# Tweede Kamer der Staten-Generaal

**2**

Vergaderjaar 2024–2025 **Aanhangsel van de Handelingen**


**Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden**

## 1187

Vragen van de leden **Six Dijkstra** (Nieuw Sociaal Contract) en **Mutluer** (GroenLinks-PvdA) aan de Minister-President en de Minister van Justitie en Veiligheid over *het onderzoeksrapport Beveiligingsproces van staatsgeheime vertrouwelijke informatie bij NCTV en politie van de Audit Dienst Rijk, alsmede de kabinetsreactie daarop* (ingezonden 20 december 2024).

Antwoord van Minister **Van Weel** (Justitie en Veiligheid) (ontvangen 31 januari 2025). Zie ook Aanhangsel Handelingen, vergaderjaar 2024–2025, nrs. 1016 en 1044.

Vraag 1
Bent u de mening toegedaan dat de constatering uit uw kabinetsreactie dat de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de politie «hun rollen onder bijzondere omstandigheden [vervullen] waarbij alertheid en veiligheidsbewustzijn hoog in het vaandel staan»[1], strookt met de bevindingen van de Audit Dienst Rijk (ADR) in zijn rapport Beveiligingsproces van staatsgeheime vertrouwelijke informatie bij NCTV en politie[2]? Zo ja, kunt u dit onderbouwen aan de hand van het ADR-rapport?

Antwoord 1
Zoals u in de kabinetsreactie heeft kunnen lezen ben ik van mening dat de NCTV en de politie een belangrijke rol spelen bij het veilig houden van ons land. Zij beschikken daartoe over een specifieke informatiepositie. Tegelijkertijd, zoals ook in de brief aan uw Kamer gemeld, onderschrijf ik de boodschap van de ADR dat de informatiebeveiliging beter kan en moet volledig en worden de aanbevelingen omarmd. Sinds de aanhoudingen zijn er binnen de NCTV en politie direct maatregelen getroffen. Het gaat dan om zowel noodmaatregelen als gelijktijdig ingezette maatregelen gericht op de lange(re) termijn. De aanbevelingen die de ADR in haar rapport heeft gedaan zijn, voor zover die nog niet waren meegenomen als onderdeel van de reeds getroffen maatregelen, weer integraal meegenomen in het continue verbeterproces. De omvangrijke stappen die sinds de aanhoudingen en naar aanleiding van het ADR rapport zijn gezet illustreren dat de aanbevelingen door zowel de NCTV als de politie met de nodige urgentie en zorgvuldigheid zijn opgepakt en zullen blijven worden opgepakt.

[1] Kamerstuk 36 600 VI, nr. 123.
[2] Bijlage bij Kamerstuk 36 600 VI, nr. 123.


ah-tk-20242025-1187
ISSN 0921 - 7398
's-Gravenhage 2025

Voor een gedetailleerde toelichting daarop verwijs ik naar de kabinetsreactie en bijbehorende bijlage die op 13 december aan uw Kamer is gestuurd. Zoals gemeld in deze Kamerbrief, heb ik ervaren dat de onderzochte organisaties de urgentie voelen en de aanbevelingen van de ADR adequaat hebben opgepakt.

Vraag 2
Wat maakte dat, zoals de ADR stelt, rapportages over het toezicht op beveiligingsmaatregelen binnen de NCTV geen impact hadden en niet door het managementteam (MT) van de NCTV werden gelezen? Wat maakte dat het MT geen baseline van beveiligingsmaatregelen liet inrichten, niet aanstuurde op compartimentering en het *need-to-know*-principe en geen controles op de beveiligingsmaatregelen liet uitvoeren? Wat zegt dit over het belang dat het management van de NCTV hecht aan beveiliging? Hoe kon deze werkcultuur ontstaan?

Antwoord 2
Het toezicht op informatiebeveiliging is, in lijn met de aanbevelingen van de ADR, versterkt. Dit heeft voor het MT van de NCTV prioriteit en er zijn door de NCTV dan ook zowel ten aanzien van de digitale als fysieke verwerking van bijzondere informatie belangrijke stappen gezet. Dit heeft er onder meer toe geleid dat de NCTV sinds 8 april 2024 een accreditatie heeft ontvangen voor de duur van 1 jaar die ziet op het digitale systeem waarmee bijzondere informatie wordt verwerkt.
ok is binnen elke afdeling opnieuw bepaald welke functionaris welke rechten heeft en zijn de meest verstrekkende rechten, zoals printen, beperkt tot enkele medewerkers. Daarbij wordt scherp gecontroleerd, aan de hand van een PDCA *(Plan, Do, Check, Act)*-cyclus die momenteel wordt ingericht, of gestelde regels worden gevolgd, of dit ordentelijk gebeurt en of er verdere verbeteringen te treffen zijn. Om dit structureler te borgen is onder meer een afdeling in oprichting die moet gaan toezien op Risicomanagement en Compliance binnen de NCTV. Ook wordt het beveiligingscoördinator (BVC)-cluster versterkt. Tot slot is een toezichtsplan opgesteld en zal dit jaarlijks worden geüpdatet. De taken in het toezicht worden daarin meegenomen. Een jaarlijkse bespreking door het managementteam van de resultaten van dit toezicht maakt hiervan onderdeel uit. Voor een uitgebreide toelichting hierop verwijs ik naar de kabinetsreactie van 13 december 2024 en de bijbehorende bijlage.

Vraag 3
Was het bij het MT van de NCTV bekend dat, naar uw kabinetsreactie, de NCTV voor het vervullen van haar rol in de bescherming van onze (nationale) veiligheid bijzondere informatie verwerkt en daarmee een interessant doelwit voor statelijke en niet-statelijke actoren is? Zo ja, wat maakte dat uit het rapport van de ADR is op te maken dat binnen het MT een volledig gebrek aan aandacht leek te zijn voor de beveiliging van die bijzondere informatie? Kunnen we hieruit opmaken dit dat de bescherming van onze (nationale) veiligheid van ondergeschikt belang was voor het MT van de NCTV? Zo nee, waar blijkt dat dan uit?

