Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

# 36 721 Initiatiefnota van de leden Six Dijkstra en Omtzigt over centraal toezicht op staatsgeheimen

**Nr. 3**

## BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 14 juli 2025

Het kabinet dankt de (voormalig) leden Six Dijkstra en Omtzigt voor het schrijven van de initiatiefnota over de beveiliging van staatsgeheimen. Het kabinet vindt het van groot belang dat onze Nederlandse belangen goed zijn beschermd. Het deelt de zorg en opvatting dat de beveiliging van staatsgeheimen onvoldoende is gebleken en dat in het huidige dreigingsbeeld dringend verbetering nodig is.

In deze brief wordt ingegaan op de initiatiefnota in volgorde van de daarin genoemde beslispunten en beschrijft het kabinet aan welke verbeteringen het begonnen is, en hoe het verder voornemens is deze verbeteringen te realiseren, waaronder de versterking van het huidige toezicht en een eventuele extra centrale toezichthouder.

### Kern

Voorop gesteld moet worden dat toezicht op staatsgeheimen niet de enige oorzaak van het probleem is bij de beveiliging van staatsgeheimen, die onvoldoende is gebleken. Het is daarmee ook niet de enige opgave bij het verbeteren van de beveiliging van onze staatsgeheimen. Die opgave ligt eveneens in het realiseren van meer- en betere middelen om veilig en Rijksbreed te kunnen werken met staatsgeheimen (beslispunt 4 uit de initiatiefnota). Op dit moment ontbreken goede Rijksbrede voorzieningen. Zoals in deze notitie wordt beschreven is hiervoor opnieuw een Rijksbreed meerjarig traject gestart, om dit te realiseren. Het kabinet zal de Kamer vertrouwelijk over de voorgang daarvan informeren.

Naast het bieden van meer- en betere middelen om veilig met staatsgeheimen te kunnen werken, is het ook essentieel om het bewustzijn over het belang van de beveiliging van staatsgeheimen te vergroten. Net als het bieden van handelingsperspectief voor de implementatie van het

kst-36721-3
ISSN 0921 - 7371
's-Gravenhage 2025

voorschrift voor omgang met staatsgeheimen (hierna VIR-BI). Ook hieraan zal extra aandacht worden besteed. Daarvoor wordt in 2025–2026 door BZK een ondersteuningsprogramma verder ontwikkeld.

Het kabinet erkent dat een wettelijke regeling van de omgang met gerubriceerde informatie beperkt is. Dit betekent niet dat er géén wettelijke regels over zijn. Zo bevat het Wetboek van Strafrecht enkele delictsbepalingen over het verstrekken van staatsgeheime informatie. De Wet bescherming staatsgeheimen biedt de mogelijkheid om verboden plaatsen aan te wijzen. Gedetailleerdere regels zijn gevat in het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013). Dit voorschrift is bindend voor de Rijksdienst. De behandeling van internationale informatie is vastgelegd in volkenrechtelijke besluiten op basis van verdragen. Hierin is de rol van de National Security Authorities (NSA's) in respectievelijk civiele en militaire aangelegenheden vastgelegd in het kader van toezicht op de uitvoering. Momenteel wordt gewerkt aan de opvolger van het VIRBI 2013.

Iedere secretaris-generaal (SG) van een ministerie is conform het VIRBI 2013 (2025 zodra het gepubliceerd is) verantwoordelijk voor het verlenen van accreditatie binnen het ministerie. Dit volgt logischerwijs uit het gegeven dat elke Minister verantwoordelijk is voor de bedrijfsvoering binnen het eigen departement. Het kabinet is dan ook van mening dat de verantwoordelijkheid voor accreditatie niet bij een centrale partij belegd kan worden. Daartegenover overweegt het kabinet een entiteit aan te wijzen die *goedkeuring* moet verlenen alvorens de SG van een ministerie accreditatie verleent voor de verwerking van nationaal gerubriceerde informatie. Dit punt zal opgenomen worden in het vervolgonderzoek.

