Ministerie van Defensie

Toezichtjaarplan 2026

Beveiligingsautoriteit

2026

Voorwoord

Het Ministerie van Defensie levert een belangrijke bijdrage aan het beschermen van het Nederlands grondgebied en dat van bondgenoten, het bevorderen van de (internationale) rechtsorde en stabiliteit, het ondersteunen van civiele autoriteiten en het leveren van bijstand bij rampen en crises. Het is van wezenlijk belang dat Defensie voldoende personeel, informatie en materieel heeft om deze hoofdtaken effectief uit te voeren. De organisatie moet bij de taakuitvoering onder alle omstandigheden kunnen vertrouwen op de continuïteit en de betrouwbaarheid van de bedrijfsprocessen en op de benodigde mensen en middelen. Door beveiligingsmaatregelen te treffen en te testen, worden de continuïteit en betrouwbaarheid van de bedrijfsprocessen gewaarborgd. Een van de beveiligingsmaatregelen is het beveiligen van de door de defensieonderdelen aangemerkte Te Beschermen Belangen (TBB's). Informatie, zowel in fysieke als in elektronische vorm, IT-diensten, fysieke locaties en materieel kunnen ook worden aangemerkt als TBB's. De ernst en omvang van potentiële schade aan TBB's bepaalt de mate van de vereiste beveiliging. Onder schade valt zowel materiële schade als immateriële schade. Beveiliging wordt uitgevoerd op basis van risicomanagement, met als doel het vinden van de juiste balans tussen het implementeren van beveiligingsmaatregelen en de beheersing van beveiligingsrisico's.

De Beveiligingsautoriteit (BA) is toezichthouder op integrale beveiliging. Integrale beveiliging (*security*) is niet hetzelfde als bedrijfsveiligheid (*safety*). Bedrijfsveiligheid omvat onder andere bedrijfshulpverlening, brandweerzorg, vliegveiligheid, arbeidsomstandigheden en de toepassing van milieuregels. Bedrijfsveiligheid valt buiten de *scope* van de BA.

In dit toezichtjaarplan kijkt de BA vooruit en stelt ze het toezichtjaarprogramma vast.

De Beveiligingsautoriteit,

voor deze,
het afdelingshoofd Beveiliging en Gegevensbescherming

Colofon

Beveiligingsautoriteit

Adres
Plein-Kalvermarktcomplex
Plein 4
2511 CR Den Haag

Postadres
Postbus 20701
2500 ES Den Haag
MPC 58B

Datum
November 2025

Inhoud

1 De Beveiligings-autoriteit

De BA maakt namens de secretaris-generaal (SG) het Defensie Beveiligingsbeleid (DBB) en houdt toezicht op de naleving daarvan bij alle defensieonderdelen. Daarnaast heeft de BA de *National Security Authority*-rol voor het militaire domein (NSA-MoD). Vanuit deze rol houdt de BA toezicht op basis van het beveiligingskader uit het NATO- en EU-beleid, of op basis van afspraken die voortvloeien uit bi- en multilaterale verdragen. Tot slot houdt de BA toezicht op de naleving van het toetsingskader Beveiligingsnormen Inlichtingen & Veiligheidsdiensten (BNIVD). Dit betreft het toezicht op de inlichtingendiensten Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD).

De BA kent drie toezichtmethoden, namelijk normatief toezicht, systeemgericht toezicht en beveiligingstesten. Deze methoden worden in paragraaf 1.4 nader uitgelegd. Daarnaast kunnen er specifieke onderzoeken met een toezichthoudend karakter worden uitgevoerd. Tevens zijn toezichthoudende taken belegd in de functionele beveiligingsketen. Deze toezichttaken worden in 2026 verder geïntensiveerd.

1.1 Defensie Beveiligingsbeleid

Het DBB bevat het geheel aan beveiligingsnormen en bestaat uit verschillende deelgebieden:

- algemene beveiliging;
- fysieke beveiliging;
- personele beveiliging;
- informatiebeveiliging (inclusief beveiligingsmaatregelen tegen compromitterende emissies en cryptografische normen);
- *special access programs;*
- industriebeveiliging.

