Ministerie van Justitie en Veiligheid

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)
t.a.v. Dhr. P.J. Aalbersberg EMPM

Ministerie van Justitie en Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon

M

@minjenv.nl

Datum
16 juli 2024

Onze referentie

nota

Toezicht Integrale Beveiliging 2023

Van

Kopie aan

Oordeel Toezicht 2023
Jaarlijks koppel ik aan u mijn bevindingen ten aanzien van de stand van zaken van de integrale beveiliging van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) terug.

In de toezichtsronde over 2023 heb ik de door u opgeleverde voortgang getoetst. Mijn bevindingen zijn mede gebaseerd op de afstemming tijdens het proces, de accountgesprekken gedurende het jaar met uw , de aangeleverde informatie en de overige bij bekende informatie.

Hieronder licht ik mijn bevindingen, oordeel en aanbevelingen toe. Daarnaast breng ik graag wat generieke informatie over de toezichtcyclus onder de aandacht alsmede een aantal op het gebied van integrale beveiliging.

Bevindingen
Ik informeer u graag in meer diepgang over een selectie van een aantal door mij vastgestelde onderwerpen waar in het kader van toezicht extra aandacht aan wordt geschonken en informatie over wordt opgevraagd bij uw onderdeel, voor zover van toepassing. In het bijzonder vielen mij bij uw organisatie de onderstaande zaken op.

Algemeen / organisatie
Gedurende 2023 heeft uw organisatie stappen gezet ten aanzien van de nadere inrichting van het interne stelsel ten behoeve van integrale beveiliging, inclusief informatiebeveiliging. De nadruk hierbij lag op het nader vormgeven van het beleid. De nieuw aangestelde zal zich, in nauwe samenwerking met uw richten op de operationalisering van het (ver)nieuw(d)e beleid. Deze personele uitbreiding

zal daarnaast leiden tot meer capaciteit ten behoeve van het uitvoeren van de reguliere integrale beveiligingswerkzaamheden.

Security Risk Assessment
De 3 jaarlijks benodigde update van uw Security Risk Assessment (SRA) is, mede door voornoemde capaciteitsuitdagingen nog niet gestart in 2023. De eerste bouwstenen voor deze update, de zogenoemde Te Beschermen Belangen (TBB), zijn echter al wel in kaart gebracht. Uw heeft aangegeven dat hij graag ondersteuning zal willen ontvangen vanuit de bij deze komende SRA exercitie (geplande aanvang medio 2024). Dit om zodoende een bij de specifieke behoefte van de organisatie passende kwalitatief afdoende analyse op te stellen waarbinnen de nieuwe ontwikkelingen en inzichten worden meegenomen. Op basis van de eerder uitgevoerde SRA zijn de maatregelen op het fysieke beveiligingsvlak geïmplementeerd en operationeel effectief. Deze operationaliseringslag had de nodige voeten in de aarde gezien de specifieke wensen en eisen vanuit NCTV en de meer standaard dienstverlening door concerndienstverlener FM Haaglanden.

Incidentmanagement
Zoals u bekend heeft er, in 2023, zich een insider threat incident voorgedaan binnen uw organisatie. Deze vorm van dreiging was reeds onderkend en daartoe waren compenserende maatregelen getroffen. Direct na het optreden van het incident zijn er aanpassingen in de wijze van werken doorgevoerd en gecommuniceerd in de organisatie. Daar waar mogelijk zijn aanpassingen in systemen en processen onderkend welke doorgevoerd worden. Een complicerende factor hierbinnen is de verplichte administratieve vastlegging van alle handelingen in relatie tot de staatsgeheim gerubriceerde informatie, daar deze informatie zich bevindt in digitale systemen. Ten aanzien van mogelijke inspecties vanuit partners / bondgenoten, zoals EU en NAVO is dit een, bij het MT bekend, afbreukrisico waarvoor nog een oplossing, mede ook op nationaal niveau, gezocht dient te worden.
Op dit moment wordt er nader onderzoek verricht naar dit bewuste incident. Indien daaruit nog andere bevindingen voortvloeien zullen deze ook in ogenschouw worden genomen.

Bijzondere informatie / rubricering
Naar aanleiding van een aantal incidenten met gerubriceerde informatie, bij diverse JenV organisaties, is in opdracht van een pilot rubriceren gestart bij DGRR. Het doel van deze pilot is het identificeren van maatregelen om de risico's op incidenten te verkleinen en de omgang met gerubriceerde informatie te verbeteren. Recent zijn de eerste resultaten hiervan besproken in de kBR, waarbij is besloten al tijdens de looptijd van de pilot de eerste maatregelen bestuursdepartement-breed uit te rollen, waaronder bij uw Uiteraard zal er bij de daadwerkelijke implementatie rekening worden gehouden met de specifieke aspecten, waaronder eigen rubriceringskader, van uw organisatie.

Vertrouwensfuncties
In 2023 en in de voorgaande jaren zijn er geen nieuwe vertrouwensfuncties aangewezen bij uw organisatie en hebben er geen wijzigingen op de bestaande lijst uit 2019 plaatsgevonden. Vanuit het oogpunt van de nationale veiligheid is het

essentieel dat uw lijst vertrouwensfuncties actueel en volledig blijft en daarom tenminste 1 keer per jaar herzien wordt. Het gaat daarbij om de vraag of alle functies (nog terecht) aangewezen zijn, of het niveau past bij de werkzaamheden en of het aantal fte vertrouwensfunctionarissen klopt.

Awareness
In het bijzonder is opgevallen dat uw organisatie op verschillende wijzen door het jaar heen de medewerkers bewust maakt van beveiliging, risico's en handelingsperspectieven aanbiedt waarbij gebruik gemaakt wordt van het intranet, de JenV brede Week van de integrale beveiliging, alsook het Rijksbrede AlertOnline programma. U zou deze activiteiten nog kunnen uitbreiden door aan te sluiten bij de e-learning modules welke vanuit Weerbaar JenV worden aangeboden. Het MT is zich hiervan bewust en streeft er naar om voor eind 2024 het gereed te hebben voor alle medewerkers.

Oordeel en aanbevelingen
Voor uw organisatieonderdeel is mijn oordeel dat de voortgang op basis van de aangeleverde informatie voldoende is.

Ik geef vooruitblikkend naar 2024 graag de volgende aanbevelingen mee:
- geef voldoende prioriteit aan de actualisatie van uw Security Risk Assessment;
- implementeer een aan de eisen voldoend sluitende administratie en registratie van toegang tot staatsgeheim gerubriceerde informatie;
- blijf inzetten op bewustwording bij uw medewerkers, in het bijzonder omtrent het omgaan met bijzondere informatie;
- evalueer jaarlijks of de bestaande lijst vertrouwensfuncties nog volledig en actueel is.

Achtergrond:
Het toezicht is ingericht met de driejaarlijkse toezichtcyclus uit het Toezichtkader 2018-2021 JenV (Brede Bestuursraad 2 februari 2018). Het toezicht richt zich op het uitvoeren van de analyse, de veranderingen, verbeterpunten en verbeterplannen en de werking in de praktijk. Deze cyclus is door een groot deel van de organisatieonderdelen inmiddels één keer volledig doorlopen. Voor een aantal onderdelen geldt dat zij de cyclus inmiddels in hun eigen ritme doorlopen.

Het Toezichtkader is eind 2023 geëvalueerd en bijgesteld. Belangrijke verandering in dit kader zit in het uitgangspunt van controle naar samenwerking. Gelet op de groei in volwassenheid op het gebied van risicomanagement en integrale beveiliging in de afgelopen jaren door de implementatie van het drie-fasen toezichtmodel, wordt het accent van het toezichtkader verlegd naar samenwerking. Samenwerken, vanzelfsprekend vanuit ieders rolverantwoordelijkheid, om te komen tot optimale integrale beveiliging. Dit kader wordt in T2 aangeboden aan de kBR, de BBR en het SBB.

Via de jaarplanaanschrijving heb ik u verzocht de door uw MT vastgestelde voortgang van de van toepassing zijnde fase uit de cyclus eind 2023 of in januari 2024 aan te bieden.

Een belangrijk onderdeel om de integrale beveiliging te waarborgen is de bevordering van het beveiligingsbewustzijn. Mijn bureau heeft het initiatief genomen om de week van de Integrale Beveiliging te organiseren. Daarbij is samenwerking met de andere disciplines op het gebied van integrale beveiliging, departementaal en interdepartementaal, in juni 2023 een week lang aandacht besteed aan diverse onderwerpen. Die aandacht is belangrijk omdat de collega's de belangrijkste schakel vormen in het veilig omgaan met informatie, het beschermen van de privacy van burgers en er voor te zorgen dat informatie niet in verkeerde handen komt. Daarnaast gaat het ook om het borgen van je eigen persoonlijke veiligheid. Eind 2024 zal wederom een week van de Integrale Beveiliging worden georganiseerd waar medewerkers van JenV welkom zijn om deel te nemen aan diverse presentaties en workshops. Binnen diverse onderdelen worden daarnaast initiatieven ontplooid om hier aandacht aan te besteden en ook mijn bureau geeft op regelmatige basis voorlichting aan afdelingen, nieuw aangetreden collega's en op verzoek bij de onderdelen.

Mijn bureau biedt ook in 2024 weer ondersteuning aan bij het uitvoeren van de benodigde stappen in de Toezichtcyclus, staat uw onderdeel bij met advies en raad en is bij spoed 24/7 bereikbaar.

In T2 van 2024 zal ik met alle onderdelen toezichtsgesprekken voeren. Hierbij kijken we in gezamenlijkheid terug, besteden we aandacht aan de integrale beveiliging. Aan de hand van de gesprekken zal ik voor heel JenV een rode draden rapportage opstellen voor die ik ter informatie eveneens zal aanbieden aan de Brede Bestuursraad en het Strategisch Bestuurlijk Beraad.

Wanneer u naar aanleiding van deze nota nog vragen heeft of u een gesprek wilt over andere beveiliging gerelateerde zaken, kunt u uiteraard altijd contact met mij opnemen. Het is vanzelfsprekend mogelijk om dit te agenderen in het toezichtgesprek.

Schouw STG-domein NCTV

Ministerie van Justitie en Veiligheid

Versie 1.00

Datum	07 november 2021
Status	Definitief

.

Maatregelen

Op basis van het rubriceringskader worden de maatregelen die de fysieke locatie omvatten weergegeven voor STG. De Schouw concentreert zich op basis van het hoogste risico op het STG-domein. De maatregelen moeten voorkomen dat de primaire processen van de NCTV stagneren en de staat of zijn bondgenoten onaanvaardbare schade lijden. De maatregelen zijn bedoeld als normen voor de beveiliging van bijzondere informatie. Zoals in de inleiding geschreven is het van belang dat een risicoanalyse het fundament is voor het wel of niet implementeren van maatregelen. Het enkele feit dat een maatregel niet is getroffen, betekent niet dat de beveiliging onvoldoende is. De reden van het niet treffen of alternatief afdekken is relevant voor de weging en het oordeel.

De Schouw wordt uitgevoerd met een interview en het fysiek inspecteren van het STG-domein bij de NCTV. Tijdens de Schouw wordt niet de SRA of enige andere risicoanalyse en/of maatregelplan beoordeeld. Het doel is om vast te stellen of de beveiliging aan het Rubriceringskader voldoet.

De maatregelen zijn in tien clusters c.q. hoofdstukken verdeeld. De nadruk bij de Schouw ligt op hoofdstuk 1 tot en met 5, 9 en 10. Hoofdstukken 6, 7 en 8 zijn reeds (grotendeels) betrokken bij de accreditatie van het systeem. Hoofdstuk 8 wordt deels meegenomen.

1. (A) Management van bedrijfsmiddelen en -informatie
2. (B) Personele beveiligingsmaatregelen
3. (C) Fysieke beveiligingsmaatregelen
4. (D) Bouwkundige beveiligingsmaatregelen
5. (E) Elektronische beveiligingsmaatregelen
6. (F) Logische toegangsbeveiliging (verwijderd)
7. (G) ICT-voorzieningen (verwijderd)
8. (H) Informatiebeveiligingsmaatregelen (deels)
9. (I) Verzending gerubriceerde informatie
10. (J) Fysieke opslag, verwerking, vernietiging en ontwikkeling

Nr.	Maatregel	Stg. C	Stg. G	Stg. ZG	
A.	Management van bedrijfsmiddelen en -informatie	Stg. C	Stg. G	Stg. ZG	
1.					
2.					
3.	Alle middelen om gerubriceerde informatie mee te verwerken en de personen aan wie deze zijn uitgereikt staan **geregistreerd**.				
4.	De locatie/standplaats van alle middelen en de toewijzing aan een eigenaar zijn **geregistreerd**.				
5.	Het **beveiligingsbewustzijn** wordt bevorderd. Hierbij is deelname aan de programma's verplicht en meetbaar is voor ten minste vertrouwensfunctionarissen.				
6.	**Informatiedragers** worden dusdanig gebruikt dat gerubriceerde informatie niet beschikbaar kan komen voor onbevoegde personen.				
7.	**Thuiswerken** met staatsgeheimen is alleen toegestaan op apparatuur die na goedkeuring door de ter beschikking gesteld is. Het is verboden privéapparatuur voor verwerking van staatsgeheime informatie te gebruiken.				
8.	Medewerkers zijn **geïnstrueerd** om zodanig om te gaan met (telefoon)gesprekken, email, faxen en ingesproken berichten op antwoordapparaten dat de kans op uitlekken van gerubriceerde informatie wordt geminimaliseerd.				
9.	Medewerkers zijn **geïnstrueerd** om zodanig om te gaan met mobiele apparatuur en verwijderbare media dat de kans op uitlekken van gerubriceerde informatie wordt geminimaliseerd.				
10.	Zonder expliciete toestemming mogen binnen beveiligde ruimten geen **opnames** (foto, video of geluid) worden gemaakt.				
11.	Alleen apparatuur die door de zijn goedgekeurd mogen een ruimte waar staatsgeheime informatie worden verwerkt/besproken betreden.				
12.					
13.					
14.					
15.	Bij melding van **verlies of diefstal** wordt de communicatiemogelijkheid met de centrale applicaties afgesloten.				
16.					
17.	Via **telewerkvoorzieningen** mogen geen staatsgeheimen verwerkt worden en de voorzieningen zijn zodanig ingericht dat er geen toegang tot **staatsgeheimen** mogelijk is.				

