Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

Aanhangsel van de Handelingen

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

1027

Vragen van het lid **Van den Berg** (JA21) aan de Ministers van Klimaat en Groene Groei, van Economische Zaken en van Justitie en Veiligheid over *de aanschaf van Chinese slimme meters door netbeheerders* (ingezonden 2 januari 2026).

Antwoord van Minister **Hermans** (Klimaat en Groene Groei) (ontvangen 3 februari 2026). Zie ook Aanhangsel Handelingen, vergaderjaar 2025–2026, nr. 964.

Vraag 1, 2 en 10
Bent u bekend met het bericht dat netbeheerders Alliander (Liander), Enexis en Stedin onderdelen voor circa vier miljoen (slimme) meters betrekken van Kaifa uit China?[1, 2, 3]
Is deze gunning volgens uw beoordeling wenselijk? Zo ja, waarom? Zo nee, waarom niet?
Kunt u uitsluiten dat via deze componenten (direct of indirect) manipulatie van meetwaarden, (direct of indirect) aanvallen op de toeleveringsketen of ongeautoriseerde toegang tot meterdata mogelijk is? Zo nee, zijn er mitigatieplannen aanwezig door het Rijk dan wel de netbeheerders, die de risico's zoveel als mogelijk beperken?

[1] De Telegraaf, 30 december 2025, «Woede om megaorder: vier miljoen slimme meters komen straks uit China». (https://www.telegraaf.nl/financieel/nieuws/woede-om-megaorder-vier-miljoen-slimme-meters-komen-straks-uit-china/119636887.html)
[2] De Telegraaf, 31 december 2025, «Privacyzorgen over slimme elektriciteitsmeters uit China: mag jij dit apparaat weigeren?». (https://www.telegraaf.nl/financieel/privacyzorgen-over-slimme-elektriciteitsmeters-uit-china-mag-jij-dit-apparaat-weigeren/120690674.html)
[3] RTL Nieuws, 31 december 2025, «Kritiek op miljoenenorder van netbeheerders in China: «Goedkoop is duurkoop»». (https://www.rtl.nl/nieuws/economie/artikel/5549178/zorgen-over-chinese-onderdelen-nieuwe-slimme-meters)

ah-tk-20252026-1027
ISSN 0921 - 7398
's-Gravenhage 2026

Antwoord 1, 2 en 10
Ja, ik ben bekend met deze berichtgeving. Zoals aangegeven in de beantwoording van eerdere Kamervragen over deze berichtgeving (Kamerstuk 2025Z22741[4]) gaat het in dit nieuwsbericht over de meetmodule, een onderdeel van de slimme meter dat alleen het elektriciteitsverbruik op digitale wijze meet. Deze meetmodule introduceert daarmee geen risico voor de leveringszekerheid van energie.
De verzending en de versleuteling van data naar de netbeheerders en de communicatie met andere apparaten loopt niet via deze meetmodule. De meetmodule bevat ook geen schakelaar en kan niet op afstand worden uitgeschakeld waardoor er geen effect is op de beschikbaarheid van energie. De leveranciers van het betreffende onderdeel en andere niet-geautoriseerde partijen kunnen niet meelezen met de data van de nieuwe generatie slimme meter. De veiligheid van de data wordt door de netbeheerders gewaarborgd door middel van encryptie en autorisaties. Het kabinet is tegen deze achtergrond van oordeel dat de betreffende inkoop geen ontoelaatbaar risico vormt voor Nederlandse consumenten. Zie voor een verdere toelichting op dataveiligheid ook de antwoorden op vraag 7, 8 en 9 in Kamerstuk 2025Z22741.[5]

Vraag 3
Klopt het dat het hier gaat om een aanbesteding/gunning voor «sensoronderdelen» en kunt u de Kamer een feitenoverzicht sturen met scope, aantallen, contractwaarde, looptijd, opties en betrokken entiteiten, inclusief Kaifa Technology Netherlands?

