten en de allocatie van het (multi) budget.</i></p>	<p>Dit is een wezenlijk verschil met een traditioneel onderdeel van de NP. Daar ligt in het kader van de uitwerking van informatiebeveiliging een dilemma van botsende waarden/regelgeving: Politierichtlijnen en richtlijnen van de andere disciplines rondom informatiebeveiliging en privacy verhouden zich in de praktijk soms niet (werkbaar) met elkaar.</p>	<p>De Inspectie neemt uw voorstel ten dele over in de rapportage. Formulering is aangepast.</p> <p>Dilemma botsende waarden/regelgeving: zie 9</p>
2	Politie	1.2	<p>[De Inspectie wilde weten of de meldkamers voldoende weerbaar zijn tegen het opzettelijk verstoren en uitschakelen van de systemen. Hiervoor is onderzocht hoe het <b>risicomanagement op de beveiliging van de meldkamersystemen</b> is ingericht en wordt toegepast.]</p>	<p><i>Dit verhoudt zich niet tot de centrale onderzoeksvraag: die gaat over de 'smallere' Scope van <b>informatiebeveiliging</b>.</i></p>	<p>De Inspectie neemt uw voorstel over in de rapportage. Formulering is aangepast.</p>
3	Politie	1.4	<p>[Het onderzoek werd uitgevoerd bij de LMS.]</p> <p>Suggestie: het onderzoek werd uitgevoerd op de dienstverlening die de LMS vanuit haar wettelijke beheertaak verricht rondom de</p>	<p>Bij de LMS suggereert dat het onderzoek alleen in de interne LMS organisatie is uitgevoerd, terwijl juist ook niet-LMS respondenten zijn betrokken.</p>	<p>De Inspectie neemt uw voorstel over in de rapportage. Formulering is aangepast.</p>

			informatiebeveiliging van de meldkamersystemen.		
4	Politie	1.5	[In de tweede stap onderzocht de Inspectie welke beheermaatregelen zijn genomen om de meldkamers weerbaar te maken tegen het opzettelijk verstoren en uitschakelen van de meldkamersystemen.]	Dit suggereert dat breder is gekeken, dan enkel binnen de onderzoeksscope van de informatiebeveiliging. Opzettelijke verstoring van MK systemen hebben bv ook te maken met fysieke beveiliging van het pand etc. En dat bedoelt de Inspectie niet.	De Inspectie neemt uw voorstel over in de rapportage. Formulering is aangepast. Niet bedoeld is de fysieke plaats van de meldkamers.
5	Politie	2.1	[Van het SMB wordt verwacht dat het toeziet dat de meldkamersystemen zijn beveiligd op basis van risicomanagement, en het de LMS aanstuurt op het beheer daarvan.]	Wiens verwachting wordt geschetst? Die o.b.v. de wet, geïnterpreteerd door de Inspectie (normstelling) of die de Inspectie ervaarde bij de respondenten (empirie)?	De Inspectie neemt uw voorstel over in de rapportage. Formulering is aangepast. Het betreft hier het wettelijk kader zoals beschreven in paragraaf 1.4.
6	Politie	2.1	De LMS coördineert deze werkzaamheden en de <b>beveiliging</b> zal bestaan uit een set van <b>beveiligingsafspraken</b>	Tip: consistent zijn in het gebruik van termen: informatiebeveiliging en informatiebeveiligingsafspraken. Beveiliging is een breder begrip.	De Inspectie neemt uw voorstel over in de rapportage. Formulering is aangepast.
7	Politie	2.2	De Inspectie aan de hand van het toetsingskader nagaan op welke onderdelen van het ontwikkelingsproces inmiddels al wel stappen zijn gezet, en welke bouwstenen voor het inrichten en borgen van risicomanagement inmiddels _____ aanwezig zijn.  Suggestie: verwijderen onderstreepte woorden.	Voelt aanmatigend richting een jonge LMS organisatie die vele ontwikkelstappen aan het zetten is. En 'inmiddels' ten opzichte van wat...	De Inspectie deelt uw zienswijze niet.  De Inspectie houdt er in de rapportage rekening mee dat de LMS een organisatie is in opbouw. Aan de andere kant zijn de meldkamersystemen onderdeel van de vitale infrastructuur en wijst de NCTV op een actuele toenemende dreiging van het opzettelijk verstoren van systemen.  In plaats van op te sommen op welke onderdelen van de informatiebeveiliging niet wordt voldaan aan het wettelijk kader,