Het DBB dient als basis en fundament voor de taak van de BA als toezichthouder. Ook controleert de BA periodiek het bestaan, de opzet en de werking van het beleid. Waar nodig herziet de BA het DBB met betrekking tot de correctheid en actualiteit van het DBB ten opzichte van veranderingen in NATO-, EU-, en VS-normeringen.

1.2 Verantwoordelijkheid voor integrale beveiliging

Binnen Defensie is de commandant (hieronder valt ook het hoofd van dienst, de lijnmanager, enzovoorts) verantwoordelijk voor de integrale bedrijfsvoering binnen zijn defensieonderdeel. Defensieonderdelen zien zelf toe op de naleving en de toepassing van het DBB. De BA ziet toe op correct gebruik en navolging van het DBB en grijpt in waar nodig, bijvoorbeeld wanneer maatregelen ontoereikend zijn.

1.3 Toezicht op overige normenkaders

Inlichtingendiensten
In het kader van de samenwerking tussen de MIVD en de AIVD, toetsen en accrediteren de BA en de beveiligingsambtenaar van de AIVD gezamenlijk de systemen en locaties van beide diensten.

F-35
Naast het nationale beleid conformeert Defensie zich met het *F-35 Air System* aan richtlijnen van de Amerikaanse overheid. De BA houdt in haar rol als *Program Security Officer* (PSO) normatief toezicht op alle *Special Access Program Facilities* (SAPF) die onder Nederlandse verantwoordelijkheid vallen. Hieronder vallen zowel gerealiseerde als in aanbouw zijnde SAPF-locaties in Nederland en in de Verenigde Staten. In haar rol als PSO houdt de BA samen met de Amerikaanse PSO toezicht. Dit doen we jaarlijks, zowel aangekondigd als onaangekondigd.

Overkoepelende nationale en internationale normenkaders
Organisaties als de Algemene Rekenkamer, de NATO en de EU zijn externe toezichthouders. Deze toezichthouders houden systeemgericht toezicht en normatief toezicht. De BA begeleidt hierbij en bereidt toezicht, onderzoeken en/of inspecties voor.

1.4 Methoden van toezicht

Binnen het DBB worden dezelfde drie toezichtmethoden gebruikt, namelijk normatief toezicht, systeemgericht toezicht, en beveiligingstesten. Deze toezichtmethoden zijn cruciaal om de opzet, het bestaan en de werking van het DBB binnen de defensieonderdelen te doorgronden en elkaar scherp te houden. Voorts bestaat de mogelijkheid thematische onderzoeken uit te voeren. Daarbij wordt een afgebakend thema meer in diepte onderzocht. Het geheel maakt dat vermijdbare risico's en incidenten zoveel mogelijk voorkomen dan wel tijdig geïdentificeerd/gesignaleerd worden. Om de onafhankelijkheid van de toezichttaak van de BA te borgen, bestaat er naast de beleidstaak een aparte sectie Toezicht voor specifieke onderwerpen, zoals accreditaties en certificeringen. Deze sectie bestaat uit vier personen, aangevuld met *subject matter experts* (SME's). Verder bestaat er een functionele beveiligingsketen, waaraan door het DBB toezichthoudende taken zijn opgedragen.

Normatief toezicht
Bij normatief toezicht stelt de BA vast of beveiligingsmaatregelen zijn geïmplementeerd en of daarmee aan beveiligingsnormen is voldaan. Normatief toezicht kan onder andere gericht zijn op TBB's. Hieronder zijn enkele processen uitgewerkt.

Accreditaties
Een accreditatie is toezicht op de ingebruikname van een informatiesysteem dat gerubriceerde gegevens verwerkt. Het betreft hier een voorafgaande en doorlopende normatieve toets van zowel het informatiebeveiligingsdeel van het informatiesysteem

als van de omgeving waarin een dergelijk systeem zich bevindt (bijvoorbeeld de personele en fysieke component). Het beleid hiertoe is in instructie D/101 en A/002 van het DBB opgenomen. Tevens voert de BA fysieke accreditaties uit op basis van de normenset BNIVD.

Certificeringen
Het distribueren en opslaan van staatsgeheimen via communicatiesystemen en IT-diensten mag uitsluitend plaatsvinden met goedgekeurde cryptoproducten en producten die bescherming bieden tegen elektromagnetische straling. De BA is de certificerende autoriteit in het proces van het goedkeuren van (cryptografische) apparatuur voor gebruik binnen Defensie.