B.	Personele beveiligingsmaatregelen	Stg. C	Stg. G	Stg. ZG	
1.	Personen die hebben te maken met bijzondere informatie dienen een **geheimhoudingsverklaring**, conform artikel 125a, derde lid, van de Ambtenarenwet, te tekenen. Hierbij wordt vastgelegd dat na de beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.				
2.	Het is niet toegestaan om met onbevoegden over gerubriceerde informatie te spreken. **Ontheffing van de geheimhoudingsplicht** kan alleen door de verantwoordelijk Minister, rubriceringsamtenaar of vaststeller van de informatie worden verleend.				
3.					
4.	Personen die frequent te maken hebben met bijzondere informatie dienen tevens te beschikken over een passende **verklaring**.	> VGB-C	> VGB-B	VGB-A	
5.	Beheerders, in het bijzonder beheerders van de digitale omgeving, zijn minimaal in het bezit van een **VGB** op B-niveau niet ouder dan 5 jaar.				
6.	Beheerders, in het bijzonder beheerders van de digitale omgeving, zijn in het bezit van een **VGB** op minimaal C-niveau niet ouder dan 5 jaar.				
7.					
8.	Een medewerker mag niet eerder met een **vertrouwensfunctie** worden belast dan nadat namens de betreffende Minister door de AIVD een VGB is afgegeven. Een medewerker kan niet na weigering, intrekken of intentie tot intrekken van de VGB op zijn positie op de vertrouwensfunctie worden gehandhaafd.				
9.	Bij **beëindiging van een functie** waarbij iemand in aanraking komt met bijzondere informatie wordt zeker gesteld dat de betreffende persoon geen toegang meer heeft tot die informatie, noch deze in zijn/haar bezit heeft.				

C.	Fysieke beveiligingsmaatregelen	Stg. C	Stg. G	Stg. ZG	
1.	De fysieke beveiligingsmaatregelen zijn volgens een **schillenstructuur** opgebouwd met toepassing van het "need-to-be"-principe.				
2.	Het compartiment met een Te Beschermen Belang (TBB) bevindt zich in een zone die met **toegangscontrole** is afgeschermd van de openbare ruimte of van ruimten die niet onder controle staan.				
3.	Er vindt **toegangscontrole** plaats bij elke beveiligingsschil.				
4.	Bijzondere informatie wordt zodanig behandeld en opgeslagen dat er een positief beveiligingsrendement[1] is, op basis van schadeacceptatie en het dreigingsprofiel.				
5.	Fysieke toegang tot het **compartiment** met een TBB is tot op individueel niveau controleerbaar.				
6.	Indien er sprake is van een **verhoogde dreiging** zullen op basis van een gerichte dreigingsappreciatie aanvullende beveiligingsmaatregelen worden getroffen.				
7.	De uitgifte van **sleutels** voor toegang tot compartimenten en opbergmiddelen met een TBB is geregistreerd. Bij de uitgifte van sleutels is gecontroleerd of men over een Autorisatie beschikt. De registratie hiervan wordt minimaal een jaar bewaard. Sleutels zijn voor zo min mogelijk personen toegankelijk.				
8.	Toegang tot het TBB of **compartiment** is alleen door middel van Two-factor Authenticatie verleend.				
9.	Alleen een geautoriseerd persoon kan zelfstandig **toegang** krijgen tot een TBB of tot een compartiment waarin zich een TBB bevindt.				
10.	De medewerker verantwoordelijk voor de verwerking van bijzondere informatie, dient zorg te dragen dat **bezoekers** geen kennis kunnen nemen van de bijzondere informatie die hij onder zijn beheer heeft.				
11.	**Bezoekers** worden begeleid wanneer zij ruimten, waarin bijzondere informatie aanwezig is, betreden.				
12.	Personen zonder autorisatie (zoals bezoekers) zijn binnen het compartiment herkenbaar door middel van een zichtbaar gedragen pas. Op de pas staat voor eenieder goed zichtbaar "**bezoeker**" vermeld.				
13.	**Bezoekers** (en de 'bezoek-verantwoordelijke') worden geregistreerd indien zij toegang (kunnen) hebben tot bijzondere informatie in ruimten die zij betreden, als de toegang tot die informatie niet op andere wijze kan worden voorkomen (bv kast/kluis/etc.). Aanwezigen zonder zichtbare pas worden behandeld als bezoekers (i.r.t. medewerkers die hun medewerkerspas niet zichtbaar dragen).				
14.	Het "**clear desk principe**" en "clear screen principe" is toegepast in alle compartimenten waar zich een TBB bevindt of kan bevinden. Een TBB wordt niet onbeveiligd achter gelaten.				

15.	Bij het verlaten van een compartiment met een TBB is een **sluitronde** gemaakt, waarbij de deur van het opbergmiddel, het compartiment en zo mogelijk het gebouw is afgesloten.				
16.	Er zijn voorzieningen getroffen om **elektronische apparatuur** die niet strikt noodzakelijk zijn voor het uitvoeren van werkzaamheden buiten de compartimenten te houden.				
17.	In het beveiligingsplan is een **sluit- en sleutelplan** opgenomen. Ramen, deuren en opbergmiddelen zijn afgesloten bij afwezigheid van geautoriseerd personeel. Sleutels worden op hetzelfde niveau beveiligd als het TBB waar de sleutel toegang toe geeft.				
18.	De sterkte van het opbergmiddel is gerelateerd aan de rubricering en de **interventietijd**[1].				
19.	**Opbergmiddelen** tot 1000 kilogram zijn chemisch verankerd.				
20.	**Opbergmiddelen** zijn voorzien van een sleutelslot en een cijfercombinatieslot.				
21.	Bij het verlaten van de werkplek wordt bijzonder informatie in een daartoe geëigend bergmiddel **opgeborgen**.				
22.	Locaties waar zich een opeenstapeling van staatsgeheimen bevinden en waar sprake is van enige concrete dreiging, worden na instemming van bij KB aangewezen als **verboden plaats**. De aanwijzing wordt met redenen omkleed en gaat vergezeld met kadastrale omschrijving van het perceel. Bij de ingangen zijn borden geplaatst waarop vermeld wordt dat de locatie een verboden plaats is, alsmede dat de toegang voor onbevoegden en opnameapparatuur verboden is.				

[1] Deze interventietijd kan op verschillende manieren worden gerealiseerd, b.v. door een elektronisch detectiesysteem met adequate opvolging, door het lopen van controlerondes, enzovoort. De interventietijd mag nooit meer dan vier uur bedragen (bij stg. ZG niet meer dan twee uur).

Rubricering Interventietijd	Stg. ZG	Stg. G	Stg. Confi
0-15 min	SAFE 3	SAFE 2	SAFE 2
15-30 min	CEN 1	SAFE 3	SAFE 2
30-120 min	CEN 2	CEN 1	SAFE 3
120-240 min	Niet toegestaan	CEN 2	CEN 1

D.	Bouwkundige beveiligingsmaatregelen	Stg. C	Stg. G	Stg. ZG	
1.	Gebouwen bieden voldoende weerstand (bepaald op basis van risicoafweging) bij gewelddadige aanvallen zoals inbraak, ICT gericht vandalisme, ontvreemding van gegevens en manipulatie.				
2.	Daar waar bestaande bouwkundige normeringen niet bekend zijn, moet de uitsteltijd worden vastgesteld aan de hand van beproevingen c.q. analyses om het weerstandsvermogen (in tijd) tegen door potentiele daders gebruikte aanvalsmethoden en -middelen te toetsen.				
3.	Ramen en gevelopeningen die open kunnen, zijn voorzien van **braakwerend glas**, hang- en sluitwerk, sponningen enzovoorts.				
4.	Toepassing van gecertificeerde sleutels.				
5.	De ramen en glazen wanden in een compartiment met een TBB zijn voorzien van **inkijk beperkende maatregelen.**				
6.	Het compartiment met een TBB bevindt zich in een zone die met **toegangscontrole** is afgeschermd van de openbare ruimte of van ruimten die niet onder controle staan.				
7.	Tegengaan van **afluisteren**, zicht op en reflectie van informatie (bv via beeldschermen of spiegelende oppervlakten).				
8.	**Compartimenten** met een TBB zijn afsluitbaar.				

E.	Elektronische beveiligingsmaatregelen	Stg. C	Stg. G	Stg. ZG	
1.	Het compartiment waarin een opbergmiddel met een TBB is geplaatst, is voorzien van een 'indringen detectie signaleringssysteem' (**IDSS**).				
2.	De **aanliggende compartimenten** van het compartiment met een TBB zijn voorzien van IDSS of een opbergmiddel met een TBB is zelf voorzien van IDSS.				
3.	Het **activeren** en **deactiveren** van een IDSS kan alleen door middel van een Two-factor Authenticatie.				
4.	Een alarm van een IDSS leidt tot een effectieve **alarmopvolging** binnen de in gestelde interventie tijd.				
5.	Bewegingsmelders beschikken bij voorkeur over **anti-masking** maatregelen.				
6.	In een ruimte met een TBB zijn zonder goedkeuring van geen camera's, smartphones, microfoons of andere **opnameapparatuur** aanwezig.				
7.	De **bewaartermijnen** voor camerabeelden worden gehanteerd conform Rijksbeleid cameratoezicht.				
8.	Een ETS (Elektronische Toegangssysteem) is uitgerust met een **Anti Pass Back** (APB) systeem.				
9.	Een ETS is voorzien van **Logging**, waarbij de logs minimaal een jaar worden bewaard.				
10.	Meldingen uit het IDSS en het ETS moeten leiden tot **tijdige Interventie**.				
11.	**Tempestmaatregelen** conform Beleidsadvies Compromitterende straling (VBV 32000).				

H.	Informatiebeveiliging	Stg. C	Stg. G	Stg. ZG	
1.	houdt toezicht op de registratie van locatie, uitgifte, inname en herkomst van alle door de organisatie in ontvangst of in beheer genomen digitale TBB.				
2.	Een TBB dat is opgeslagen op **mobiele apparatuur** is alleen toegestaan met toepassing van door het Rijk goedgekeurde procedures en middelen zoals: vercijfering, alleen hoogstnoodzakelijke hoeveelheid informatie in opslag en mag niet gebruikt worden in publieke ruimten.				
3.	**Telewerken** is niet toegestaan.				
4.	Na beëindiging van de opdracht worden de gegevensdragers fysiek **vernietigd**. Een proces-verbaal van vernietiging is opgesteld.				
5.					
6.	Gegevens op **verwijderbare media** moet vercijferd worden opgeslagen om hun vertrouwelijkheid te waarborgen.				
7.					
8.	**Systemen** waarop zich een grote concentratie van TBB van STG-C bevindt, zijn geplaatst in een ruimte die op **TBB 2 niveau** is beveiligd.				
9.	**Systemen** waarop zich een grote concentratie van TBB van STG-G bevindt, zijn geplaatst in een ruimte die op **TBB 1 niveau** is beveiligd.				
10.	Hergebruik van ICT-middelen is toegestaan mits het dezelfde TBB betreft en is gewist door gebruik te maken van de door het Rijk goedgekeurde middelen. Een procesverbaal van vernietiging (wissen) is opgesteld.				
11.					
12.	Het gebruik van **draadloze communicatie** is niet toegestaan zonder daarvoor goedkeurde voorzieningen.				
13.					
14.					
15.					
16.					
17.					
18.					

I.	Verzending gerubriceerde informatie	Stg. C	Stg. G	Stg. ZG	
1.	**Digitale verzending** van bijzondere informatie dient met ministerieel goedgekeurde **crypto grafische middelen** te geschieden.				
2.	**Fysieke verzending** van bijzondere informatie dient te geschieden met ministerieel goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.				
3.	**Fysieke verzending** geschiedt door: – Een geautoriseerde medewerker, waarbij de informatie te allen tijde onder beheer van de drager blijft en niet wordt geopend tijdens transport. – Fysieke verzending geschiedt met een ministerieel goedgekeurde koerier. – Een militaire, overheids- of diplomatieke koerier.				
4.	Nationale verzending uitsluitend via een **overheidskoerier**.				
5.	Internationale verzending uitsluitend als **diplomatieke koerier** zending of militair transport.				
6.	Zowel digitaal als niet digitaal is er een onweerlegbare **bevestiging van ontvangst**.				
7.	Verzending vindt plaats in dubbele enveloppe of door goedgekeurde sealbag. De enveloppe of sealbag wordt zodanig gesloten dat openen zonder verbreken van de sluiting of beschadigingen niet mogelijk is.				
8.	Indien gebruik wordt gemaakt van dubbele enveloppen draagt de binnen enveloppe de rubricering welke ook het document als geheel draagt. De buitenenveloppe draagt geen rubricering.				
9.	Voor verzending worden zodanige enveloppen gebruikt dat met behulp van een technisch middel kennis nemen van de inhoud zonder openen van de enveloppen niet mogelijk is.				
10.	Het maken, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling en vernietigen van bijzondere informatie wordt **vastgelegd**.				
11.	Van alle exemplaren van bijzondere documenten worden de volgende gegevens **vastgelegd**: – Exemplaarnummer; – Maker; – Ontvanger.				
12.	Medewerkers maken zonder uitdrukkelijke voorafgaande toestemming van Opdrachtgever op geen enkele wijze **publiekelijk bekend** aan welke bijzondere opdracht en met welke bijzondere informatie wordt gewerkt voor de Nederlandse overheid.				