Tot slot is het kabinet, met u, van mening dat het ook van belang is dat het toezicht op de beveiliging van staatsgeheimen wordt verbeterd. Het kabinet zet op de korte termijn in eerste instantie in op verduidelijking en versterking van het huidige toezichtstelsel. Afgelopen periode heeft dat onvoldoende invulling gekregen, zowel op de departementen, als op Rijksbreed niveau. Inmiddels is het veiligheidsbewustzijn sterk gestegen o.a. door veranderde geopolitieke verhoudingen. Daarom wordt ook het toezicht versterkt. In deze brief staat beschreven hoe het kabinet dit komende periode gaat realiseren.

Aanvullend zal het kabinet komende periode onderzoeken of in aanvulling op het versterken van het bestaande stelsel, een externe toezichthouder noodzakelijk en/of wenselijk is. Dit heeft voor- en nadelen en is een complexer vraagstuk, wat ook initiatiefnemers al benoemen. Zo streeft het kabinet naar een efficiënte Rijksdienst en wil het onnodige stapeling van toezicht of het inrichten van een «control-toren» voorkomen. Dit vraagstuk vraagt derhalve meer tijd en zal zorgvuldig in kaart worden gebracht. Eind 2025 wordt u geïnformeerd over de stand van zaken en het kabinets-standpunt hierover.

De initiatiefnota verwijst naar het rapport Digitale Kroonjuwelen[1]. Hierover is toegezegd dat u voor de zomer over de opvolging ervan zou worden gerapporteerd[2]. Gelet op de samenhang met de initiatiefnota wordt u hierover eveneens eind 2025 geïnformeerd.

[1] *Kamerstukken II*, 2022–23, 26 643, nr. 1044
[2] Toezegging TZ202409-069, *Kamerstukken II*, 2024–25, 26 643, nr. 1277

## 1. Beslispunt: Wettelijke basis

Het kabinet erkent dat een wettelijke regeling van de omgang met gerubriceerde informatie beperkt is. Dit betekent niet dat er géén wettelijke regels over zijn. Zo bevat het wetboek van strafrecht enkele delictsbepalingen die het delen en openbaren van gerubriceerde inlichtingen strafbaar stellen. Ook biedt de Wet bescherming staatsgeheimen Ministers de mogelijkheid om verboden plaatsen aan te wijzen, waartoe de toegang beperkt is in het belang van de bescherming van de aldaar bewaarde en verwerkte staatsgeheimen. Dat deze wettelijke bepalingen niet de door de initiatiefnemers gewenste volledigheid hebben, is evident. Voor zover het gaat om digitaal opgeslagen gerubriceerde informatie is verder het wetsvoorstel Cyberbeveiligingswet relevant. Daarin worden ter implementatie van de zogenoemde NIS2-richtlijn regels voorgesteld voor de beveiliging van netwerk- en informatiesystemen van onder andere ministeries. Dit wetsvoorstel bevat ook toezicht- en handhavingsbevoegdheden.

Gedetailleerdere regels over de omgang met gerubriceerde informatie bestaan echter wel. Deze regels zijn gevat in het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013). Dit voorschrift is weliswaar geen wet in formele zin, maar is desalniettemin bindend voor de Rijksdienst. Dit voorschrift bevat onder andere regels over het delen en beveiligen van gerubriceerde informatie, alsook nadrukkelijk de instructie om rubriceringen periodiek te heroverwegen. Het VIRBI gaat, overeenkomstig de constatering van de initiatiefnemers, voornamelijk uit van beheer van gerubriceerde informatie per ministerie. Een belangrijke rol wordt hierbij toegekend aan de secretarissen-generaal en de beveiligingsautoriteiten van de afzonderlijke ministeries. Volledig gescheiden is de werking van het VIRBI niet, de toelichting maakt duidelijk dat waar de BVA het eerste en centrale aanspreekpunt binnen het ministerie vormt, de AIVD (tevens NSA in civiele aangelegenheden) deze rol heeft voor de gehele Rijksdienst met uitzondering van het Ministerie van Defensie waar deze taak is belegd bij de beveiligingsautoriteit van het Ministerie van Defensie (tevens NSA in militaire aangelegenheden).