					heeft de Inspectie onderzocht wat er inmiddels al wel is, welke stappen zijn gezet om te voldoen aan de voorgeschreven inrichting en borging van de informatiebeveiliging zoals bedoeld in het wettelijk kader beschreven in paragraaf 1.4.
8	Politie	2.2	<p>Van het SMB wordt verwacht dat <b>dit</b> het risicomanagement voor de veiligheid van informatie inricht en borgt.</p> <p>Suggestie: dit vervangen door zij (de LMSopdracht geeft om..).</p>	Naast de suggestie, Zie ook opm. 5. Norm? Dan graag duidelijk maken dat dit de toetsnorm van de Inspectie is. (en waarom mag worden verwacht?)	De Inspectie neemt uw voorstel ten dele over. Formulering is aangepast.
9	Politie	p.11		Onder het kopje 'verantwoordelijkheden' mist de spanning in het uitwisselen van informatie tussen disciplines op de MK doordat wetgeving van disciplines niet consistent op elkaar zijn afgestemd. (verwerker of verwerkingsverantwoordelijkheid, met als heet hangijzer het medisch beroepsgeheim).	<p>De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.</p> <p>De geldende norm NEN 7510 voor informatiebeveiliging in de zorgsector is een specifieke uitwerking van ISO/IEC 27001. Integratie van medische gegevens binnen de toepassing van de BIO is daarmee goed mogelijk. Daarmee is het medisch beroepsgeheim verre van een heet hangijzer. Het omgaan met de risico's van het medisch beroepsgeheim is een goed voorbeeld van wat binnen het inrichten en borgen van de informatiebeveiliging als risico zou moeten worden benoemd en ingepast in de informatiebeveiliging.</p>



10	Politie	2.4	Paragraaf 2.3 beschrijft dat de toetsing op de meest voorkomende bedreigingen het lastig maakt om een <b>volledig</b> en actueel beeld te vormen van de specifieke risico's voor de meldkamersystemen.	Graag kiezen voor 'een zo volledig mogelijk', een volledig beeld is een illusie.	De Inspectie neemt uw voorstel over in de rapportage. Formulering is aangepast.
11	Politie	Bijlage II	[De meldkamers worden bestuurd door vertegenwoordigers van de ministeries van Justitie en Veiligheid en Volksgezondheid, Welzijn en Sport, de veiligheidsregio's, Ambulancezorg Nederland, Koninklijke Marechaussee, Brandweer Nederland en de Nationale Politie. Hiervoor zijn verschillende gremia ingericht:...] Suggestie: vervangen door: Het beheer van de meldkamers als genoemd in de Wijkingswet wordt bestuurd door..... De wet en regelgeving richt daarvoor de volgende gremia/sleutelrollen in. De meldkamerfunctie wordt door de afzonderlijke disciplines binnen hun eigen organisatievorm, sturings- en verantwoordingslijnen bestuurd.	Is niet geheel correct geformuleerd en doet de suggestie dat op de meldkamers aan zich een vorm van governance (voor zowel de functie als de voorziening) op van toepassing is.	De Inspectie neemt uw voorstel ten dele over. Formulering is aangepast.
12	Politie	algemeen		Eigenlijk mist een stukje over de commissie gegevensverwerking die is ingesteld om vraagstukken op het gebied van gegevensverwerking, informatieveiligheid en privacy	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.