Antwoord 3
Ik weerspreek de conclusie dat de bescherming van onze nationale veiligheid van ondergeschikt belang was voor het MT van de NCTV. Het veilig houden van ons land is juist waar de NCTV en haar medewerkers zich hard voor inzetten. Dat bestaat uit meer dan informatiebeveiliging alleen. Dat neemt niet weg dat, zoals de ADR ook concludeert, er meer aandacht voor informatiebeveiliging nodig is.
Er is, zoals aangegeven in de Kabinetsreactie van 13 december 2024, een andere aanpak en bewustzijn over de hele breedte van de omgang met bijzondere informatie bij de NCTV en de politie nodig. Daar zijn omvangrijke stappen toe gezet. Zie hiervoor ook de beantwoording van vraag 2 en de kabinetsreactie van 13 december 2024 en de bijbehorende bijlage.

Vraag 4
Wat doet het met de geloofwaardigheid van dreigingsbeelden mede opgesteld door de NCTV, zoals het Dreigingsbeeld Statelijke Actoren 2 uit 2022, als de NCTV blijkens de bevindingen van de ADR niet handelde naar de door zichzelf hoog ingeschatte dreiging vanuit statelijke actoren en niet de benodigde basismaatregelen trof om zich tegen de inlichtingenactiviteiten daarvanuit te weren?

Antwoord 4
De analyses van de NCTV komen op een zorgvuldige wijze tot stand, waarbij gebruik wordt gemaakt van informatie van partners, als de AIVD, MIVD, de Politie en open bronnen waaronder online en offline media en wetenschappelijke literatuur. De analyses komen tot stand volgens een validatieproces, waarbij zowel intern als extern een inhoudelijke beoordeling op kwaliteit plaatsvindt.

Vraag 5
Kunt u alle documenten aan de Kamer verstrekken over de beveiligingssituatie van de NCTV die in de afgelopen tien jaar bij de NCTV, de directeur-generaal van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de secretaris-Generaal van het Ministerie van Justitie en Veiligheid (JenV) of de Minister van JenV zijn aangeleverd?

Antwoord 5
Gelet op de omvang van het informatieverzoek en de zorgvuldigheid waarmee dit verzoek behandeld dient te worden is het niet gelukt dit af te ronden voor het verstrijken van de termijn van de beantwoording. Uw Kamer wordt op een later moment en in ieder geval voor het debat nader geïnformeerd.

Vraag 6
Zijn er meer rapporten door de ADR over de NCTV geschreven in de afgelopen tien jaar? Zo ja, kunt u die aan de Kamer verstrekken?

Antwoord 6
De ADR doet regulier bij het Ministerie van Justitie en Veiligheid, waar ook de NCTV onderdeel van is, audits. Dit betreft de jaarlijkse auditrapporten bij het jaarverslag van het Ministerie van Justitie en Veiligheid en onderzoeken op verzoek van de NCTV of departementale leiding. De openbaar gemaakte rapporten van de ADR over onderwerpen die vallen onder verantwoordelijkheid van het Ministerie van JenV zijn hier te vinden: ADR-rapporten ministerie van Justitie en Veiligheid | Rijksoverheid | Rijksoverheid.nl
Voor wat betreft onderzoeken op verzoek van de NCTV heeft de ADR er een groot aantal uitgevoerd in de afgelopen tien jaar, variërend van de Beleidsdoorlichting van Artikel 36.2[3] tot Pentesten op bijvoorbeeld websites of systemen. Vanwege de veiligheidsrisico's zijn de ICT-onderzoeken zoals de Pentesten niet openbaar gemaakt.

Vraag 7
Welke acties gaat u ondernemen om het toezicht op de NCTV op de lange termijn te verbeteren?

Antwoord 7
Er zijn verschillende maatregelen getroffen om het toezicht op de informatiebeveiliging bij de NCTV te versterken. Deze maatregelen zijn onderdeel van een continu proces middels een PDCA-cyclus. Voor een uitgebreide toelichting op die maatregelen verwijs ik naar de kabinetsreactie en bijbehorende bijlage die op 13 december 2024 aan uw Kamer is toegezonden. Daarnaast wijs ik op het herhaalonderzoek dat door de ADR zal worden uitgevoerd. Uw Kamer wordt over de uitkomsten daarvan geïnformeerd.

[3] Onderzoeksrapport Beleidsdoorlichting Artikel 36.2 Nationale veiligheid en terrorismebestrijding | Rapport | Rijksoverheid.nl.

Vraag 8, 9 en 10
Zijn er NCTV-medewerkers geweest die op basis van vertrouwen extra ruimte kregen om zich niet aan alle geldende beveiligingsmaatregelen te houden, zoals dat ze vanuit huis met staatsgeheimen mochten werken? Zo ja, welke afspraken zijn hierover gemaakt? Op welk niveau is daar toestemming voor gegeven?
Zijn er situaties bij de NCTV geweest waarbij toegestaan of gedoogd werd dat medewerkers tegen de beveiligingsregels in vertrouwelijke of staatsgeheime informatie van de NCTV op gegevensdragers verzamelden en mee naar huis namen?
Zijn er situaties bij de NCTV geweest waarbij toegestaan of gedoogd werd dat medewerkers tegen de beveiligingsregels in een eigen schaduwadministratie bijhielden van Nederlandse personen of organisaties?

Antwoord 8, 9 en 10
Alle medewerkers van de NCTV moeten zich bij hun werkzaamheden aan de voorwaarden houden die op basis van wet- en regelgeving gelden. Het is soms noodzakelijk en daarmee dus ook binnen de geldende wet- en regelgeving mogelijk gemaakt om onder strikte voorwaarden staatsgeheime informatie buiten de NCTV (en andere overheidspartijen) te verwerken, bijvoorbeeld ten behoeve van overleggen of informatie-uitwisseling. Dat was het en dat is het nu ook. Het ADR Rapport geeft duidelijk aan dat betere voorbereiding nodig is op mogelijk misbruik van gerechtvaardigde toegang tot bijzondere informatie. Die conclusie onderschrijf ik en daartoe zijn ook maatregelen getroffen. Tegelijkertijd valt nooit volledig uit te sluiten dat iemand met beroepshalve gerechtvaardigde toegang niet goed met bijzondere informatie omgaat.

Vraag 11
Hoe beoordeelt u de uitspraak van de NCTV in 2021 dat hij zich niet herkende in het «geschetste beeld van een medewerker die een eigen harde schijf mee zou nemen» en dat het «medewerkers niet toegestaan [is] privéapparaten aan te sluiten op werkcomputers»[4]? Had de NCTV op dat moment inderdaad geen zicht op het gebruik van eigen gegevensdragers of apparatuur door medewerkers binnen de organisatie? Is er nog nadere informatie in deze context waarover de Kamer geïnformeerd moet worden?

