Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

31 125 Defensie Industrie Strategie

Nr. 116

LIJST VAN VRAGEN EN ANTWOORDEN

Vastgesteld 4 december 2020

De vaste commissie voor Defensie heeft een aantal vragen voorgelegd aan de Staatssecretaris van Defensie over de brief van 2 november 2020 inzake het BIT-advies Grensverleggende IT (GrIT) en reactie van Defensie, de business case GrIT en het voornemen tot gunning Kamerstuk 31 125, nr. 115).

De Staatssecretaris heeft deze vragen beantwoord bij brief van 3 december 2020. Vragen en antwoorden zijn hierna afgedrukt.

De voorzitter van de commissie,
A. de Vries

Adjunct-griffier van de commissie,
Mittendorff

kst-31125-116
ISSN 0921 - 7371
's-Gravenhage 2020

1.
Welke gevolgen heeft de splitsing van IBM voor een bestendige uitvoering van GrIT?
2.
Met welk onderdeel of welke entiteit van IBM zal Defensie (blijven) samenwerken?
3.
Betekent de voorgenomen splitsing van IBM dat een nieuwe BIT-toets wenselijk of noodzakelijk is?
Omdat de aanbesteding nog loopt en gerubriceerd is doet Defensie geen uitspraken over individuele partijen die deel uit zouden maken van het consortium. Defensie informeert u in een separate brief over commercieel-vertrouwelijke aspecten van de aanbesteding en het consortium[1].

4.
In hoeverre en op welke wijze is de vormgeving van GrIT getoetst aan de uitgangspunten van de Defensie Industrie Strategie?
De aanbesteding is niet specifiek getoetst aan de actuele Defensie Industrie Strategie welke van na de datum van de publicatie van de Startvraag GrIT in juni 2016, de formele start van het aanbestedingstraject, is. Aan deze aanbesteding is wel een marktconsultatie vooraf gegaan waar geïnteresseerde Nederlandse marktpartijen aan meegedaan hebben. Voorts zal de opdracht uitgevoerd worden door in Nederland gevestigde bedrijven en vallen de hard- en softwareproducten in de categorie *commercial off the shelf* (COTS).

5.
Hebt u het BIT-advies van 2018 opgevolgd ten aanzien van het loslaten van de ambitie om zelf mobiel operator te worden, aangezien dit «onnodig beslag legt op schaarse personele en financiële capaciteit»? Zo nee, waarom niet?
Het BIT stelt in zijn advies van 30 april 2018 dat de functie van Mobiele Netwerk Operator (MNO) de eisen aan GrIT compliceren en onnodig beslag leggen op schaarse eigen personele en financiële middelen. Defensie heeft in haar reactie op deze BIT-toets (Kamerstuk 31 125, nr. 84) aangegeven deze behoefte nogmaals tegen het licht te houden en afhankelijk van de uitkomsten daarvan, de scope van GrIT op dit punt eventueel aan te passen.
De eigen MNO-functie is voor Defensie belangrijk en onderdeel van de scope van GrIT. De functie moet voor Defensie bijdragen aan de verhoging van de beschikbaarheid, betrouwbaarheid en beveiliging van de mobiele dekking in binnen- en buitenland. Defensie realiseert daarmee een verbeterde operationele inzet en verhoging van de veiligheid. Door de MNO-functie zelf in te vullen is Defensie:
- Niet langer afhankelijk van een enkele externe provider aangezien Defensie via de eigen MNO-functie een nationale dekking kan realiseren door gebruik te maken van de radionetwerken van meerdere commerciële providers. Hierdoor is geborgd dat bij uitval van een commercieel netwerk Defensie de communicatie kan voortzetten;
- In staat zelf netwerken te realiseren in gebieden waar geen commerciële netwerken beschikbaar zijn of niet door Defensie kunnen worden gebruikt;
- In staat zelf de controle over de security en encryptie van het netwerk te beheersen en te monitoren.