				<p>t.b.v. meldkamers te signaleren, en daar waar het voor het collectief waarde heeft, van advies te voorzien.</p> <p>Dat valt weliswaar niet onder de LMS, maar werkt wel samen met de LMS en heeft een link naar het SMB. Deze commissie is in de gesprekken wel aan bod geweest.</p>	<p>Het is juist dat in een gesprek het werk van de commissie gegevensverwerking onderwerp van gesprek is geweest. Omdat de commissie niet rechtstreeks onder de LMS valt en er geen direct verband is met het inrichten en borgen van de informatiebeveiliging op basis van risicoanalyse, heeft de Inspectie gekozen om dit weg te laten.</p>
13	Politie	algemeen		<p>Gevoelsmatig wordt de brede scope van risicobeoordeling en beveiliging ten aanzien van de continuïteit van meldkamers en de wat smallere scope van het onderzoeksonderwerp `de informatiebeveiliging, door elkaar heen gebruikt. Vanzelfsprekend maakt het één deel uit van het ander. De brede context en smallere onderzoeksscope loopt nu door elkaar, waardoor het op verschillende plekken in de rapportage de vraag oproep wat precies wordt bedoeld (en dus ook wie daar eigenaar van is, of uitvoeringsverantwoordelijkheid toe draagt.). Een scherpere afbakening op de smalle scope maakt het onderzoek, de bevindingen en de conclusies en aanbevelingen scherper en krachtiger.</p>	Zie 2.
14	Politie	TITEL	[Beveiliging van meldkamer-systemen]	Zie voorgaande opmerking: het onderzoek gaat niet over de totale beveiliging, maar	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.

			<p>Suggestie: vervangen door: Informatiebeveiliging in meldkamersystemen. (NB. pas dan ook de kopteksten aan)</p>	<p>juist over het deel informatiebeveiliging daarbinnen. (het gaat niet over toegangspassen, hekken, slagbomen etc.)</p> <p>Zie ook jullie eigen bewoordingen in p.1.1 'Dit onderzoek naar het risicomanagement op de informatiebeveiliging is een aanvulling op de genoemde onderzoeken naar de continuïteit van de meldkamers.'</p>	<p>Het betreft hier het toepassen van risicomanagement zodat de meldkamersystemen veiliger worden. Dat risicomanagement vindt niet specifiek 'in' deze systemen plaats. Het betreft hier de beveiliging van meldkamersystemen. De toevoeging binnen de titel dat het specifiek over informatiebeveiliging gaat, is dan met het oog op de leesbaarheid niet nodig.</p>
15	Politie	Ondertitel	<p>[Een onderzoek naar het inrichten en borgen van risicomanagement]</p> <p>Suggestie: Een onderzoek naar het inrichten en borgen van risicomanagementinzake de informatiebeveiliging in meldkamersystemen in beheer bij de LMS</p>	<p>Tip: preciezer formuleren zodat de lezer de waarde van de rapportage correct kan inschatten</p>	<p>Zie 14.</p>
16	Politie (LMS)	Bijlage 2, pagina 22	<p>De Kwartiermakers Bedrijfsvoering zorgen op de meldkamers voor de continuïteit van dit beheer en de aansturing van beheerders van de meldkamersystemen. Daarnaast is een regionale kwartiermaker aangesteld die een verdere samenwerking voorbereidt door een samenvoeging van 13 naar 10 meldkamerlocaties in 2023.</p>	<p>Deze bijlage beschrijft de besturing op de LMS. De Kwartiermakers zijn in dienst van de LMS en worden dus intern aangestuurd. Suggestie: Kwartiermakersbedrijfsvoering hier verwijderen of beschrijving over centraal beheer toevoegen en de titel van Bijlage 2 aanpassen.</p>	<p>De Inspectie neemt uw voorstel over in de rapportage. Formulering is aangepast.</p>
17	Politie (LMS)	Par 2.2. Laatsteline	<p>Het SMB..... Wel zijn ten dele criteria opgesteld</p>	<p>Uit de voorgaande tekst in paragraaf 2.2 kan uitsluitend worden afgeleid dat er criteria</p>	<p>De Inspectie neemt uw voorstel over in de rapportage. Formulering is aangepast.</p>