Risicomanagement
Het DBB maakt het voor verantwoordelijke commandanten mogelijk om eventuele restrisico's te accepteren. Dat is een formeel en gedocumenteerd proces. De BA houdt toezicht op de risicoacceptaties van commandanten ten aanzien van de zwaarst-beveiligde objecten, in de categorieën TBB-1 en TBB-2.

Systeemgericht toezicht
Met systeemgericht toezicht bekijkt de BA de opzet, het bestaan en de effectieve werking van processen en beheersingsmaatregelen die voor een defensieonderdeel noodzakelijk zijn om aan het DBB te voldoen. Bij deze vorm van toezicht staat de mate van borging van de zogenaamde *Plan-Do-Check-Act*-cyclus (PDCA-cyclus) door het management centraal.

Beveiligingstesten
Met beveiligingstesten toetst de BA de effectiviteit van beveiligingsmiddelen en houdt de BA toezicht op de (operationele) naleving van instructies en relevant beleid. Testmethodieken zijn onder andere fysieke en digitale penetratietesten en *social engineering*. De resultaten maken het mogelijk om risico's en kwetsbaarheden te identificeren. Hieruit kan gericht advies voor verbeteringen gegenereerd worden. Penetratietesten in het digitale domein vormen ook een belangrijk element in het accreditatietraject van informatiesystemen, zoals in paragraaf 1.1 weergegeven.

Overige toezichtactiviteiten
Naast toezicht op naleving omvat het toezichtraamwerk:
- vervolgtoezicht, waarbij veranderingen en verbeteringen in de loop van de tijd worden gemonitord;
- signaalgestuurd toezicht, om snel te reageren op onverwachte gebeurtenissen;
- thematisch toezicht, waarbij de nadruk ligt op specifieke relevante thema's;
- ondersteuning aan defensieonderdelen, om operaties positief te ondersteunen en om mee te denken bij complexe zaken waar de defensieonderdelen zelf niet uitkomen. Dit is belangrijk om stagnatie van operaties te voorkomen.

Deze diverse benaderingen versterken de toezichtinspanningen en dragen bij aan de conformiteit en kwaliteit van het toezicht.

1.5 Samenwerking

Gezamenlijke inzet Toezichtnetwerk Defensie
De toezichthouders en -autoriteiten binnen Defensie werken samen in het Toezichtberaad, dat we komende jaren willen uitbreiden met een Toezichtnetwerk. Deelnemers zijn de Beveiligingsautoriteit (BA), de Functionaris voor Gegevensbescherming (FG), de Inspectie Militaire Gezondheidszorg (IMG), de Inspectie Veiligheid Defensie (IVD), het Korps Militaire Controleurs Gevaarlijke Stoffen (KMCGS) en de Militaire Luchtvaart Autoriteit (MLA). De Inspecteur Generaal Krijgsmacht (IGK) is toehoorder. Het Bureau Toezicht Defensie (BTD)heeft een centrale rol als coördinerend en adviserend bureau. Het voorzitterstrio (VZtrio) bestaande uit de MLA, IMG en IVD, heeft het jaarlijks roulerend voorzitterschap. Tot juli 2026 is de MLA de voorzitter, daarna neemt de IVD het over.

Met elkaar zetten we strategische lijnen uit, stemmen gezamenlijke thema's af en borgen we de verbinding met beleid en uitvoering. We werken aan de ontwikkeling van gedeelde toezichtinstrumenten, onze positionering en onze effectiviteit. Het BTD organiseert de Leergang Toezicht Defensie (LTD): een leertraject voor alle toezichtcollega's gericht op verdieping, uitwisseling en versterking van het gezamenlijke toezichtvak.

Komend jaar focussen we ons op thema's die aansluiten bij de (versnelde) gereedstelling voor hoofdtaak 1 en de groei van de organisatie. Dit zijn onder andere: bewuste en effectieve toepassing van integraal risicomanagement (IRM) en het voorkomen van *normalisation of deviance*. Om effectief toezicht te houden zetten we ook in op het ontwikkelen van effectievere toezichtmethoden, het verbeteren van onze informatiepositie en onze relatie met de organisatie.

