Ministerie van Defensie

Toezichtjaarverslag 2023

Beveiligingsautoriteit

Colofon

Beveiligingsautoriteit

Adres
Kalvermarkt 32
Postbus 20701
2511 CB ‘s-Gravenhage

Postadres
2500 ES ’s-Gravenhage
MPC 58B

Opsteller
Dhr. M. van Ree MIM
Toezichthouder integrale beveiliging

Datum
Maart 2024

Voorwoord

Met genoegen presenteren wij ons toezichtjaarverslag 2023. Dit jaarverslag markeert een overgangsfase, want de Beveiligingsautoriteit (BA) gaat stapsgewijs van traditioneel toezicht (voornamelijk normatief toezicht) naar een aanpak waarbij parallel systeemgericht toezicht wordt ingezet. Dit leidt uiteraard ook tot wijzigingen in de opzet van de jaarverslagen. In dit jaarverslag worden deze wijzigingen toegelicht.

De BA wil van de vertrouwde toezichtvormen het goede behouden en tegelijk verrijken met systeemgericht toezicht, waarbij data en kwaliteitsmanagementsystemen een grotere rol gaan spelen. Dit verbetert de kwaliteitscirkel (*Plan-Do-Check-Act*-cyclus, kortweg PDCA-cyclus), wat weer leidt tot een versterking van het zelflerend vermogen van Defensie op het gebied van integrale beveiliging.

Traditioneel toezicht concentreert zich op het beoordelen van de naleving van normen en eisen. Daarmee controleren wij of in de praktijk aan de gestelde eisen wordt voldaan. Met systeemgericht toezicht kijken we 'dieper'. We kijken ook naar de opzet, het bestaan en de effectiviteit van het kwaliteitsmanagementsysteem. In hoeverre is het kwaliteitsmanagementsysteem 'volwassen'? Wordt er geleerd van gemaakte fouten? Bestaat er een cultuur waarin leren en verbeteren centraal staan? Op basis hiervan kan ook een oordeel worden gevormd over de interne samenwerkingen.

Het doel voor de BA is om in de toekomst meer te kijken naar de mate waarin Defensie in het beveiligingsdomein *in control* is. Waar traditioneel toezicht zich met name richt op naleving, stelt de combinatie met systeemgericht toezicht ons in staat om de *Plan-Do-Check-Act*-cyclus te toetsen en te bezien of continu en actief naar verbetering wordt gezocht. Beveiliging is immers van cruciaal belang bij het waarborgen van de continuïteit en betrouwbaarheid van de bedrijfsprocessen. Hiervoor dienen niet alleen de betreffende onderdelen intern goed samen te werken, maar dient vanuit toezicht ook te worden gekeken naar de manieren waarop onderdelen samenwerken en van elkaar leren, om steeds opnieuw te komen tot optimale beveiliging van onze Te Beschermen Belangen (TBB). Dat is in ons aller belang.

De Beveiligingsautoriteit,
voor deze,
het afdelingshoofd Beveiligingsautoriteit en Gegevensbescherming,

Hendrik J Schuthof
Digitally signed by Hendrik J Schuthof
Date: 2024.03.09 08:35:41 +01'00'

Kolonel H.J. Schuthof, MSc, EMSD, MA

Inhoud

1 De Beveiligingsautoriteit

Binnen het Ministerie van Defensie houdt de BA toezicht op de integrale beveiliging. Op basis van de aanwijzing SG-A948 is de BA in zijn rol als toezichthouder formeel aangewezen als interne toezichthouder en als lid van het Toezichtberaad Defensie.

De toezichthoudende taak van de BA betreft in het algemeen het toezicht houden op de naleving van het Defensie Beveiligingsbeleid (DBB) bij alle defensieonderdelen. Daarnaast voert de BA de *National Security Authority*-rol uit voor het militaire domein (NSA-MoD). Deze rol vloeit voort uit het NATO-beleid. 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) als het toezicht op de inlichtingendiensten betreft.