Antwoord 3
Zoals toegelicht in het voorgaande antwoord gaat het hier over de meetmodule, een onderdeel van de slimme meter dat het elektriciteitsverbruik op digitale wijze meet.
De netbeheerders hebben – conform Europese aanbestedingsregels – deze component gegund middels een aanbesteding met openbare selectie. Het gevraagde feitenoverzicht is te vinden in het door de netbeheerders openbaar gepubliceerde aanbestedingsdocument. In het aanbestedingsdocument is opgenomen dat de verwachte aantallen voor deze meetmodule 7.933.740 eenheden zijn en de contractwaarde € 592.517.432 is. De totale opdracht zal worden geleverd door 2 leveranciers: 60% door Kaifa Technology Netherlands B.V. uit China en 40% door Sagemcom Energy & Telecom uit Frankrijk. De afzonderlijke netbeheerders zijn overeenkomsten aangegaan voor een initiële periode van acht jaar, met de mogelijkheid tot verlenging met 3 keer 2 jaar. Het is aan de netbeheerders om te beslissen of zij gebruik maken van deze verlengingsoptie. Verdere details zijn te vinden in het aanbestedingsdocument dat is opgesteld door de netbeheerders.[6]

Vraag 4
Kunt u toelichten welke onderdelen van de meter(s) uit China komen (sensor, printplaten, communicatiemodule, firmware, etcetera) en welke onderdelen in Nederland en de Europese Unie worden geproduceerd of geassembleerd?

Antwoord 4
In de nieuwe generatie slimme meter zijn in de basis vijf separate componenten te onderscheiden die ieder apart worden ingekocht.
(1) Basis elektriciteit meetmodule (hardware). Deze inkoop is verlopen zoals beschreven in de beantwoording van deze Kamervragen en in Kamerstuk 2025Z22741[7].

---

[4] Kamerstuk 22 741, 14 jan 2026. Antwoord op vragen van de leden Boswijk, Jumelet, Peter de Groot, Van der Burg, Grinwis, Paternotte en Klos over het artikel «Woede om miljoenenorder: vier miljoen slimme meters komen straks uit China».
[5] Kamerstuk 22 741, 14 jan 2026. Antwoord op vragen van de leden Boswijk, Jumelet, Peter de Groot, Van der Burg, Grinwis, Paternotte en Klos over het artikel «Woede om miljoenenorder: vier miljoen slimme meters komen straks uit China».
[6] Op deze openbare bron te vinden: https://s2c.mercell.com/today/90866?type=description
[7] Kamerstuk 22 741, 14 jan 2026. Antwoord op vragen van de leden Boswijk, Jumelet, Peter de Groot, Van der Burg, Grinwis, Paternotte en Klos over het artikel «Woede om miljoenenorder: vier miljoen slimme meters komen straks uit China».

(2) De gateway (hardware met een besturingssysteem). Voor dit onderdeel loopt op dit moment de aanbestedingsprocedure. Als eis is assemblage en productie van kritieke onderdelen in een GPA-land opgenomen.[8]
(3) De applicatielaag (software). Dit onderdeel is gegund aan een Nederlandse partij.
(4) De gasmeter (hardware). Dit onderdeel is gegund aan twee Europese leveranciers.
(5) De Public Key Infrastructure (encryptie). Bij dit onderdeel zijn vertrouwelijke veiligheidsmaatregelen toegepast en het onderdeel wordt geleverd door een Nederlandse partij.

Vraag 5 en 14
Kunt u bevestigen welke (in)directe staatsinvloed er is en hoe dit is meegewogen in de risicoafweging, aangezien in de berichtgeving wordt gesteld dat China Electronics Corporation (CEC) een belang van 35% heeft in Kaifa?
Is onderzocht of sprake is van een abnormaal lage inschrijving (onder kostprijs) en/of een verstorend effect van staatssteun? Zo ja, wat was de uitkomst. Zo nee, waarom niet?