[1] Ter vertrouwelijke inzage gelegd, alleen voor de leden, bij het Centraal Informatiepunt Tweede Kamer

Defensie heeft in 2018 extern commercieel-vertrouwelijk onderzoek laten doen naar de noodzaak van de door Defensie gestelde behoeftes om zelf over een eigen MNO-functie te beschikken. Hieruit bleek dat de combinatie van een eigen MNO-functie en de controle over de beveiligingsketen passen bij de taakuitvoering van Defensie in binnen- en buitenland en dat deze functionaliteit daarmee een noodzaak is voor de defensieorganisatie. Het MNO-concept voorziet daarbij in de mogelijkheid om de MNO-functionaliteit van Defensie (in crisissituaties) ook aan de politie en hulpdiensten aan te bieden.
De beoogde operationele MNO-functionaliteit is niet uit de markt te halen. Defensie haalt de benodigde hard- en softwarecomponenten die nodig zijn om zelf operator te worden, wel uit de markt. Deze componenten zijn standaard en beschikbaar. Door te kiezen voor deze «COTS»-oplossing kan Defensie de beoogde MNO-oplossing flexibel, kostenefficiënt en op een technisch haalbare wijze realiseren. Het op te stellen uitvoeringsplan voor het realiseren van de MNO-functie zal aan het BIT ter toetsing worden voorgelegd.

6.
Op basis waarvan kan Defensie besluiten derde partijen te laten toetreden als terugvaloptie wanneer het consortium niet presteert? Welke partij wordt in zo'n geval verantwoordelijk voor beheer en integratie?
Defensie kan op basis van het concept contract op verschillende manieren derde partijen introduceren. Dit kan onder andere bij het niet accepteren van het ontwerp van een uitvoeringsplan of als er geen overeenstemming is over de vergoeding voor uitvoering van een uitvoeringsplan.
Defensie kan aan een derde partij een opdracht geven binnen het contract welke als onderaannemer van het consortium zal fungeren. Defensie kan echter ook een opdracht geven aan een derde partij, naast en onafhankelijk van het consortium.
In het eerste geval blijft het consortium verantwoordelijk voor het beheer en de integratierol van alle werkzaamheden waartoe zij opdracht heeft gekregen van Defensie. In het tweede geval, wanneer Defensie een leverancier introduceert naast en onafhankelijk van het consortium, dan is Defensie verantwoordelijk voor de integratie van dat deel. Het consortium blijft wel verantwoordelijk voor de integratie van de overige delen van het project.

7.
Welke concrete maatregelen neemt u om te voldoen aan de adviezen inzake onder meer een centrale inrichting van proces- en inhoudelijke regie en voldoende gekwalificeerde eigen medewerkers in regiefuncties?
Om te kunnen voldoen aan de BIT-adviezen inzake een meer centrale inrichting van proces- en inhoudelijke regie richt Defensie een nieuwe governance op drie niveaus in:
- Op het hoogste niveau betreft dit een overleg waar alle stakeholders zijn vertegenwoordigd;
- Op programmaniveau vindt de aansturing en bewaking van de onderliggende GrIT-projecten in samenhang plaats;
- Op (deel)projectenniveau is de governance, tot slot, gericht op de uitvoering van de realisatie, migratie en implementatie van de nieuwe IT-infrastructuur.

Middels deze drie niveaus borgt Defensie dat er centraal regie kan worden gevoerd gedurende de gehele overeenkomst.
Om te kunnen voldoen aan voldoende gekwalificeerde eigen medewerkers in regiefuncties voorziet Defensie in:
- De werving van een directielid JIVC die verantwoordelijk is voor regie, transitie en implementatie van GrIT.

- De werving via een werving- & selectiebureau van eigen medewerkers in vaste dienst die ervaring hebben met complexe, omvangrijke IT-sourcingscontracten in de verschillende fases van een sourcingstraject.
- Een actief opleidingstraject voor de medewerkers van de regie organisatie, zoals het volgen van diverse doelgerichte trainingen bij gerenommeerde regie-organisaties, individuele coaching en gerichte competentie trainingen van medewerkers.

Defensie richt voorts een multidisciplinair team in ter ondersteuning van de opdrachtnemer, waarin alle benodigde complementaire specialistische kennis en ervaring aanwezig is. Defensie trekt daarnaast aanvullende expertise aan om de aanwezige interne expertise binnen het architectenteam te versterken met «landschapsdenkers». Aanvullend zal op het aspect enterprise architectuur extra expertise op centraal niveau worden aangetrokken.