Toezichtberaad

In 2020 verenigden de interne toezichthouders zich in het Toezichtberaad Defensie, met als doel de kwaliteit en de samenhang van het interne toezicht te verbeteren en te versterken. Het Toezichtberaad wordt ondersteund door BTD. De Inspecteur-Generaal der Krijgsmacht (IGK) en een vertegenwoordiger van het Bureau Secretaris-Generaal nemen als toehoorder deel aan het beraad. De IGK is geen toezichthouder, maar zijn onderzoeken verrijken wel het inzicht in de staat en het functioneren van de defensieorganisatie.

Kwaliteitszorg en -monitoring

De bewaking van kwaliteit op het gebied van beveiliging en aangrenzende gebieden is niet alleen een taak van toezichthouders. Ook de interne kwaliteitszorg van de defensieorganisatie is cruciaal. Kwaliteitszorg en -monitoring vinden bijvoorbeeld plaats door de *Chief Privacy Officer* (CPO) en de *Chief Information Security Officer* (CISO). Resultaten uit kwaliteitszorg en -monitoring zijn van groot belang voor het toezicht van de BA. Een voorbeeld hiervan is het informatiebeveiligingsbeeld dat de CISO jaarlijks maakt.

1.6 Ontwikkelingen in Toezicht

Herziening DBB en I-BA-001 'Integrale beveiliging & Governance'

Om de spanwijdte van de beveiligingsketen in kaart te brengen en bevoegdheden te borgen, is gewerkt aan de herziening van DBB en het document I-BA-001: Integrale beveiliging & *Governance.* Deze twee documenten bevatten de kaders voor taken, verantwoordelijkheden en bevoegdheden met betrekking tot integrale beveiliging op strategisch, tactisch en operationeel niveau.

Beleidsmatige borging en uitvoering beveiligingstesten

De BA is in het voorgaande toezichtjaar gestart met de beleidsmatige borging van fysieke beveiligingstesten. Defensie zet deze beveiligingstesten als derde toezichtvorm in om de werkelijke effectiviteit van geïmplementeerde beveiligingsmaatregelen te testen. Deze inspanning is mede het gevolg van het verantwoordingsonderzoek 2022 van de Algemene Rekenkamer. Naast de beleidsmatige borging zette de BA ook stappen om de randvoorwaarden te inventariseren en uit te werken. Hierbij kijkt de BA naar de uitvoerbaarheid en ondersteuning door interne en externe dienstverleners.

2

Geplande activiteiten 2026

Voor 2026 zet de BA een toezichtarrangement neer, waarin het reguliere, systeemgerichte, normatieve en test gebaseerde toezicht onverminderd wordt voortgezet. Naast deze toezichtactiviteiten zullen wij extra aandacht besteden aan de bevinding van de Algemene Rekenkamer, die een ernstige onvolkomenheid signaleert ten aanzien van de fysieke beveiliging van militaire objecten.

2.1 Toezichtactiviteiten

Normatief toezicht
In 2026 worden verschillende activiteiten ontplooid omtrent normatief toezicht, zowel door toezichthouders in de beveiligingsketen als door de BA. De BA focust daarbij met name op de hoogst geclassificeerde TBB's en internationale verplichtingen. Het gaat hierbij zowel om toezicht vooraf (toezicht voorafgaand aan afgifte van accreditaties en certificeringen) en periodieke vernieuwing daarvan, als om nalevingstoezicht (toezicht na afgifte van accreditaties en certificeringen). Ten aanzien van internationale verplichtingen verwacht de BA toezichtactiviteiten te ontplooien in het kader van de NAVO, de EU en de samenwerking met de VS. Dit zal een aanzienlijk gedeelte van de toezichtcapaciteit vergen.

Systeemgericht toezicht
Het beveiligingsbeleid schrijft voor dat systeemgericht toezicht jaarlijks plaatsvindt. In 2025 is hier meer nadruk op gelegd. Op basis van een vragenlijst is per defensieonderdeel het volwassenheidsniveau onderzocht conform een eenduidig en breed geldend beoordelingskader. Door inzicht in de volwassenheid, krijgt het management de mogelijkheid te sturen op ambitie en gerichte verbetering. Op het moment van schrijven van dit jaarplan worden de resultaten uitgewerkt. In 2026 ligt met name een focus op monitoren van de opvolging van resultaten en aanbevelingen ten aanzien van het beeld dat is gebaseerd op de resultaten van 2025.