			voor het accepteren van beveiligingsrisico's	zijn vastgesteld voor de risicoanalyse C2000 uit 2017. Die risicoanalyse is op initiatief van het Meldkamer Dienstencentrum (MDC) uitgevoerd. Het SMB is daar op geen enkele wijze in betrokken geweest. De bedoelde criteria zijn derhalve vastgesteld binnen het MDC, niet in het SMB.	
18	Politie (LMS)	Par. 2.3 kopje Identificeren van risico's voor bedrijfsmiddelen, 1e alinea	Dit blijkt uit de gesprekken en de conceptnotitie Verbetering Informatiebeveiliging LMS en MK's uit 2020 (20). Dit was naar aanleiding van een rapportage van KPMG uit 2020 over de risico's en hiaten in de technische architectuur.	De conceptnotitie Verbetering Informatiebeveiliging LMS en MK's is niet opgesteld naar aanleiding van de in voetnoot 20 bedoelde KPMG rapportage, maar op basis van de door de informatiebeveiligingsfunctionaris geschetste noodzaak, die was gebaseerd op diverse bronnen, maar juist niet het bedoelde document. De inhoud van dat document is niet bekend bij de informatiebeveiligingsfunctionaris.	De Inspectie neemt uw voorstel ten dele over. Formulering is aangepast.
19	Politie (LMS)	Par 2.3 kopje Identificeren van risico's voor bedrijfsmiddelen, 1 <sup>e</sup> alinea	"Dit was naar aanleiding van een rapportage van KPMG uit 2020 over risico's en hiaten in de technische architectuur." Versus één na laatste alinea "De onderzoeken naar de technische infrastructuur brachten kwetsbaarheden aan het licht die ten tijde van het onderzoek projectmatig met beheermaatregelen worden verholpen."	En laatste alinea "De onderzoeken zijn uitgevoerd aan de hand van de CIS-20 controls. Hiermee is de informatiebeveiliging van de meldkamers getoetst op weerbaarheid tegen de wereldwijd meest voorkomende soorten cyberaanvalen." De een na laatste en laatste alinea maken m.i. duidelijk dat ook in de 1 <sup>e</sup> alinea de in voetnoot 21 bedoelde Quickscans en Security scans meldkamers (Deloitte 2019-2020) worden	De Inspectie neemt uw voorstel over in de rapportage. Formulering is aangepast.

				bedoeld, en niet het in voetnoot 20 bedoelde KPMG rapport.	
20	Politie (LMS)	Par 2.3 Conclusie	"Hierdoor heeft het SMB geen volledig actueel inzicht van de specifieke risico's voor de meldkamer-systemen. De informatiebeveiliging van C2000 vormt hierop een uitzonderling.."	De risicoanalyse C2000 uit 2017 is op initiatief van het MeldkamerDienstenCentrum (MDC) uitgevoerd. Het SMB is daar op geen enkele wijze in betrokken geweest, en de resultaten zijn ook niet aan het SMB gepresenteerd. Ook voor C2000 heeft het SMB dus niet dit inzicht.	De Inspectie neemt uw voorstel ten dele over. Formulering is aangepast.
21	Politie (LMS)	Par 2.4 kopjeVerwachting	"Van het SMB wordt verwacht dat het maatregelen kiest voor risicobeperking, dat het deze maatregelen vaststelt en dat het de LMS aanstuurt op het uitvoeren van deze maatregelen."	Dit is niet juist. Het SMB is verantwoordelijk voor het vaststellen van de criteria voor het evalueren en accepteren van risico's. De LMS is, binnen die kaders, en binnen de kaders van de Regeling hoofdlijnen beleid en beheer meldkamers en het vastgestelde Beleids- en bestedingsplan, zelfstandig verantwoordelijk voor het kiezen van maatregelen voor risicobeperking, en, daar waar die maatregelen niet binnen die kaders zelfstandig door de LMS kunnen worden getroffen, het door het SMB laten kiezen van maatregelen.	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.  De Inspectie is ervan op de hoogte dat de LMS zelfstandig maatregelen treft. De getroffen maatregelen zijn waardevol voor de informatiebeveiliging van de meldkamersystemen. Het probleem is echter dat niet inzichtelijk is of deze maatregelen voldoende zijn om de meldkamersystemen als onderdeel van de vitale infrastructuur te beveiligen. Daarvoor is het noodzakelijk om risicomanagement op de informatiebeveiliging toe te passen zoals bedoeld in ISO 270005 en dat het SMB hierin een sturende rol vervult zoals bedoeld in de Regeling hoofdlijnen beleid en beheer meldkamers. Zie ook wederhoortabel JenV bij 1 en 3.