8.
Welke variabelen vormden het afwegingskader in het heroverwegingstraject?
Het afwegingskader bestaat uit tien variabelen, die betrekking hebben op onder andere toegevoegde waarde, beheersbaarheid en impact op personeel van Defensie. Dit kader is in de Technische Briefing van 12 maart 2020 aan uw Kamer gepresenteerd en is toegevoegd aan de separate commercieel-vertrouwelijke bijlage.
Op basis van dit afwegingskader is een analyse gemaakt. Hieruit is naar voren gekomen dat Plan A» voor Defensie het beste hoofdscenario is. Defensie heeft Plan B daarna niet verder uitgewerkt. In het geactualiseerde Plan A» zijn de aanbevelingen van BIT verwerkt binnen de lopende aanbesteding. Dit heeft geleid tot een sterk gewijzigde en verbeterde versie van het oorspronkelijke plan, zoals ook gedeeld met uw Kamer in de brief d.d. 11 september 2020 (Kamerstuk 31 125, nr. 115).

9.
Wordt er tussen het afronden van blokken ook integraal geëvalueerd?
Defensie monitort en evalueert het programma en de afzonderlijke blokken te allen tijde integraal. Het afronden en opstarten van blokken valt daarmee onder de reguliere manier waarop Defensie het programma- en projectmanagement voor GrIT inricht. Dit is onderdeel van de instrumenten waarmee Defensie kwaliteit garandeert. Evaluatie tussen Defensie en het consortium is een regulier agendaonderwerp en geborgd in de governance. Daarnaast laat Defensie de uitvoeringsplannen van de blokken toetsen door het BIT.

10.
Betekent het verdelen in blokken ook dat de IT-infrastructuur al operationeel kan zijn zonder dat het volledig is uitgerold?
Het BIT adviseerde in zijn tweede en derde advies om het werk te verdelen in kleinere en meer beheersbare blokken, waarbij de blokken opzichzelfstaande toegevoegde waarde opleveren voor de bedrijfsvoering of operationele inzet, of op terreinen waar concrete IT-problemen zijn. Conform deze adviezen maakte Defensie een planning van 42 blokken, die allemaal een afgebakende scope hebben en zelfstandig zijn af te roepen. Gedurende de transitie werken elementen van de huidige en nieuwe IT-infrastructuur samen tot het moment dat de nieuwe IT-infrastructuur de functionaliteit kan overnemen. De huidige IT-infrastructuur wordt vervolgens afgebouwd en uitgefaseerd.

11.

Welke bedrijven en organisaties vormen het consortium?
Het beoogde consortium bestaat uit circa zeventig bedrijven die binnen het consortium gaan bijdragen aan de dienstverlening. In Plan A», dat uw Kamer vertrouwelijk is toegekomen, schetst Defensie een beeld van de opbouw van het consortium. Omdat de aanbesteding nog loopt en gerubriceerd is doet Defensie geen uitspraken over individuele partijen die deel uitmaken van het consortium. Defensie informeert u in een separate brief over commercieel-vertrouwelijke aspecten van de aanbesteding en het consortium.

12.
Zijn er voor het geval dat de contractperiodes met leveranciers vroegtijdig worden opgezegd ook vervangende onderaannemers in kaart gebracht om er voor te zorgen dat de verloren tijd in het geval van opzegging geminimaliseerd wordt?
Defensie beschikt over een terugvalplan waarin de voorbereidingen aan Defensiezijde zijn beschreven in het geval van een gedeeltelijke of gehele exit. Het terugvalplan is een «levend» document en wordt periodiek geactualiseerd op basis van laatste ontwikkelingen en inzichten. Onderdeel van dit plan is een overzicht van potentieel alternatieve marktpartijen die als leveranciers kunnen worden ingezet. De daadwerkelijke inzet van deze leveranciers vereist echter wel nieuwe aanbestedingen en zal daardoor naar verachting extra doorlooptijd vergen. Indien Defensie besluit opdrachten zelf uit te voeren, beschikt Defensie over raamovereenkomsten voor het inhuren van personeel en aanschaffen van IT-middelen, welke indien nodig kunnen worden aangewend.