Antwoord 11
Zoals aangegeven in de Kamerbrief van 13 december 2024, had de bewuste medewerker toestemming voor het gebruik van een beperkt aantal specifieke datadragers die vanuit de werkgever waren verstrekt. Datadragers werden in het algemeen onder andere gebruikt ten behoeve van presentaties die medewerkers moesten geven, of transport van documenten, als dit niet op een andere manier kon. In die gevallen ging het doorgaans om niet-gerubriceerde informatie. Medewerkers die door de werkgever uitgegeven datadragers nodig hadden, moesten deze via een specifieke procedure aanvragen. Deze aanvraag en uitgifte werd vastgelegd. De journalist in kwestie stelde tijdens het interview echter dat er sprake zou zijn van het gebruik van een eigen harde schijf. Het gebruik van een eigen harde schijf, dus een privéschijf, zou een veiligheidsincident zijn. Dit is, op basis van de toen beschikbare informatie, zorgvuldig uitgelopen door de NCTV. Op basis daarvan is geconcludeerd dat er geen sprake was van het gebruik van een eigen harde schijf, dus een privéschijf. Uw Kamer heeft op dit onderwerp alle reeds bekende informatie ontvangen. Dat misbruik van datadragers in zijn algemeenheid nadere aandacht had verdiend, onderschrijf ik. Om deze reden worden datadragers alleen nog beperkt in noodzakelijke gevallen en onder toezicht uitgegeven en is de administratie daarvan en monitoring daarop aangescherpt.

[4] NRC, 13 juni 2024, «Advocaat vraagt om getuigenis van Dick Schoof in zaak van NCTV-medewerker» (https://www.nrc.nl/nieuws/2024/06/13/advocaat-vraagt-om-getuigenis-van-dick-schoof-in-zaak-van-nctv-medewerker-a4856371).

Vraag 12 en 14
Hoe kijkt u aan tegen het handelen van de BVA van het Ministerie van JenV tot aan het moment dat het lek bekend werd? Hoe kon het dat de BVA in de nota uit 2022 geen opmerking maakte over de gedateerde basis van de beveiligingsmaatregelen van de NCTV, noch over het ontbreken van Stg-accreditatie? Hoe kon het daarnaast dat de BVA geen maatregelen trof wanneer NCTV-analisten geen rechtsgeldige VGB hadden? Kwam dit enkel door het gebrek van een (voldoende) eigenstandige informatiepositie van de BVA, of zijn er ook situaties geweest waarin de BVA niet of onvoldoende geacteerd heeft wanneer daar wel aanleiding toe was? Zo ja, wat vindt u daarvan?
Hoe kan met het oog op de in het ADR-rapport genoemde misstanden in de toekomst worden gegarandeerd dat de BVA van JenV als derdelijns toezichthouder tijdig op de hoogte is van beveiligingsfouten en deze mitigeert?

Antwoord 12 en 14
Zoals aangegeven in de Kamerbrief van 13 december 2024, blijkt uit het rapport dat de BVA van JenV niet altijd over een (voldoende) eigenstandige informatiepositie beschikte en bepaalde beveiligingsincidenten door de eerste of tweede lijn niet als zodanig herkend en dus gemeld werden. Hierdoor kon onvoldoende invulling worden gegeven aan de toezichthoudende taak van de BVA. De BVA zal daartoe tot andersoortige toezicht komen op en samenwerking met alle onderdelen van het departement die met bijzondere informatie werken.
De BVA van JenV zal daartoe in de reguliere overleggen die periodiek worden gevoerd met alle JenV organisatieonderdelen, waaronder beveiliging van de NCTV, structureel meer aandacht besteden aan diverse onderwerpen, waaronder de omgang met bijzondere informatie. Doel daarvan is dat de BVA zelf meer informatie ophaalt bij de organisaties binnen het departement waar gewerkt wordt met bijzondere informatie en op basis daarvan aandachtspunten in de informatiebeveiliging identificeert. De versterking van de samenwerking tussen de BVA en NCTV zal prioriteit hebben, mede gelet op de te nemen stappen richting de accreditatie van de digitale verwerking van bijzondere informatie en de fysieke context waarbinnen dat gebeurt binnen de NCTV in 2025 en ten aanzien van de vertrouwensfuncties en veiligheidsonderzoeken.
Daar is de afgelopen periode reeds invulling aan gegeven. De BVA van JenV is nauw betrokken bij de maatregelen die worden ingericht om de informatiebeveiliging bij de NCTV, mede naar aanleiding van het ADR Rapport, te verbeteren. Het VIR, VIR-BI en de BIO gelden daarbij als uitgangspunt. Aan de hand daarvan wordt ook door de BVA van JenV de voortgang getoetst. De BVA heeft daarin een eigenstandige informatiepositie en adviseert ten aanzien van de invulling die wordt gegeven aan maatregelen.

Vraag 13
Hoe wordt de Beveiligingsautoriteit (BVA) van J&V aangestuurd en aan wie legt deze verantwoording af? In welke mate is de BVA in staat om onafhankelijk te handelen? Welke mogelijkheden had en heeft de BVA om in geval van misstanden te escaleren?

Antwoord 13
De BVA van JenV is beheersmatig ondergebracht bij de directie Informatievoorziening en Inkoop. Deze directie valt onder de Hoofddirecteur bedrijfsvoering. De Beveiligingsautoriteit JenV stuurt het Bureau BVA aan Conform het Besluit BVA-stelsel Rijksdienst 2021, heeft BVA een onafhankelijke positie en rechtstreeks toegang tot de secretaris-generaal.Voor de maatregelen die zijn genomen ter versterking van het derdelijns toezicht vanuit de BVA binnen JenV verwijs ik naar de Kabinetsreactie en bijbehorende bijlage.
In het Besluit BVA-stelsel Rijksdienst 2021, zijn verder de formele positie, taken en bevoegdheden van onder andere de BVA Rijk, BVA en BVC zijn vastgelegd. Daarin is vastgelegd dat de BVA kaderstellende, adviserende en toezichthoudende rol over de integrale beveiliging van het departement. In algemene zin geldt dat de BVA's functioneel worden aangestuurd door de BVA Rijk. De BVA kan aanwijzingen geven en/of maatregelen (laten) treffen.