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* en
- industriebeveiliging.

1.2 Verantwoordelijkheid voor integrale beveiliging

Binnen Defensie is de BA, namens de Secretaris-Generaal (SG), verantwoordelijk voor het opstellen van het beveiligingsbeleid en heeft daardoor een richtende positie. De Commandant der Strijdkrachten (CDS) is verantwoordelijk voor de aansturing en coördinatie; een inrichtende positie. Tot slot is de commandant (hieronder valt ook het hoofd van dienst, de lijnmanager, enzovoorts) verantwoordelijk voor de integrale uitvoering bij zijn organisatie-eenheid binnen de kaders van het DBB; een verrichtende positie. De toezichttaak is op basis van een decentraal concept ingericht en belegd binnen de gehele functionele beveiligingsketen. De BA is daarbij in zijn rol als toezichthouder formeel benoemd tot interne toezichthouder. Defensieonderdelen zien zelf ook toe op de toepassing en de naleving van het DBB.

1.3 Toezicht op overige normenkaders

Inlichtingendiensten

In het kader van de samenwerking tussen de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), toetsen en accrediteren de BA Defensie 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 zijn 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 zijn rol als PSO houdt de BA het toezicht samen met de Amerikaanse PSO. Het toezicht vindt jaarlijks plaats, zowel aangekondigd als onaangekondigd.

Overig

Organisaties als de Auditdienst Rijk, 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

Bij normatief toezicht kijkt de toezichthouder naar de geïmplementeerde beveiligingsmaatregelen en beoordeelt of aan beveiligingsnormen is voldaan. Ook kunnen beveiligingsmaatregelen op effectiviteit worden onderzocht door middel van beveiligingstesten. Normatief toezicht kan onder andere gericht zijn op TBB, fysieke en elektronische informatie, IT-voorzieningen en fysieke locaties. Toezicht kan ook gericht zijn op samengestelde en complexe belangen, zoals een informatiesysteem of wapensysteem. Naast het toezien op de naleving omvat het toezicht tevens:

- vervolgtoezicht, waarbij veranderingen en verbeteringen in de loop van de tijd worden gemonitord;
- signaalgestuurd toezicht, om snel te reageren op onverwachte gebeurtenissen en
- thematisch toezicht, waarbij de nadruk ligt op specifieke relevante thema's.

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

Met systeemgericht toezicht bekijkt de BA de opzet, het bestaan en de effectieve werking van de processen en beheersingsmaatregelen die noodzakelijk zijn voor een defensieonderdeel om te garanderen dat aan het DBB wordt voldaan. Bij deze vorm van toezicht staat de mate van borging van de PDCA-cyclus centraal.

1.5 Samenwerking

Om de samenhang en de kwaliteit van toezicht te verbeteren, werken de interne toezichthouders bij Defensie samen. De interne toezichthouders zijn: de 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). Zij zoeken de samenwerking op verschillende onderdelen, zoals de afstemming van toezichtagenda's. Ook versterken zij gezamenlijk het toezichtproces op het gebied van methodologie en redactie.

Toezichtberaad

In 2020 verenigden de interne toezichthouders zich in het Toezichtberaad Defensie met als doel de kwaliteit te verbeteren en de samenhang en effectiviteit van het interne toezicht te versterken. 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. De Inspecteur-Generaal Veiligheid is als coördinerend toezichthouder voorzitter van het beraad.

Functionaris voor gegevensbescherming

De aandacht voor de beveiliging van persoonsgegevens is in sterke mate toegenomen vanwege maatschappelijke ontwikkelingen en de inwerkingtreding van de Algemene verordening gegevensbescherming. De BA en de FG werken samen en houden gezamenlijk toezicht.