J.	Fysieke opslag, verwerking, vernietiging en ontwikkeling	Stg. C	Stg. G	Stg. ZG	
1.	**Geregistreerd** is wie werkzaamheden aan bijzondere informatie heeft uitgevoerd of bijzondere informatie heeft ingezien.				
2.	De bijzonder informatie is geregistreerd en van een **kenmerk** (labeling) voorzien.				
3.	De **reproductie** van Informatie geschiedt alleen met toestemming van degene die de rubricering heeft vastgesteld. Gemaakte reproducties zijn geregistreerd.				
4.	Het maken van **reproducties** is voorbehouden aan daartoe aangewezen geautoriseerd personeel dat ook zorgdraagt voor de registratie hiervan.				
5.	**Reproducties** kennen dezelfde rubricering als het origineel, ook als slechts delen van het origineel is gebruikt.				
6.	Er worden niet meer **reproducties** van bijzondere informatie gemaakt dan strikt noodzakelijk.				
7.	In geval van **vernietiging** wordt door een aangewezen medewerker met de juiste Autorisatie een proces-verbaal van vernietiging opgemaakt.				
8.	Uitgangspunt van de gekozen **vernietigingsmethode** van gerubriceerde informatie moet zijn dat het onmogelijk moet zijn om uit de resten enig staatsgeheim of anderszins gerubriceerde, bruikbare informatie te halen.				
9.	Een document dat gerubriceerde informatie bevat wordt **vernietigd** door middel van een door de voor de desbetreffende rubricering goedgekeurde wijze. Het residu is ongerubriceerd als het volgens deze normen wordt versnipperd. STG-ZG: L<20mm/B<1,5 mm, STG-G: L<25mm/B<3mm, STG-C/Dep-V: L<50mm/B<5mm.				
10.	Door NBV/NDA uitgeleverde cryptosleutels moeten bij de cryptobeheerder worden ingeleverd. Cryptosleutels dienen vervolgens onder toezicht te worden **verbrand**.				

Bijlage 1: De gouden regels

samengevat

Waar wordt de rubricering op het document aangebracht?

- Rechtsboven en –onder op ieder blad, vet, onderstreept en in kapitalen op elke pagina.

Wie rubriceert en stelt vast?

- De opsteller van de informatie doet een voorstel tot rubricering en rubricerings duur en brengt deze aan op de informatie (zie H2 voor meer informatie).
- De vaststeller[2] van de inhoud van de informatie stelt tevens de rubricering en rubriceringsduur vast.

Wat zijn de eisen aan medewerkers.

- Een medewerker die frequent (Dep. V: 10x per jaar, Stg. C: 6x per jaar, Stg. G/ZG: 3x per jaar) gaat werken met gerubriceerde informatie, dient, naast een eed, gelofte of

[2] De vaststeller van informatie is naast de minister, STAS, SG of aangewezen rubriceringsamtenaar, de gemandateerde lijnmanager die voor zijn directie/onderdeel, namens JenV, minister, STAS of SG mag tekenen.

geheimhoudingsverklaring een betrouwbaarheidsonderzoek te ondergaan: VOG voor Dep. V en een VGB voor Stg. C, G, en ZG.

- Medewerkers die met gerubriceerde informatie hoger dan dep-V werken, dienen een geheimhoudingsverklaring te tekenen of een eed/belofte af te leggen.
- Daarnaast moeten zijn een relevante (awareness)training volgen. Ditzelfde geldt voor medewerkers die zichzelf toegang kunnen verschaffen tot gerubriceerde informatie (lees: systeembeheerders).

Staatsgeheim CONFIDENTIEEL

- Aanmaken van een Stg. C-document is uitsluitend toegestaan op een PC of laptop die goedgekeurd is voor dat STG-C doel (stand alone apparaat/geëvalueerd netwerk).
- Het maken, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken d.m.v. doorzending, verspreiding of enige andere vorm van terbeschikkingstelling en vernietigen van bijzondere informatie moet worden vastgelegd zodat te allen tijde te achterhalen is, wie kennis heeft genomen.
- Verzenden via e-mail (over Justitienet of over het Internet) is uitsluitend toegestaan door gebruik te maken van versleutelingssoftware wanneer men beschikt over een Stg. Confi-certificaat.
- Niet meer reproducties maken dan strikt noodzakelijk.
- Bewaren uitsluitend in een kluis. Generieke kluis i.c.m. sealbag.
- Verzenden geschiedt door: a. een geautoriseerde en gescreende medewerker, waarbij de informatie te allen tijde onder beheer van de drager blijft en niet wordt geopend tijdens het transport; b. een door de beveiligingsautoriteit goedgekeurde koerier (zie voor meer info: hoofdstuk 3, paragraaf I).
- Bij verspreiding voorzien van: Rubriceringsniveau, -duur, bladzijdenummering en totaalaantal bladzijden waaruit het document bestaat.
- Verplicht vastleggen: exemplaarnummer, maker, vaststeller, afzender en ontvanger.

Staatsgeheim GEHEIM

- Aanmaken van een Stg. G-document is uitsluitend toegestaan op een PC of laptop die geen verbinding heeft met andere niet- of lager beveiligde systemen. Betreffende PC of laptop behandelen als Stg. G.
- Het maken, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken d.m.v. doorzending, verspreiding of enige andere vorm van terbeschikkingstelling en vernietigen van bijzondere informatie moet worden vastgelegd zodat te allen tijde te achterhalen is, wie kennis (na goedkeuring eigenaar) heeft genomen.
- Verzenden via e-mail is niet toegestaan.
- Niet meer reproducties dan strik noodzakelijk. Het bijmaken van reproducties wordt geregistreerd en is voorbehouden aan daartoe aangewezen personen.
- Bewaren uitsluitend in een (generieke) kluis.
- Fysieke verzending geschiedt door: a. een geautoriseerde en gescreende medewerker, waarbij de informatie te allen tijde onder beheer van de drager blijft en niet wordt geopend tijdens het transport; b. een door de beveiligingsautoriteit goedgekeurde koerier.
- Bij verspreiding voorzien van: rubriceringsniveau, -duur, bladzijdenummering en totaalaantal bladzijden waaruit het document bestaat.
- Verspreiding naar anderen alleen na overeenkomst met de bron.
- Verplicht vastleggen: exemplaarnummer, maker en ontvanger.

Staatsgeheim ZEER GEHEIM

- Aanmaken en bewaren in DigiJust (of ander DMS) en op het netwerk is niet toegestaan.
- Aanmaken van een Stg. ZG-document is uitsluitend toegestaan op een pc, laptop die geen verbinding heeft met andere niet of lager beveiligde systemen. Betreffende PC of laptop behandelen als Stg. ZG. Maatwerkoplossing en-proces per documenttype is aan te bevelen.
- Het maken, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken d.m.v. doorzending, verspreiding of enige andere vorm van terbeschikkingstelling en vernietigen van bijzondere informatie moet worden vastgelegd zodat te allen tijde te achterhalen is, wie kennis (na goedkeuring eigenaar) heeft genomen.
- Verzenden via e-mail is niet toegestaan.
- Niet meer reproducties dan strikt noodzakelijk. Het bijmaken van reproducties wordt geregistreerd en is voorbehouden aan daartoe aangewezen personen.
- Bewaren uitsluitend in een kluis, wanneer mogelijk i.c.m. sealbag.
- Een Stg. ZG-document mag uitsluitend persoonlijk in handen van de geadresseerde worden gesteld.
- Bij verspreiding voorzien van: Rubriceringsniveau, -duur, bladzijdenummering en totaal aantal bladzijden waaruit het document bestaat.
- Verplicht vastleggen: exemplaarnummer, maker en ontvanger.

Overige

- De beveiligingsautoriteit (in samenwerking met de [redacted] en [redacted]) houden namens [redacted] toezicht op de bijzondere informatie en adviseert het lijnmanagement dienaangaande.
- Voorafgaand aan verwerking toestemming nodig van [redacted] na verantwoording over de getroffen passende beveiliging obv risicomanagement, ook tov het dreigingsbeeld en de specifieke beveiligingseisen die door [redacted] is aangereikt.
- Elke ambtenaar is verplicht de beveiligingsautoriteit onmiddellijk te informeren van inbreuken op de beveiliging die redelijkerwijs kan leiden, dan wel vermoedelijk of vaststaand heeft geleid, tot compromitterend van bijzondere informatie.

Ministerie van Justitie en Veiligheid

Cluster secretaris-generaal
Directie
Bestuursondersteuning
Afdeling Advies en
Stukkenstroom

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon

M
@minjenv.nl

Datum
18 november 2024

Onze referentie

nota

Appreciatie nota NCTV

1. Gevraagde beslissing

U wordt verzocht kennis te nemen van deze nota.

2. Kern

- De NCTV heeft belangrijke stappen heeft gezet in het verbeteren van de informatiebeveiliging, onder andere op basis van het ADR rapport.
- Op 26 september jl. is door de NCTV een nota met de stand van zaken t.a.v. de informatiebeveiliging aan u voorgelegd (zie ook onder 3.1 Achtergrond).
- Op 13 november jl. heeft de een definitieve reactie op deze nota uitgebracht.
- Voorliggende nota bevat de appreciatie van de op de nota van de NCTV d.d. 26 september jl. De nota van de van 13 november jl. ligt aan deze nota ten grondslag.
- Dat oordeel is dat momenteel voldoende aanvullende en mitigerende maatregelen zijn genomen om te verzekeren dat de huidige werkwijze ten aanzien van (informatie)beveiliging valt binnen de daartoe afgesproken kaders. Voor die zaken die in de komende periode nog nadere uitwerking behoeven zijn momenteel geen aanvullende maatregelen nodig.

3. Appreciatie

Er zijn drie elementen te onderscheiden t.a.v. de stand van zaken informatiebeveiliging NCTV, te weten de digitale verwerking en opslag van staatsgeheim gerubriceerde informatie bij de NCTV (zie onder 3.1.), de overige verwerking van staatsgeheim gerubriceerde informatie uitwisseling binnen de NCTV (zie onder 3.2.) en de stand van zaken van de vertrouwensfuncties en veiligheidsonderzoeken (zie onder 3.3.) aangaande medewerkers van de NCTV. Deze komen hieronder, inclusief appreciatie (zie onder 3.4.), afzonderlijk aan bod.

<u>3.1. Digitale verwerking STG informatie</u>

- De NCTV stelt te voldoen aan alle gestelde eisen om met staatsgeheime (STG) informatie te werken binnen de organisatie en op het standalone .
- De onderschrijft dat op basis van de reeds genomen maatregelen een zogenaamde *Interim Approval to Operate* (IATO) is verleend voor de periode van een jaar. Deze IATO ziet op het digitale waarmee informatie wordt verwerkt. In deze periode dient de NCTV een aantal

Cluster secretaris-generaal
Directie
Bestuursondersteuning
Afdeling Advies en
Stukkenstroom

Datum
18 november 2024

Onze referentie

verbetermaatregelen te nemen, waarna een *Final Approval to Operate* (FATO) kan worden aangevraagd. U bent op 14 november jl. per nota geïnformeerd over deze stand van zaken (reactie op nota stand van zaken NCTV).
- De constateert dat er voldoende vertrouwen is dat deze verbetermaatregelen door de NCTV in samenspraak met de worden opgepakt. In de komende periode zal er regulier overleg plaatsvinden tussen de en NCTV om de voortgang te monitoren. De verslaglegging daarvan zal aan de worden doorgeleid.

3.2. Fysieke context
- De NCTV verwerkt behalve op het ook op andere manieren staatsgeheime informatie, waaronder op papier en mondeling. Daarnaast kan het niet los gezien worden van de fysieke context waarin het zich bevindt en de personen die ermee werken.
- Om te toetsen of de NCTV ook op deze facetten voldoet aan de vereisten voor het werken met staatsgeheime informatie heeft de , in samenspraak met de NCTV, een schouw uitgevoerd.
- Op basis van de bevindingen n.a.v. de schouw concludeert de dat de NCTV momenteel voldoet aan de vereisten voor het werken met staatgeheime informatie. Een aantal verbeterpunten zijn met de NCTV gedeeld. U bent op 14 november jl. per nota geïnformeerd over deze stand van zaken (reactie op nota stand van zaken NCTV).
- Een diepgaande audit, die kan leiden tot een accreditatie van de fysieke omgeving, vereist meer tijd en zal op verzoek van de NCTV in 2025 plaatsvinden.
- De constateert dat er voldoende vertrouwen is dat deze verbetermaatregelen door de NCTV in samenspraak met de worden opgepakt. Er zullen daartoe reguliere overleggen worden georganiseerd tussen de NCTV en De verslaglegging daarvan zal aan de worden doorgeleid.

3.3. Veiligheidsonderzoeken en vertrouwensfuncties
- De NCTV stelt momenteel enkel te werken met geldige VGB's binnen de organisatie, ondanks dat een aantal van de VGB's ouder is dan 5 jaar.
- De is van mening dat de NCTV deze conclusie op basis van de nu bekende informatie niet kan trekken.
- Dit heeft geleid tot verschillende (hoog)ambtelijke overleggen om de feitelijke situatie scherp te krijgen. Hierover bent u eerst geïnformeerd op 5 november jl., waarna is aangegeven per direct personen die tijdens naloop niet over juiste VGB blijken te beschikken geen werkzaamheden meer laten verrichten op dat niveau.
- U bent op 14 november jl. per nota geïnformeerd over deze stand van zaken (reactie op nota stand van zaken NCTV) alsmede over i) het procesvoorstel van de NCTV t.a.v. verschillende VGB vraagstukken en ii) de reactie van de daarop.
- De is van oordeel dat op 14 november jl. definitief is besloten dat van medewerkers die een VGB-B hebben, maar werkzaam zijn in functies waarvan in 2019 in overleg met de is aangegeven daar een formele VGB-A-functie van te maken, het VGB-B moet worden beoordeeld als niet rechtsgeldig.
- Onder 3.2 vindt u de mitigerende maatregelen die reeds getroffen zijn t.a.v. deze medewerkers.