Antwoord 5 en 14
Dat er mogelijk sprake kan zijn van (in)directe staatsinvloed is een van de redenen geweest waarom de netbeheerders een risicoanalyse hebben uitgevoerd. Hierbij is onder andere gekeken naar cyber- en energie leveringszekerheidsrisico's, zoals beïnvloeding op afstand, ongeautoriseerde toegang tot meterdata, alsook naar productleveringszekerheidsrisico's.
Voor de verschillende onderdelen van het systeem is een uitgebreide marktconsultatie gedaan. Voor de componenten die niet als risicovol beschouwd zijn, is gekozen voor maximale concurrentie om de maatschappelijke kosten zo laag mogelijk te houden.
Om zo goed mogelijk te verifiëren of er eventueel sprake zou zijn van een inschrijving onder kostprijs, hebben de netbeheerders een uitvraag gedaan bij de Europese Commissie in het «Foreign Subsidies Regulation» mechanisme. Het Foreign Subsidies Regulation (FSR) is een EU-verordening die bedoeld is om oneerlijke concurrentie op de interne markt tegen te gaan wanneer bedrijven financiële steun krijgen van landen buiten de EU. Uit deze melding heeft de Europese Commissie geen belemmeringen waargenomen en gecommuniceerd aan de netbeheerders.

Vraag 6 en 7
Is vooraf door of namens het kabinet een nationale veiligheids- of ketenafhankelijkheidsanalyse uitgevoerd voor deze aanbesteding (AIVD/MIVD/NCTV/RDI of anders)? Zo ja, door wie en met welke hoofdconclusies? Zo nee, waarom niet?
Heeft u in dit dossier geïntervenieerd of een toets gevraagd, aangezien in 2022 door het kabinet is gesteld dat de overheid bij een Nederlands project kan interveniëren als de nationale veiligheid in het geding is? Zo nee, waarom is dit niet als «veiligheidsdossier» behandeld?

Antwoord 6 en 7
Zoals ook toegelicht in beantwoording van eerdere Kamervragen[9] hebben de netbeheerders een risicoanalyse en onderzoek uitgevoerd. Hierbij is gebruik gemaakt van verschillende analyses, waaronder het Dreigingsbeeld Statelijke Actoren (DBSA) en het Cybersecuritybeeld Nederland, beide gepubliceerd door de NCTV. Daarnaast hebben de netbeheerders de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) bevraagd over risico's in dit

[8] Het betreft een land dat partij is bij de multilaterale Overeenkomst inzake overheidsopdrachten (Government Procurement Agreement – GPA). Dit zijn landen zoals Canada, Japan, Noorwegen en Zwitserland. Deze overeenkomst beoogt wederzijdse openstelling van overheidsopdrachten tussen deelnemende landen op basis van transparantie, non-discriminatie en rechtszekerheid. De Europese Unie onderhoudt met deze GPA-partijen structurele en wederkerige handelsrelaties die zijn gebaseerd op internationale afspraken, hetgeen bijdraagt aan een betrouwbare samenwerking binnen publieke aanbestedingen.

[9] Kamerstuk 22 741, 14 jan 2026. Antwoord op vragen van de leden Boswijk, Jumelet, Peter de Groot, Van der Burg, Grinwis, Paternotte en Klos over het artikel «Woede om miljoenenorder: vier miljoen slimme meters komen straks uit China».

aanbestedingstraject. In overleg met de netbeheerders en het Ministerie van Klimaat en Groene Groei heeft de AIVD in algemene zin het dreigingsbeeld, conform bovengenoemde analyses, geschetst op het concept van de nieuwe generatie slimme meter.
De nieuwe generatie slimme meters is opgebouwd uit verschillende hard- en softwarecomponenten en voor ieder van deze componenten geldt een ander risicoprofiel. De berichtgeving gaat over de meetmodule, een onderdeel van de slimme meter dat het elektriciteitsverbruik op digitale wijze meet. Zoals beantwoord in Kamerstuk 2025Z22741[10], kent de elektriciteit meetmodule daardoor een laag risicoprofiel. Mede op basis van deze informatie hebben de netbeheerders maatregelen toegepast waarmee er geen ontoelaatbaar risico is. Het betreft mitigerende maatregelen ten aanzien van de energie- en productleveringszekerheid en dataveiligheid.