Korps Militaire Controleurs Gevaarlijke Stoffen

Het KMCGS en de BA hebben een gemeenschappelijk toezichtgebied: de opslag en het vervoer van munitie, explosieven en springmiddelen. De gehanteerde normering is voor beide toezichthouders wel verschillend. Het KMCGS vervult voor de BA een 'oog- en oorfunctie' voor de naleving van de DBB-normering.

2 Beoordelingssysteem

2.1 Openbaarheid gegevens versus bescherming defensiegegevens

De BA staat achter de wens van Defensie om openheid te bieden over bedrijfsvoering en behaalde resultaten. De belastingbetaler dient uiteraard in te kunnen zien hoe Defensie de financiën aanwendt. 'In hoeverre is de beveiliging bij Defensie op orde?', is een terechte, algemene vraag. Tegelijk gaat de informatie over beveiliging binnen Defensie over gevoelige zaken. De BA heeft inzicht in de stand van zaken op specifieke beveiligingsgebieden en exacte locaties. Deze informatie wekt interesse bij andere geopolitieke spelers, echter niet altijd met nobele motieven. Dat is dan ook de reden waarom er in dit document geen specifieke of lokale informatie staat. Dit verslag biedt inzage in de mate waarin Defensie wat betreft beveiliging *in control* is. De BA onderzoekt bijvoorbeeld of geluidsdichte kamers bij Defensie voldoen aan de gestelde eisen. Hier geeft de BA een algemene waardering voor en geen exacte percentages.

Gerubriceerde informatie

De BA informeert de specifieke defensieonderdelen met alle bevindingen en alle specifieke aanbevelingen na toezichtbezoeken.

Waardering in sterren

De BA hanteert de komende drie jaar een sterrensysteem. De uitdrukking van de mate waarin een onderdeel van het kwaliteitsmanagementsysteem *in control* is, werkt als volgt:

Aantal sterren	Kwaliteitsduiding
*	Zeer slecht
**	Slecht
***	Onvoldoende
****	Voldoende
*****	Goed

3 Hoofdlijnen uit het toezicht

Het jaarverslag geeft een overzicht van de belangrijkste bevindingen gebaseerd op de resultaten van het toezichtjaar 2023. Het is belangrijk op te merken dat de personele uitbreiding die in 2023 was voorzien ter versterking van de toezichtcapaciteit bij de BA, nog niet is gerealiseerd. Met de beperkte toezichtcapaciteit heeft de BA op de hoofdonderwerpen wel het toezichtjaarplan gevolgd, maar zijn niet alle geplande toezichtonderwerpen aan bod gekomen. Zo zijn bijvoorbeeld de geplande gezamenlijke toezichtbezoeken met de FG verplaatst naar toezichtjaar 2024.

3.1 Beveiliging algemeen

Binnen Defensie zijn alle processen rondom integrale beveiliging ingericht op basis van de PDCA-cyclus. Echter wordt op basis van de toezichtresultaten de effectieve werking hiervan als onvoldoende beoordeeld. Dit is vooral geconstateerd op de CHECK- en ACT-fases, waarbij randvoorwaarden erg relevant zijn, zoals capaciteit, kwaliteit van de functionele beveiligingsketen, maar ook het beveiligingsbewustzijn van medewerkers en commandanten. Daarbij merkt de BA op dat de uitvoering door de CDS van het plan van aanpak *Fysieke Beveiliging* van de BA en het plan van aanpak *Crypto* van de BA, van belang zijn om tot verbeteringen te komen.

De effectieve werking van de PDCA-cyclus, wat betreft de CHECK-fase en met de nadruk op de ACT-fase, wordt beoordeeld als onvoldoende.	*** onvoldoende

Aanbeveling 1
De toezichthouder beveelt de CDS en de functionele beveiligingsorganisatie aan om specifieke aandacht te besteden aan de CHECK- en ACT-fases van de PDCA-cyclus. De effectieve werking van deze fases worden als onvoldoende beoordeeld. Het is van belang om gerichte verbeteringen door te voeren om de prestaties te verhogen. De verbeteringen zijn gerelateerd aan capaciteit, kwaliteit en beveiligingsbewustzijn van medewerkers, eigenaren van TBB en/of informatie en commandanten.