13.
Is in kaart gebracht hoeveel meer energie de nieuwe IT-infrastructuur gaat kosten ten opzichte van de oude infrastructuur? Zo nee, waarom niet?
Het energiegebruik van de huidige IT-infrastructuur is niet bekend. In algemene zin zorgen binnen IT-infrastructuur de datacenters voor het hoogste energieverbruik, ook het energieverbruik van de bestaande datacenters is niet specifiek toe te wijzen.
De nieuwe IT-infrastructuur wordt gebouwd op basis van de laatste stand van de techniek en energienormen. De nieuwe, schaalbare en efficiëntere datacenters voldoen aan de strengere eisen (zoals de EN 50600) en werken energiezuiniger ten opzichte van de huidige datacenters.

14.
Kan de Kamer een overzicht krijgen van alle tussenmijlpalen voor het neerleggen van de IT-infrastructuur?
De blokkenplanning (inclusief de tussenmijlpalen) zijn opgenomen in de commercieel-vertrouwelijke business case die uw Kamer op 2 november 2020 van Defensie ontving (Kamerstuk 31 125, nr. 115).

15.
Is militair personeel zelf betrokken bij het aanleggen van de IT-infrastructuur? Zo ja, wat wil Defensie hiermee bereiken?
Defensie ontwikkelt en realiseert met GrIT betrouwbare, veilige, toekomstbestendige, flexibele en interoperabele IT-infrastructuur voor de komende tien jaar die de defensieorganisatie in staat stelt informatiegestuurd te werken en de haar opgedragen taken effectief uit te voeren. De nieuwe IT-infrastructuur zal worden gebouwd door gemengde teams bestaande uit personeel van het consortium en Defensie. Ook militair personeel maakt deel uit van de gemengde teams. De inbreng van militairen zorgt voor een goede uitwisseling van specifieke operationele karakteristieken en omstandigheden en borgt de aansluiting en ondersteuning van de nieuwe IT-infrastructuur op het primaire proces van Defensie.

16.
Zijn er al plannen voor de overgangsfase en uitfasering van de oude IT-infrastructuur?
De blokkenplanning voorziet in een gefaseerde transitie van huidige IT-infrastructuur naar de nieuwe IT-infrastructuur. Onderdeel van ieder uitvoeringsplan is de uitwerking van deze transitie naar nieuwe IT-infrastructuur. Dit borgt een beheerste transitie met borging van de door Defensie vereiste continuïteit.
Op basis van de blokkenplanning voorziet Defensie binnen GrIT in het plannen en realiseren van de afbouw en uitfasering van de huidige IT-infrastructuur na een succesvolle transitie.

17.
Voldoet de huidige IT-infrastructuur, die gebruikt wordt tijdens missies, nog aan de eisen die aan een moderne krijgsmacht worden gesteld?
Uit onderzoek van Deloitte blijkt dat de continuïteit van de generieke IT-dienstverlening zonder extra aanvullende maatregelen gegarandeerd is tot in de periode 2020–2022. De IT van Defensie is voor dit moment op haar taak berekend en de continuïteit is niet in het geding. Via proactief *lifecycle management* wordt de continuïteit van IT-infrastructuur geborgd. Om de continuïteit echter te kunnen blijven waarborgen voor de lange termijn investeert Defensie met GrIT in de IT-infrastructuur van morgen, zodat ook in de toekomst de IT-infrastructuur voldoet aan de eisen van een moderne krijgsmacht.

18.
Wanneer zal de volledige GrIT-infrastructuur operationeel zijn?
Naar aanleiding van de eerdere BIT-toetsen is een beheerste overgang voorzien naar de nieuwe IT-infrastructuur. De planning is dat de nieuwe IT-infrastructuur na zeven jaar volledig operationeel is.

19.
Zijn mogelijke zwaktes geïdentificeerd die in de overgangsfase als bijeffect kunnen optreden (bijvoorbeeld een grote kwetsbaarheid tegen cyberaanvallen)? Zo ja, heeft Defensie of het consortium de kennis om hier mee om te gaan en op te handelen?
Defensie voorziet in de overgangsfase geen verhoogde kwetsbaarheid, bijvoorbeeld voor cyberaanvallen. Bij grote vernieuwingsprogramma's liggen evenwel altijd risico's op de loer. Defensie brengt veiligheidsrisico's periodiek in kaart middels de principes van risicomanagement. Op basis hiervan neemt Defensie mitigerende maatregelen die de continuïteit en daarmee de veiligheid van de IT zo goed mogelijk waarborgen.