

Vergaderjaar 2016–2017

34 588

Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..)

D

NADER VOORLOPIG VERSLAG VAN DE VASTE COMMISSIE VOOR BINNENLANDSE ZAKEN EN DE HOGE COLLEGES VAN STAAT / ALGEMENE ZAKEN EN HUIS VAN DE KONING¹

Vastgesteld 6 juni 2017

1. Algemeen

De leden van de **SP**-fractie danken de regering voor de in de memorie van antwoord gegeven antwoorden op hun vragen. Ze hebben nog een aantal nadere vragen.²

De leden van de **PvdA**-fractie hebben met belangstelling kennisgenomen van de antwoorden van de regering. Op enkele onderdelen willen zij nog nadere vragen stellen.

De leden van de fractie van **GroenLinks** hebben kennisgenomen van de antwoorden van de regering en willen graag een aantal aanvullende vragen aan de regering stellen.

2. De verwerking van gegevens door de diensten

Uit de antwoorden van de regering blijkt dat er hoofdzakelijk een technische beoordeling (negatieve filtering, positieve filtering en selectie) van de bij een onderzoeksoopdrachtgerichte interceptie verzamelde data plaatsvindt, waarvan de overgebleven data «in beginsel» relevant worden geacht. Alleen als de verzamelde data «evident niet relevant» zijn, zouden deze moeten worden vernietigd, zo lezen de leden van de **SP**-fractie. Blijkbaar is «potentiële relevantie» voldoende volgens de regering. De

¹ Samenstelling:

Engels (D66) (*voorzitter*), Nagel (50PLUS), Ruers (SP) (*vice-voorzitter*), Van Bijsterveld (CDA), Duthler (VVD), Ten Hoeve (OSF), Huijbregts-Schiedon (VVD), Van Kappen (VVD), Koffeman (PvdD), Strik (GL), De Vries-Leggedoor (CDA), Flierman (CDA), Barth (PvdA), De Graaf (D66), Schouwenaar (VVD), Van Strien (PVV), P. van Dijk (PVV), Gerkens (SP), Van Hattem (PVV), Köhler (SP), Lintmeijer (GL), Pijlman (D66), Rombouts (CDA), Schalk (SGP), Verheijen (PvdA), Bikker (CU), Klip-Martin (VVD), Sini (PvdA), Van der Sluijs (PVV).

² Deze zijn deels gebaseerd op een brief van Bits of Freedom van 26 mei 2017. Zie bijlage.

verplichting om de vergaarde data zo snel mogelijk op daadwerkelijke relevantie te toetsen, ontbreekt.

De toezichthouder op de inlichtingen- en veiligheidsdiensten, de CTIVD, pleit al geruime tijd voor expliciete wettelijke waarborgen om de verzamelde data zo spoedig mogelijk te beperken tot wat daadwerkelijk relevant is («verantwoorde databeperking»). De regering weigert echter deze aanbeveling over te nemen. Volgens de regering zou de aanbeveling van de CTIVD om te toetsen op daadwerkelijke relevantie geen recht doen aan het onderscheid dat moet worden gemaakt tussen gerichte interceptie en onderzoeksopdrachtgerichte interceptie. Bestaat dit onderscheid eruit dat de toets op relevantie voor data die vergaard worden via onderzoeksopdrachtgerichte interceptie lager is – onderzoeken op «potentiële relevantie» in plaats van «daadwerkelijke relevantie» – dan bij gerichte interceptie? Zo ja, wat is de legitimatie voor deze lagere norm? Zo niet, waaruit bestaat dit onderscheid dat de regering benoemt dan precies?

Kan de regering uitleggen waarom data die via onderzoeksopdrachtgerichte interceptie worden vergaard, slechts vernietigd hoeven te worden als deze «evident niet relevant» zijn en niet zo spoedig mogelijk getoetst moeten worden op daadwerkelijke relevantie? Hoe kan de inzet van onderzoeksopdrachtgerichte interceptie leiden tot een zo gericht mogelijke inzet – zoals de regering beoogt – als niet vereist is dat de verzamelde data zo spoedig mogelijk op daadwerkelijke relevantie worden getoetst?

