Ministerie van Justitie en Veiligheid

MJenV

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Strafrechtelijke handhaving

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Datum
2 oktober 2026

Bijlage(n)
1

nota

Brief TK rapport commissie Smit

1. Aanleiding

Op 27 augustus jongstleden heeft Jaap Smit aan u het rapport "Van 'brand meester' naar 'brandveilig'. Onderzoek naar de ICT-inbreuk bij het Openbaar Ministerie" overhandigd. Het rapport is een evaluatie van de ICT-inbreuk bij het OM in juli 2025. Op 21 september jongstleden heeft u over het rapport met het College van PG's gesproken tijdens de Overlegvergadering. U heeft de Tweede Kamer tijdens het commissiedebat strafrechtketen op 8 september jongstleden toegezegd het rapport met een brief in het derde kwartaal (uiterlijk september) van 2026 aan de Kamer te zullen toezenden. Bijgaand treft u het rapport met een concept-Kamerbrief aan.

2. Geadviseerd besluit

Instemmen met de verzending van bijgevoegde brief met het rapport van de commissie Smit aan de Tweede Kamer.

3. Kernpunten

In de brief worden de opvallendste punten uit het rapport toegelicht:

- Het OM heeft adequaat ("begrijpelijk en in dit geval verstandig") op het incident gereageerd door alle interne systemen los te koppelen van het internet.
- De beveiliging van de ICT-systemen voorafgaand aan de ICT-inbreuk was onvoldoende. Dit komt onder meer tot uiting in het ontbreken van een permanente monitoring op een cruciaal systeem als de Citrix NetScaler (geavanceerd netwerkapparaat dat zorgt voor veilige en geoptimaliseerde levering van applicaties) binnen de kantooromgeving, waardoor verdachte activiteiten of afwijkingen meteen kunnen worden gesignaleerd. Inmiddels is deze monitoring wel aanwezig.
- Signalen over de (beveiligings-)problematiek binnen de organisatie werden onvoldoende opgemerkt en zijn anderzijds onvoldoende krachtig gecommuniceerd.
- De commissie constateert dat al voor het incident goede eerste stappen zijn gezet om het IV-landschap maatschappelijk weerbaarder en robuuster te maken en de positionering van IV binnen de organisatie te versterken.
- Het zal echter ruime tijd en capaciteit vergen om de achterstand weg te werken en het niveau van 'brandveilig' te hebben bereikt.
- Het rapport wordt afgesloten met een aantal geleerde lessen voor de toekomst. Belangrijke elementen daarin zijn dat gewerkt dient te worden aan businesscontinuïteit en risicobeheersing, zowel intern OM als in ketenverband. De commissie adviseert daarnaast om te investeren in het op orde brengen van de informatiebeveiliging en de organisatie ervan daarop aan te passen. Ook adviseert

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Strafrechtelijke handhaving

Datum
2 oktober 2026

de commissie om frequent tot op het hoogste niveau de voortgang van de ontwikkelingen rond de IV te evalueren.

In de brief wordt toegelicht:

- Dat inmiddels op verschillende geconstateerde knelpunten, zoals de genoemde monitoring en de positie van de voor beveiliging van de ICT verantwoordelijke functionarissen binnen de organisatie, belangrijke verbeteringen zijn gerealiseerd.
- Dat op grond van het coalitieakkoord vanaf 2027 structureel oplopend tot €50 miljoen extra per jaar beschikbaar is voor de ontwikkeling van de ICT bij het OM.
- Dat ten behoeve van de IV-opgave en de besteding van deze middelen het OM op dit moment een I-plan opstelt en dat voor de uitvoering van dit plan een externe en onafhankelijke reviewboard wordt ingesteld.
- Dat de reviewboard zal worden gevraagd om expliciet aandacht te hebben voor de door de commissie geconstateerde ontwikkelpunten.
- De Audit Dienst Rijk wordt gevraagd om een onderzoek uit te voeren naar de aanpak die het OM hanteert om te voldoen aan de regels van de Baseline Informatiebeveiliging Overheid.

In het rapport wordt ook aandacht besteed aan de afhankelijkheden op het gebied van de ICT binnen de strafrechtketen en de noodzaak voor ketenorganisaties om goed samen te werken. In de brief wordt toegelicht dat deze bevinding wordt meegenomen bij de uitwerking van de motie Mutluer, waarin de regering wordt verzocht te onderzoeken hoe de centrale regie op ICT binnen de justitiële keten kan worden versterkt. U zult de Kamer hierover dit jaar nader informeren.

Tijdens het commissiedebat strafrechtketen op 8 september 2026 heeft u toegezegd in deze brief ook in te zullen gaan op de aansluiting van het OM bij het Shared Service Center-ICT (SSC-ICT) van de Rijksoverheid. In bijgevoegde brief wordt toegelicht dat het proces om de standaard werkplekken, waar het overgrote deel van de medewerkers bij het OM gebruik van maakt, aan te laten sluiten bij het SSC-ICT loopt.

Over de instelling van bovengenoemde reviewboard wordt u binnen afzienbare tijd nader geïnformeerd.

4. Toelichting

4.1. Politieke context

Met de verzending van bijgevoegde brief wordt nader toegelicht hoe uitvoering wordt gegeven aan het coalitieakkoord waarin staat dat het OM vanaf 2027 oplopend tot €50 miljoen extra ter beschikking krijgt voor de ICT-problematiek. Ook wordt uitvoering gegeven aan uw toezegging aan de Tweede Kamer tijdens het commissiedebat strafrechtketen op 8 september jongstleden om toe te lichten om in te gaan op de aansluiting van het OM op het Shared Service Center van het Rijk (SSC-ICT).

4.2. Financiële overwegingen

Er zijn aan de verzending van de brief geen financiële consequenties verbonden.

4.3. Krachtenveld

De brief is met het OM afgestemd en intern met de relevante directies (Directie Informatievoorziening & Inkoop en Directie Rechtsbestel).

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Strafrechtelijke handhaving

Datum
2 oktober 2026

4.4. Overige punten

Tijdens de Overlegvergadering op 21 september jongstleden werd de suggestie door de voorzitter van het College gedaan om de namen van de leden van de reviewboard in de brief op te nemen. Dat is gebeurd.

Mede naar aanleiding van de Overlegvergadering zijn een paar passages in het rapport onleesbaar gemaakt omdat deze passages informatie bevat waarmee – wanneer deze publiekelijk bekend wordt – kwaadwillenden hun voordeel mee kunnen doen.

5. Informatie die niet openbaar gemaakt kan worden

De persoonsgegevens van de ambtenaren zijn niet openbaar ter bescherming van de persoonlijke levenssfeer.