Vraag 15
Is het functioneren van het BVA-stelsel conform artikel 11 van het Besluit BVA-stelsel Rijksdienst 2021 drie jaar na inwerkingtreding (oftewel 1 januari 2024) geëvalueerd[5]? Zo ja, wilt u de resultaten aan de Kamer doen toekomen? Zo nee, wilt u het stelsel op korte termijn alsnog laten evalueren, de controle op de verwerking van staatsgeheim gerubriceerde informatie hiervoor expliciet als aandachtspunt meegeven en de Kamer over de resultaten informeren?

Antwoord 15
In 2023 is vanuit het BVA-beraad gestart met de evaluatie van het BVA-stelsel. De evaluatie is nog niet afgerond door onderbezetting en personeelswisseling. BVA-rijk is verantwoordelijk voor de evaluatie van het BVA-stelsel en in 2025 wordt dit alsnog opgepakt. Toezicht op het VIR-BI (waaronder staatsgeheimen) is hier onderdeel van. Resultaten zullen zo ver als mogelijk gedeeld worden met uw Kamer door de Minister van Binnenlandse Zaken en Koninkrijksrelaties.
Daarnaast is relevant om te vermelden dat ook intensivering van het toezicht is voorgenomen. In 2025 zal dat zijn beslag krijgen. Waarbij wordt vermeld dat de belangrijkste winst bij de beveiliging van staatsgeheimen in eerste instantie te vinden is in het bieden van (betere en Rijksbrede) voorzieningen en hogere bewustwording. Aanvullend is het VIR-BI geëvalueerd om te bezien of de regelgeving aanscherping of verduidelijking behoeft. Deze actualisatie is in het eerste kwartaal van 2024 gestart en is nagenoeg gereed. Naar verwachting wordt het in april gepubliceerd.

Vraag 16 en 17
In welke mate hebben klokkenluiders binnen de NCTV en het CTER-cluster van de politie voldoende mogelijkheden om misstanden binnen de eigen organisatie op het gebied van *insider threat* en het ontbreken van beveiligingsmaatregelen aan te kaarten, en genieten zij genoeg bescherming?
Is de klokkenluidersregeling in het domein van staatsgeheim gerubriceerde informatie voldoende ingericht? Welke mogelijkheden zijn er op dit gebied voor klokkenluiders?

Antwoord 16 en 17
Op basis van de Wet bescherming klokkenluiders kunnen werkenden een melding van een vermoedelijke misstand doen bij de werkgever (intern) of bij een aangewezen bevoegde autoriteit (extern; waarbij het Huis voor klokkenluiders geldt als een last resort als er geen andere bevoegde autoriteit is). In de Wet bescherming klokkenluiders zijn diverse beschermingsmaatregelen opgenomen. Zo mogen melders van een vermoeden van een misstand niet worden benadeeld door hun werkgever tijdens en na de behandeling van hun melding. Daarnaast schrijft de Wet bescherming klokkenluiders voor dat werkgevers en bevoegde autoriteiten meldingen vertrouwelijk moeten behandelen en de identiteit van de melder in beginsel geheim moeten houden.
Voor de NCTV als onderdeel van het Ministerie van Justitie en Veiligheid geldt bij vermoedens van misstanden de meldprocedure volgens de CAO Rijk (zie: 13.2 Voorzieningen bij melden vermoeden van een misstand). Voor politieambtenaren, waaronder het CTER-cluster, zijn regels over het melden van een vermoeden van een misstand opgenomen in het Besluit algemene rechtspositie politie (Barp). Binnen het klokkenluidersmeldpunt van de politie werken een aantal vertrouwenspersonen met verschillende screeningsniveaus. Hierdoor kunnen ook meldingen vanuit het werkgebied van CTER met deze functionarissen besproken worden. Voor werkzaamheden die zien op het uitvoeren van de Wet inlichtingen- en veiligheidsdiensten geldt een specifieke procedure bij de Afdeling Klachtbehandeling van de CTIVD.
Hier voeg ik aan toe dat in de initiatiefnota van het lid Omtzigt over voorstellen ter aanmoediging van het melden van misstanden en ter verbetering van de bescherming van klokkenluiders[6] het voorstel is opgenomen om een apart meldkanaal op te zetten voor het melden van geheime (staats)informatie bij

[5] https://wetten.overheid.nl/BWBR0044617/2021-01-01.
[6] Kamerstuk 36 079, nr. 2.

de Tweede Kamer of de Algemene Rekenkamer (voorstel 6). De Minister van Binnenlandse Zaken en Koninkrijksrelaties heeft toegezegd dat zij in het voorjaar van 2025 met een stand-van-zakenbrief onder meer ingaat op de voorstellen uit de initiatiefnota van het lid Omtzigt.[7]
Daarnaast geldt dat op grond van het VIRBI 2013 (artikel 8, lid 1) elke ambtenaar verplicht is de Beveiligingsautoriteit (BVA) onmiddellijk mededeling te doen van een inbreuk op de beveiliging die redelijkerwijs kan leiden, dan wel vermoedelijk of vaststaand heeft geleid, tot compromittering van bijzondere informatie.
Uw Kamer heeft recent de motie van het lid Van Waveren aangenomen die de regering verzoekt te onderzoeken welke aanvullende waarborgen in de Wet bescherming klokkenluiders of in de uitvoering van de wet nodig zijn om klokkenluiders bij de veiligheids- en opsporingsdiensten in het kader van de anonimiteit en de veiligheid beter te beschermen en dit te betrekken bij het wetsvoorstel aanpassing Wet bescherming klokkenluiders.[8] De Minister van BZK zal de Kamer hier verder over informeren.

Vraag 18
Van hoeveel gegevensdragers met daarop staatsgeheim gerubriceerde informatie is op dit moment nog onbekend waar deze zich bevinden? Hoe schat u de impact hiervan in op onze nationale veiligheid?