Aanbeveling 2
De toezichthouder beveelt de CDS aan uitvoering te geven aan het plan van aanpak Fysieke Beveiliging van de BA en Plan van aanpak Crypto van de BA.

3.2 NATO- en Special Acces Program Facilities

De BA voert inspecties uit op de registratie van specifieke NATO-documentatie en houdt toezicht op alle *Special Acces Program Facilities* (SAPF).

De toezichthouder beoordeelt de mate waarin de organisatie in control is voor wat betreft NATO-inspecties en toezicht op alle *Special Access Program Facilities*, als goed.	***** goed

3.3 Crypto

Hoewel het onderwerp crypto geen verplicht onderdeel is van het managementsysteem ten behoeve van integrale beveiliging, is het essentieel genoeg om te vermelden in dit jaarverslag vanwege de overlappende verantwoordelijkheden op het gebied van richtinggevend en inrichtend beleid. De BA is verantwoordelijk voor het richtinggevende beleid, maar is ook al jarenlang betrokken op inrichtend niveau. De BA zal zich, overeenkomstig het besturingsmodel Defensie, in de toekomst meer richten op de richtende positie. Vanwege de betrokkenheid van de BA op zowel richtend als inrichtend niveau en het holistisch beeld dat hierdoor is ontstaan, wordt hieronder de status van de logistieke processen en beleidsprocessen beschreven.

De processen voor uitgifte, beheer en inname van cryptomiddelen en -sleutels zijn ingericht op basis van de PDCA-cyclus. Deze processen worden in opzet beoordeeld als voldoende.	**** voldoende
In de processen wordt tijdens crypto-*audits* vastgesteld dat met name de ACT-fase verbetering behoeft. De opvolging van aanbevelingen uit controles en monitoring krijgt onvoldoende aandacht, wat het zelflerende vermogen van het managementsysteem belemmert. In bestaan en werking wordt het proces daarom beoordeeld als onvoldoende.	*** onvoldoende

3.4 Beoordeelde onderdelen van het kwaliteitsmanagementsysteem

Voor informatiesystemen en koppelingen geldt dat hiertoe genestelde PDCA-cycli aanwezig zijn in verschillende processen. Dit betekent dat op verschillende niveaus binnen de organisatie specifieke PDCA-processen bestaan, elk gericht op de continue verbetering en evaluatie van integrale beveiliging ten behoeve van informatiesystemen en koppelingen. In dit toezichtjaarverslag wordt alleen de opzet, het bestaan en de werking beoordeeld, gerelateerd aan de kritieke informatiesystemen.

- **Fysieke beveiliging - beveiligingsplannen**
  Voor elke defensielocatie dient een actueel beveiligingsplan aanwezig te zijn. Dit is een onderdeel van het kwaliteitsmanagementsysteem. In een beveiligingsplan staat beschreven hoe de beveiliging van de locatie en de beveiliging van de lokale TBB georganiseerd is, met inbegrip van beveiligingsrisico's en mitigerende maatregelen.

De status van de beoordeelde beveiligingsplannen laat zien dat hoewel de processen volgens de PDCA-cyclus zijn opgezet, de plannen in de praktijk niet altijd actueel zijn of precies overeenkomen met de werkelijkheid. Hieruit blijkt dat gerichte inspanningen nodig zijn om de actualiteit en nauwkeurigheid van de beveiligingsplannen te verbeteren.	*** onvoldoende

- **Incidentbeheersing**
  De BA kan alle gemelde beveiligingsincidenten inzien en voert hierop analyses uit.