In de memorie van antwoord geeft de regering aan dat «(de) metadata die niet op basis van de negatieve filtering is uitgesloten, worden bewaard». Dit antwoord suggereert dat er op de metadata die via onderzoeksopdrachtgerichte interceptie worden vergaard, uitsluitend negatieve filtering wordt toegepast voordat de gegevens bewaard worden. Dit zou betekenen dat er een lagere selectiestandaard geldt voor metadata dan voor de overige vergaarde gegevens. Het is uiterst zorgelijk dat er voor de verzamelde metadata minder waarborgen zouden gelden dan voor de overige data. Inmiddels wordt breed aanvaard dat metadata een zeer intiem beeld kunnen geven van de persoonlijke levenssfeer van individuen. Het van oudsher gemaakte onderscheid tussen de inhoud en metadata van communicatie is dan ook niet meer relevant voor de mate van inbreuk op de in het geding zijnde grondrechten. De regering heeft dit in de memorie van toelichting ook onderkend. Het categorisch anders behandelen van metadata in de vorm van minder waarborgen is daarom naar de mening van de leden van de SP-fractie onterecht.

Klopt het dat de diensten metadata mogen bewaren als deze niet op basis van negatieve filtering zijn uitgesloten, zonder dat hierop positieve filtering en selectie worden toegepast? Zo ja, kan de regering uitleggen hoe wordt voorkomen dat de metadata van grote groepen onschuldige burgers bewaard zullen worden, als uitsluitend negatief gefilterd wordt alvorens de metadata worden bewaard? Zo niet, kan de regering dan bevestigen dat voor zowel de metadata als voor de inhoud van communicatie dezelfde selectienorm geldt, waarbij uitsluitend die gegevens worden bewaard die na alle selectiestappen – negatieve filtering, positieve filtering en selectie – overblijven als daadwerkelijk relevante data?

De diensten krijgen de mogelijkheid om realtime en geautomatiseerd toegang te krijgen tot de gegevensbestanden van meewerkende bedrijven, overheidsinstanties en andere organisaties. Voor de inzet van deze bevoegdheid gelden geen extra waarborgen – zoals voorafgaande toetsing door de TIB – die wel gelden voor de inzet van bijzondere bevoegdheden. In haar antwoord legitimeert de regering het gebrek aan

waarborgen doordat de aangezochte partijen niet verplicht zijn om mee te werken. Maar het feit dat deze wijze van gegevensvergaring op basis van vrijwilligheid van de aangezochte partijen plaatsvindt, maakt volgens de leden van de SP-fractie de inbreuk op de rechten van burgers die hun data aan deze partijen hebben toevertrouwd, niet kleiner. Bovendien vindt deze medewerking, in tegenstelling tot wat de regering suggereert, heimelijk plaats. Meewerkende partijen mogen niets over hun samenwerking met de diensten zeggen.

Kan de regering uitleggen waarom zij van oordeel is dat het vergaren van gegevens uit een gegevensbestand met behulp van de heimelijke, vrijwillige medewerking van een aangezochte partij, minder ingrijpend is voor de personen waarop deze gegevens betrekking hebben, dan als deze gegevens via de inzet van een bijzondere bevoegdheid worden vergaard? Gelden er extra waarborgen als de diensten via deze heimelijke samenwerking toegang krijgen tot gegevensbestanden van bijvoorbeeld onderwijsinstellingen of ziekenhuizen? Zo ja, waaruit bestaan deze extra waarborgen dan? Zo niet, waarom ziet de regering dan geen noodzaak om voor de toegang tot dergelijke gegevensbestanden met zeer intieme informatie nadere waarborgen in te voeren?

In haar antwoord geeft de regering aan dat de bevraging van gegevens via realtime toegang tot gegevensbestanden gericht plaatsvindt op hit/no hit basis. Kan de regering bevestigen dat de diensten uitsluitend deze gerichte bevragingmethode toepassen en niet volledig toegang krijgen tot alle gegevens in de gegevensbestanden? Zo niet, welke andere bevragingmethoden kunnen de diensten dan nog toepassen en welke beperkingen gelden er in dat geval? Welke bevragingmethoden kunnen de diensten toepassen op de gegevensbestanden die aan de diensten door meewerkende partijen worden verstrekt? Passen de diensten dan dezelfde bevragingmethode toe die zij gebruiken bij de (op afstand) realtime toegang tot gegevensbestanden van meewerken partijen? Zo niet, welke bevragingmethoden kunnen de diensten dan toepassen? Mogen de diensten in dat geval alle gegevens die zich in deze bestanden bevinden analyseren?

