bijlage

Bijlage bij Beleidsreactie met stand van zaken aanbevelingen

Bijlage nummer	1
Datum	13 november 2025
Behorende bij	Beleidsreactie CTIVD-rapporten nr. 81 en nr. 82

CTIVD rapport 81

1. *Maak beleid en een proces voor de informatie-uitwisseling gedurende het veiligheidsonderzoek tussen de inlichtingenteams (A- en D-taak) enerzijds en de veiligheidsonderzoekers (B-taak) anderzijds*

    - Deze aanbeveling wordt overgenomen.
    - In deze aanbeveling is reeds voorzien. In april 2024 is beleid ingesteld over de informatie uitwisseling tussen de A- en D-taak enerzijds en de B-taak anderzijds. Nieuw is de interne melding, een laagdrempelige manier van interne informatieverstrekking. Te allen tijde, dus ook gedurende een veiligheidsonderzoek, kan informatie worden uitgewisseld.
    - Met de melding wordt schriftelijk vanuit de A- en D-taak informatie verstrekt richting de B-taak. De Unit Veiligheidsonderzoeken (UVO) beoordeelt vervolgens of de melding betrekking heeft op een persoon die een vertrouwensfunctie vervult of een veiligheidsonderzoek ondergaat. Als dit het geval is, wordt beoordeeld of de informatie nieuwe feiten of omstandigheden bevat die een hernieuwd veiligheidsonderzoek rechtvaardigen of van belang zijn voor het lopende veiligheidsonderzoek.
    - Indien een negatief besluit in het veiligheidsonderzoek wordt gebaseerd op de informatie uit de A- en D-taak, dient aan de UVO een interne *mededeling* te worden verstrekt. Dit is een zwaardere procedure dan de interne *melding*. De interne mededeling wordt onderbouwd met onderliggende stukken, zodat de conclusie in de interne mededeling kan worden gecontroleerd. De bezwarencommissie en rechter kunnen deze stukken onder geheimhouding inzien.

2. *Concretiseer in het beleid wanneer en op welke wijze inlichtingenteams inlichtingeninformatie kunnen delen met de UVO ten behoeve van een veiligheidsonderzoek*

    - Deze aanbeveling wordt overgenomen.
    - Ten behoeve van het hiervoor toegelichte meldingenproces is een centraal punt (mailbox) ingericht voor de inlichtingenteams waarop zij middels een meldingenformulier informatie met de UVO kunnen delen.
    - Daarnaast kan inlichtingeninformatie met de UVO worden gedeeld middels een interne mededeling, wat een zwaardere procedure is. Dit hangt samen met het feit dat deze informatie veelal ten grondslag ligt aan de weigering of intrekking van een VGB en/of clearance.

3. *Concretiseer het beleid om zorgvuldige besluitvormingsprocedures en vastlegging van afwegingen over persoonlijke gedragingen en omstandigheden te waarborgen voor de gevallen waarin twijfel bestaat over het al dan niet afgeven van een VGB*

    - Deze aanbeveling wordt overgenomen, met de volgende nuance.
    - Alles dat relevant is in een zaak, alsmede de afwegingen die door een bewerker worden gemaakt ten aanzien van het afgeven dan wel weigeren of intrekken van een VGB, worden vastgelegd in het dossier in het UVO-systeem. Dit gebeurt in alle zaken, dus ook in de gevallen waarin wordt getwijfeld. Daarbij is iedere bewerker (inmiddels) doordrongen van het belang van een goede vastlegging. Het is onderdeel van de opleiding voor nieuwe bewerkers en komt aan bod in werkoverleggen en werkinstructies.
    - Er zijn richtlijnen waarin is opgenomen hoe bepaalde persoonlijke gedragingen en omstandigheden (PGO) in het veiligheidsonderzoek moeten worden gewogen. Het wegen van PGO in een veiligheidsonderzoek zal echter altijd maatwerk blijven, dus niet alles is vast te leggen in beleid.
    - Ten aanzien van het volgen van een zorgvuldige besluitvormingsprocedure wordt opgemerkt dat er vaste accorderingslijnen zijn, die gevolgd dienen te worden. Daarin is voorzien in de noodzaak van een hoger belegd akkoord (unithoofd) als sprake is van de intrekking van een VGB, als het een weigering betreft van een A+ onderzoek, een weigering op grond van inlichtingeninformatie en alle zogenoemde artikel 13 Wvo zaken. Maar ook positieve besluiten moeten aan het unithoofd worden voorgelegd als in het voorgenomen besluit nog was gekomen tot een weigering of intrekking (tenzij de voorgenomen weigering was gebaseerd op onvoldoende gegevens).