Het aantal gemelde incidenten is in 2023 met 25% toegenomen ten opzichte van 2022. Alle incidenten worden grondig beoordeeld en dienen als basis voor verbeteracties op korte termijn en/of lange termijn. De organisatie is wat betreft incidentbeheersing in voldoende mate *in control*.	**** voldoende

• Risicobeheersing

Afhankelijk van het classificatieniveau worden de restrisico's aan de BA voorgelegd. Hierdoor heeft de BA zicht op geaccepteerde restrisico's van de hogere TBB en kunnen deze worden bewaakt. Voor informatiesystemen geldt dat risicobeheersing geborgd is in het accreditatieproces.

Net als bij het onderdeel incidentbeheersing zijn de processen voor risicobeheersing ingericht op basis van de PDCA-cyclus. De BA heeft kennis van alle restrisico's op de hogere TBB. Het aantal bij de BA gemelde beveiligingsrisico's is in 2023 gelijk gebleven ten opzichte van 2022. Daarbij merkt de BA op dat tijdens toezicht beveiligingsrisico's zijn ontdekt die niet eerder door de organisatie zijn geïdentificeerd en behandeld volgens het beleid. Dit betreft risico's van toepassing op alle TBB-classificaties. Op dit onderdeel is de organisatie onvoldoende in control, waarbij specifieke aandacht nodig is voor de CHECK-fase. Mogelijke oorzaken kunnen gerelateerd zijn aan aansturing, uitvoering, capaciteit en beveiligingsbewustzijn binnen de organisatie.	**[1] slecht

Aanbeveling 3

Effectieve risicobeheersing is essentieel voor de organisatie, omdat het de organisatie in staat stelt te kunnen sturen op risico's. Zo kan proactief worden omgegaan met potentiële dreigingen, maar ook met kansen. Tevens biedt effectieve risicobeheersing een solide basis voor weloverwogen besluitvorming. Aan de defensieonderdelen wordt aanbevolen om gerichte verbeteringen door te voeren in de CHECK-fase met betrekking tot risicobeheersing. Dit betreft zowel het tijdig identificeren van beveiligingsrisico's, als het behandelen ervan overeenkomstig het beleid.

Risicobeheersing voor informatiesystemen zit verankerd in het accreditatieproces en is voldoende *in control*.	**** voldoende

• Personele beveiliging

Onderdeel van personele beveiliging betreft het uitvoeren van veiligheidsonderzoeken door de Unit Veiligheidsonderzoeken (UVO). Met de Tweede Kamer is afgesproken dat 90% van de veiligheidsonderzoeken binnen de wettelijke termijn van acht weken dient te worden afgerond. Het blijkt dat de wettelijke termijn en de 90%-norm binnen de DO-fase niet gehaald worden, wat effect heeft op de ACT-fase.

Defensie loopt een risico in de ACT-fase op het onderdeel personele beveiliging, omdat veiligheidsonderzoeken niet binnen de afgesproken termijn worden afgerond en de 90%-norm niet wordt gehaald.	*** onvoldoende

• Accreditatie kritieke informatiesystemen

Samen met de beveiligingsketen houdt de BA zicht op de voortgang van de accreditaties van kritieke informatiesystemen.

De beoordeling van het proces ten behoeve van het accrediteren van kritieke informatiesystemen toont aan dat de processen ingericht zijn volgens de PDCA-cyclus. Daarbij staat het streven naar continue verbetering centraal. Voor alle kritieke informatiesystemen geldt dat deze zijn voorzien van een (tijdelijke) accreditatie. Verbeterplannen gekoppeld aan tijdelijke accreditaties worden gemonitord. Accreditaties hebben een beperkte geldigheid, wat betekent dat deze cyclisch worden herzien en aangepast op basis van de PDCA-principes.	**** voldoende

[1] De beoordeling van dit onderdeel is zwaar, omdat effectieve risicobeheersing de organisatie in staat stelt te kunnen sturen op risico's en dat is van essentieel belang.