22	Politie (LMS)	Par 2.4 kopje Bevinging	"Het SMB heeft naar aanleiding van de onderzoeken naar de kwetsbaarheden in de technische infrastructuur van de meldkamers maatregelen voor beperking vastgesteld. De LMS voert deze maatregelen uit (24)."	Dit is niet correct. De maatregelen voor beperking worden intern LMS vastgesteld. Voorstellen worden voorbereid door een binnen het project Verbeteren Informatiebeveiliging LMS en MK's ingerichte expertgroep en ter besluitvorming voorgelegd aan een Stuurgroep. Uitsluitend beleidsmatige kwesties worden middels concept beleidsstukken via de Werkgroep Informatiebeveiliging Meldkamers voorgelegd aan het SMB.	De Inspectie neemt uw voorstel over in de rapportage. De formulering is aangepast.
23	Politie (LMS)	Par 2.4 kopje Bevinging, 2 <sup>e</sup> alinea	"De gekozen maatregelen worden op dit moment projectmatig uitgevoerd onder coördinatie van de Werkgroep Informatiebeveiliging meldkamers." Versus Par. 2.1, kopje Bevinging, 3 <sup>e</sup> alinea. "De uitwerking van de beveiligingsafspraken is in handen van de Werkgroep Informatiebeveiliging Meldkamers die is samengesteld uit vertegenwoordigers van Ambulancezorg Nederland, Nationale Politie, de ministeries van Defensie en JenV, Brandweer Nederland, de veiligheidsregio's en de LMS."	Uit de tekst kan worden geconcludeerd dat hier de zelfde werkgroep wordt bedoeld. De in paragraaf 2.1 bedoelde werkgroep is echter een geheel andere dan de in paragraaf 2.4. bedoelde. De in par. 2.1 bedoelde werkgroep is ingesteld i.o.v. het SMB met de daar beschreven samenstelling. De in par. 2.4 bedoelde werkgroep is ingericht vanuit het project Verbeteren Informatiebeveiliging LMS en MK's. Dit is de in opmerking 8 bedoelde expertgroep. Dit is ook de in paragraaf 2.5 bedoelde expertgroep, zie ook opmerking 13.	De Inspectie neemt uw voorstel over in de rapportage. De formulering is aangepast.
24	Politie (LMS)	Par 2.4 kopje Bevinging, 3 <sup>e</sup> alinea	"De genoemde risicoanalyse op C2000 werd uitgevoerd voorafgaand aan de oplevering, en niet op de feitelijke werking van het systeem. Het Ministerie van JenV liet	De risicoanalyse C2000 uit 2017 is op initiatief van het MeldkamerDienstenCentrum (MDC) uitgevoerd en heeft geen relatie met de door Min-	De Inspectie neemt uw voorstel over in de rapportage. De formulering is aangepast.