Verwant aan het VIRBI 2013 is het besluit BVA-stelsel Rijksdienst 2021. Dit besluit bevat niet alleen de verplichting voor de secretarissen-generaal om een beveiligingsautoriteit aan te wijzen, het definieert tevens de rol van de Beveiligingsautoriteit Rijk (BVA Rijk). De BVA Rijk is belast met het bewaken van het integrale karakter en de consistentie van Rijksbrede kaders voor integrale beveiliging, het bevorderen van een interdepartementale aanpak van beveiligingsissues, alsmede het toezicht op de werking van de integrale beveiliging van de Rijksdienst. Het besluit BVA-stelsel Rijksdienst 2021 laat ruimte voor uitzonderingen voor het Ministerie van Defensie.
De behandeling van internationale informatie is vastgelegd in volkenrechtelijke besluiten op basis van verdragen zoals het Noord-Atlantisch Verdrag en de verdragen inzake de (werking van) de Europese Unie. Daarnaast worden met landen beveiligingsverdragen afgesloten die geratificeerd worden door de Staten-Generaal. Hierin is de rol van de NSA's in respectievelijk civiele en militaire aangelegenheden vastgelegd in het kader van toezicht op de uitvoering.

Tot slot kan het kabinet mededelen dat momenteel gewerkt wordt aan de opvolger van het VIRBI 2013.

## 2. Beslispunt: Centrale toezichthouder

Op dit moment is het toezicht getrapt in gevuld. Er zijn drie lijnen van verdediging, zoals de initiatiefnota ook beschrijft, die bijdragen aan het toezicht:

1. De 1e lijn betreft de medewerkers zelf en het lijnmanagement van het betreffende dienstonderdeel.
2. de 2e lijn is de staforganisatie. Een beveiligingscoördinator (BVC'er) van een betreffend dienstonderdeel en chief information security officer (CISO).
3. De derde lijn is de centrale Beveiligingsautoriteit (BVA) van een departement. Daarnaast is de Beveiligingsautoriteit Rijk erbij gekomen en de CISO Rijk bij BZK, vanuit de Rijksbrede verantwoordelijkheid.
4. De ADR is de interne auditor van de Rijksoverheid en geeft inzicht geven in naleving van wet- en regelgeving. De ADR voert daarvoor onderzoeken uit vanuit haar wettelijke controletaak (conform de Comptabiliteitswet 2016) en in opdracht van de departementsleiding en rijksbrede stelselhouders. In de meerjarige programmering voor 2025 staat onderzoek gepland naar hoger gerubriceerde omgevingen.
5. De NAVO, en ook de EU voert periodiek toezicht uit op de behandeling van respectievelijk NAVO of EU informatie. Daarbij worden bezoeken afgelegd bij diverse departementen.

De rol van BVA Rijk wordt door initiatiefnemers niet benoemd. De BVA Rijk is belast met het bewaken van het integrale karakter en de consistentie van rijksbrede kaders voor integrale beveiliging, het bevorderen van een interdepartementale aanpak van beveiligingsissues, alsmede het toezicht op de werking van de integrale beveiliging van de Rijksdienst. Deze rol was tot op heden slechts zeer beperkt ingevuld en o.a. de centrale toezichttaak heeft afgelopen periode nauwelijks invulling gekregen. Het BVA-stelsel Rijksdienst geeft hiervoor echter wel een duidelijke basis. Hoewel deze basis niet volledig overeenkomt met de in de initiatiefnota beoogde doorzettingsmacht en bindende bevoegdheden, kan dit voor een deel al tegemoetkomen aan de beschreven tekortkomingen. Zo is deze rol buiten de departementen geplaatst en kan deze in bepaalde mate als escalatie buiten het departement dienen. Bevoegdheden en mandaten zijn daarvoor reeds vastgesteld in het besluit BVA-stelsel Rijksdienst 2021. Door het toenemende belang van veiligheid was het kabinet al begonnen om de rol van BVA Rijk beter in te vullen en te versterken. Het bureau BVA Rijk wordt uitgebreid ook met functies voor de invulling van toezicht en ook de positie van het bureau wordt versterkt.

