Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

35 728 Programma Grensverleggende IT (GrIT)

Nr. 4 **BRIEF VAN DE STAATSSECRETARIS VAN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 14 januari 2022

Hierbij wil ik u bedanken voor de uitgangspuntennotitie «Groot Project Grensverleggende IT» (GrIT) van 9 december 2021[1]. Ik heb kennisgenomen van de notitie en zal deze gebruiken als leidraad voor de GrIT-rapportages. Conform de wens van de Kamer streef ik naar actieve informatievoorziening waarbij ik zoveel als mogelijk conform de uitgangspunten zal rapporteren. Wel verzoek ik de Kamer kennis te nemen van onderstaande overwegingen en waarom ik niet alle uitgangspunten volledig kan overnemen. De uitgangspunten waar onderstaande overwegingen niet op van toepassing zijn verwerk ik in de rapportages.

Verschijningsmomenten en planning

Ik neem kennis van het voorstel van de Kamer aangaande de frequentie en timing van de voortgangsrapportages en zal de Kamer, zoals gevraagd, twee keer per jaar een rapportage doen toekomen. Wel vraag ik begrip voor de beoogde omvang van de rapportages en de capaciteit die hiermee gemoeid zal zijn. Om zo doelmatig en doeltreffend mogelijk, in de aankomende tien jaar, de Kamer van de juiste informatie te kunnen voorzien, is een solide basisrapportage randvoorwaardelijk. Om deze op te stellen vraag ik voldoende tijd. Ik verwacht de Kamer een goede basisrapportage rond de zomer, maar uiterlijk voor 1 oktober 2022, te kunnen doen toekomen. Daarin zal ik ook de periode van 1 januari 2022 tot en met het verschijnen van de basisrapportage meenemen. Ik stel voorts voor de rapportages gelijk uit te sturen met de accountantscontrole van de Auditdienst Rijkt (ADR). De Kamer zal tot het verschijnen van de basisrapportage geïnformeerd worden via het Defensieprojectenoverzicht (DPO). Tot slot streef ik ernaar de rapportages, conform de wens van de Kamer, zo compact en visueel mogelijk te maken.

[1] Raadpleegbaar via www.tweedekamer.nl

kst-35728-4
ISSN 0921 - 7371
's-Gravenhage 2022

Nieuwe gezamenlijke organisatie

De Kamer geeft aan dat GrIT naast een nieuwe IT-infrastructuur ook een nieuwe gezamenlijke organisatie oplevert die verantwoordelijk is voor de uitvoering van het project en de exploitatie van de nieuwe IT-infrastructuur. De Kamer wenst geïnformeerd te worden over de verdere ontwikkeling hiervan, zodat zij inzicht heeft in de manier waarop Defensie in alle omstandigheden borgt dat zij zelfstandig operaties kan uitvoeren.

GrIT wordt gebouwd en geëxploiteerd in samenwerking met een consortium van marktpartijen in gezamenlijke teams, bestaande uit personeel van Defensie en een marktconsortium. In zowel de basisrapportage als in de voortgangsrapportages zal ik de Kamer hierover informeren. Ik wijs er echter op dat GrIT de vernieuwing van een groot deel van de IT-infrastructuur van Defensie betreft, maar dat GrIT niet de volledige digitale transformatie bewerkstelligt die Defensie in staat stelt zelfstandig operaties te kunnen blijven uitvoeren. Hiervoor zijn ook andere projecten en activiteiten binnen het IT-landschap relevant die buiten de programmascope van GrIT vallen.

In de reactie op het vierde BIT-advies heeft mijn voorganger de Kamer inzicht gegeven in de drie niveaus die Defensie hanteert bij de governance van GrIT (Kamerstuk 31 125, nr. 115). Zoals ik hierboven aangaf zal ik de Kamer met de GrIT-rapportages informeren over hetgeen zich afspeelt op het programmaniveau van GrIT. Wel zal ik in mijn rapportages rekenschap geven van alle drie niveaus, waarvoor ik in het bijzonder inzicht in de regie-organisatie noem.

Inzicht in beveiligingsincidenten en -maatregelen

De Kamer schrijft dat de nieuwe IT-infrastructuur gebruikt zal worden voor het verzamelen, koppelen, analyseren en toepassen van data. Om deze reden verzoekt de Kamer in de rapportages een overzicht te geven van vigerende wet- en regelgeving alsmede een vermelding of Defensie hieraan voldoet en om daarbij ook in te gaan op de (cyber)veiligheidsrisico's, beveiligingsincidenten en consequenties en maatregelen hieromtrent.

Op de vernieuwde IT-infrastructuur kunnen uiteenlopende activiteiten, met behulp van aansluitende materiële infrastructuur en applicaties, uitgevoerd worden. De door de Kamer opgebrachte activiteiten omtrent het verzamelen en toepassen van data valt echter niet binnen de programmascope van GrIT. Ook de manier waarop Defensie omgaat met data en beveiligingsincidenten, en het registreren van welke er zijn geweest, is geen onderdeel van het programma GrIT.