Blijkens de notitie over kwetsbaarheden, evenals de antwoorden van de regering op vragen in de eerste inbreng van de leden van de Eerste Kamer, zouden onbekende kwetsbaarheden gemeld kunnen worden, tenzij daar een uitzondering op wordt gemaakt. Die uitzonderingen zijn niet limitatief en laten bovendien ruimte om nooit te hoeven melden. Uit recente gebeurtenissen blijkt dat het achterhouden van zulke kwetsbaarheden grote risico's voor grote groepen burgers kan opleveren. Een herbezinning van het meldingsstandpunt is volgens de leden van de SP-fractie dus op zijn plaats. Bovendien is er geen meldingsregime, althans dat is niet publiek bekend. Daarbij ontbreekt ook een extern toetsingsregime bij het inzetten van kwetsbaarheden.

Het achterhouden van onbekende kwetsbaarheden kan grote risico's voor grote groepen gebruikers opleveren. Het achterhouden van onbekende kwetsbaarheden moet daarom zo veel mogelijk beperkt worden. Kan de regering aangeven in hoeveel gevallen er in het verleden is besloten het melden van kwetsbaarheden uit te stellen? En kan de regering aangeven in hoeveel gevallen er in het verleden is besloten het melden van kwetsbaarheden achterwege te laten?

Verandert het recente nieuws over het uitlekken van door (buitenlandse) inlichtingendiensten gevonden onbekende kwetsbaarheden en het daaropvolgende gebruik door criminelen, zoals bij de «Wannacry-ransomware» iets aan het Nederlandse standpunt over het gebruik van

onbekende kwetsbaarheden door inlichtingen- en veiligheidsdiensten? Zo nee, waarom niet? Hadden de Nederlandse inlichtingen- en veiligheidsdiensten bij de onbekende kwetsbaarheid die ten grondslag lag aan de «Wannacry-ransomware» een andere afweging gemaakt dan de NSA, dat wil zeggen: wel melden en niet zelf jaren achterhouden? Is er een (interne) richtlijn voor het mogen achterhouden van kwetsbaarheden en de termijn die daaraan gebonden is? Zo nee, wanneer komt deze richtlijn?

Uit de notitie blijkt dat het toezicht op het gebruiken en achterhouden van kwetsbaarheden bij de CTIVD ligt. Dat betekent dat er geen voorafgaande externe toets is op het mogen gebruiken en achterhouden van kwetsbaarheden. Gezien het grote risico dat bestaat bij het achterhouden van kwetsbaarheden is het verstandig om externe toetsing vooraf in te voeren. Waarom is er geen externe toetsing vooraf voor het gebruiken en het mogen achterhouden van kwetsbaarheden? Kan de voorafgaande toetsing voor het mogen gebruiken en achterhouden van kwetsbaarheden bij de TIB worden belegd?

De reikwijdte van de nieuwe bevoegdheid tot onderzoeksopdrachtgerichte interceptie is naar de mening van de leden van de SP-fractie nog steeds te onbepaald. In haar beantwoording van vragen van leden van de Eerste Kamer geeft de regering aan dat er geen sprake van ongericht interceptie zou zijn, omdat deze bevoegdheid zich beperkt tot de «onderzoeksopdracht». Onderzoeksopdrachten dienen weliswaar binnen de doelstellingen van een Geïntegreerde Aanwijzing te vallen, dit voorkomt niet dat de formulering van zeer algemene aard kan zijn en bijvoorbeeld kan zien op alle communicatie tussen een bepaalde stad in Nederland en een regio in het buitenland.