Vraag 8
Vindt u (slimme) energiemeters, gezien hun rol in netbeheer en gegevensverwerking, onderdeel van vitale infrastructuur of «kritieke ketencomponenten»? Welke definitie hanteert u, en wie beslist daarover?

Antwoord 8
Binnen de Aanpak Vitaal[11] zijn door het kabinet processen binnen de energiesector aangemerkt als vitaal. Het betreft elektriciteit (transport, distributie en productie van elektriciteit op land en op zee) en gas (transport, distributie, productie, hervergassing en opslag van gas op land en op zee)[12]. Een vitaal proces is een proces waarvan uitval, verstoring of manipulatie tot dusdanig ernstige effecten kan leiden dat dit de nationale veiligheid kan schaden en daarmee maatschappelijke ontwrichting kan veroorzaken.
Binnen deze processen gelden de regionale netbeheerders als vitale aanbieders. De regionale netbeheerders Alliander, Enexis en Stedin verwerven gezamenlijk de nieuwe slimme meter. De netbeheerders hebben zelf de verantwoordelijkheid om de mate waarin een component kritiek is vast te stellen en daar ook rekening mee te houden bij hun verwervingstrategieën. De Minister van Klimaat en Groene Groei kan, indien nodig, de netbeheerders opdragen om maatregelen te treffen.

Vraag 9
Netbeheer Nederland stelt dat het om een meetsensor zonder schakelaar of telecommunicatietechnologie gaat en dat audits niets hebben opgeleverd; welke audits waren dit (scope, frequentie, onafhankelijke partij, bevindingen) en kan de Kamer inzage krijgen?

Antwoord 9
De audit rapporten zijn vertrouwelijk omdat deze bedrijfsgevoelige informatie bevatten. De netbeheerders hebben contractueel vastgelegd deze concurrentiegevoelige informatie niet te delen.

Vraag 11
Hoe borgt u dat burgers niet worden gedwongen een meter te accepteren waarvan de risico's niet transparant zijn beoordeeld, aangezien de Energiewet per 1 januari 2026 is ingegaan en de vervanging van analoge meters verplicht maakt (meewerkingsplicht)?

Antwoord 11
Bij de vervanging van de laatste analoge meters wordt dit jaar en volgend jaar nog de huidige (5e generatie) slimme meter aangeboden en nog niet de nieuwe meter, aangezien de bestaande voorraad naar verwachting strekt tot in het najaar van 2027. Consumenten kunnen de vervanging van een oude analoge meter met de Energiewet niet meer weigeren, maar er zijn wel twee alternatieven als iemand bezwaar heeft tegen het op afstand uitlezen van de

[10] Kamerstuk 22 741, 14 jan 2026. Antwoord op vragen van de leden Boswijk, Jumelet, Peter de Groot, Van der Burg, Grinwis, Paternotte en Klos over het artikel «Woede om miljoenenorder: vier miljoen slimme meters komen straks uit China».
[11] Website NCTV: Overzicht vitale processen. https://www.nctv.nl/onderwerpen/v/vitale-infrastructuur/overzicht-vitale-processen
[12] Kamerstuk 30 821, nr. 176, Brief van de Minister voor Klimaat en Energie.

meter. Zo kan de communicatiefunctionaliteit van de slimme meter op verzoek van de afnemer worden uitgezet. Ook kan worden gekozen voor een zogeheten digitale meter. Beide meten verbruik en invoeding apart. Als consumenten hiervoor kiezen, moeten ze net als nu wel de meterstanden zelf blijven doorgeven aan de energieleverancier.

Vraag 12
Welke aanbestedingsruimte hebben netbeheerders benut om leveringszekerheid, staatsinvloeden en cybersecurity als (uitsluitings)criteria te hanteren, en welke ruimte is volgens u onbenut gebleven?