Antwoord 18
Het ADR rapport geeft aan dat onduidelijk is wat er met de uitgegeven USB-sticks is gebeurd, waar deze zich bevinden en welke informatie daarop is opgeslagen. Het ADR rapport geeft aan dat volgens de administratie circa 200 USB sticks in omloop zijn die mogelijk staatsgeheime informatie bevatten. In het ADR Rapport is tevens opgenomen dat de NCTV heeft aangegeven dat het aantal lager is dan 200. Feit blijft dat de administratie niet op orde was. Bij het uitgeven van USB's werd dit vaak wel geregistreerd, maar bij inname is dit niet altijd het geval geweest. Daardoor ontbreken exacte getallen hoeveel van deze USB's zijn ingeleverd en/of vernietigd, waar een aantal USB's zich bevinden en wat er op deze dragers stond. Die onzekerheid is bij bijzondere informatie zeer onwenselijk. Het moet altijd duidelijk zijn waar bijzondere informatie op welk moment is. Ook moet altijd geborgd worden dat bijzondere informatie na gebruik weer op de juiste manier wordt opgeslagen of vernietigd. Daarom zijn maatregelen getroffen om het proces omtrent het gebruik van gegevensdragers te verbeteren.
Ter nadere context geef ik nog het volgende mee. Het gaat om USB-sticks die tot september 2021 bij de NCTV werden gebruikt om bijvoorbeeld presentaties op te slaan die ergens anders gegeven moesten worden. Het ging hierbij veelal om presentaties voor gemeenten en lokale partners om de dreiging te duiden, waarbij geen staatsgeheime informatie werd gebruikt. Een zeer beperkt aantal werd daadwerkelijk gebruikt voor staatsgeheime informatie, bijvoorbeeld om informatie over te zetten van het interdepartementale staatsgeheime netwerk dat in beheer is bij de AIVD, op het netwerk voor de staatsgeheime informatie binnen de NCTV. Dit zijn twee *stand alone* netwerken die niet op elkaar aangesloten zijn. Verder is het van belang om te melden dat het om USB's gaat die beveiligd waren met een wachtwoord. Mocht een USB vermist raken, dan is de informatie dus niet zomaar voor een ieder toegankelijk. Ook passen deze USB-sticks sinds september 2021 niet meer op het staatsgeheime netwerk. De informatie die erop staat is dus niet zomaar voor een ieder toegankelijk en ze kunnen niet meer gebruikt worden om informatie van de huidige systemen af te halen.
Zoals ook eerder aan uw Kamer gemeld, zijn er geen signalen zijn die erop wijzen dat de nationale veiligheid (en/of de vitale infrastructuur) acuut gevaar loopt.

Vraag 19 en 21
Van hoeveel Nederlandse burgers (exact of naar schatting) is via dit lek persoonlijke informatie bij de Marokkaanse inlichtingen- en/of veiligheidsdienst terecht gekomen?

---

[7] Kamerstuk 35 851, nr. 65.
[8] Kamerstuk 35 851, nr. 66.

Wat betekent dit lek voor de persoonlijke situatie en veiligheid van de Nederlandse burgers in kwestie? Hoe beoordeelt u de rechtspositie van deze burgers? Hoe schat u het risico in dat hun informatie door de Marokkaanse diensten als chantagemateriaal gebruikt kan worden? Kunt u dit onderbouwen?

Antwoord 19 en 21
Ik begrijp de zorgen van uw Kamer. In algemene zin geldt dat op het moment dat duidelijk is dat er informatie over individuen bij een datalek betrokken zijn, er conform de wettelijke regelgeving moet worden bepaald of er maatregelen getroffen dienen te worden. Dat vereist concreet inzicht om welke informatie het dan gaat. In het voorliggende geval geldt dat niet met zekerheid vast te stellen is welke informatie naar buiten is gebracht of welke informatie waar terecht is gekomen. Dat betekent dat er niet met zekerheid is vast te stellen op basis van welke documenten een risico-inschatting gemaakt moet worden.
Er is vooralsnog bij mijn departement geen aanleiding geweest om over te gaan tot het informeren van personen in lijn met de geldende wet- en regelgeving. Daarnaast geldt vanzelfsprekend dat bij nieuwe informatie waar relevant dit opnieuw en doorlopend gewogen zal worden. Wel is er bijzondere aandacht besteed aan de gevolgen van de casus voor de (positie van) medewerkers binnen de relevante organisaties. De risico's voor de politie zijn in kaart gebracht en waar nodig zijn maatregelen in de operatie getroffen om deze risico's te beheersen.
Ik verwijs voor het antwoord op deze vraag ook naar het antwoord op vragen 23 en 24.

Vraag 20
Welke overige informatie is bij de Marokkaanse inlichtingen- en/of veiligheidsdienst terecht gekomen?

Antwoord 20
Deze vraag ziet op het strafrechtelijk onderzoek en daar kan ik niet op ingaan.

Vraag 22
Van hoeveel van deze burgers waren de gegevens zonder geldend wettelijk kader door de NCTV verworven?

Antwoord 22
Het is van belang om twee onderwerpen van elkaar te scheiden, namelijk het wettelijk kader voor het verwerken van staatsgeheime informatie en de verwerking van persoonsgegevens door de NCTV. Voor een nadere toelichting op het wettelijk kader voor het verwerken van staatsgeheime informatie verwijs ik u naar de beantwoording van vraag 29, 30 en 35. Ten aanzien van het verwerken van persoonsgegevens door de NCTV geldt dat hierover op verschillende momenten met uw Kamer is gecommuniceerd.[9] Dit heeft geleid tot de Wet coördinatie terrorismebestrijding en nationale veiligheid, waarin de coördinatietaak van de NCTV is afgebakend en vastgelegd.

Vraag 23 en 24
Hoe gaat u ervoor zorgen dat al deze burgers conform de Algemene Verordening Gegevensbescherming (AVG) geïnformeerd worden over het feit dat hun gegevens betrokken zijn bij een datalek? Verwacht u dat burgers voor dit feit gecompenseerd moeten worden?
Heeft u hierover contact gehad met de Autoriteit Persoonsgegevens? Zo ja, wat is uit de gesprekken gekomen? Zo nee, bent u bereid dit alsnog te doen en de Kamer over de uitkomst te informeren?