Daarnaast is versterking van de overige bestaande lijnen cruciaal omdat daarmee de organisatie die zich bezig houdt met staatsgeheime informatie, direct wordt bereikt. Juist de goede samenwerking van al deze lijnen zorgt voor een betere naleving van de bestaande wet en regelgeving op dit vlak. Het is cruciaal dat hierin meer wordt geïnvesteerd, waarna het voor de toezichthouders eenvoudiger wordt om de goede naleving te controleren.

Europese landen hanteren verschillende modellen voor toezicht op gerubriceerde informatie. In Italië, Frankrijk en Luxemburg fungeert de NSA als centrale autoriteit voor de beveiliging van nationaal en internationaal gerubriceerde informatie. Estland belegt het centrale toezicht bij de interne veiligheidsdienst. Zweden wijkt af door geen centrale autoriteit te hebben, maar laat toezicht uitvoeren door de civiele en militaire inlichtingendiensten.

Naast versterking van genoemde bestaande lijnen kan het toezicht ook worden versterkt door het creëren van een «aanvullende lijn» met een nieuwe extra externe toezichthouder, zoals in de initiatiefnota beschreven. Dit heeft voor- en nadelen en is een complexer vraagstuk, waarin ook initiatiefnemers al diverse zaken benoemen. Dit vraagt meer tijd en zal zorgvuldig in kaart worden gebracht. Waaronder de vergelijking met de rol van de NSA en het internationale en nationale domein. Komende periode wordt dit nader onderzocht en eind 2025 wordt u geïnformeerd over de stand van zaken en het kabinetsstandpunt hierover.

Onafhankelijkheid

Er is sprake van diverse gradaties in de mate van onafhankelijkheid. Er is altijd sprake van een bepaald «eindstation» in het afleggen van verantwoording. In het huidige toezicht op de beveiliging van staatsgeheimen is dat bij de Rijksoverheid al op hoog-ambtelijk niveau. In het huidige stelsel is een hoge mate van onafhankelijkheid voorzien binnen de Rijksoverheid. De Beveiligingsautoriteit als 3e lijn toezichthouder, is bewust voorzien buiten de normale lijnstructuur en kent een hoge mate van onafhankelijk positie, heeft een sterk mandaat en bevoegdheden die zijn vastgelegd in het Besluit BVA-stelsel Rijksdienst 2021. Deze heeft directe toegang tot de hoogste ambtelijke leiding (SG). Aanvullend is er een rol voor de Beveiligingsautoriteit Rijk voorzien. Deze voert rijksbreed toezicht uit en staat onafhankelijk van departementen, vanuit de coördinerende verantwoordelijkheid van BZK.

Tegelijkertijd realiseert het kabinet zich dat de huidige organisatorische-invulling bij departementen grote verscheidenheid kent, ook in de gradatie van onafhankelijkheid. Daarom zal komende periode kritisch worden bezien hoe het toezicht momenteel per departement is ingevuld en waar versterking/verbetering nodig is. De in de initiatiefnota genoemde «eisen aan de toezichthouder» (7.) worden hierin betrokken. Dit onderzoek naar het bestaande toezicht is in aanvulling op het eerder genoemde onderzoek naar een nieuwe extra externe toezichthouder. U wordt over beide geïnformeerd bij de verdere reactie op uw initiatiefnota eind 2025.