4. *Neem in beleid op hoe de AIVD invulling geeft aan de discretionaire bevoegdheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties om periodieke herhaalonderzoeken in te stellen*
    - Deze aanbeveling wordt overgenomen, met de volgende nuance.
    - De wijziging van de Wvo, die in 2026 van kracht wordt, introduceert een register van actieve vertrouwensfuntionarissen en voert een aan- en afmeldplicht in voor werkgevers. Met dit register komt de Minister van BZK op termijn te beschikken over een

actueel en volledig overzicht van vertrouwensfunctionarissen en wordt het voor de minister van BZK mogelijk om invulling te geven aan de discretionaire bevoegdheid om een herhaalonderzoek te doen instellen. De UVO onderzoekt momenteel op welke wijze hier via het register invulling aan kan worden gegeven.

5. *Neem in beleid op hoe de AIVD invulling geeft aan de discretionaire bevoegdheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties om incidentele herhaalonderzoeken in te stellen, in het geval dat bij de AIVD feiten en omstandigheden over een vertrouwensfunctionaris bekend zijn*

    - Deze aanbeveling wordt overgenomen.
    - De UVO beoordeelt of nieuwe feiten of omstandigheden een hernieuwd veiligheidsonderzoek rechtvaardigen na, bijvoorbeeld, een melding uit "automatisch alerteren" of van een inlichtingenteam. Enkele maanden geleden is het zogenoemde meldingenproces ingericht waarbij inlichtingteams die beschikken over informatie over een vertrouwensfunctionaris, op een laagdrempelige manier de UVO hier van op de hoogte kunnen stellen. Aan dit meldingenproces is op verschillende manieren dienstbreed aandacht besteed en het is opgenomen in het Handboek Inlichtingenwerk.
    - Tevens heeft de UVO het beleid rondom het instellen van een incidenteel herhaalonderzoek geconcretiseerd. Er zijn criteria opgesteld waaraan de UVO eenvoudig kan toetsen of de ontvangen signalen aanleiding zijn om een hernieuwd veiligheidsonderzoek in te stellen.

6. *Leg twijfels of bijzonderheden over het al dan niet afgeven van een VGB vast. Raadpleeg bij een herhaalonderzoek het procesformulier van het vorige veiligheidsonderzoek, zodat indien nodig extra aandacht kan worden gegeven aan onderwerpen waarbij twijfel bestond of bijzonderheden waren*

    - Deze aanbeveling wordt overgenomen.
    - Zoals ook is opgemerkt bij aanbeveling 1 zullen twijfels en bijzonderheden worden vastgelegd in het dossier.

7. *Maak beleid hoe veiligheidsonderzoekers in het kader van het criterium "eerlijk" moeten omgaan met niet volledig of niet juiste ingevulde OPG's*

    - Deze aanbeveling wordt overgenomen, met de volgende nuance.
    - In de bestaande werkwijze is het ontbreken van essentiële informatie in de OPG in beginsel aanleiding om betrokkene hierover te bevragen en indien nodig, de OPG aan te laten vullen. Geconstateerde tegenstrijdigheden in de OPG zijn altijd reden het dossier voor te leggen aan Triage of direct door te sturen voor diepteonderzoek.
    - Voor deze werkwijze zal extra aandacht worden gevraagd bij de veiligheidsonderzoekers.