Cluster secretaris-generaal
Directie
Bestuursondersteuning
Afdeling Advies en
Stukkenstroom

Datum
18 november 2024

Onze referentie

- De constateert dat er naast deze mitigerende maatregelen op dit moment geen aanvullende maatregelen nodig zijn.

3.4. Appreciatie

- De constateert dat er voldoende vertrouwen is dat de geïdentificeerde verbetermaatregelen door de NCTV in samenspraak met de naar tevredenheid worden opgepakt.
- De constateert dat er t.a.v. de veiligheidsonderzoeken nadere mitigerende maatregelen genomen worden. Deze zijn hieronder nader uitgewerkt.
- De constateert dat er in de tussentijd geen aanvullende extra maatregelen nodig zijn.

- **Mitigerende maatregelen**

De volgende maatregelen worden getroffen t.a.v. de veiligheidsonderzoeken en vertrouwensfuncties.

4.1. Mitigerende maatregelen in geval van ongeldige VGB
Ten aanzien van medewerkers die met een vervallen VGB-B werkzaam zijn op een functie die in 2019 is aangewezen om formeel op te hogen naar een VGB-A, is afgesproken dat de volgende mitigerende maatregelen worden getroffen:

- Toegang tot STG informatie is ontzegd, zowel digitaal als fysiek;
- Toegang tot de NCTV is ontzegd;
- De autorisatie van toegang tot de NCTV afdeling is ingetrokken;
- Het takenpakket wordt aangepast naar taken waarvoor geen STG informatie wordt geraadpleegd;
- De medewerkers kunnen in de reguliere DWR omgeving werkzaamheden blijven verrichten;
- Bij gebrek aan toegang kunnen de medewerkers werken vanuit huis of buiten de beveiligde schil van de NCTV, op andere afdelingen van het departement.

De NCTV heeft aangegeven dat bovenstaande maatregelen zijn doorgevoerd na een gesprek met betreffende medewerkers. Ten aanzien van geldt de volgende bijzonderheid:

-
-

Door de toegang tot STG informatie en NCTV zelf aan deze medewerkers te ontzeggen wordt t.a.v. deze functies vanaf dit moment voldaan aan de verplichtingen van de Wet Veiligheidsonderzoeken.

4.2. Aanvullende maatregelen
Daarnaast worden de volgende maatregelen getroffen:

Cluster secretaris-generaal
Directie
Bestuursondersteuning
Afdeling Advies en
Stukkenstroom

Datum
18 november 2024

Onze referentie
[redacted]

- T.a.v. personen met een verkeerde VGB is per direct een spoedonderzoek voor een VGB-A aangevraagd. Daarmee is het proces voor deze personen in lijn gebracht met de verplichtingen die voortvloeien uit de Wet veiligheidsonderzoeken t.a.v. het aanvragen van veiligheidsonderzoeken.
- Dit is een noodzakelijke stap in het uiteindelijk voldoen aan de screeningsvereisten van de functie ingevolge de Wet veiligheidsonderzoeken, namelijk dat de medewerker werkzaam daarop een VGB op het juiste niveau heeft;
- Er wordt onverminderd doorgewerkt aan het controleren van de screeningniveaus van alle medewerkers in relatie tot de informatie die wordt verwerkt, waarbij de meest kwetsbare functies worden geprioriteerd;
  - [redacted]
    T.a.v. deze groep wordt toegewerkt naar afronding uiterlijk 20 november as. T.a.v. medewerkers bij wie een hiaat daarin wordt geconstateerd worden per direct bovenstaande mitigerende maatregelen ingezet.
  - [redacted] wordt uiterlijk 20 november as. getoetst op het hebben van een geldig VGB. T.a.v. medewerkers bij wie een hiaat daarin wordt geconstateerd worden mitigerende maatregelen ingezet.
  - Voor alle overige afdelingen geldt dat ook wordt bezien dat B-functies niet in aanraking komen met A-specifieke informatie. T.a.v. deze afdelingen wordt toegewerkt naar afronding binnen voor het einde van het jaar. Daar waar sprake is van een geldig VGB-B zal als mitigerende maatregel worden genomen dat toegang tot A-specifieke informatie wordt ontzegd.
- De [redacted] kan zich vinden in dit proces en geeft aan dat er geen aanvullende maatregelen nodig zijn op dit moment.

4.3. Herzien lijst vertrouwensfuncties

- De lijst vertrouwensfuncties wordt, in samenspraak met de [redacted], herzien conform de wettelijke vereisten en in lijn gebracht met de actuele functies bij de NCTV. In dit proces worden ook de andere functies van de NCTV opnieuw bezien en worden conform gestelde eisen alle functies in lijn gebracht met het nieuwe besluit.
- Tot de lijst vertrouwensfuncties is herzien, wordt gewerkt op basis van de huidige lijst, waarbij niemand onrechtmatig op een functie zal zitten. Dit betekent dat óf dat het screeningsniveau in lijn is met de aangewezen vertrouwensfuncties óf de mitigerende maatregelen zijn toegepast.
- Inzet zal zijn om de eerste tranche (van sleutelposities) uiterlijk voor het kerstreces met een motivering tot herwaardering bij de AIVD in te dienen.
- De NCTV zal de administratie t.a.v. VGB's op orde maken en inregelen dat er periodiek wordt stilgestaan bij de geldigheid van VGB's op individueel niveau en tijdig herhaalonderzoeken worden aangevraagd. Hier volgt een apart plan van aanpak voor.

- **Afstemming**

NCTV, [redacted]

Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~DEP. VERTROUWELIJK / CONCEPT~~

Ministerie van Justitie en Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon

Datum
11 november 2024

Onze referentie
n.t.b.

nota

Reactie op voorstel NCTV inzake vertrouwensfuncties

Aanleiding

Op 7 november 2024 heeft de de NCTV geadviseerd over de vertrouwensfunctionarissen bij de NCTV waarvan de screening (VGB) mogelijk niet voldoet aan de in de Wet veiligheidsonderzoeken (Wvo) en regelgeving gestelde eisen. Op 8 november heeft de NCTV een procesvoorstel gedaan hoe in deze situaties te handelen, waarbij vier scenario's onderscheiden zijn. De is hierop verzocht te reageren. In voorliggende nota treft u de visie van de aan.

Advies

1. Indien medewerkers op een functie werken die is aangewezen op VGB-A niveau, maar betrokken op VGB-B gescreend zijn (geweest):
   - De steunt het voorstel per direct een veiligheidsonderzoek op het juiste niveau (A) aan te vragen. De NCTV heeft dit inmiddels gedaan in gevallen die tot nu toe geïdentificeerd zijn. De heeft aan deze aanvragen bij uitzondering een spoedstatus toegekend richting de AIVD om zo snel mogelijk uitsluitsel te krijgen over het veiligheidsonderzoek. NB: een spoedverzoek kent prioriteit toe aan het onderzoek, maar is geen garantie voor een snellere uitkomst.
   - De steunt het voorstel betrokkenen tijdelijk uit de VGB-A functie te ontheffen in afwachting van het veiligheidsonderzoek.
   - De adviseert niet in te stemmen met het voorstel deze medewerkers tijdelijk over te plaatsen naar een andere vertrouwensfunctie waarvoor een VGB-B (of C) vereist is. De kernreden hiervoor is dat de VGB-B van deze medewerkers van rechtswege is vervallen op het moment dat de functie werd aangewezen op niveau A. Deze medewerkers beschikken dus, anders dan in de nota van de NCTV beschreven, in het geheel *niet over een VGB*. Zij voldoen hiermee dan ook niet aan de wettelijke vereisten voor het uitoefenen van een vertrouwensfunctie (artikel 4 lid 3 Wvo).
   - De NCTV vormt een compartiment waarbinnen alle functies zijn aangewezen als vertrouwensfunctie en iedereen dus moet beschikken over een VGB. Gezien het gebrek aan een VGB van betrokkenen, stelt de voor om betrokkenen in afwachting van het onderzoek geen werkzaamheden voor de NCTV te laten verrichten en de toegang tot de NCTV te beperken. Het bezwaar van de op het voorstel van de NCTV ziet daarmee niet op de voorgestelde ongerubriceerd/ Dep. V. werkzaamheden, maar de onverenigbaarheid van het niet hebben van een VGB met het werken binnen het NCTV-compartiment. Het is wel mogelijk om betrokkenen tijdelijk een niet-vertrouwensfunctie elders bij JenV te laten vervullen.

- Mocht de VGB uiteindelijk geweigerd worden, steunt de [redacted] het voorstel de vaste procedure (definitieve plaatsing op een niet-vertrouwensfunctie elders bij JenV danwel beëindiging arbeidsovereenkomst) te volgen.

2. Indien medewerkers van de NCTV een VGB blijken te hebben die ouder is dan vijf jaar, maar wel op het juiste niveau, stelt de NCTV voor onmiddellijk een veiligheidsonderzoek op het juiste niveau aan te vragen. In de tussentijd kunnen medewerkers hun functie blijven uitoefenen, omdat de VGB verouderd maar nog rechtsgeldig is. Bij een negatieve uitkomst van het veiligheidsonderzoek wordt de toegang tot de NCTV ontzegd en de medewerkers conform de wettelijke procedure uit functie ontheven (artikel 10 lid 2 Wvo).
   - De [redacted] steunt het procesvoorstel van de NCTV.

3. Indien een medewerker een VGB zou hebben die ouder is dan tien jaar, stelt de NCTV voor onmiddellijk een nieuw veiligheidsonderzoek aan te vragen en in afwachting hiervan de toegang tot de NCTV te ontzeggen.
   - De [redacted] steunt het procesvoorstel van de NCTV.

4. Indien een NCTV-medewerker niet zou blijken te beschikken over een A of B-VGB, stelt de NCTV voor een onmiddellijk een veiligheidsonderzoek aan te vragen en in afwachting hiervan de toegang tot de NCTV te ontzeggen.
   - De [redacted] steunt het procesvoorstel van de NCTV, met dien verstande dat dit enkel betrekking heeft op functies waarvoor een A- of B-screening vereist is. Deze eis mag niet gesteld worden voor de NCTV-functies die op niveau C zijn aangewezen.

Toelichting
De [redacted] beperkt de toelichting op bovenstaand advies tot de punten waar het advies van de [redacted] afwijkt van het procesvoorstel van de NCTV (Ad.1 en Ad.4).

Ad1.
De nota van de NCTV is gestoeld op de veronderstelling dat de medewerkers op de VGB-A functies beschikken over een rechtsgeldige VGB-B. Hierop is ook de risicoafweging gebaseerd dat deze medewerkers in afwachting van hun veiligheidsonderzoek op niveau A tijdelijk een bestaande vertrouwensfunctie op niveau B kunnen vervullen. Dit uitgangspunt is, hoewel begrijpelijk, gebaseerd op een onjuiste interpretatie van de Wet veiligheidsonderzoeken. Een afgegeven VGB blijft geldig, tenzij de functie wijzigt of ophoudt te bestaan. Op het moment dat een functie wordt opgehoogd in niveau, vervalt als het ware de eerdere aangewezen functie. Wanneer er geen nieuw veiligheidsonderzoek wordt aangevraagd op het juiste niveau, vervalt ook van rechtswege de VGB die op de oude functie was afgegeven. De termijn die hiervoor staat is 4 weken (artikel 5 lid 1 Wvo). In het geval van de NCTV heeft de ophoging naar niveau A plaatsgevonden in 2019. De wettelijke termijn is daarmee ruimschoots overschreden. De VGB-B's waarover medewerkers eerder beschikten is, ongeacht de afgiftedatum, van rechtswege vervallen omdat deze niet meer voldoet aan de screeningsvereisten van de functie.

De medewerkers in kwestie beschikken dus, anders dan gesteld in de nota van de NCTV, niet over een VGB. Van het tijdelijk kunnen meenemen van de VGB-B naar een andere functie binnen de NCTV is derhalve ook geen sprake; de regels van

Functieclustering vereisen bovenal een rechtsgeldige VGB om mee te nemen. De Wet veiligheidsonderzoeken laat geen ruimte voor afwijking van deze vereisten. Afwijking van deze wettelijke bepalingen is strafbaar gesteld. De adviseert daarom negatief op dit punt van het NCTV-voorstel. De stelt als alternatief voor om betrokkenen tijdelijk op een niet-vertrouwensfunctie bij JenV te plaatsen.

De uiteindelijke beslissing over de wijze waarop wordt omgegaan met de medewerkers die niet beschikken over een (actuele) VGB ligt bij het lijnmanagement. Bij deze afweging is het essentieel dat eventuele andere dringende belangen, zoals bedrijfscontinuïteit, weloverwogen worden afgezet tegen het kader uit de Wet veiligheidsonderzoeken en het belang dat deze wet dient: de bescherming van de nationale veiligheid.

Ad4.

De gaat er van uit dat het voorstel van de NCTV niet deze functies betreft, maar enkel de functies die zijn aangewezen op niveau A of B. Immers, het is wettelijk gezien niet toegestaan om de medewerkers op C-functies op een A- of B-niveau te laten screenen. Indien men desondanks van mening is dat het C-niveau niet meer volstaat, zal de aangewezen vertrouwensfunctie eerst via de daarvoor geëigende procedures gewijzigd moeten worden. De en beslissen uiteindelijk samen of dit inderdaad wettelijk gezien genoodzaakt is.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

~~DEP. VERTROUWELIJK~~

www.rijksoverheid.nl/jenv
Contactpersoon
@minjenv.nl

Datum
8 november 2024

Onze referentie
XXX

nota

Reactie NCTV inzake advies NCTV

Aanleiding
Op donderdag 7 november jl. heeft de een advies gegeven aan de NCTV hoe om te gaan met de vertrouwensfuncties binnen de NCTV, indien er sprake is van een medewerker met een VGB-B op een functie waar een VGB-A wordt verwacht. In deze nota treft u een reactie aan van de NCTV met de beoogde vervolgacties.