Antwoord 12
Zoals beantwoord in Kamerstuk 2025Z22741[13] is de slimme meter modulair ontworpen en is voor de afzonderlijke componenten een risicobeoordeling opgesteld. De beschikbare analyses en informatie zijn bij het opstellen van deze risicobeoordelingen meegenomen. De risicobeoordeling heeft geresulteerd in mitigerende maatregelen, waaronder die ten aanzien van productleveringszekerheid en dataveiligheid.
Daarnaast zijn de netbeheerders gehouden aan de nationale en Europese aanbestedingsregels. Ter verdere bevordering van de bescherming van vitale processen in de energiesector zijn in de nieuwe Energiewet – die sinds 1 januari van kracht is – regels opgenomen voor de bescherming van deze processen. Deze regels worden momenteel nader uitgewerkt in onderliggende regelgeving.

Vraag 13
Zijn Europese leveranciers in dit traject aantoonbaar in staat geweest om mee te dingen en te leveren (volume/tijd), en kunt u de Kamer informeren welke Europese aanbieders zijn afgevallen en om welke redenen?

Antwoord 13
Ja, Europese aanbieders hebben zich kunnen inschrijven voor deze aanbesteding. De netbeheerders hebben – conform Europese aanbestedingsregels – dit onderdeel gegund middels een openbare aanbesteding. Er is geen restrictie geweest op deelname uit landen. Iedere aanbieder heeft kunnen inschrijven voor de selectiefase van de aanbesteding. Gekwalificeerde aanbieders konden in de gunningsfase van de aanbesteding een aanbieding doen.
Kandidaten kunnen niet openbaar gemaakt worden. Deze gegevens zijn bedrijfsvertrouwelijk en concurrentiegevoelig. De gegunde leveranciers bestaan uit Kaifa Technology Netherlands B.V. en Sagemcom Energy & Telecom SAS. Dit is weergegeven op Tenderned.[14]

Vraag 15
Welke scenario's zijn uitgewerkt voor het geval leveringen/onderhoud/updates vanuit China (tijdelijk) wegvallen door geopolitieke spanningen, en welke buffer/alternatieve leveranciers zijn (contractueel) geborgd?

Antwoord 15
Zoals beantwoord in Kamerstuk 2025Z22741[15] zijn betrouwbare waardeketens voor vitale energie-infrastructuur essentieel voor het waarborgen van de leveringszekerheid en onze nationale veiligheid. Leveringszekerheid in de product waardeketen is één van de onderdelen van de risicoanalyse die is uitgevoerd door de netbeheerders. Om risico's ten aanzien van de leveringszekerheid te mitigeren, is onder andere besloten voor elke hardware component in de slimme meter voor twee verschillende leveranciers te kiezen. Eén van de twee leveranciers dient afkomstig te zijn uit een land dat partij is bij de multilaterale Overeenkomst inzake overheidsopdrachten

---

[13] Kamerstuk 22 741, 14 jan 2026. Antwoord op vragen van de leden Boswijk, Jumelet, Peter de Groot, Van der Burg, Grinwis, Paternotte en Klos over het artikel «Woede om miljoenenorder: vier miljoen slimme meters komen straks uit China».
[14] 11 dec. 2025 - Aankondiging gegunde opdracht DSMR6 E-meter.
[15] Kamerstuk 22 741, 14 jan 2026. Antwoord op vragen van de leden Boswijk, Jumelet, Peter de Groot, Van der Burg, Grinwis, Paternotte en Klos over het artikel «Woede om miljoenenorder: vier miljoen slimme meters komen straks uit China».

(Government Procurement Agreement – GPA).[16] In dit geval betekent dit dat de meetmodule die Kaifa Technology levert, ook wordt geleverd door het Franse Sagemcom. Indien noodzakelijk kunnen de netbeheerders een beroep doen op de Franse leverancier om alle leveringen over te nemen en de dienstverlening te continueren. Dit houdt in dat, indien één van de partijen niet in staat is om te leveren, de andere partij over voldoende capaciteit beschikt om de levering tot 100% te continueren. Hierdoor is de leveringszekerheid van dit onderdeel geborgd. Voor dit leveranciersmodel is ook gekozen om de Europese productie van meetmodules te versterken en beschikbaar te houden.