8. *Waarborg informatiedeling tussen de afdelingen die zicht hebben op signalen over de informatiebeveiliging bij andere (overheids)organisaties waarmee wordt samengewerkt*

9. *Vergroot de bekendheid en bevorder de meldingsbereidheid <door AIVD medewerkers> om vermoedens over gebrekkige informatiebeveiliging bij andere (overheids)organisaties bij de BVA van de AIVD te melden*

    - Deze aanbevelingen worden overgenomen.
    - De BVA heeft het initiatief genomen voor een regulier overleg met de NSA, specifiek met dit doel: zijn er voor zover men daar vanuit de eigen taakuitvoering zicht op heeft signalen bij andere (overheids)organisaties dat de beveiliging van staatsgeheime gegevens in gevaar raken of dat de inrichting of werking van veiligheidsmaatregelen tekortschiet? Dit overleg heeft voor het eerst plaatsgevonden in oktober 2025, en zal periodiek worden herhaald.
    - Daarnaast zal de BVA werken aan bekendheid en bewustwording bij alle AIVD'ers, zodat zij vermoedens over gebrekkige informatiebeveiliging bij andere (overheids)organisaties bij de BVA van de AIVD melden. De BVA neemt dit per oktober 2025 mee in de presentatie bij de instroom van nieuwe AIVD-collega's en zal dezelfde boodschap ook via Intranet en een toevoeging aan de Leidraad Integrale Beveiliging bekend maken.

10. *Draag er zorg voor dat NL-Net voldoet aan beveiligingseisen, zodat veilige verzending wordt geborgd*

    - Deze aanbeveling wordt overgenomen.
    - In juli 2025 is door de AIVD intern prioriteit gegeven aan de accreditatie van NL-Net. Eventuele restrisico's worden in kaart gebracht en plannen voor mitigerende maatregelen worden opgesteld.
    - De verwachting is dat de door het management getekende accreditatiedocumentatieset in november 2025 aan de BVA AIVD voor beoordeling wordt aangeboden. De BVA AIVD en BA Defensie zullen vervolgens bij een positieve beoordeling gezamenlijk NL-Net accrediteren.

11. *Leg in beleid vast waarom (categorieën van) producten worden gedeeld met andere overheidsinstanties. Besteed daarbij aandacht aan het bieden van handelingsperspectief en het need-to-know-principe*

    - Deze aanbeveling wordt overgenomen.
    - In beleid zal voor de belangrijkste afnemers worden vastgelegd waarom zij bepaalde producten kunnen ontvangen. Daarbij wordt aangegeven ten behoeve van welke taakuitvoering zij producten ontvangen, welke handelingsperspectieven deze producten dienen en wat de *need to know* is van (onderdelen van) deze organisaties.
    - Dit zal generiek beleid zijn. Het is goed om zulk generiek beleid vast te stellen omdat het een richtlijn geeft voor de opstellers en leidinggevenden.

- Specifieke verstrekking van producten is altijd casus afhankelijk en er kan aanleiding zijn voor een uitzondering op het beleid.
- Het beleid zal helpen om voor individuele producten vast te stellen of deze passen in de reguliere exploitatie aan afnemers. Indien de exploitatie afwijkend is helpt het beleid bij het scherp krijgen waarom een afnemer een product toch moet ontvangen, c.q. of de ontvanger wel een handelingsperspectief en een *need to know* heeft.
- Het beleid zal zodoende compliance bevorderen.
- Tevens zal bekeken worden of het mogelijk is om de reguliere afnemers standaard in te vullen als geadresseerde, zodat de verzending minder foutgevoelig wordt.

12. *Concretiseer het NSA-beleid. Houd bij de formulering van het beleid rekening met de verwachtingen vanuit internationale regelgeving*

    - Deze aanbeveling wordt overgenomen.
    - Na aanleiding van het incident bij de NCTV is dit in een eerder stadium al geconcludeerd. Derhalve is de herziening en uitwerking van het NSA-beleid opgenomen in jaarplanregels voor 2025.
    - De actualisering richt zich op (1) het interpreteren van de internationale regelgeving naar Nederlandse beleidsuitvoering, (2) het opstellen van inspectie- en schouwplannen om overheidsorganisaties de komende jaren te controleren op naleving van internationale regelgeving en (3) het vaststellen van een strategie hoe de NSA de overheid kan bedienen, vanuit een ondersteunende en adviserende rol, rondom de internationale regelgeving.