Voorstel
De NCTV stelt het volgende proces voor:

- Indien personen binnen de NCTV op een functie werkzaam blijken te zijn waar een VGB-A wordt verwacht, maar over een VGB-B blijken te bezitten:
  - Wordt onmiddellijk een herhaalonderzoek aangevraagd bij de AIVD op niveau A (doorloop tijd maximaal 8 weken, in de praktijk sneller).
  - Wordt betrokkene tijdelijk uit de functie gehaald die een VGB-A vereist.
  - Betrokkene wordt dan tijdelijk in een andere functie geplaatst binnen de NCTV, waarvoor de werkzaamheden geen toegang vereisen tot het staatsgeheime netwerk of het lezen van stg-informatie.
  - Voor deze tijdelijke overplaatsing wordt aangesloten bij de voorwaarden die de in andere gevallen hanteert voor het 'meenemen' van een VGB naar een andere functie:
    1. Er moet sprake zijn van eenzelfde grondslag
    2. De functie mag geen hoger screeningsniveau hebben dan de VGB die de medewerker heeft
    3. De VGB mag niet langer dan 5 jaar geleden zijn afgegeven
  - Betrokkene werkt op dat moment alleen met informatie die beschikbaar is op de DWR-omgeving en open bronnen.
  - Indien het herhaalonderzoek leidt tot het niet afgeven van een VGB, wordt de toegang van de medewerker tot de NCTV ontzegd in afwachting van de te volgen standaard procedure.

- Indien personen binnen de NCTV een VGB blijken te hebben dat ouder is dan vijf jaar, maar wel op het juiste niveau:

  - Wordt onmiddellijk een herhaalonderzoek aangevraagd bij de AIVD op het vereiste niveau (doorloop tijd maximaal 8 weken, in de praktijk sneller).
  - Mogen medewerkers hun werkzaamheden blijven verrichten, omdat het VGB weliswaar verouderd is, maar wel geldig.
  - Indien het herhaalonderzoek leidt tot het niet afgeven van een VGB, wordt de toegang van de medewerker tot de NCTV ontzegd in afwachting van de te volgen standaard procedure.

- Indien een medewerker een VGB zou hebben dat ouder is dan tien jaar, wordt de medewerker de toegang tot de NCTV ontzegd in afwachting van het resultaat van een herhaalonderzoek.
- Indien een NCTV-medewerker niet zou blijken te beschikken over een A of B-VGB, wordt betrokkene de toegang tot de NCTV ontzegd, in afwachting van het resultaat van een A of B-onderzoek door de AIVD.

Toelichting
In haar nota van 7 november jl. adviseert bij een onjuist VGB van een medewerker bij de NCTV om:

- De geïdentificeerde functionarissen van hun functie te (laten) halen,
- een A-onderzoek aan te laten vragen door de NCTV en
- op basis van uitkomst van het Veiligheidsonderzoek te besluiten of zij hun werkzaamheden al dan niet kunnen hervatten.

Bij gevolg stelt dat een medewerker van de NCTV met een VGB-B waar een VGB-A wordt vereist, op dit moment niet werkzaam zou mogen zijn op de gangen van de NCTV.

Het risico van de aanwezigheid van NCTV-medewerkers met een VGB-B, waar een A wordt verwacht, acht de NCTV dan ook klein, temeer omdat toegang tot staatsgeheime informatie tijdelijk voor die medewerker wordt stopgezet.
Dit gebeurt in de praktijk alleen bij een disciplinaire maatregel of op het moment dat een VGB wordt ingetrokken. Gelet op de zeer zware consequenties voor medewerkers dat iemand geen toegang meer heeft tot de werkomgeving, moet dit dan ook grondig beargumenteerd zijn.

De NCTV kan aan de hand van het advies van de onvoldoende vaststellen waarop de zware interpretatie van de geldende wet- en regelgeving door de gebaseerd is. De NCTV vindt het dan ook noodzakelijk dat de aan de hand van de Wvo de juridische redenering onderbouwt dat personen die korter dan vijf jaar geleden een VGB-B hebben gekregen, dat gebaseerd is op een zelfde grondslag waarop ook andere NCTV-medewerkers hun taken uitoefenen, niet werkzaam zouden mogen zijn op de gangen van de NCTV.

Dat het niet hebben van een VGB op het juiste niveau, consequenties heeft voor werkzaamheden van een medewerker tot het moment dat dit juiste VGB wel ontvangen is, acht de NCTV begrijpelijk, maar proportionaliteit is hierbij van belang. Het hebben van een VGB-B is voor medewerkers binnen de NCTV voldoende om op de gangen van de NCTV te verblijven. Het risico van de aanwezigheid van NCTV-medewerkers met een VGB-B, waar een A wordt verwacht, acht de NCTV dan ook klein, temeer omdat toegang tot staatsgeheime informatie tijdelijk voor die medewerker wordt stopgezet.

Mocht blijken uit onderzoek dat medewerkers een sterk verouderd VGB hebben (ouder dan tien jaar), dan acht de NCTV dit risico te groot en wordt toegang tot de NCTV wel tijdelijk stopgezet in afwachting van de resultaten van een herhaalonderzoek. Medewerkers die in dienst zijn bij de NCTV hebben minimaal een VGB-B nodig. Indien mocht blijken dat iemand niet over de minimaal vereiste VGB-B beschikt, dan wordt toegang tot de NCTV ook tijdelijk ontzegd in afwachting van de resultaten van een herhaalonderzoek op niveau A of B, afhankelijk van de functie.

Ministerie van Justitie en Veiligheid

~~DEP. VERTROUWELIJK~~

De minister van JenV

Hoofddirectie
Bedrijfsvoering
Directie Informatievoorziening en Inkoop

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon

nota

Reactie op NCTV-nota stand van zaken (informatie)beveiliging n.a.v. ADR-onderzoek kenmerk

Datum
13 november 2024

Onze referentie

Paraaf Paraaf Paraaf

In afschrift aan
De NCTV

Aanleiding

U heeft naar aanleiding van een nota van de NCTV over de stand van zaken inzake (informatie)beveiliging in reactie op een ADR-onderzoek, aan de gevraagd of de verschillende onderdelen die door de NCTV zijn genoemd kunnen worden gevalideerd. De heeft de van JenV, in de rol als gevraagd hem hierin te adviseren.

Bevindingen

- *Accreditatie*

  De NCTV stelt te voldoen aan alle gestelde eisen om met staatsgeheime (STG) informatie te werken binnen de organisatie en op het standalone De NCTV geeft aan hiertoe geaccrediteerd te zijn per 8 april 2024.

  De onderschrijft dat er accreditatie heeft plaatsgevonden van het van de NCTV op niveau Staatsgeheim-Geheim. JenV heeft op advies van de op 8 april jl. een zogenaamde Interim Approval to Operate (IATO) verleend voor de periode van een jaar. In deze periode dient de NCTV een aantal verbetermaatregelen te nemen, waarna een Final Approval to Operate (FATO) kan worden aangevraagd. Voor de verstrekking van deze FATO zal een nieuwe beoordeling door de moeten plaatsvinden. Het is van belang te benadrukken dat de accreditatie enkel betrekking heeft op het verwerken van STG-informatie op het Het verwerken van STG-informatie op andere wijze door of bij de NCTV valt hierbuiten en is na overleg met de NCTV separaat beoordeeld door de , zie het kopje "Schouw".

- *Schouw*

  De NCTV verwerkt behalve op het ook op andere manieren staatsgeheime informatie, waaronder op papier en mondeling. Daarnaast kan het niet los gezien worden van de fysieke context waarin het zich bevindt en de personen die ermee werken. Om te toetsen of de NCTV ook

Hoofddirectie Bedrijfsvoering
Directie Informatievoorziening en Inkoop

Datum
13 november 2024

Onze referentie

op deze facetten voldoet aan de vereisten voor het werken met staatsgeheime informatie heeft de , in samenspraak met de NCTV, een schouw uitgevoerd. Hierbij is gekozen voor een schouw op hoofdlijnen vanwege de wens van de minister op korte termijn een eerste indicatie te krijgen van de stand van zaken bij de NCTV. Een diepgaande audit, die kan leiden tot een accreditatie van de fysieke omgeving, vereist meer tijd en zal op verzoek van de NCTV in 2025 plaatsvinden. Bij de schouw is enkel gekeken naar de omgang met staatsgeheime informatie. De omgang met EU/NAVO informatie dient separaat en in samenspraak met de National Security Authority (NSA) beoordeeld te worden. De heeft gekeken naar de getroffen organisatorische, fysieke, personele en informatiebeveiligingsmaatregelen. Daarbij is gebruik gemaakt van de volgende toetsingskaders: het VIRBI 2013 en het rubriceringskader Schouw NCTV STG._Domein d.d. 7-11-2024 (zie voor format bijlage)[1].

De bevindingen van de zijn als volgt:
Op basis van de bevindingen n.a.v. de schouw concludeert de dat de NCTV momenteel voldoet aan de vereisten voor het werken met staatgeheime informatie. De heeft een aantal kleine aanbevelingen, die separaat in een advies met de NCTV zullen worden gedeeld. Er is één aandachtspunt, dat nu niet onmiddellijk tot grote risico's leidt, maar waar nader onderzoek naar moet worden gedaan ingeval van accreditatie van de fysieke omgeving.

[2]. In de schouw is enkel ingegaan op de fysieke beveiliging en geen bevindingen opgenomen ten aanzien van de VGB's. Daar wordt hieronder separaat op ingegaan.

- *VGB*
  De NCTV stelt momenteel enkel te werken met geldige VGB's binnen de organisatie, ondanks dat een aantal van de VGB's ouder is dan 5 jaar.

  De is van mening dat de NCTV deze conclusie op basis van de nu bekende informatie niet kan trekken. De reden hiervoor is tweeledig. Ten eerste is de administratie van functiecodes, aangewezen functies en veiligheidsonderzoeken niet op orde bij de NCTV, waardoor niet met zekerheid kan worden vastgesteld dat alle medewerkers werkzaam op een functie waarvoor een VGB-A is vereist, ook daadwerkelijk hierover beschikken. De NCTV stelt dat deze medewerkers in ieder geval beschikken over een geldige VGB-B, omdat de medewerkers in het verleden op dit niveau gescreend zijn en een VGB in principe niet verloopt. Dit uitgangspunt is, hoewel begrijpelijk, gestoeld op een onjuiste interpretatie van de Wet veiligheidsonderzoeken. Een afgegeven VGB blijft geldig, tenzij de functie wijzigt of ophoudt te bestaan. Op het moment dat een functie wordt opgehoogd in niveau, zoals bij deze A-functies gebeurd is, vervalt als het ware de eerdere aangewezen functie op niveau B. Wanneer er geen nieuw veiligheidsonderzoek wordt aangevraagd op het juiste niveau, vervalt ook van rechtswege de VGB-B die op de oude functie was afgegeven. De termijn die voor deze aanvraag staat is 4 weken (artikel 5 lid 1 Wvo). In het geval van de NCTV heeft de ophoging naar niveau A

[1] Het ingevulde rubriceringskader is STG.C en zal met de adviezen, separaat met de NCTV en met u worden gedeeld.
[2] Het VIRBI vereist dat iedere ruimte waarin STG. informatie wordt verwerkt is afgesloten.

Hoofddirectie
Bedrijfsvoering
Directie Informatievoorziening en Inkoop

Datum
13 november 2024

Onze referentie

plaatsgevonden in 2019. De wettelijke termijn is daarmee ruimschoots overschreden. De VGB-B's waarover medewerkers eerder beschikten is, ongeacht de afgiftedatum, daarmee van rechtswege vervallen omdat deze niet voldoet aan de screeningsvereisten van de functie. De medewerkers in kwestie beschikken dus mogelijk, anders dan gesteld in de nota van de NCTV, in het geheel niet over een VGB. De heeft in een separate nota advies gegeven over het handelingsperspectief in deze gevallen. De NCTV heeft toegezegd diepgaand onderzoek te doen naar welke medewerker op welke functie(code) is geplaatst.

Ten tweede stelt de NCTV dat er sprake is van geldige VGB's, ook wanneer deze verouderd zijn. Het is correct dat de Wet veiligheidsonderzoeken (Wvo) geen vervaltermijn bevat voor een afgegeven VGB. In die zin verloopt de rechtsgeldigheid van een VGB dus inderdaad niet. De Wvo stelt echter dat de AIVD (uit hoofde van MinBZK) na een periode van 5 jaar of een veelvoud daarvan een herhaalonderzoek kan instellen, dan wel eerder wanneer omstandigheden hiertoe aanleiding geven. Het is daarmee evident dat de wetgever wenst periodiek te laten toetsen of er voortschrijdend geen bezwaar bestaat tegen het uitoefenen van de vertrouwensfunctie door de functionaris. Dit om de nationale veiligheid gedegen te beschermen. De 'geldigheid' van VGB's dient ook in dat licht bezien te worden.

Bij JenV is verder uitvoering gegeven aan het bepaalde in artikel 9 Wvo door in intern beleid vast te leggen dat, voor elk niveau VGB (A, B of C) elke 5 jaar een herhaalonderzoek uitgevoerd dient te worden (zie brief 7 december 2017, kenmerk). Het niet of niet tijdig aanvragen van een herhaalonderzoek is daarmee in principe in strijd met intern JenV beleid dat uitvoering geeft aan de Wvo. Wel heeft de AIVD het afgelopen jaar te maken gehad met forse achterstanden vanwege capaciteitsgebrek, waarbij in voorkomende gevallen voorrang is gegeven aan initiële verzoeken. Het is mogelijk dat dit mede van invloed is geweest op de voortgang van de procedure inzake herhaalonderzoeken bij de NCTV.