Vraag 16 en 17
Welke concrete artikelen en AMvB's in de huidige Energiewet geven netbeheerders nu wél/geen handvatten om hoog-risico leveranciers te weren bij (digitale/slimme) meters, aangezien in 2022 het kabinet aangaf dat wijzigingen (o.a. mogelijkheid tot gebruik Aanbestedingswet Defensie en Veiligheid) in de Energiewet zouden landen?
Bent u bereid om zo spoedig mogelijk met een kader voor vertrouwde leveranciers voor vitale energiecomponenten (incl. meters) te komen, met heldere criteria (staatsinvloed, ketentransparantie, cybersecurity) en een toetsingsproces voor netbeheerders?

Antwoord 16 en 17
Netbeheerders hebben op grond van de Energiewet de verplichting om de veiligheid en betrouwbaarheid van de netten en het transport over de netten op de meest doelmatige wijze te waarborgen. Daarnaast geldt de verplichting de netten te beschermen tegen invloeden van buitenaf. Dit is een wettelijke taak van netbeheerders.
De netbeheerders kunnen via drie kaders producten of diensten aanschaffen. Deze kaders hebben ieder in meer of mindere mate mogelijkheden om de veiligheid van de producten en diensten en daarmee de nationale veiligheid te waarborgen.[17] Er zijn veiligheidsmaatregelen mogelijk in de Aanbestedingswet 2012 (AW2012), de Aanbestedingswet op Defensie en Veiligheidsgebied (ADV) en er kan gebruik gemaakt worden van het inroepen van artikel 346 van het Verdrag betreffende de Werking van de Europese Unie.[18] Om een veilige energietransitie te borgen, heeft het kabinet besloten de mogelijkheden voor de netbeheerders om veiligheidsmaatregelen te nemen uit te breiden en te uniformeren. Er wordt tevens verkend in hoeverre harmonisatie van bevoegdheden op termijn mogelijk en wenselijk is, met het oog op een meer uniforme en uitvoerbare systematiek. De nieuwe Energiewet creëert onder artikel 3.18 de bevoegdheid voor de Minister van Klimaat en Groene Groei om aanvullende eisen te stellen aan kritieke processen van de netbeheerders ter bescherming van de nationale veiligheid. Deze regels worden momenteel nader uitgewerkt in onderliggende regelgeving. Hierdoor wordt het voor de netbeheerders gemakkelijker om gebruik te maken van de veiligheidsmaatregelen in de hierboven beschreven wettelijke kaders. Daarnaast heeft het Ministerie van Justitie en Veiligheid momenteel in de onderliggende conceptwetgeving van de Wet weerbaarheid kritieke entiteiten en de Cyberbeveiligingswet, te weten het Besluit weerbaarheid kritieke entiteiten en het Cyberbeveiligingsbesluit, een artikel opgenomen waarbij entiteiten verplicht kunnen worden om bepaalde producten of diensten van specifieke leveranciers niet te gebruiken. De desbetreffende vakminister kan een dergelijke bevoegdheid inzetten – in overeenstemming met de Minister van Justitie en Veiligheid – indien dat noodzakelijk is om risico's voor de nationale veiligheid te voorkomen, te beperken of te beheersen. De vakminister dient hiervoor een beoordelingskader te doorlopen en aan de hand daarvan te bepalen of er al dan niet sprake is van de noodzaak om de verplichting op te leggen.

---

[16] Zie voor toelichting het antwoord op vraag 4.
[17] Kamerstuk 16 183 Mogelijkheden aanbestedingswetten m.b.t. (in)direct uitsluiten leveranciers.
[18] Dit artikel bepaalt dat een lidstaat niet verplicht is informatie te verstrekken waarvan openbaarmaking volgens die lidstaat schadelijk is voor de essentiële belangen van de nationale veiligheid.