13. *Maak de controle op de naleving van de afgifte en verlenging van PSCC's onderdeel van accreditaties en inspecties*

    - Deze aanbeveling wordt overgenomen.
    - De AIVD is voornemens dit onderdeel te maken van het inspectiebeleid zoals beschreven in aanbeveling 12.

14. *Betrek de gesignaleerde discrepantie tussen internationale regelgeving en het Nederlandse stelsel bij de herziening van het VIRBI 2013*

    - Deze aanbeveling wordt overgenomen met de volgende nuancering.
    - De AIVD heeft als NSA een *centrale* verantwoordelijkheid met betrekking tot bescherming van internationaal gerubriceerde informatie. De taak van de NSA omvat onder meer het accrediteren en inspecteren van alle informatiestromen van (overheids)instanties die dergelijke informatie verwerken, waaronder de NCTV.
    - Het beleid van de AIVD zoekt echter ook aansluiting bij het VIRBI, dat een *decentrale* benadering heeft. In het VIRBI zijn de SG's van departementen verantwoordelijk voor de omgang met gerubriceerde gegevens, waaronder internationaal gerubriceerde gegevens. De CTIVD ziet hier een discrepantie die betrokken dient te worden bij de herziening van het VIRBI.

- Hoewel het VIRBI uitgaat van een decentrale benadering is van belang dat de AIVD centraal verantwoordelijk is voor de accreditatie, wanneer (overheids)instanties internationaal gerubriceerde informatie verwerken. De NSA geeft een accreditatie af wanneer aan alle internationaal vastgestelde beveiligingseisen is voldaan om het juiste beveiligingsniveau te waarborgen. Als nog niet aan alle eisen is voldaan, kan de NSA een tijdelijke accreditatie met verbeteractiviteiten binnen een bepaalde termijn afgeven of besluiten de accreditatie af te wijzen. Een afwijzing, of het ontbreken van een accreditatie, heeft als gevolg dat een (overheids)instantie geen internationaal gerubriceerde informatie mag verwerken.
- Deze bevoegdheid geeft de AIVD het instrument om centraal verantwoordelijkheid uit te oefenen. Op dit moment wordt het NSA-beleid zoals uitgeoefend door de AIVD herzien, om tot strenger en frequenter handhavingsbeleid te komen. Hierdoor wordt nadrukkelijker handen en voeten gegeven aan de internationale verantwoordelijkheid van de AIVD als NSA.
- Het bovenstaande zal waar nodig worden betrokken bij de eerstvolgende wijziging van het VIRBI.

15. *Zorg voor betere vastlegging van de uitvoering van de NSA-taak. Leg dit vast in het beleid*

    - Deze aanbeveling wordt overgenomen.
    - Zie aanbeveling 12 en 13.

16. *Betrek in de accreditatie van NL-NET de standaarden voor internationaal gerubriceerde informatie*

    - Deze aanbeveling wordt overgenomen.
    - De beveiligingsvereisten in de Beveiligingsnormen Inlichtingen- en Veiligheidsdiensten (BNIVD), gebaseerd op de belangrijkste beveiligingsnormen waaronder het VIRBI, zullen in beginsel overeenkomen met de standaarden voor de beveiliging van internationaal gerubriceerde informatie.
    - De accreditatie van NL-Net zal langs de BNIVD zijn, conform AIVD en MIVD-beleid. De BVA zal de NSA vervolgens betrekken bij het doornemen van de accreditatiedocumentatieset om naar een tijdelijke of permanente goedkeuring voor de verwerking van internationaal gerubriceerde informatie toe te werken, zoals benoemd bij aanbeveling 10.