In het JenV-beleid is bovendien vastgelegd dat uitzonderingen hierop, zoals uitdiensttreding op korte termijn, dienen te worden beoordeeld door de . Over genoemde medewerkers die bij de NCTV gaan vertrekken, heeft destijds geen afstemming plaatsgevonden met de . Daarnaast is een VGB vertrouwensfunctie gebonden. Dit betekent dat als een vertrouwensfunctie ophoudt te bestaan, of de medewerker tussentijds een andere functie vervult die niet is aangemerkt als vertrouwensfunctie, de VGB van rechtswege vervalt. Op basis van informatie die is aangeleverd door de NCTV concludeert de dat dit voor een deel van de medewerkers geldt. De NCTV heeft toegezegd in kaart te brengen voor welke functionarissen dit geldt en de herhaalonderzoeken onmiddellijk aan te vragen. De eerste stappen hierin zijn inmiddels gezet, waarbij moet worden opgemerkt dat als de NCTV nog niet precies weet wie op welke functie is geplaatst, de reeds aangevraagde veiligheidsonderzoeken op niveau A, moeten worden stilgelegd als achteraf zou blijken dat de functie geen A-functie betreft en dat dit mogelijk betekent dat eerder aangevraagde veiligheidsonderzoeken onrechtmatig zijn geweest.

Tot slot merkt de op dat mede gelet op het bovenstaande er al langere tijd zorgen bestaan over de vertrouwensfuncties bij de NCTV. De is hier

Hoofddirectie Bedrijfsvoering
Directie Informatievoorziening en Inkoop

Datum
13 november 2024

Onze referentie

sinds 2023 intensief over in gesprek met de NCTV. Dit betreft onder meer de lijst vertrouwensfuncties, die sterk verouderd is en wettelijk gezien geactualiseerd moet worden (artikel 3 lid 4 Wvo). De heeft geconstateerd dat de bestaande motiveringen van de vertrouwensfuncties volgens de hedendaagse vereisten niet langer voldoen en dat er incidenteel VGB's worden aangevraagd onder functiecodes die bij een andere functie horen. Dit is niet toegestaan. Daarnaast worden gewijzigde omstandigheden bij vertrouwensfunctionarissen niet altijd (tijdig) gemeld bij de . Hierover heeft een gesprek plaatsgevonden tussen de NCTV, AIVD en . Een en ander is ook op hoofdlijnen meegenomen door de in de toezichtbrief d.d. 16 juli jl. en zal ook onderwerp van gesprek zijn in het toezichtgesprek dat dit jaar nog plaatsvindt. Met de NCTV is afgestemd dat zij voorrang geven aan het in kaart brengen van de niveaus zoals hierboven beschreven en het aanvragen van de (herhaal)onderzoeken. Vervolgens zal de NCTV in samenspraak met de zo spoedig mogelijk de actualisatie van de lijst vertrouwensfuncties ter hand nemen.

- *AVG*
  is in samenspraak met de hierover in gesprek met de NCTV.

- *WCoTNV*
  De nieuwe Wet coördinatie terrorismebestrijding en nationale veiligheid beoogt de coördinerende taken van de NCTV van een duidelijke wettelijke grondslag te voorzien en waar nodig aanvullende bevoegdheden te geven. Zolang de wet niet in werking is getreden mag de NCTV geen persoonsgegevens verwerken voor deze aanvullende taken. Voor de bestaande taken lijkt er wel een wettelijke grondslag te zijn. De verantwoordelijk voor verwerkingen die vallen onder die Grondslagenwet is hierover in gesprek met de NCTV.

- *Nieuwe organisatiestructuur*
  De is ermee bekend dat er een transitie in gang is gezet. De heeft vernomen dat er functiescheiding heeft plaatsgevonden en dat de functie van en niet langer bij een en dezelfde persoon is belegd. De onderschrijft dit initiatief mede vanuit het oogpunt van lastenverlichting waardoor er meer tijd beschikbaar is voor zowel de als de om de taken en verantwoordelijkheden te vervullen. De staat in nauw contact met de NCTV over hoe deze ontwikkeling verder wordt vormgegeven.

Reactie op nadere toelichting
In de nadere toelichting heeft de NCTV bovenstaande onderwerpen verder uitgediept. Ten aanzien van deze toelichting merkt de nog het volgende op:

Informatiebeveiliging
De NCTV stelt dat de leidraad voor de beveiliging van ongerubriceerde, Dep.-V of STG-informatie wordt gevormd door de BIO. De benadrukt dat het VIR en het VIR-BI leidend zijn voor bijzondere informatie, d.w.z. Dep.-V en STG. De BIO is een uitvoeringsrichtlijn die gehanteerd wordt om de implementatie te vergemakkelijken en gaat niet over STG.
De departementale is gevraagd om te onderschrijven of de NCTV voldoet aan bepaalde niveaus van de NBA-LIO Volwassenheidsniveau Informatiebeveiliging.

Hoofddirectie
Bedrijfsvoering
Directie Informatievoorziening en Inkoop

Datum
13 november 2024

Onze referentie

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

~~Dep. VERTROUWELIJK~~

Aan de minister van Justitie en Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
[redacted]
[redacted]@minjenv.nl

Datum
17 september 2024

Ons kenmerk
[redacted]

Dossiernummer
Dossiernummer

Bijlagen
1

nota

Stand van zaken (informatie)beveiliging NCTV n.a.v. ADR-casus

Aanleiding

Recent heeft u het conceptrapport van de ADR over de omgang met (staatsgeheime) informatie door NCTV en politie in het licht van de arrestatie van twee (oud-)medewerkers van de NCTV en politie ontvangen. Op basis hiervan heeft u verzocht om een nota die nadere toelichting geeft op de gebeurtenissen bij de NCTV, de huidige stand van zaken rond informatiebeveiliging, informatiehuishouding en grondslagen. Deze nota gaat hier nader op in.

Gevraagde actie

Kennisnemen van deze nota.

Kern

- De NCTV voldoet aan alle gestelde eisen om met staatsgeheime informatie te werken binnen de organisatie en op het stand-alone [redacted] Hiertoe is de NCTV geaccrediteerd door [redacted] die hiervoor verantwoordelijk is, op advies van de [redacted] De accreditatie is op 8 april 2024 verleend. De AIVD heeft meegekeken op dit traject.
- De NCTV werkt op dit moment uitsluitend met geldige VGB's binnen de organisatie. Van 29 NCTV medewerkers zijn de VGB's ouder dan 5 jaar, maar dit maakt ze niet ongeldig. Van deze 29 VGB's zijn er 18 op dit moment in de procedure van een herhaalonderzoek. De overige VGB's behoren aan medewerkers die op dit moment niet werkzaam zijn bij de NCTV of binnen enkele maanden vertrekken.
- De NCTV werkt op dit moment binnen de nu geldende kaders van de AVG.
- Bij de inwerkingtreding van de Wet coördinatie terrorismebestrijding en nationale veiligheid (WCoTNV) heeft de NCTV een grondslag voor het verwerken van persoonsgegevens. Deze wet zal op zijn vroegst per 1 januari 2025 van start gaan.
- Er is een separate afdeling opgericht bij de NCTV die verantwoordelijk is voor risicomanagement en compliance. Deze taken worden niet langer ondergebracht bij de [redacted] Bovendien zijn en worden er nieuwe medewerkers geworven voor deze taak, om de NCTV op het gewenste niveau blijvend te laten functioneren. Voor het einde van het jaar wordt deze afdeling middels een addendum op het O&F geformaliseerd.
- Sinds 1 september 2024 is de [redacted] direct verantwoordelijk voor informatiebeveiliging binnen de NCTV en zal hier actief op sturen.

Informatiebeveiliging
De NCTV moet alle informatie die hij tot zijn beschikking heeft beveiligen, of dit nu ongerubriceerde, departementaal vertrouwelijke of staatsgeheime informatie is. Leidraad voor deze beveiliging vormt de Baseline Informatiebeveiliging Overheid (BIO). Binnen het ministerie van Justitie en Veiligheid is het *NBA-LIO Volwassenheidsmodel Informatiebeveiliging* gebruikt om te meten wat het volwassenheidsniveau van informatiebeveiliging is op vier in het model vastgestelde aandachtsgebieden, te weten governance, organisatie, risicomanagement en incidentmanagement.

Het NBA-LIO Volwassenheidsmodel kent vijf niveaus, waarbij niveau 1 grofweg betekent dat er nog veel moet gebeuren, op niveau 2 eerste stappen zijn gezet, niveau 3 betekent dat het beleid is vastgelegd en er ook mee gewerkt wordt, en op niveau 4 een hele PDCA-cyclus doorlopen kan worden. Op niveau 5 heeft de informatiebeveiliging een sturende werking op de organisatie. Het BD JenV heeft als gewenst niveau en als ambitie niveau 4 binnen de eerder genoemde aandachtsgebieden te halen. Op dat niveau is informatiebeveiliging binnen die aandachtsgebieden 'beheerst en meetbaar'.

Voordat de casus rond de gearresteerde (oud-)medewerkers van de NCTV aan het licht kwam, schatte de NCTV het volwassenheidsniveau voor de genoemde aandachtsgebieden binnen de eigen organisatie in op 3 met uitzicht op het halen van niveau 4. Dit was binnen de kaders die werden gesteld vanuit het departement. Op grond van nader onderzoek, mede naar aanleiding van de casuïstiek, bleek echter dat dit niveau niet volledig werd gehaald, omdat nieuwe risico's in beeld kwamen.

Op dat moment kon ervoor worden gekozen om het staande beleid te repareren. Hierin zag de NCTV echter risico's, omdat dan mogelijk zaken over het hoofd kunnen worden gezien, waardoor het fundament van het informatiebeveiligingsbeleid onvolledig zou zijn en alle vervolgstappen daarmee ook. Om die redenen gaf de NCTV er de voorkeur aan om nieuw beleid vast te stellen. De NCTV heeft met het vaststellen van het nieuwe beleid dus welbewust een stap teruggezet, met als oogmerk alle risico's die nu bekend zijn ook daadwerkelijk aan te kunnen pakken en te werken op basis van een robuust fundament qua informatiebeveiliging.

Inmiddels is de NCTV, met het vaststellen van het nieuwe beleid in januari 2024, voor de genoemde aandachtsgebieden niveau 2 voorbij en worden op onderdelen niveau 3 en 4 gehaald. Dit is echter nog niet volledig het geval. De NCTV zal in de zomer van 2025 niveau 3 volledig bereiken en later dat jaar ook volledig voldoen aan niveau 4 en daarmee, zoals gewenst, continu een volledige PDCA-cyclus kunnen doorlopen.

Het feit dat niveau 4 nog niet over de volle breedte wordt gehaald, betekent nadrukkelijk niet dat de informatiebeveiliging van de NCTV op dit moment niet op orde is. De inrichting van een PDCA-cyclus en het nastreven van een hoog volwassenheidsniveau leidt tot een beheerste en meetbare informatiebeveiliging. Daarnaast staat dat de feitelijke beveiliging op een niveau moet zijn waarbij alle bekende risico's tot een acceptabel niveau gereduceerd zijn. In die gevallen waar

risico's te hoog zijn, moeten maatregelen genomen of worden systemen (tijdelijk) niet meer gebruikt. Die feitelijke informatiebeveiliging is op dit moment binnen de NCTV op orde en zodoende wordt er gewerkt binnen de kaders van de geldende wet- en regelgeving.

Staatsgeheime informatie binnen de NCTV

Het concept ADR-rapport concludeert dat de NCTV onvoldoende de beveiliging van staatsgeheime informatie op orde had op het moment dat de arrestaties van de twee (oud-) collega's plaatsvonden. Voordat de casus bekend werd, had de NCTV al trajecten ingezet om de beveiliging van en omgang met staatsgeheime informatie te verbeteren, omdat een aantal risico's reeds waren geïdentificeerd. Na de arrestaties zijn de volgende additionele maatregelen getroffen:

- Per direct zijn alle processen waarbij staatsgeheime informatie werd verwerkt stopgezet. Verspreiding van staatsgeheime informatie via het [redacted] waarop de NCTV staatsgeheime informatie verwerkt, werd buiten werking gesteld en met instemming en onder toezicht van de AIVD werd een papieren proces ingericht, zodat de NCTV wel zijn taken kon blijven verrichten. Alle medewerkers die Stg-informatie tot zich namen werden geregistreerd evenals welke informatie zij tot zich namen. [redacted] werd in deze periode uitsluitend gebruikt voor eigen stukken van de NCTV die geproduceerd moesten worden en staatsgeheim waren. Deze konden immers niet op het open DWR-systeem gemaakt worden.
- Terwijl bovengenoemde noodmaatregelen van kracht waren is gewerkt aan het opnieuw vormgeven van de staatsgeheime werkprocessen van de NCTV, met als doel accreditatie van de NCTV om weer volledig met Stg-informatie te kunnen werken. Deze accreditatie, een verantwoordelijkheid van de [redacted] is gerealiseerd op 8 april 2024. In het accreditatieproces zijn risicoanalyses en het risicoregister up tot date gebracht.
- Dit alles heeft recent geleid tot het heropstarten van de verspreiding van staatsgeheime stukken via [redacted] Hiertoe is de NCTV dus ook gerechtigd, gegeven de accreditatie.
- Naast staatsgeheime informatie is er ook EU- en NAVO-gerubriceerde informatie. Voor beiden geldt een separate accreditatie. Deze heeft de NCTV op dit moment niet en daarom wordt er ook niet met deze informatie op de gangen van de NCTV gewerkt. In de loop van 2025 beoogt de NCTV ook deze accreditaties te realiseren.