			in 2019 tweemaal een penetratietest uitvoeren, waarbij diverse technische kwetsbaarheden aan het licht kwamen. De uitkomsten daarvan zijn verwerkt in het Beveiligingsplan C2000.”	JenV (programma IVC) uitgevoerde penetratietests. De uitkomsten van de door programma IVC uitgevoerde penetratietests en andere onderzoeken zijn verwerkt in het Beveiligingsplan C2000. De uitkomsten van de risicoanalyse C2000 uit 2017 zijn daar niet in verwerkt.	
25	Politie (LMS)	Par 2.4 Conclusie	“De gekozen maatregelen voor C2000 vormen hierop een uitzondering en zijn wel gebaseerd op risicoanalyse zoals bedoeld in ISO/IEC 27005.”	De risicoanalyse C2000 uit 2017 is op initiatief van het MeldkamerDienstenCentrum (MDC) uitgevoerd. Het SMB is daar op geen enkele wijze in betrokken geweest, en de resultaten zijn ook niet aan het SMB gepresenteerd.	De Inspectie neemt uw voorstel over in de rapportage. Zie 24.
26	Politie (LMS)	Par 2.4 kopje Verwachting	“Van het SMB wordt verwacht dat het aandeel van de risicocriteria beschrijft welke rest-risico's het aanvaardt. Daarnaast dat het goedkeuring verleent aan de overblijvende risico's en de LMS aanstuurt op het beheer van deze risico's.”	Dit is niet juist. Het SMB is verantwoordelijk voor het aandeel van de risicocriteria beschrijven welke rest-risico's het aanvaardt. De LMS is, binnen die kaders, en binnen de kaders van de Regeling hoofdlijnen beleid en beheer meldkamers en het vastgestelde Beleids- en bestedingsplan, zelfstandig verantwoordelijk voor het accepteren van rest-risico's, en, daar waar die rest-risico's niet binnen die kaders zelfstandig door de LMS kunnen worden geaccepteerd, deze door het SMB laten accepteren.	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.  De uitleg die u geeft volgt niet rechtstreeks uit de Regeling hoofdlijnen beleid en beheer meldkamers en het vastgestelde Beleids- en bestedingsplan, waarnaar u verwijst.  Het probleem is dat het SMB te weinig in staat is om op basis van risicomangement en monitoring te sturen op het aanvaarden van rest-risico's. Het SMB loopt hiermee een te groot risico te sturen op een onvolledig beeld van de informatieveiligheid van de meldkamersystemen. Zie ook 10 wederhoortabel JenV.

27	Politie (LMS)	Par 2.5 kopjeBe- vinding	"De notitie beschrijft een werkwijze waarin een expertgroep voor informatiebeveiliging onder leiding van de LMS advies geeft aan een stuurgroep van het SMB over het accepteren van risico's."	De expertgroep geeft advies aan een LMS-interne stuurgroep, niet aan het SMB. Slechts die zaken waarvan de stuurgroep van mening is dat zij hier nietover kan beslissen worden doorgeleid naar het SMB.	De Inspectie neemt uw voorstel over in de rapportage. De formulering is aangepast.
28	Politie (LMS)	-- (algemeen)	Het rapport maakt geen onderscheid tussen functionele kaders en technische kaders. Voor kaderstelling wordt verwezen naar het SMB.	Het rapport zou meer bruikbaar kunnen worden als de Inspectie nuances aanbrengt tussen functionele kaders en technische kaders.	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage.  De Inspectie heeft ervoor gekozen om geen onderscheid te maken tussen functionele kaders en technische kaders. Dit vanwege het doel van het onderzoek en het rapport moet ook door mensen buiten het meldkamerdo- me-in toegankelijk zijn.
29	Politie (LMS)	-- (algemeen)	Het rapport zou meer duidelijkheid kunnen (moeten?) geven ten aanzien van de rol van het SMB in relatie tot de wettelijke verantwoordelijkheid van de korpschef in deze.	Het rapport aanvullen met de zienswijze van de Inspectie over de rol van het SMB in relatie tot de wettelijke verantwoordelijkheid van de korpschef in deze. Daarbij aangevuld de zienswijze van de Inspectie over de stelselverantwoordelijkheid van het ministerie van JenV in relatie tot het SMB en het BMB.	De Inspectie neemt uw argument en onderbouwing niet over in de rapportage. Wel is de formulering van bijlage II verduidelijkt.  De Inspectie geeft geen zienswijze over de stelselverantwoordelijkheid van het ministerie van JenV in relatie tot het SMB en het BMB. De Inspectie onderzoekt de naleving van wet- en regelgeving en let daarbij op de kwaliteit van de taakuitvoering. Zie de bevindingen in paragraaf 2.2 'verantwoordelijkheden'. Het ministerie van JenV is verantwoordelijk voor de inrichting van



					het bestel. Daar kunt u en verzoek indienen voor een zienswijze.
--	--	--	--	--	--