Heldere en concrete criteria ontbreken vooralsnog. De regering geeft uitsluitend anekdotische voorbeelden van een onderzoeksopdracht. Een abstracte toets aan de algemene eisen van noodzakelijkheid, proportionaliteit en subsidiariteit biedt bovendien onvoldoende houvast. Hierdoor is deze verstreckende interceptiebevoegdheid onvoldoende voorzienbaar. De burger weet daardoor niet goed waar die aan toe is en effectief toezicht voor- en achteraf wordt hierdoor bemoeilijkt. Kan de regering aangeven welke concrete (wettelijke) criteria in acht moeten worden genomen om vast te stellen of een onderzoeksopdracht voldoende gericht geformuleerd is? Wordt er bijvoorbeeld gekeken naar de geografische reikwijdte, het aantal personen dat potentieel geraakt kan worden en het type communicatie dat men wil onderscheppen? Is de regering bereid om nadere criteria te formuleren, al dan niet in lagere regelgeving, die helpen bij de beoordeling of de onderzoeksopdracht en daaruit voortvloeiende interceptie van communicatie voldoende gericht is? Zo niet, waarom niet?

De leden van de **PvdA**-fractie memoreren dat zij in het voorlopig verslag de regering hebben verzocht om een inhoudelijke reactie op elk onderdeel van de door hen aangehaalde redenering van de Afdeling advisering van de Raad van State. Deze leden menen dat dit in de memorie van antwoord nog niet genoegzaam is gebeurd. Zij vragen daarom de regering uiteen te zetten hoe de TIB, bestaande uit relatieve buitenstaanders en met een zeer beperkte inhoudelijke ondersteuning (één secretaris en één plaatsvervangend secretaris, zo blijkt uit de memorie van antwoord), de veiligheidsrisico's enerzijds en anderzijds de noodzaak, evenredigheid en subsidiariteit van grootschalige, abstract aangeduide en technisch complexe operaties zodanig goed kan inschatten dat zij daadwerkelijk de rol kan vervullen die haar in het wetsvoorstel wordt toebedeeld.

In de memorie van antwoord heeft de regering naar aanleiding van een vraag van deze leden over de uitleg van de motie van het voormalige Tweede Kamerlid Recourt geantwoord dat het gebruik van de genoemde wettelijke criteria leidt tot een zo gericht mogelijke inzet van bevoegdheden. De regering voegt daaraan toe dat als resultaat van de toepassing van deze criteria daarvan ook op enigerlei wijze zal moeten blijken en dat de Minister erop zal toezien dat dit het geval is. Deze leden vragen de regering waaraan zij concreet moeten denken bij «op enigerlei wijze»?

Op de vraag van deze leden naar de uitleg van de CTIVD van de zorgplicht heeft de regering geantwoord dat de wettelijke verankering van de zorgplicht naar haar oordeel de CTIVD voldoende handvatten biedt om op de uitwerking daarvan binnen het kader van de aan haar opgedragen taak toe te zien. De regering stelt vervolgens dat dit iets anders is dan de uitleg die de CTIVD daaraan meent te moeten geven in haar brief van 22 maart 2017, waarbij de CTIVD suggereert dat het instrumentarium van gegevensbeschermingsbeleid, gegevensbeschermingseffectbeoordelingen en audits volgens de regering onder de zorgplicht begrepen moet worden geacht. De leden van de PvdA-fractie vragen de regering hoe de CTIVD de naleving van de zorgplicht kan toetsen als aan de invulling daarvan geen duidelijk instrumentarium (zoals gegevensbeschermingsbeleid, gegevensbeschermingseffectbeoordelingen en audits) ten grondslag ligt. Deze leden verzoeken de regering bij haar antwoord te betrekken de in voornoemde brief door de CTIVD geuite hartenkreet dat bij het ontbreken van zo'n instrumentarium de toezichthouder bij elk gegevensverwerkingsproces eerst zelf moet vaststellen op welke wijze invulling moet worden gegeven aan normen van kwaliteit en rechtmatigheid en als gevolg daarvan niet meer aan toezicht zal toekomen.