Verklaringen Geen Bezwaar

Om bij de NCTV te werken moet een medewerker een Verklaring Geen Bezwaar (VGB) hebben, als gevolg van een met goed gevolg doorlopen veiligheidsonderzoek door de AIVD. Binnen de NCTV hebben alle medewerkers een A of B-onderzoek doorlopen. Beleid binnen de NCTV is dat een dergelijk onderzoek elke vijf jaar moet worden herhaald. Als de vijf jaar wordt overschreden betekent dit niet dat de VGB niet meer geldig is, maar uitsluitend dat de NCTV niet voldoet aan zijn eigen beleid. Streven is natuurlijk wel te allen tijde te voldoen aan dat beleid.

Op dit moment zijn er 29 personen met een VGB dat ouder is dan 5 jaar. Van de 29 personen zijn er 18 die een herhaalonderzoek hebben lopen. Van de 11 personen die overblijven zijn er vier langdurig gedetacheerd, waarbij er óf geen VGB nodig is óf die verantwoordelijkheid ligt bij de indetacherende partij. Deze

mensen zijn niet werkzaam op de gangen van de NCTV.

Grondslagen
De NCTV kijkt in het kader van zijn taken naar ontwikkelingen op de thema's die raken aan de nationale veiligheid, zoals terrorisme, cybersecurity en statelijke dreigingen. Om deze ontwikkelingen te monitoren, wordt er ook gekeken op internet, waaronder sociale media. Op het moment dat dit soort bronnen worden geraadpleegd komen er onvermijdelijk ook persoonsgegevens mee.

Naar aanleiding van publicaties in NRC en het daaropvolgende politieke debat is door de toenmalige Minister van JenV geconcludeerd dat een aanvullende wettelijke grondslag voor de NCTV noodzakelijk was om in het kader van zijn coördinatietaken persoonsgegevens te kunnen verwerken. Hiertoe is de Wet Coördinatie Terrorismebestrijding en Nationale Veiligheid (WCoTNV) ontstaan. De wet is op 26 oktober 2023 aangenomen door de Tweede Kamer en op 5 december 2023 door de Eerste Kamer. Sindsdien is de NCTV bezig met de implementatie van de wet, zodat deze op juiste wijze kan worden toegepast binnen de NCTV.

In een Algemene Maatregel van Bestuur moeten bepaalde kaders en waarborgen voor de toepassing van de wet nader worden uitgewerkt. Deze AMvB ligt op dit moment ter advies bij de Autoriteit Persoonsgegevens, en zal na dit advies voor een voorhangprocedure worden voorgelegd aan de Eerste en Tweede Kamer. Vervolgens gaat de AMvB ter toetsing naar de Raad van State.

Dit betekent dat de WCoTNV op zijn vroegst kan worden ingevoerd op 1 januari 2025, maar dat rekening gehouden moet worden met een latere inwerkingtreding. In de tussentijd bereidt de NCTV intern alle processen voor om binnen de NCTV op de juiste wijze met de wet te werken en hier ook verantwoording over af te kunnen leggen richting Inspectie JenV en AP.

Op dit moment worden binnen de NCTV alleen persoonsgegevens verwerkt voor processen waarvoor al een specifieke wettelijke basis is, zoals de Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding en de Politiewet in het kader van bewaken en beveiligen. Ook worden in voorkomende gevallen gegevens verwerkt van personen indien coördinerende werkzaamheden in zware CT-casuïstiek noodzakelijk zijn, ter ondersteuning van besluitvorming door de minister van Justitie en Veiligheid in specifieke casuïstiek (bijvoorbeeld gerelateerd aan het intrekken van het Nederlanderschap, repatrieringsverzoeken van uitreizigers en listing- of delistingszaken) en worden op grond van machtigingen van persoonsgegevens verwerkt ten behoeve van de toetsing van visumverlening aan mogelijke extremistische sprekers.

De NCTV verwerkt persoonsgegevens binnen de nu geldende kaders van de AVG. Dit levert overigens wel beperkingen op bij de uitvoering van de taak van de NCTV. Deze beperkingen zullen bij de inwerkingtreding van de WCoTNV grotendeels zijn opgelost.

Nieuwe organisatiestructuur
Vanzelfsprekend betreurt de NCTV dat een dergelijk ernstige zaak, zoals onderhavige casus, onvolkomenheden aan het licht heeft moeten brengen. Om die reden is ervoor gekozen ook aanpassingen te doen aan de organisatiestructuur binnen de NCTV. Waar de informatiebeveiliging en de fysieke beveiliging van de NCTV was belegd bij de [redacted] is ervoor gekozen om te komen tot een separate afdeling die zich specifiek bezig gaat houden met risicomanagement en compliance. Deze afdeling is op dit moment in oprichting.

De verantwoordelijkheid voor deze afdeling, alsmede [redacted] is in de nieuwe organisatiestructuur belegd bij de [redacted], om zeker te stellen dat de leiding van de NCTV actief op de hoogte is van ontwikkelingen en hier ook actief op kan sturen. Zodoende verwacht de organisatie op het hoge niveau te kunnen blijven functioneren, die van een cruciale speler binnen het domein van de nationale veiligheid verwacht mag worden.

Tot slot
Zowel het concept ADR-rapport als de interne procedures binnen de NCTV hebben in het afgelopen jaar laten zien dat er onvolkomenheden waren die moeten worden opgelost. Zoals gesteld voldoet de NCTV op dit moment aan de vereisten die nodig zijn om met genoemde informatie te werken. Daarnaast zijn er op dit moment strengere procedures ingericht volgens het principe van need-to-know, zoals informatiescheiding en een inperking van het aantal mensen dat kennis mag nemen van specifieke informatie. Ook is het printen van [redacted] ingeperkt en worden de resterende mensen die nog mogen printen permanent gelogd.

Op basis van de nu geldende maatregelen acht de NCTV het verantwoord om de werkzaamheden, ook binnen het staatsgeheime domein, op te pakken. Er zullen echter nog aanvullende maatregelen worden getroffen. Hierbij moet worden gedacht aan geautomatiseerde processen binnen het documentatie mangementsysteem, waardoor de need-to-know nog kleiner wordt. Ook zal er nog met de AIVD worden gewerkt aan het inperken van risico's die zijn geïdentificeerd rond het [redacted]

Dit laat onverlet dat ook hier geldt dat 100% garantie op veiligheid niet bestaat. Ook in de nieuwe situatie zijn er individuele medewerkers binnen de NCTV met aanzienlijke toegang tot gevoelige informatie. Een medewerker die heimelijk activiteiten verricht die tot doel hebben om staatsgeheime informatie ongeoorloofd mee te nemen en te delen met een buitenlandse inlichtingendienst is een zeer complexe situatie die nooit volledig kan worden uitgesloten. De omvang van een dergelijk incident zou in de huidige situatie gezien de aangepaste werkprocessen wel minder groot zijn dan de casus die nu speelt.

nota

De Nationaal Coördinator Terrorismebestrijding en Veiligheid
dhr. P.J. Aalbersberg EMPM

Ministerie van Justitie en Veiligheid
Ministerie Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon

Datum
30 oktober 2020

Ons kenmerk

Toezicht integrale beveiliging 2019

Van

Datum/eindparaaf

Kopie aan

Datum/paraaf

Concipiënt

Datum/paraaf

Oordeel Toezicht 2019
Hierbij ontvangt u mijn bevindingen ten aanzien van de stand van zaken van de integrale beveiliging van de NCTV.

Deze zijn mede gebaseerd op de afstemming die ik heb gehad tijdens het proces van de risicoanalyse en over de aangeleverde informatie met uw De Security Risk Assessment (SRA) is op 17 februari 2020 voorgelegd aan het MT. Vanuit het MT zijn aanvullende vragen gesteld over de uitgevoerde SRA. In de jaarplanning is vervolgens opgenomen dat hernieuwde uitvoering voor het vaststellen TBB/KWAS in 2020 plaats zou vinden d.m.v. interviews. Door de Covid-19 uitbraak zijn de interviews verschoven naar 2021 en daarmee ook het bijstellen van het rapport. Uw is een regelmatige deelnemer aan het maandelijkse BVC-overleg.

Gelet op het bovenstaande is mijn oordeel voor uw organisatieonderdeel dat de voortgang op basis van de aangeleverde informatie nog verbeterd kan worden. Uw heeft aangegeven dit te herkennen en de SRA in 2021 daar waar nodig bij te zullen stellen. Waar wenselijk kan mijn bureau hierbij ondersteuning geven.

Ministerie van Justitie en Veiligheid
Ministerie Binnenlandse Zaken en Koninkrijksrelaties

Datum
30 oktober 2020

Ons kenmerk

Daarnaast is in 2019 sterk ingezet op het bevorderen van het beveiligingsbewustzijn. Ik heb in de tweede helft vorig jaar de georganiseerd. Daarmee wordt stevig invulling gegeven aan het feit dat de medewerkers de belangrijkste schakel in de integrale beveiliging zijn. Veilig omgaan met informatie, privacy van burgers beschermen, zorgen dat informatie niet in verkeerde handen komt moet onderdeel zijn van ons ambtelijk vakmanschap. Maar ook bewustzijn van het borgen van je persoonlijke veiligheid. Daarnaast wordt door mijn bureau op regelmatige basis voorlichting gegeven aan afdelingen, nieuw aangetreden collega's en op verzoek bij de onderdelen.

Ik zal in T3 2020 voor heel JenV een rode draden rapportage opstellen voor de die ter informatie tevens wordt aangeboden aan de Brede Bestuursraad en het Strategisch Bestuurlijk Beraad.

Ook in 2020 wordt door mij ondersteuning aangeboden bij het uitvoeren van de SRA's. Daarnaast zal ik in 2020 en 2021 naar aanleiding van mijn uitvraag voor de 3e fase van de driejaarlijkse cyclus, een toezichtsbezoek in laten plannen ter toetsing van de voortgang van de implementatie, de weerstandtesten en het verbeterplan dat in 2020 moet worden aangeleverd.

Graag ga ik met u in gesprek over de bevindingen over 2019. Wanneer u naar aanleiding van deze nota nog vragen heeft of u al eerder een gesprek wilt over andere beveiliging gerelateerde zaken, kunt u uiteraard altijd contact met mij opnemen.

Achtergrond:
Om het aantal uitvraagmomenten en de administratieve last te beperken ben ik in 2018 gestart met de nieuwe driejaarlijkse toezichtcyclus uit het Toezichtkader 2018-2021 JenV (Brede Bestuursraad 2 februari 2018). Uitgangspunt vormt risicogestuurd toezicht. Dat betekent dat niet jaarlijks de gehele balans wordt opgemaakt zoals dat tot 2018 gebeurde, maar het toezicht zich richt op het uitvoeren van de analyse, de veranderingen, verbeterpunten en verbeterplannen en de werking in de praktijk.

De driejaarlijkse cyclus is gebaseerd op de Deming circle, met constant doorlopen van deze stappen wordt de integrale beveiliging structureel verbeterd en geborgd:

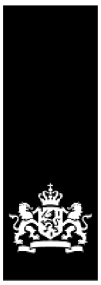
1. Dreiging/risicoanalyse (Plan) -> 2018
2. Implementatie en voortgang (Do) -> 2019
3. Weerstandtesten (Check) en verbeterplan (Act) -> 2020

Op 26 juli 2019 heb ik u verzocht mij de door uw MT vastgestelde voortgang van het implementatieplan voor eind november 2019 aan te bieden. De gevraagde termijn bleek voor de diverse onderdelen van JenV redelijk ambitieus. In goed overleg is besloten de termijn te verlengen tot juli 2020.

Ministerie van Justitie en Veiligheid
Ministerie Binnenlandse Zaken en Koninkrijksrelaties

Datum
30 oktober 2020

Ons kenmerk



nota

Document vrijgegeven bij publicatie

[redacted]

Ministerie van Justitie en Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag

Datum
26 maart 2024

Ons kenmerk
[redacted]

Contactpersoon
[redacted]

Datum
26 maart 2024

Ons kenmerk
[redacted]

Verlenen van accreditatie aan het [redacted] NCTV
(Interim Approval To Operate) tot 08-04-2025

Van
[redacted]
Datum/eindparaaf

Concipiënt
[redacted]
Datum/paraaf

Advies:
Ik verzoek u in te stemmen met:

- Het verlenen van de Interim Approval To Operate (IATO) aan het [redacted] van de NCTV.
- In te stemmen met bijgaande conceptnota aan de NCTV (met bijlage).

Toelichting:

- U bent de Security Accreditatie Autoriteit voor Staatsgeheime netwerken. U wordt daarbij geadviseerd door mij.
- De NCTV heeft u verzocht op 14 maart 2024 (kenmerk [redacted] tot het verlenen van toestemming (accreditatie) voor de verwerking van Staatgeheim Geheime informatie op het [redacted] NCTV.
- De IATO wordt verleend voor de duur van maximaal 1 jaar, gedurende het jaar wordt door de NCTV voor 10 resterende risico's aanvullende maatregelen getroffen. De 10 als M (medium) ingeschaalde risico's zijn reeds gemitigeerd met aanvullende maatregelen tot L (laag) ingeschaalde restrisico's. Er is daarnaast één overgebleven M risico dat door het lijnmanagement is geaccepteerd. De risico's op L worden in de tussenliggende tijd tot de aanvullende maatregelen zijn getroffen geaccepteerd.
- Door mij is dit beoordeeld als ruim voldoende voor het verstrekken van de IATO. De NCTV is volledig in control. Ik heb daartoe beoordeling uitgevoerd op de documentatie, interviews gehouden met specifieke medewerkers en in de praktijk beoordeeld of de voorgestelde maatregelen

Ministerie van Justitie en Veiligheid

Datum
26 maart 2024

Ons kenmerk

voor de geconstateerde risico's afdoende waren. Mijn adviezen zijn daar bij opgevolgd.