17. *Adresseer de onderliggende factoren – het ontbreken van regelgeving, capaciteit en bestuurlijke prioritering – die een zorgvuldige uitvoering van de NSA-taak bemoeilijken in relatie tot overheidsorganisaties. Onder meer om te bewerkstelligen dat de NSA over voldoende doorzettingsmacht en escalatiemogelijkheden beschikt*

    - Deze aanbeveling wordt overgenomen.
    - Zoals genoemd bij aanbeveling 14 geeft de NSA een accreditatie af wanneer aan alle internationaal vastgestelde beveiligingseisen is voldaan om het juiste beveiligingsniveau te waarborgen. Als nog niet aan alle eisen is voldaan, kan de NSA een tijdelijke

accreditatie met verbeteractiviteiten binnen een bepaalde termijn afgeven of besluiten de accreditatie af te wijzen. Een afwijzing, of het ontbreken van een accreditatie, heeft als gevolg dat een (overheids)instantie geen internationaal gerubriceerde informatie mag verwerken.

- Deze bevoegdheid geeft de AIVD het instrument om centraal verantwoordelijkheid uit te oefenen. Op dit moment wordt het NSA-beleid zoals uitgeoefend door de AIVD herzien, om tot strenger en frequenter handhavingsbeleid te komen. Hierdoor wordt nadrukkelijker handen en voeten gegeven aan de internationale verantwoordelijkheid van de AIVD als NSA.
- De NSA adresseert momenteel het capaciteitsvraagstuk door de lege formatieplaatsen voor inspecteurs met voorrang te gaan vullen. Hierdoor ontstaat meer capaciteit om de toezichtsrol richting overheidsorganisaties voor wat betreft internationaal gerubriceerde informatie intensiever te gaan invullen. Ook kan er door de NSA meer focus worden aangebracht op de NSA-taak voor de rijksoverheid doordat de werkzaamheden inzake de industrieveiligheid, die eerst bij de NSA waren belegd, zijn ondergebracht bij het Nationaal Bureau Industrieveiligheid (NBIV).
- De NSA zal de bestuurlijke prioritering adresseren in het beleid (zie aanbeveling 12). De NSA constateert dat de bestuurlijke prioritering voornamelijk ontbreekt bij overheidsorganisaties. Het beeld is dat dit mede komt door het gebrek aan bewustzijn bij overheidsorganisaties dat er voor internationale regelgeving andere voorwaarden gelden dan in het nationale stelsel van toepassing is. De NSA wil derhalve de ondersteuning en het advies richting overheidsorganisaties gaan intensiveren. De concrete invulling daarvan zal worden verwerkt in de actualisatie van het beleid.

CTIVD rapport 82

1. *Maak beleid en vergroot de bekendheid om vermoedens over gebrekkige informatiebeveiliging bij andere overheidsinstanties of defensieonderdelen <door medewerkers van de MIVD> bij de BC van de MIVD te melden*
    - Deze aanbeveling wordt overgenomen.
    - De MIVD is voornemens beleid op te stellen en de bekendheid te vergroten om vermoedens over gebrekkige informatiebeveiliging bij andere overheidsinstanties of defensieonderdelen door medewerkers van de MIVD bij de Beveiliging coördinator (BC) van de MIVD te melden.
    - Daarbij verdient het opmerking dat er reeds diverse procedures en meldpunten zijn waar incidenten ten aanzien van informatiebeveiliging reeds kunnen worden gemeld. In het opvolgen van de aanbeveling zal de MIVD de bekendheid van deze meldpunten en procedures extra belichten.

2. *Leg in beleid vast waarom (categorieën van) producten worden gedeeld met andere overheidsinstanties. Besteed daarbij aandacht aan het bieden van handelingsperspectief en het need-to-know-principe*
    - Deze aanbeveling wordt overgenomen.
    - De MIVD is reeds bezig met het opstellen van dit beleid. Momenteel wordt er gewerkt aan duidelijke richtlijnen wanneer en met wie er bepaalde informatie/producten gedeeld mag worden en onder welke voorwaarden dit kan.
    - Na het vaststellen van deze richtlijnen zullen deze onder de aangewezen medewerkers worden verspreid en worden deze tevens meegenomen in de opleidingen.