Ik begrijp de wens tot inzicht in de voorziene beveiliging van data en de borging van digitale weerbaarheid in de door Defensie gebruikte systemen en onderschrijf het belang hiervan. Waar relevant voor het programma GrIT zal ik de Kamer hierover met de GrIT-rapportages informeren.

Commerciële vertrouwelijkheid en (technische) afhankelijkheid van derden

Voor sommige uitgangspunten rond GrIT geldt dat Defensie in voorkomende gevallen informatie aanmerkt als (commercieel-)vertrouwelijk. Indien sprake is van informatie die niet openbaar gemaakt kan worden zal ik u met een commercieel-vertrouwelijke bijlage bij de rapportages

informeren, zoals dit door Defensie ook eerder rond GrIT is gedaan. Als basis zal altijd de *business case* gelden die mijn voorganger de Kamer vertrouwelijk toezond op 11 februari 2021 (Kamerstuk 35 728, nr. 2). In de begeleidende brief bij de *business case* heeft mijn voorganger de Kamer ook meer verteld over de overwegingen die Defensie maakt aangaande commerciële vertrouwelijkheid.

Voor dit punt wil ik specifiek ingaan op het verzoek van de Kamer om aan te geven van welke organisaties, bedrijven en landen Defensie momenteel (technisch) afhankelijk is en om daarbij in te gaan op welke wijze Defensie een relatie met deze derden heeft en welke risico's hier spelen. Hierover deel ik u mee dat Defensie, mede naar aanleiding van eerdere BIT-adviezen, te allen tijde het recht blijft voorbehouden om blokken aan andere marktpartijen te gunnen (Kamerstuk 31 125, nr. 115). Defensie werkt hiervoor met terugval- en exitplannen, waarover Defensie ook (vertrouwelijk) rapporteert aan de Kamer. Voorts is relevant dat hetgeen Defensie aankoopt of opbouwt eigendom zal zijn van Defensie en dat Defensie hiervoor eigen personeel opleidt.

Een overzicht van derde partijen kan ik, gelet op commerciële vertrouwelijkheid, niet opnemen in de openbare basisrapportage. Voor een overzicht van derde partijen waar Defensie via het consortium mee samenwerkt wijs ik op de eerder met de Kamer gedeelde *business case*. Dit overzicht kan ik bijvoegen in een commercieel vertrouwelijke bijlage bij de basisrapportage. Indien er zich wijzigingen binnen de *business case* voordoen of voor zullen doen, bijvoorbeeld wanneer Defensie GrIT-blokken aan een andere partij zal gunnen dan aanvankelijk was beoogd, zal ik de Kamer hierover informeren, eventueel via vertrouwelijke bijlage.

Financiële informatievoorziening

Ik streef in de openbare rapportage naar een zo volledig mogelijk beeld van de financiële voortgang en zal, waar relevant, meer details verwerken in een vertrouwelijke bijlage. Het uitsplitsen van financiële informatie per blok beschouw ik als commercieel-vertrouwelijke informatie. Dit omdat het openbaar worden ervan een risico vormt voor de onderhandelingspositie van Defensie wanneer Defensie voor een andere leverancier voor de blokken zou (willen) kiezen.

Voor de volledigheid wijs ik er voorts op dat de exploitatiekosten van de reguliere bedrijfsvoering van Defensie niet onder de verantwoordelijkheid vallen van het programma GrIT. Uiteraard kunnen ontwikkelingen in exploitatiekosten wel van invloed zijn op het programma. Indien sprake is van ontwikkelingen die raken aan het programma GrIT zal ik daarover rapporteren. In de basisrapportage zal ik dit verder vorm geven. In algemene zin geef ik alvast aan dat ik voor wat betreft de financiële informatie aansluit bij de reikwijdte van de eerder met de Kamer gedeelde *business case*.

Accountantscontrole van de Auditdienst Rijk

De ADR zal voorafgaand aan de basisrapportage een voorstel doen voor het door haar uit te voeren onderzoek voor de basisrapportage en de verdere (jaarlijkse) voortgangsrapportages. Ik informeer u voorts dat informatie van derden die bij Defensie beschikbaar is, vanzelfsprekend beschikbaar is voor controle door de Algemene Rekenkamer en de ADR. Informatie die valt onder de *non-disclosure agreements* kan daarbij derhalve worden ingezien. De ADR heeft daarnaast de mogelijkheid om, bij uitzondering en in afstemming met Defensie en opdrachtnemer(s),

informatie in te winnen of een onderzoek in te stellen naar activiteiten van opdrachtnemer(s).

Met de beperking ten aanzien van het openbaar maken van informatie dient de controlerende instantie in diens rapportage rekening te houden.

De Staatssecretaris van Defensie,
C.A. van der Maat