• Accreditatie locaties

In zijn rol als *Security Accreditation Authorithy* (SAA) behandelt de BA meerdere locatie-accreditatieverzoeken van locaties en/of compartimenten (hierna: locaties) voor een beperkt aantal hoog gerubriceerde informatiesystemen.

Voor een beperkt aantal informatiesystemen geldt dat locaties met een werkplek moeten worden beoordeeld aan de hand van de van toepassing zijnde beveiligingsnormen. De goedkeuring, de locatie-accreditatie, is randvoorwaardelijk. Net als bij de accreditatie van kritieke informatiesystemen zijn de processen voor een locatie-accreditatie ingericht volgens de PDCA-cyclus. Het afgelopen jaar lag de focus van de BA als toezichthouder vooral op de CHECK-fase bij het accrediteren van locaties. Het blijkt echter belangrijk om verbeterplannen actief te monitoren en daarom zal de BA de komende periode ook aandacht besteden aan de ACT-fase bij het accrediteren van locaties. Zo streeft de BA naar een evenwichtige benadering van het gehele PDCA-proces.	*** onvoldoende

• Elektronische Veiligheidsonderzoeken

Elektronische Veiligheidsonderzoeken (EVO) moeten uitsluiten dat er ongeautoriseerd meegeluisterd kan worden met hoog gerubriceerde gesprekken in gerubriceerde ruimtes.

Defensieonderdelen wijzen gerubriceerde gespreksruimtes aan en een interne dienstverlener onderzoekt of deze aan de eisen voldoen. De onderzoekscapaciteit bleek in de voorgaande toezichtjaren onvoldoende om aan de vraag te kunnen voldoen. Na een eerste uitbreiding in 2022 is de onderzoekscapaciteit van de interne dienstverlener in 2023 verder uitgebreid tot een verdubbeling ten opzichte van 2021. Met de huidige onderzoekscapaciteit kan deze dienstverlener een groot deel van de EVO-aanvragen behandelen. Dit onderwerp omvat echter meer dan alleen het uitvoeren van onderzoeken, zoals het toewijzen en beheren van gerubriceerde gespreksruimtes door de defensieonderdelen. In het proces gericht op het toewijzen en beheren van gerubriceerde gespreksruimtes, de ACT-fase, zijn de defensieonderdelen nog onvoldoende *in control*.	*** onvoldoende

• Industriebeveiliging

Bedrijven die voor Defensie gerubriceerde en/of vitale opdrachten uitvoeren, moeten voldoen aan de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO).

De processen ten behoeve van industriebeveiliging zijn ingericht op basis van de PDCA-cyclus. De verantwoordelijkheden voor dit onderdeel zijn bij verschillende entiteiten belegd en de organisatie is voldoende *in control*. Ondanks dit oordeel hangt het succes vooral af van het vroegtijdig identificeren van de ABDO-plicht in bijvoorbeeld het behoeftestellingenproces.	**** voldoende

4 Bijlage

Afkortingen

ABDO	Algemene Beveiligingseisen voor defensieopdrachten
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BA	Beveiligingsautoriteit
BIV	Bureau Industrieveiligheid
BNIVD	Beveiligingsnormen Inlichtingen- & Veiligheidsdiensten
CDS	Commandant der Strijdkrachten
DBB	Defensie Beveiligingsbeleid
DSA	*Designated Security Authority*
EU	Europese Unie
EVO	Elektronische Veiligheidsonderzoeken
FG	Functionaris voor Gegevensbescherming
IGK	Inspecteur-Generaal der Krijgsmacht
IMG	Inspectie Militaire Gezondheidszorg
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	*National Security Authority*
NSA-MoD	*National Security Authority – Ministry of Defence*
PDCA	*Plan-Do-Check-Act*
PSO	*Program Security Officer*
SAA	*Security Accreditation Authority*
SAPF	*Special Access Program Facilities*
SG	Secretaris-Generaal
TBB	Te Beschermen Belangen
UVO	Unit Veiligheidsonderzoeken