## 3. Beslispunt: Accreditatie, beleid en advies

Het kabinet hanteert de volgende definities die relevant zijn voor het beslispunt:
- *Accreditatie:* het verlenen van toestemming voor ontvangst, beheer, vernietiging, verwerking en verdere verspreiding van gerubriceerde informatie.
- *Goedkeuring:* het na onderzoek vaststellen of de beveiliging van nationaal en internationaal staatsgeheim gerubriceerde informatie voor wat betreft de bescherming van de nationale en internationale belangen aan de vereisten voldoet en vervolgens akkoord hierop geven.
- *Beleid:* de rijksbrede kaders voor de verwerking en beveiliging van nationaal en internationaal staatsgeheim gerubriceerde informatie
- *Advies:* advisering aan de betrokken overheidsorganisaties over implementatie van hetgeen in het *beleid* is vastgesteld.

In het huidige informatiebeveiligingsstelsel zijn deze rollen thans op verschillende plaatsen belegd. Iedere SG van een ministerie is conform het VIRBI 2013 (2025 zodra het gepubliceerd is) verantwoordelijk voor het verlenen van accreditatie binnen het ministerie. Dit volgt logischerwijs uit het gegeven dat elke Minister verantwoordelijk is voor de bedrijfsvoering van diens ministerie (artikel 4.1 Comptabiliteitswet). Het kabinet is dan ook van mening dat de verantwoordelijkheid voor accreditatie niet bij een

centrale partij belegd kan worden. Immers, er is dan één partij die accreditatie verleend voor alle departementen – en daarmee dus de verantwoordelijkheid draagt voor de verwerking van nationaal en internationaal staatsgeheim gerubriceerde informatie bij alle departementen. Dit is strijdig met de Comptabiliteitswet; en tevens volgens het kabinet niet gewenst, omdat het de ministeries zelf van hun verantwoordelijkheid voor een deugdelijke verwerking van staatsgeheimen zou ontslaan.

Daartegenover overweegt kabinet een entiteit aan te wijzen die *goedkeuring* moet verlenen alvorens de SG van een ministerie accreditatie verleent voor de verwerking van nationaal gerubriceerde informatie. Deze constructie bestaat thans enkel voor internationaal gerubriceerde informatie, waarbij goedkeuring vereist is van de NSA alvorens de Security Accreditation Authority (SAA)[3] accreditatie verleent (conform VIRBI en internationale afspraken). Het kabinet is van mening dat deze constructie ook passend zou kunnen zijn voor nationaal gerubriceerde informatie. Defensie heeft deze accreditatie opzet al beschreven in haar Defensie beveiligingsbeleid en past deze al langer toe. Dit punt zal opgenomen worden in het vervolg onderzoek, waaronder waar deze rol dan belegd zou worden.

Voor wat betreft beleid heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties een coördinerende rol, belegd bij de BVA Rijk en de CISO Rijk, zoals vastgelegd in respectievelijk het Besluit BVA-stelsel Rijksdienst 2020 en het Besluit CIO-stelsel Rijksdienst 2020. Het kabinet is van mening dat deze coördinerende beleidsrol hier ook moet blijven.

Advies over de beveiliging van nationaal en internationaal als staatsgeheim gerubriceerde informatie, wordt op dit moment gegeven door de AIVD, specifiek het Nationaal Bureau voor Verbindingsbeveiliging (NBV), onderdeel van de Unit Weerbaarheid voor de Rijksoverheid met uitzondering van Defensie. Op grond van het Organisatiebesluit AIVD 2023 is het NBV aangewezen als NSA in civiele aangelegenheden. Wettelijke basis voor deze rol in nationale aangelegenheden vormt artikel 8, lid 2, sub c van de Wet op de inlichtingen- en veiligheidsdiensten 2017: «het bevorderen van maatregelen [...] ter beveiliging van gegevens waarvan de geheimhouding door de nationale veiligheid wordt geboden». Voor Defensie is advies en toezicht belegd bij de Beveiligingsautoriteit, tevens NSA in militaire aangelegenheden op NAVO en EU informatie. Daarnaast is dit voor de overige lijnen vastgelegd in bijvoorbeeld het VIRBI 2013 en het Besluit BVA-stelsel Rijksdienst 2021. Op internationaal niveau zijn afspraken gemaakt en vastgelegd in beveiligingsverdragen en in besluiten op basis van het Noord-Atlantisch Verdrag, het ESA-verdrag en EU-verdragen. In de nadere kabinetsreactie zal verder worden ingegaan op de belegging van deze verantwoordelijkheid, omdat die sterk samenhangt met de rollen van toezicht en goedkeuring.