- De reeds getroffen maatregelen en de behandelplannen voor de 10 resterende risico's zijn passend bij het risicoavers profiel van de verwerkte informatie.

nota

~~Dep. VERTROUWELIJK~~

Document vrijgegeven bij publicatie

~~Dep. VERTROUWELIJK~~

NCTV
Dhr P.J. Aalbersberg EMPM

Ministerie van Justitie en Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon

Datum
25 maart 2024

Ons kenmerk
BWA-AGC-2024-NCTV-001

Bijlagen
1

Het verlenen van accreditatie aan het van de NCTV (Interim Approval To Operate)

Algemene leiding

Datum/eindparaaf

Door tussenkomst van

Datum/paraaf

Van

Datum/paraaf

Aanleiding

Uw verzoek, dd. 14 maart 2024 (kenmerk tot het verlenen van toestemming (accreditatie) voor de verwerking van Staatgeheim Geheime informatie op het

Besluit

Gelet op de operationele noodzaak, het gerealiseerde niveau van de beveiliging, de resterende informatiebeveiligingsrisico's welke door de proces- en systeemeigenaar zijn geaccepteerd en het advies van , verleent de hierbij tijdelijke toestemming voor verwerking [Interim Approval to Operate (IATO)] onder de volgende voorwaarden:

1. De verwerking van gerubriceerde informatie tot maximaal het rubriceringsniveau Staatsgeheim Geheim;
2. Voor het van de NCTV, zoals is opgenomen in de Statement of Compliance;
3. Gelimiteerd tot en met 8 april 2025 of, indien dat eerder het geval is, tot dat er belangrijke wijzigingen worden doorgevoerd, van welke aard dan ook, die consequenties kunnen hebben voor de beveiliging van onderhavig Informatiesysteem;
4. Bij het actueel houden van het maatregelenplan;

Ministerie van Justitie en Veiligheid

Datum
25 maart 2024

Ons kenmerk

5. Het implementeren van de voorgestelde (rest)maatregelen conform de Statement of Compliance en de voortgang maandelijks te monitoren;
6. De uitkomsten uit het risicomanagementproces doorlopen voor het einde van de looptijd op relevantie en geldigheid;
7. En aanvragen van de accreditatie voor einde van de looptijd van de IATO.

kan, mede op advies van de toestemming herzien of intrekken op basis van wijzigingen in de scope en/of veroudering van de uitkomsten uit het risicomanagementproces (voorwaarden 3, 4, 5 en 6).

Toelichting
Voor de uitvoering van de werkzaamheden van NCTV wordt gebruik gemaakt van het Hierin wordt informatie tot en met het niveau Staatsgeheim Geheim verwerkt. Conform nationale regelgeving op het gebied van beveiliging van bijzondere informatie moet de Security Accreditation Authority (SAA) voor dit informatiesysteem vooraf toestemming verlenen voor de verwerking en nadere verspreiding van gerubriceerde informatie[1]. De SAA voor gerubriceerde systemen is die hiertoe wordt geadviseerd door .

Voor dit systeem is de NCTV proces- en systeemeigenaar, die dit belegd heeft bij het binnen de NCTV. Deze heeft de betrouwbaarheidseisen (uitgesplitst naar beschikbaarheid, integriteit en vertrouwelijkheid), risico's en compenserende maatregelen geïdentificeerd in het risicomanagementproces. De uitkomsten zijn vastgesteld en middels het aangeleverde accreditatiedossier onderbouwd in de Quikscan (uitkomst BBN3-niveau), de Risicoanalyse met behulp van de MAPGOOD methodiek en het beoordelen van het op basis van de maatregelen uit de BIO op BBN2 niveau, aangevuld met de maatregelen die genoemd zijn in de ABDO-regeling voor het verwerken van Stg. Geheim gerubriceerde informatie, het Maatregelenplan voor de geïdentificeerde (10) risico's (voor deze risico's zijn behandelplannen opgesteld met daarin mitigerende maatregelen of het voorstel tot acceptatie(1)) en Statement of Compliance (Nota MT-NCTV met kenmerk . vastgesteld op 15 maart 2024 door de NCTV dhr. P.J. Aalbersberg EMPM).

Ter validatie van het risicomanagementproces is door mijn een beoordeling uitgevoerd op de documentatie en met de volgende van uw medewerkers een interview gehouden:
-
-
-
-
-
-
Daarnaast is in de praktijk beoordeeld of de voorgestelde maatregelen voor de geconstateerde risico's afdoende waren. Voor bevindingen uit de beveiligingsonderzoeken (review) zijn nog enkele verbeteringen doorgevoerd, ook

[1] VIRBI, artikel 3, onder b; BVA-besluit, artikel 4, lid 3.

Ministerie van Justitie en Veiligheid

Datum
25 maart 2024

Ons kenmerk

is door uw MT nog op enkele punten een aanscherping in het maatregelplan getroffen passend bij het risicoavers profiel van de verwerkte informatie.

Een met positief resultaat doorlopen accreditatieproces, FATO of IATO, stelt zeker dat de risicoafweging op een verantwoorde wijze is gemaakt en dat de verantwoordelijke proces- en systeemeigena(a)r(en) eventuele restrisico's bewust aanvaard(t/en). Accreditatie impliceert nooit het overnemen van verantwoordelijkheden door de accrediterende instantie.

Voor stakeholders is een ongerubriceerd accreditatiecertificaat opgesteld.
Bijlage 1 – Certificaat IATO

Onderbouwing accreditatiedossier:

nota

De Nationaal Coördinator Terrorismebestrijding en Veiligheid
Dhr. P.J. Aalbersberg EMPM

Ministerie van Justitie en Veiligheid
Ministerie Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon

Datum
9 mei 2022

Ons kenmerk

Bijlagen
1

Toezicht integrale beveiliging 2021

Van

Datum/eindparaaf

Kopie aan

Datum/paraaf

Oordeel Toezicht 2021
Jaarlijks koppel ik aan u mijn bevindingen ten aanzien van de stand van zaken van de integrale beveiliging van de NCTV terug.

In de toezichtronde over 2021 heb ik de door u opgeleverde voortgang getoetst. Mijn bevindingen zijn mede gebaseerd op de afstemming tijdens het proces en over de aangeleverde informatie met uw

Uw Jaarrapportage over 2021 geeft een uitgebreid beeld van de staat van de Integrale Beveiliging bij uw onderdeel. De Integrale Beveiliging krijgt op al haar aspecten ruim voldoende aandacht en er worden duidelijke vorderingen gemaakt. Terecht constateert u dat er afhankelijkheden zijn en wordt op sommige dossiers (EBI) door de afhankelijkheden zelfs niet het gewenste resultaat geboekt. In samenspraak met uw kan ik deze punten bespreekbaar maken met de betrokken partijen. Tot slot beveel ik u aan om de SRA in 2022 verder te verdiepen om zo eventuele aanvullende aandachtspunten in beeld te krijgen. U had reeds dit voornemen, maar door COVID heeft dit niet plaats kunnen vinden in 2021.

Voor uw organisatieonderdeel is mijn oordeel dat de voortgang op basis van de aangeleverde informatie voldoende is.

Ten aanzien van de bevordering van het beveiligingsbewustzijn is mijn bureau bezig om in samenwerking met de andere disciplines op het gebied van integrale beveiliging in mei 2022 een week van de integrale beveiliging te organiseren. Aandacht voor de integrale beveiliging is belangrijk omdat de collega's de belangrijkste schakel vormen in het veilig omgaan met informatie, het beschermen van de privacy van burgers en er voor zorgen dat informatie niet in verkeerde handen komt. Daarnaast gaat het ook om het borgen van je persoonlijke veiligheid. Binnen diverse onderdelen worden initiatieven ontplooid om hier aandacht aan te besteden en ook mijn bureau geeft op regelmatige basis voorlichting aan afdelingen, nieuw aangetreden collega's en op verzoek bij de onderdelen.

In T2 2022 zal ik voor heel JenV een rode draden rapportage opstellen voor de die ik ter informatie eveneens zal aanbieden aan de Brede Bestuursraad en het Strategisch Bestuurlijk Beraad.

Mijn bureau biedt ondersteuning aan bij het uitvoeren van de benodigde stappen in de Toezichtcyclus. In de eerste helft van 2022 zal ik met alle onderdelen toezichtsgesprekken voeren. Hierbij kijken we in gezamenlijkheid terug, besteden we aandacht aan de integrale beveiliging en wil ik graag met u de functie van de verder bespreken aan de hand van het en -besluit.

Tot slot maak ik u graag nog attent op de geactualiseerde missie en visie van mijn bureau. In de bijlage treft u deze aan. Graag licht ik die in het toezichtgesprek kort toe.

Wanneer u naar aanleiding van deze nota nog vragen heeft of u een gesprek wilt over andere beveiliging gerelateerde zaken, kunt u uiteraard altijd contact met mij opnemen.

Achtergrond:
Het toezicht is ingericht met de driejaarlijkse toezichtcyclus uit het Toezichtkader 2018-2021 JenV (Brede Bestuursraad 2 februari 2018). Het toezicht richt zich op het uitvoeren van de analyse, de veranderingen, verbeterpunten en verbeterplannen en de werking in de praktijk. Deze cyclus is door een groot deel van de organisatieonderdelen inmiddels één keer volledig doorlopen. Voor een aantal onderdelen geldt dat zij de cyclus inmiddels in hun eigen ritme doorlopen.

Via de jaarplanaanschrijving heb ik u verzocht de door uw MT vastgestelde voortgang van de van toepassing zijnde fase uit de cyclus eind 2021 of in januari 2022 aan te bieden.

Ministerie van Justitie en Veiligheid
Ministerie Binnenlandse Zaken en Koninkrijksrelaties

Datum
9 mei 2022

Ons kenmerk

nota

De Nationaal Coördinator Terrorismebestrijding en Veiligheid
dhr. P.J. Aalbersberg EMPM

Ministerie van Justitie en Veiligheid
Ministerie Binnenlandse Zaken en Koninkrijksrelaties

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon

Datum
1 november 2021

Ons kenmerk

Toezicht integrale beveiliging 2020

Van

Datum/eindparaaf

Kopie aan

Datum/paraaf

Concipiënt

Datum/paraaf

Oordeel Toezicht 2020
Hierbij ontvangt u mijn bevindingen ten aanzien van de stand van zaken van de integrale beveiliging van de NCTV.

In de toezichtsronde over 2020 heb ik de door u opgeleverde voortgang getoetst. Mijn bevindingen zijn mede gebaseerd op het toezichtsgesprek dat wij in de eerste helft van 2021 hebben gehad en de afstemming tijdens het proces en over de aangeleverde informatie met

Bij uw onderdeel zijn meerdere TBB-en onderscheiden en hiervoor is eerder een SRA opgesteld. Uw MT heeft de wens geuit om de SRA analytischer te bekijken en verder te verdiepen. Deze aanpak onderschrijf ik. In 2020 zijn interviews voor de KWAS gehouden en is de inventarisatie geactualiseerd om de SRA aan te vullen. Door COVID is dit laatste nog niet gedaan en wordt dit in 2021 verder vorm gegeven. Daarnaast constateer ik dat integrale beveiliging hoog bij u op de agenda staat en permanent invulling krijgt.

Voor uw organisatieonderdeel is mijn oordeel dat de voortgang op basis van de aangeleverde informatie voldoende is.

Ministerie van Justitie en Veiligheid
Ministerie Binnenlandse Zaken en Koninkrijksrelaties

Datum
1 november 2021

Ons kenmerk

In 2020 is door de gehele situatie rondom corona sprake van een andere aanpak bij bevordering van het beveiligingsbewustzijn. Ik hoop dat de situatie in de 1e helft van in 2022 zich er voor leent om wederom dagen te organiseren. Immers, de collega's vormen de belangrijkste schakel in de integrale beveiliging. Veilig omgaan met informatie, privacy van burgers beschermen en zorgen dat informatie niet in verkeerde handen komt moet onderdeel zijn van ons ambtelijk vakmanschap. Maar ook bewustzijn van het borgen van je persoonlijke veiligheid. Mijn bureau geeft op regelmatige basis voorlichting aan afdelingen, nieuw aangetreden collega's en op verzoek bij de onderdelen.

In T3 2021 zal ik voor heel JenV een rode draden rapportage opstellen voor de , die ik ter informatie eveneens zal aanbieden de Brede Bestuursraad en het Strategisch Bestuurlijk Beraad.

Mijn bureau biedt eveneens ondersteuning aan bij het uitvoeren van de benodigde stappen in de Toezichtcyclus. In 2021 heb ik met alle onderdelen toezichtsgesprekken gevoerd. Hierbij hebben we in gezamenlijkheid terug gekeken naar 2019 en ook 2020 kort in beschouwing genomen. Ik zal in de 1e helft van 2022 wederom een toezichtgesprek met u in laten plannen.

Wanneer u naar aanleiding van deze nota nog vragen heeft of u een gesprek wilt over andere beveiliging gerelateerde zaken, kunt u uiteraard altijd contact met mij opnemen.

Achtergrond:
Om het aantal uitvraagmomenten en de administratieve last te beperken ben ik in 2018 gestart met de driejaarlijkse toezichtcyclus uit het Toezichtkader 2018-2021 JenV (Brede Bestuursraad 2 februari 2018). Het toezicht richt zich op het uitvoeren van de analyse, de veranderingen, verbeterpunten en verbeterplannen en de werking in de praktijk. De cyclus is door een groot deel van de organisatieonderdelen inmiddels één keer volledig doorlopen. Voor een aantal onderdelen geldt dat zij de cyclus in een hun eigen ritme doorlopen.

Ik heb u via de jaarplanaanschrijving voor 2020 verzocht mij de door uw MT vastgestelde voortgang van de weerstandtesten eind 2020 of begin 2021 aan te bieden.