Antwoord 23 en 24
Op het moment dat er sprake is van een datalek kan er melding worden gedaan bij de Autoriteit Persoonsgegevens. Toen de oud-medewerkers van de NCTV werden aangehouden, had de NCTV geen zicht op welke documenten precies onrechtmatig in bezit waren van betrokkenen en of deze documenten

[9] Onder meer in Aanhangsel van de Handelingen II 2023–2024, nr. 1713.

persoonsgegevens bevatten. Om die reden is er destijds geen melding van een datalek gedaan door de NCTV aan de Autoriteit Persoonsgegevens. Echter, gelet op de informatie die inmiddels is gedeeld in het openbaar, schat de NCTV op dit moment de kans reëel in dat er tussen de gegevens van de NCTV ook persoonsgegevens zitten. Om die reden is er recent alsnog een melding van een datalek gedaan. In hoeverre personen geïnformeerd moeten worden en indien nodig de wijze waarop, zal worden afgestemd met de Autoriteit Persoonsgegevens. Hierbij is van belang op te merken dat op dit moment nog niet kan worden aangegeven welke gegevens dit exact behelst. Dit is ook in de melding aangegeven.
De politie heeft bij de Autoriteit Persoonsgegevens formeel melding gedaan van het datalek. Ten tijde van de melding bij de Autoriteit Persoonsgegevens was er geen zicht op welke documenten en persoonsgegevens van burgers al dan niet betrokken waren bij het datalek. Uit het gesprek met de Autoriteit Persoonsgegevens toentertijd is derhalve niet voortgevloeid dat de politie burgers moest informeren.

Vraag 25
Zijn het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI 2013) en de Rubriceringsregeling Politie 2015 ooit geëvalueerd? Zo ja, wilt u de resultaten aan de Kamer doen toekomen? Zo nee, acht u in het kader van de door de ADR onderzochte lekken van toegevoegde waarde om dit wel te doen?

Antwoord 25
Het VIR-BI wordt op dit moment onder leiding van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties geactualiseerd. De resultaten daarvan zullen met uw Kamer worden gedeeld.
De politie heeft begin 2025 haar Rubriceringsregeling geactualiseerd. De nieuwe rubriceringsregeling sluit nu beter aan bij de rubriceringsregeling van de Rijksoverheid: het VIR-BI. De politie is weliswaar geen onderdeel van de Rijksoverheid, maar op het gebied van informatiebeveiliging is nu gekozen om zoveel mogelijk aan te sluiten bij het beleid van de Rijksoverheid. Dit omdat informatie steeds meer wordt verwerkt in ketenverband en het van belang is om in de keten dezelfde terminologie te hanteren en eenzelfde mate van beveiliging toe te passen op vergelijkbare rubriceringsniveaus.

Vraag 26 en 27
Kunt u een overzicht geven van waar binnen de overheid sinds de invoering van het VIRBI 2013 onderzoek is gedaan door instanties als de ADR, de Algemene Rekenkamer (ARK) of de National Security Authority (NSA)[10] naar de verwerking van nationaal gerubriceerde informatie of internationaal gerubriceerde informatie (zoals informatie met een rubricering van partnerlanden of EU-, NAVO- of ESA-gerubriceerde informatie)?
Kunt u een overzicht geven van de sinds de invoering van het VIRBI 2013 geconstateerde onvolkomenheden op het gebied van de verwerking van nationaal of internationaal gerubriceerde informatie, zoals de door de ARK geconstateerde onvolkomenheden in systemen van het Ministerie van Buitenlandse Zaken[11]?

Antwoord 26 en 27
Een dergelijk overzicht is niet voorhanden. Wel merk ik op dat het Beveiligingsautoriteiten-beraad, waar de beveiligingsautoriteiten van alle departementen aan deelnemen, naar aanleiding van dit incident heeft besloten om een Rijksbreed onderzoek te starten naar de wijze waarop het beleid omtrent en toezicht op de omgang met bijzondere informatie, specifiek staatsgeheime informatie, is ingeregeld en geborgd bij de verschillende departementen. Het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere

[10] https://wetten.overheid.nl/BWBR0047897/2023-02-23.
[11] Algemene Rekenkamer, 2019, «Resultaten verantwoordingsondezoek Ministerie van Buitenlandse Zaken 2018» (https://www.rekenkamer.nl/binaries/rekenkamer/documenten/rapporten/2019/05/15/resultaten-verantwoordingsonderzoek-2018-ministerie-van-buitenlandse-zaken/VO+Ministerie+van+Buitenlandse+Zaken.pdf).

Informatie, de Council Security Rules[12] van de Europese Raad (EC) en de C-M(2002)/49 van de NAVO dienen hierbij als toetsingskader.

Vraag 28
Hoe frequent worden de overheidssystemen voor de verwerking van nationaal of internationaal gerubriceerde informatie gecontroleerd door instanties als de ADR, de ARK en de NSA? Kunt u aangeven wanneer elk van de departementen die gerubriceerd materiaal verwerken voor het laatst in het kader hiervan extern zijn onderzocht?

Antwoord 28
Ik kan alleen ingaan op de informatiebeveiliging bij het Ministerie van Justitie en Veiligheid. Het ADR Rapport dat op 13 december 2024 aan uw Kamer is toegezonden is het meest recente onderzoek dat naar de beveiliging van bijzondere informatie bij de NCTV en politie is uitgevoerd. Zoals aangegeven is het BVA-Beraad een rijksbreed onderzoek gestart naar de wijze waarop het beleid omtrent en toezicht op de omgang met bijzondere informatie, specifiek staatsgeheime informatie, is ingeregeld en geborgd bij de verschillende departementen.
De ADR kan, vanuit haar rol als huis auditor van de Rijksoverheid, gevraagd worden door de systeemeigenaar om een audit onderzoek uit te voeren naar het stelsel van de beveiliging van het te accrediteren informatiesysteem. Het staat de systeemeigenaar echter vrij om eventueel een andere audit organisatie hiervoor te benaderen. Daarnaast heeft de ADR, vanuit haar taak inzake Comptabiliteitswet, de mogelijkheid om beheeronderzoeken uit te voeren naar financiële systemen.
De ARK hanteert eigen kaders t.a.v. van uitvoer van haar controlerende taak. Audits die zij verrichten zijn merendeel op een hoger abstractieniveau en worden vaak ook gebaseerd op uitkomsten van eerdere ADR audits.
De NSA heeft een toezichthoudende rol t.a.v. de wijze waarop de beveiliging van gerubriceerde informatie van internationale herkomst is beveiligd. Naast dat de NSA wordt geconsulteerd tijdens het accreditatieproces van dergelijke informatiesystemen, heeft de NSA een eigenstandige verantwoordelijkheid hierin.
De NSA voert, bijvoorbeeld voortkomend uit de vigerende internationale regelgeving, (periodiek) controle uit op de beveiliging indien het nieuwe systemen betreft, bij wijzigingen die raken aan de beveiliging van bestaande systemen of wanneer de NSA dit nodig acht.
De EU en NAVO inspecteren Nederland ongeveer eens per vijf tot zeven jaar. De laatste inspecties dateren (respectievelijk) uit 2013 en 2019.