Ten slotte merkt het kabinet op dat het Nationaal Bureau Industrieveiligheid (NBIV) is opgericht op 28 maart 2025.[4] Het NBIV heeft tot taak het bevorderen van maatregelen ten aanzien van de beveiliging van gegevens en materiaal waarvan de bescherming door de nationale veiligheid wordt geboden. Hiervoor controleert en begeleidt het NBIV bedrijven die voor de Rijksoverheid (waaronder het Ministerie van Defensie) en de Nationale Politie opdrachten uitvoeren die, vanwege hun karakter, beveiligingsmaatregelen vereisen om de nationale veiligheid te borgen. In essentie

[3] De secretaris-generaal van het ministerie is de SAA voor civiele omgevingen en de Beveiligingsautoriteit van het Ministerie van Defensie voor defensieomgevingen.
[4] Regeling Nationaal Bureau Industrieveiligheid, Stcrt. 2025, nr. 6982

begeleidt het NBIV de uitvoering en naleving van het voorschrift Algemene Beveiligingseisen Rijksoverheid Opdrachten (ABRO) en voert het NBIV hier controle op. Dit doet het NBIV zowel voor nationaal als internationaal gerubriceerde informatie; zo zal het NBIV ook Facility Security Clearances (FSC's) afgeven voor bedrijven die opdrachten voor EU, NAVO of ESA uitvoeren. Daarmee vervult het NBIV een belangrijke functie in de beveiliging van informatie in de toeleveringsketen.

**4. Beslispunt: Hoog gerubriceerde informatievoorziening (HGI)**

Er is een stijgende trend te herkennen in het werken met hoog gerubriceerde informatie (Staatsgeheim CONFIDENTIEEL, Staatsgeheim GEHEIM en Staatsgeheim ZEER GEHEIM) binnen de Rijksoverheid. Elk departement heeft zijn eigen staatsgeheime informatie en op interdepartementaal niveau bestaat toenemende behoefte om ook met staatsgeheime informatie samen te werken. Momenteel is het landschap om staatsgeheime informatie te verwerken en onderling digitaal te kunnen uitwisselen versnipperd en niet volledig geharmoniseerd binnen de rijksdienst. Voor het beschermen van onze staatsgeheimen moeten we de ICT-systemen en andere randvoorwaarden op orde te hebben en zorgen dat deze voorzieningen interoperabel zijn met andere hoog gerubriceerde informatievoorzieningen. Defensie loopt hierin voorop vanwege haar primaire taakstelling en internationale samenwerking.

1. Het onderwerp een *Rijksbrede HGI-voorziening* is een speerpunt en het voornemen is om een Rijksbreed meerjarig traject te starten om dit te realiseren. Besluitvorming is komende periode voorzien in het Secretarissen-Generaal Overleg (SGO).
2. In dit traject wordt er ingezet op het versterken en uitbreiden van bestaande hoog gerubriceerde informatievoorzieningen en te zorgen dat deze voorzieningen toekomstbestendig zijn.
3. Voor het onderwerp High Assurance is er een reeds bestaand programma binnen de Rijksoverheid, de Nationale Cryptostrategie (NCS). Dit programma richt zich op het versneld ontwikkelen van eersteklas informatiebeveiligingsproducten voor hoog gerubriceerde informatie en het stimuleren van kennisontwikkeling. De NCS zet in op versterking van de samenwerking tussen en binnen Rijksoverheid, bedrijfsleven, universiteiten en kennisinstellingen. Bij relevante ontwikkelingen op het gebied van High Assurance en de NCS zal de Kamer op passende wijze hierover geïnformeerd worden.
4. Zie 2.

U wordt over de voortgang van het traject HGI separaat en vertrouwelijk geïnformeerd.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
J.J.M. Uitermark