In antwoord op vragen van onder meer de leden van de PvdA-fractie inzake databeperking, is de regering ingegaan op het proces van filtering. De regering heeft daarbij uiteengezet dat er enerzijds negatief wordt gefilterd en anderzijds positief. In de positieve filtering zit volgens de regering het vakmanschap van de inlichtingen- en veiligheidsdienst. Met behulp van samengestelde filters kan op intelligente wijze worden gefilterd, waardoor niet relevante communicatie niet hoeft te worden opgeslagen, aldus de regering. Over metadata merkt de regering vervolgens op dat metadata die niet op basis van de negatieve filtering zijn uitgesloten, worden bewaard. De leden van de PvdA-fractie vragen de regering of het voorgaande betekent dat op metadata die via onderzoeksgerichte interceptie worden vergaard enkel negatieve filtering en geen positieve filtering en selectie wordt toegepast voordat de gegevens worden bewaard. Voor het geval het antwoord van de regering op de voorgaande vraag bevestigd luidt, vragen deze leden waarom er voor metadata een lagere selectiestandaard geldt dan voor de overige gegevens. Zij verzoeken de regering bij haar antwoord te betrekken de uiteenzetting op p. 97 van de memorie van toelichting dat het van oudsher gemaakte onderscheid tussen metadata enerzijds en de inhoud van de telecommunicatie anderzijds aan relativering toe is. Voorts vragen zij de regering hoe wordt voorkomen dat de metadata van grote groepen onschuldige burgers zullen worden bewaard als enkel negatief gefilterd wordt alvorens de metadata worden bewaard.

De leden van de PvdA-fractie vragen de regering of het klopt dat in het wetsvoorstel de diensten de mogelijkheid krijgen om realtime en geautomatiseerd toegang te krijgen tot de gegevensbestanden van meewerkende bedrijven, overheidsinstanties en andere organisaties en dat voor de inzet van deze bevoegdheid niet de extra waarborgen gelden (zoals voorafgaande toetsing door de TIB) die wel gelden voor de inzet van bijzondere bevoegdheden. Indien het antwoord van de regering op

voorgaande vraag bevestigend luidt, verzoeken deze leden de regering in te gaan op alle opmerkingen en vragen die door Bits of Freedom bij brief van 26 mei 2017 aan deze Kamer zijn geformuleerd onder punt 3.³

Voor de leden van de fractie van **GroenLinks** is het belangrijk dat er bij de inzet van de onderzoeksopdrachtgerichte interceptie zo gericht mogelijk te werk gegaan wordt. De regering stelt in haar beantwoording echter dat er hoofdzakelijk een technische beoordeling van de verzamelde data plaatsvindt waarvan de overgebleven data in beginsel relevant worden geacht: alleen «evident niet relevante» data zouden dus moeten worden vernietigd. Is de regering het met de leden van de fractie van GroenLinks eens dat er dus – blijkbaar – een dwingende verplichting ontbreekt om de overgebleven data streng te toetsen op daadwerkelijke relevantie? De CTIVD heeft bijvoorbeeld gepleit voor expliciete wettelijke waarborgen om de verzamelde data op een zo kort mogelijke termijn te beperken tot datgene wat daadwerkelijk relevant is. Kan de regering toelichten of, en zo ja, aan de hand van welke kenmerken in de toekomst getoetst zal worden of data potentieel relevant zijn?

De regering geeft in haar beantwoording aan dat metadata, die niet op basis van de negatieve filtering zijn uitgesloten, worden bewaard. Kunnen de veiligheids- en politiediensten dus metadata gaan bewaren zonder dat hierop positieve filtering en selectie zullen worden toegepast? Ondergaan metadata daarmee een lagere selectiestandaard dan de overige vergaarde gegevens? Hoe moet dit gemaakte onderscheid gezien worden in het licht van de memorie van toelichting, waarin de regering onderkent dat het onderscheid tussen inhoud en metadata van communicatie niet relevant is voor de mate van inbreuk op de in het geding zijnde grondrechten?

De regering heeft in haar antwoorden aangegeven dat er geen waarborgen zijn bij realtime toegang tot de gegevensbestanden van meewerkende bedrijven, overheidsinstanties en andere organisaties omdat de aangezochte partijen niet verplicht zijn om mee te werken aan een onderzoek. Waarom is het vergaren van gegevens uit een gegevensbestand met behulp van de vrijwillige medewerking van een aangezochte partij minder ingrijpend voor de personen waarop deze gegevens betrekking hebben dan als deze gegevens via de inzet van een bijzondere bevoegdheid worden vergaard?

Recent werd in het geval van de Wannacry-ransomware nogmaals duidelijk dat het achterhouden van onbekende kwetsbaarheden grote risico's voor burgers kan opleveren: 230.000 instellingen, bedrijven en mensen in 99 landen werden geraakt door de ransomware. Is de regering het met de leden van de fractie van GroenLinks eens dat dit soort kwetsbaarheden zoveel mogelijk moeten worden beperkt? Kan de regering aangeven hoe – en, indien mogelijk, hoe vaak – er in het verleden tot het besluit is gekomen om het melden van kwetsbaarheden uit te stellen? Bestaat er een richtlijn voor het mogen achterhouden van dusdanige kwetsbaarheden en de termijn die daaraan gebonden is?