Vraag 29
Kunt u aangeven wat de vigerende wet- en regelgeving is van elk van de typen gerubriceerde informatie die in Nederland verwerkt worden, zoals nationaal gerubriceerde informatie, informatie met een rubricering van partnerlanden, en EU-, NAVO- en ESA-gerubriceerde informatie?

Antwoord 29
De wet- en regelgeving die in elk geval van toepassing is op het Ministerie van Justitie en Veiligheid zijn:
1) het Besluit voorschrift informatiebeveiliging rijksdienst 2007 voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie;
2) het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013, in aanvulling op het VIR, daar waar het gaat om bijzondere informatie,
3) het Besluit BVA-stelsel Rijksdienst 2021 ten aanzien van de integrale beveiliging van de Rijksdienst.

Deze wet- en regelgeving is waar nodig uitgewerkt in nadere onderliggende (beleids)regels. Ten aanzien van EU-, NAVO-, en ESA-gerubriceerde informatie merk ik op dat hiervoor andere accreditatieregimes gelden die los staan van de nationale accreditatieregimes die in algemene zin gelden voor het

[12] Council decision 488/2013

Ministerie van Justitie en Veiligheid. Daar zijn aanvullende maatregelen voor nodig. Sinds de aanhoudingen is daarom het beleid binnen de NCTV dat EU en NAVO informatie in principe niet kan en mag worden verwerkt. Daar waar verwerking nodig is voor de uitvoering van wettelijke taken en/of de nationale veiligheid is de NCTV in overleg met de BVA, mede met het oog op het verkrijgen van een accreditatie voor het verwerken van deze informatie.
De politie verwerkt gegevens ter uitvoering van de politietaak op basis van de Wet politiegegevens (Wpg). Politiegegevens kunnen worden uitgewisseld met de bevoegde autoriteiten in andere lidstaten van de Europese Unie of aan organen en instanties daarvan. De Wpg eist dat er passende informatiebeveiligingsmaatregelen worden getroffen. Daar wordt o.a. invulling aan gegeven door gebruik te maken van de Rubriceringsregeling politie 2015.

Vraag 30
Kunt u voor elk van deze typen aangeven door wie en hoe hier a) toestemming/accreditatie voor wordt verleend; en b) toezicht op wordt gehouden?

Antwoord 30
Zoals vastgelegd in het VIR-BI mogen alleen personen die daartoe zijn geautoriseerd bijzondere informatie behandelen of inzien voor zover dit noodzakelijk is voor een goede uitoefening van hun taak. Wie welke informatie mag inzien is derhalve afhankelijk van de specifieke taak en daarmee niet per type informatie inzichtelijk te maken. Voor de opbouw van het toezicht op bijzondere informatie alsmede de maatregelen die zijn getroffen teneinde dit toezicht te versterken verwijs ik naar de kabinetsreactie en bijbehorende bijlage die op 13 december 2024 aan uw Kamer is toegezonden.

Vraag 31 en 32
Hoe wijken deze regimes van toestemming/accreditatie en toezicht af van hoe EU-partnerlanden als Frankrijk en Duitsland deze hebben ingericht, zowel voor nationaal als internationaal gerubriceerde informatie?
Zijn deze regimes naar uw inzicht zowel in theorie als in praktijk passend gezien o.a. door de NCTV opgestelde dreigingsbeelden? Zo ja, wat is uw onderbouwing daarvoor? Zo nee, welke verbeteringen bent u van plan door te voeren?

Antwoord 31 en 32
Er is geen overzicht voorhanden van de regimes die van toepassing zijn in de verschillende lidstaten en de wijze waarop invulling is gegeven aan relevante internationale regelgeving. Het is daarnaast niet aan mij om uitspraken te doen over de (waardering van) regimes van andere partnerlanden of instellingen in relatie tot onze eigen regimes.

Vraag 33
Wat is uw reactie op de aanbeveling in het rapport «Digitale Kroonjuwelen» van Twynstra Gudde dat «centraal, nationaal toezicht noodzakelijk is om tot een adequaat en uniform niveau van beschikbaarheid, vertrouwelijkheid en integriteit van de gegevens, documenten en registraties van Nationaal Belang te komen», waarbij «het toezicht zou kunnen worden ingericht vergelijkbaar met het toezicht op de beveiliging van gerubriceerde informatie van de EU en de NAVO» en «ingezet [wordt] op een initiële accreditatie van de betreffende beveiliging bij de overheidspartijen vóóraf, aangevuld door periodieke inspecties»[13]?

Antwoord 33
Voor het antwoord op deze vraag verwijs ik naar de Kamerbrief van 29 juni 2023 waarin de (toenmalig) Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties – Digitalisering en Koninkrijksrelaties het rapport aan uw Kamer heeft aangeboden.

[13] Bijlage bij Kamerstuk 26 643, nr. 1044.

Vraag 34
Naast nationaal gerubriceerde informatie, welke typen internationaal gerubriceerde informatie (zoals informatie met een rubricering van partnerlanden of EU-, NAVO- of ESA-gerubriceerde informatie) verwerken de NCTV en de politie? Waren die allemaal in scope voor het onderzoek van de ADR? Zo nee, waarom niet?

Antwoord 34
Ten aanzien van EU-, NAVO-, en ESA-gerubriceerde informatie merk ik op dat hiervoor andere accreditatieregimes gelden dan de accreditatieregimes die nationaal gelden voor het Ministerie van Justitie en Veiligheid. Sinds de aanhoudingen is daarom het beleid binnen de NCTV dat EU en NAVO informatie in principe niet kan en mag worden verwerkt. Daar waar verwerking nodig is voor de uitvoering van wettelijke taken en/of de nationale veiligheid is de NCTV in overleg met de BVA, mede met het oog op het verkrijgen van een accreditatie voor het verwerken van deze informatie.
De politie verwerkt nationaal gerubriceerde informatie. Daarnaast vindt gegevensuitwisseling plaats binnen de EU (zie ook antwoord bij vraag[14].
Voor de scope van het ADR onderzoek verwijs ik naar hetgeen daarover opgenomen in het ADR rapport.

Vraag 35
Kunt u aangeven wat per type gerubriceerde informatie de onderliggende grondslag/toestemming/accreditatie is op basis waarvan de NCTV en/of de politie deze verwerkt?