Beveiligingstesten
Vanuit de Commandant der Strijdkrachten (CDS) is in 2025 een reeks aan beveiligingstesten georganiseerd. Ook toezichthouders in de beveiligingsketen voerden die uit. In navolging daarvan vindt onderzoek plaats naar de meer structurele uitvoering van beveiligingstesten. Los daarvan voert de BA in 2026 zelfstandig enkele fysieke beveiligingstesten uit of laat dat doen.

Binnen Defensie worden in het kader van de accreditatie van informatiesystemen ook beveiligingstesten uitgevoerd. Dit is geborgd in de DBB-instructie D/102: *Cybersecurity*-onderzoek van informatiesystemen. Bij het bepalen van de *Security* Accreditatie Strategie (SAS) als onderdeel van het accreditatieproces, wordt per systeem bepaald of en wat voor soort *cybersecurity*-onderzoek noodzakelijk is. Dit draagt dus bij aan het toezicht op informatiesystemen en de oordeelsvorming van een informatiesysteem. In 2026 komt er een nieuwe versie van deze instructie.

Thematisch onderzoek
De sectie Toezicht van de BA is voornemens in 2026 een thematisch onderzoek uit te voeren rondom de kwaliteit van de beveiligingsketen. Bij een thematisch onderzoek kan de BA een thema meer uitdiepen. De BA kijkt dan niet alleen of de beveiligingsketen voldoet aan de bestaande normen, maar kan ook vanuit toezichtperspectief adviezen meegeven over deze normen. Voorts verricht de BA in 2026 een thematisch onderzoek naar een vernieuwing in de keten van cryptografische beveiligingsmaatregelen.

2.2 Versterking toezichtdomein

Kennisdeling
De BA is een formele interne toezichthouder. Tegelijkertijd hebben de beveiligingscoördinatoren van de defensieonderdelen middels het DBB ook toezichthoudende taken opgedragen gekregen. De BA zet zich in om de samenwerking met deze beveiligingscoördinatoren te versterken. Voor 2026 betekent dit onder andere dat de BA in de prioritering van het toezicht rekening houdt met de toezichtactiviteiten die de beveiligingscoördinatoren al voor hun rekening nemen. Daarnaast zet de BA in 2026 in op het verstevigen van de methodologie in het toezicht. Dit doet de BA zowel in samenwerking met toezichthouders in de functionele beveiligingsketen als breder met de toezichthouders in het Toezichtberaad,

Beveiligingstesten
In 2025 is gewerkt aan de beleidsmatige borging van fysieke beveiligingstesten middels een DBB-instructie. Inmiddels zijn er bij defensieonderdelen meerdere beveiligingstesten uitgevoerd. Dit gebeurde vooral op projectbasis en nog niet structureel. De BA zet zich in 2026 in om de capaciteit voor het uitvoeren van beveiligingstesten in de defensieorganisatie structureel te borgen.

3

Bijlage

3.1 Afkortingen

AIVD	Algemene Inlichtingen en Veiligheidsdienst
BTD	Bureau Toezicht Defensie
BA	Beveiligingsautoriteit
BNIVD	Beveiligingsnormen Inlichtingen & Veiligheidsdiensten
CDS	Commandant der Strijdkrachten
CISO	*Chief Information Security Officer*
CPO	*Chief Privacy Officer*
DBB	Defensie Beveiligingsbeleid
EU	Europese Unie
FG	Functionaris voor Gegevensbescherming
IGK	Inspecteur-Generaal der Krijgsmacht
IMG	Inspectie Militaire Gezondheidszorg
IT	Informatietechnologie
IVD	Inspectie Veiligheid Defensie
KMCGS	Korps Militaire Controleurs Gevaarlijke Stoffen
MIVD	Militaire Inlichtingen en Veiligheidsdienst
MLA	Militaire Luchtvaart Autoriteit
NATO	*North Atlantic Treaty Organization*
NSA-MoD	*National Security Authority – Ministry of Defence*
PDCA	*Plan-Do-Check-Act*
PSO	*Program Security Officer*
SAPF	*Special Access Program Facilities*
SG	secretaris-generaal
SME	*Subject Matter Expert*
TBB	Te Beschermen Belang