De leden van de fractie van GroenLinks menen ten slotte dat uit de antwoorden van de regering nog steeds niet duidelijk genoeg wordt wat de reikwijdte is van de nieuwe bevoegdheid tot onderzoeksopdrachtgerichte interceptie. Welke concrete, wettelijke criteria gaan er gelden om vast te stellen of een onderzoeksopdracht voldoende gericht geformuleerd is? Staat de regering open voor de suggestie van verschillende betrokken partijen om nadere criteria te formuleren – mogelijk in lagere regelgeving – die helpen bij de beoordeling of de onderzoeksopdracht

³ Zie bijlage.

voldoende gericht is? Deze leden menen dat heldere en concrete criteria ervoor zorgen dat de Nederlandse burger weet waar hij aan toe is en dat daarmee effectief toezicht pas echt goed mogelijk wordt.

3. Toezicht, klachtbehandeling en behandeling van meldingen van vermoedens van misstanden

Niet geheel duidelijk is of artikel 114 de mogelijkheid biedt aan belangenorganisaties (NGO's) om klachten in te dienen namens een bepaalde groep mensen en/of in het algemeen belang (*actio popularis*). Deze mogelijkheid zou volgens de leden van de **SP**-fractie wel moeten bestaan. Onder het huidige klachtrecht bij de Nationale ombudsman is dit immers al jaren mogelijk en al jaren staande praktijk. Is de regering het eens met deze stellingname?

4. Grondrechtelijke en mensenrechtelijke aspecten

Vanuit het maatschappelijk veld is er veel kritiek gekomen op het wetsvoorstel, zo constateren de leden van de **GroenLinks**-fractie. Onder meer de Nederlandse Vereniging van Journalisten (NVJ), de Nederlandse Vereniging van Strafrechtadvocaten (NVSA), de Stichting Platform Bescherming Burgerrechten en de Stichting Privacy First hebben herhaaldelijk aangegeven dat als het voorliggende wetsvoorstel wordt aangenomen dit een forse aantasting van het recht op privacy en andere fundamentele burgerrechten zal betekenen. Een aantal bezwaren is vervat in een concept-dagvaarding.⁴ Hoe beoordeelt de regering – los van de vorm van een dagvaarding – de fundamentele bezwaren en de juridische bedenkingen die deze coalitie aandraagt?

De voorafgaande rechterlijke toetsing indien veiligheidsdiensten bijzondere bevoegdheden jegens advocaten willen inzetten – direct tappen – is opgenomen in het wetsvoorstel, maar de leden van de fractie van GroenLinks hebben nog wel twijfels omtrent het ontbreken van een systeem van nummerherkenning voor het indirect tappen. De Nederlandse Orde van Advocaten bepleitte onlangs dat het van evident belang is voor de advocatuur en het rechtsbestel dat een systeem van nummerherkenning wordt ingevoerd. In antwoord op vragen van de Tweede Kamer berichtte de regering dat zij zal onderzoeken of aan een systeem van nummerherkenning gestalte kan worden gegeven. Is dit onderzoek inmiddels opgezet, en zo ja, in welke fase bevindt het zich? Hoe verhoudt de voorgestelde regeling voor indirect tappen zich tot de wettelijke geheimhoudingsplicht van de advocaat jegens zijn cliënt?

5. Overig

De leden van de **PvdA**-fractie vragen wat de stand van zaken is betreffende de met dit wetsvoorstel samenhangende lagere regelgeving.

⁴ Zie https://www.privacyfirst.nl/images/stories/PDFs/Concept-dagvaarding_Wiv_tegen_Nederlandse_Staat_30maart2017.pdf.

De commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis van de Koning ziet met belangstelling uit naar de memorie van antwoord en ontvangt deze graag binnen **vier weken** na vaststelling van dit voorlopig verslag.

De voorzitter van de vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis van de Koning,
Engels

De griffier van de vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis van de Koning,
Bergman