Antwoord 35
Ik verwijs voor het Ministerie van Justitie en Veiligheid naar het antwoord op vraag 29. Alle nationaal gerubriceerde informatie (stg-gerubriceerd) kan worden gedeeld met een overheidspartij, waarvan de ruimtes en de systemen die worden gebruikt voor de verwerving en verwerking van stg-informatie moeten zijn geaccrediteerd en medewerkers in het bezit moeten zijn van een verklaring van geen bezwaar (VGB). Deze accreditatie vindt plaats door de secretaris-generaal van een departement op advies van de beveiligingsautoriteit binnen dat departement.
Voor EU en NAVO-gerubriceerde informatie geldt dat deze accreditatie ook door de secretaris-generaal van een departement moet worden afgegeven op advies van de BVA van het departement, maar dat hiervoor ook een positief oordeel door de National Security Authority (NSA) moet worden afgegeven. Deze rol is voor het civiele domein belegd bij de AIVD. Periodiek wordt door zowel EU als NAVO-inspecteurs getoetst of ontvangende partijen voldoen aan geldende wet- en regelgeving.
Internationaal gerubriceerde informatie die niet valt binnen EU- of NAVO-rubricering is een afweging van de verzendende partij zelf. Die bepaalt welke partijen onder welke voorwaarden informatie mogen ontvangen en verwerken.
De politie verwerkt gegevens ter uitvoering van de politietaak op basis van de Wet politiegegevens (Wpg). Politiegegevens kunnen worden ter beschikking gesteld aan de bevoegde autoriteiten in andere lidstaten van de Europese Unie of aan organen en instanties daarvan. Bij algemene maatregel van bestuur (AMvB) worden nadere regels gesteld over de ter beschikkingstelling van politiegegevens, alsmede over de verdere verwerking en de daarbij te stellen voorwaarden aan het gebruik daarvan door ontvangstgerechtigde autoriteiten of internationale organen en instanties, en over de ontvangst van politiegegevens vanuit andere lidstaten van de Europese Unie.
De Wpg eist dat er passende informatiebeveiligingsmaatregelen worden getroffen. Daar wordt o.a. invulling aan gegeven door gebruik te maken van de Rubriceringsregeling politie 2015. Deze is in 2025 geactualiseerd en sluit nu beter aan bij de rubriceringsregeling van de Rijksoverheid: het VIR-BI. In de rubriceringsregeling is een vertaaltabel opgenomen, zodat informatie die

[14] het Besluit voorschrift informatiebeveiliging rijksdienst 2007 voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie;

binnen de EU wordt uitgewisseld op een vergelijkbaar niveau en met vergelijkbare maatregelen wordt behandeld door de politie.

Vraag 36
Welk van deze typen gerubriceerde informatie zijn mogelijk gecompromitteerd in de door de ADR onderzochte lekken?

Antwoord 36
Er wordt rekening gehouden met het feit dat alle typen gerubriceerde informatie in meer of mindere mate zijn gecompromitteerd.

Vraag 37
Wat is er tot het moment van onderzoek door de ADR vanuit het toezicht aan audits en inspecties geweest? Welke maatregelen hebben de NCTV en de politie over de jaren genomen op basis van die audits en inspecties?

Antwoord 37
De BVA van het Ministerie van Justitie en Veiligheid houdt toezicht op de NCTV en de verwerking van informatie, zoals ook geschetst in het antwoord op de vragen 12 en 14. De BVA brengt daarbij vanaf 2019 in principe ieder jaar de bevindingen van dit toezicht samen in een toezichtsnota. Dit is evenwel niet voor ieder jaar gebeurd in de afgelopen jaren. De NCTV is begin 2023 begonnen met het project digitale weerbaarheid om de informatiebeveiliging te verbeteren. Dit resulteerde er onder andere in dat het eerste geactualiseerde beleid in januari 2024 vastgesteld werd binnen de NCTV. De werking van het beleid en de maatregelen wordt vormgegeven in een PDCA (Plan-Do-Check-Act) -cyclus zoals is uiteengezet in de genoemde kabinetsreactie op het ADR-rapport van 13 december.
Bij de politie is de derdelijns toezichthoudende taak belegd bij de concern audit. Door de concern audit zijn in de afgelopen jaren aanbevelingen gedaan, maar deze zijn niet altijd opgevolgd door de politie. Zoals aangegeven in de kabinetsreactie op het ADR-rapport zal de politie de doorwerking van interne audits versterken. De korpsleiding zal toezien op de opvolging en borging van aanbevelingen die door concern audit worden gedaan. Tevens zal de politie bezien of de expertise van concern audit kan worden versterkt door politiemensen uit de operationele werkpraktijk toe te voegen aan audits op informatiebeveiliging.

Vraag 38
Wat is zowel in het heden als op de lange termijn de impact van de lekken op de slagkracht en internationale reputatie van Nederlandse instanties als de I&V-diensten, bijvoorbeeld doordat bronnen en partnerlanden terughoudender zijn geworden in samenwerking? Wat voor maatregelen zijn er genomen om deze impact te minimaliseren?

Antwoord 38
Over operationele aangelegenheden van de inlichtingen- en veiligheidsdiensten kan ik in de openbaarheid geen uitspraken doen. Het is ook niet aan mij om te speculeren over de internationale reputatie.

Vraag 39
In hoeverre bent u bereid om een onafhankelijke commissie samen te stellen die het proces van herstel en bewustwording bij de NCTV kan begeleiden?

Antwoord 39
De ADR heeft de afgelopen maanden onafhankelijk onderzoek bij de NCTV en politie uitgevoerd. Voor de komende tijd is het belangrijk de vinger aan de pols te houden. Ik heb de ADR gevraagd om een aanvullend onderzoek te doen bij de NCTV naar de opvolging van de aanbevelingen en waar nodig aanvullende aanbevelingen te doen.
De ADR heeft aangegeven hiertoe bereid te zijn en te verwachten na 12 maanden een goed beeld van te kunnen geven. De politie gaat de aanbevelingen opnemen in de interne auditcyclus en zal aan de ADR rapporteren over de voortgang. Uw Kamer zal vanzelfsprekend over de uitkomsten worden geïnformeerd.

Vraag 40
Wilt u deze vragen afzonderlijk en binnen drie weken beantwoorden?

Antwoord 40
De vragen zijn binnen de reguliere termijn beantwoord. Mede gelet op de omvangrijkheid van de set zijn daar waar opportuun vragen in samenhang beantwoord.