35 728 Programma Grensverleggende IT (GrIT)

Nr. 27 Brief van de staatssecretaris van Defensie

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 30 september 2026

Hierbij ontvangt u de negende voortgangsrapportage van het programma Grensverleggende IT (GrIT). Deze rapportage beslaat de periode 1 januari 2026 tot en met 31 juli 2026 en geeft inzicht in de gerealiseerde resultaten, de financiële ontwikkeling, de status op gebied van governance, het risicomanagement en de verwachtingen voor de komende maanden.

Bijgaand treft u ook de vertrouwelijke bijlage[1] aan waarin de gedetailleerde kosten- en risico-specificaties zijn opgenomen. De bijlage bevat commercieel vertrouwelijke informatie; openbaarmaking zou de aanbestedingsprocedure kunnen verstoren en kan daarom de positie van de betrokken bedrijven en van Defensie schaden.

Met GrIT moderniseert Defensie de IT-infrastructuur van de krijgsmacht en legt zij de basis voor een veilige en toekomstbestendige informatievoorziening. Deze basis is essentieel voor zowel de bedrijfsvoering als de uitvoering van militaire operaties. De huidige veiligheidssituatie laat zien dat betrouwbare IT, snelle informatie-uitwisseling en veilige communicatie cruciale randvoorwaarden zijn voor militair optreden. GrIT levert de digitale ruggengraat waarmee Defensie haar informatiepositie versterkt, samenwerking verbetert en zich beter kan beschermen tegen digitale dreigingen.

Terugblik eerste helft 2026

Release Vijf van het programma heeft in de eerste helft van 2026 de beoogde resultaten behaald. Zoals eerder met uw Kamer gedeeld, wordt gewerkt aan de ontwikkeling van de ‘Modules Ontplooid’. Dit zijn modules die samen een mobiel datacenter vormen, waardoor eenheden in het veld tijdens missies toegang hebben tot essentiële IT-diensten en beveiligde verbindingen met NAVO-partners. De ontwikkeling hiervan is cruciaal voor de ondersteuning van hoofdtaak 1 van Defensie. De ontwikkeling van deze modules heeft inmiddels een belangrijke mijlpaal bereikt. Er zijn prototypes ontwikkeld die zijn onderworpen aan strenge val-, tril- en elektromagnetische testen om operationele inzetbaarheid te garanderen. Daarnaast zijn de eerste Proof-of-Concepts succesvol uitgevoerd, waarbij de inzetbaarheid in de praktijk is getest.
Ook is het Private Cloud Platform in de acceptatie-omgeving opgeleverd, door Defensie getest, geaccepteerd en geaccrediteerd. Het Private Cloud Platform is een eigen cloud platform voor Defensie, dat een veilige en flexibele cloudomgeving biedt en daarmee dus niet afhankelijk is van technologie van een van de grote *hyperscalers*. Eindgebruikers kunnen hiermee eenvoudig geautomatiseerde Private Clouddiensten aanvragen, wat bijdraagt aan de uitbreiding van de digitale capaciteit van Defensie.

Daarnaast is Het Protected Core Network - een beveiligde, eigen netwerkinfrastructuur voor kritieke defensietoepassingen – in de eerste helft van 2026 beschikbaar gemaakt. Het netwerk kan nu automatisch de benodigde

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

configuraties genereren. Ook kunnen nieuwe functionaliteiten sneller worden toegevoegd, zonder dat daarvoor afzonderlijke test- en acceptatiefasen nodig zijn. Deze functionaliteit maakt een snellere en veiligere aansluiting van vaste defensielocaties mogelijk en ondersteunt daarmee direct de uitvoering van Hoofdtaak 1.

Het onafhankelijke adviesbureau Gartner heeft het afgelopen half jaar een bijdrage geleverd aan de Quality Assurance (QA) en risicobeheersing van het programma. Zij constateerden dat het programma in de eerste helft van 2026 verdere stappen heeft gezet in het beheersen van risico's en knelpunten. Wel blijven ze aandacht vragen voor de afhankelijkheid van het Private Cloud Platform voor de migratie van geselecteerde Defensie-applicaties (Keep Applicaties). De door Gartner gesignaleerde beheersmaatregelen zijn opgenomen in de werkwijze van het programma.

Herstel- en verbeterplan
In oktober 2025 gaf de IT-infrastructuurpartner aan de afgesproken mijlpalen voor het Private Cloud Platform niet te kunnen behalen. Om deze vertraging te mitigeren is de samenwerking met de leverancier versterkt via een gezamenlijk herstelplan. De uitvoering hiervan verloopt volgens planning; ruim 75% van de verbeteracties zijn afgerond. De focus ligt nu op de structurele borging van verbeterde governance- en kwaliteitsaspecten.

Maatregelen die bijdragen aan het behalen van resultaten zijn:
- een versnelde sturingscyclus via sprints van drie weken;
- een gezamenlijk change-team dat de planmatige koppelingen met de bestaande IT-omgeving beheert;
- een eenduidig proces voor testen en accreditatie om de verantwoordelijkheden tussen partijen te borgen.

Vooruitblik tweede helft 2026
In de tweede helft van 2026 staat Release Zes centraal binnen het programma. De kerndoelen van deze release zijn:
- Modules ontplooid: de verdere ontwikkeling van de modules voor het mobiele datacenter. In deze fase worden de verschillende hardwareconfiguraties uitgebreid getest en definitief goedgekeurd. Daarna kan de grootschalige assemblage van de modules starten. Daarnaast wordt de software klaargemaakt voor gebruik, zodat de opleiding van personeel binnen de operationele commando's kan worden opgestart.
- Gereedheid Private Cloud Platform: na de eerdere vertraging wordt de productieomgeving van het Private Cloud Platform opgeleverd. Hiermee is de noodzakelijke stabiele infrastructuur aanwezig om de migratie van geselecteerde Defensie-applicaties te starten.

Door de vertraagde oplevering van het Private Cloud Platform eind 2025, vindt de migratie van de geselecteerde Defensie-applicaties naar de nieuwe IT-infrastructuur later plaats. De planning wordt, vanwege complexe onderlinge afhankelijkheden, nog verder gedetailleerd. De eindmijlpaal van 2030 van het programma blijft ongewijzigd.

De staatssecretaris van Defensie,
D.G. Boswijk