STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 15497
12 juni
2013

Besluit van de Minister-President, Minister van Algemene Zaken van 1 juni 2013, nr. 3124134, houdende voorschrift informatiebeveiliging Rijksdienst – bijzondere informatie 2013

De Minister-President, Minister van Algemene Zaken,

Handelend in overeenstemming met het gevoelen van de ministerraad,

Besluit:

Artikel 1 Begripsbepalingen

In dit besluit wordt verstaan onder:
a. *Bijzondere informatie:* informatie waar kennisname door niet geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries;
b. *Compromittering:* kennisname dan wel mogelijkheid tot kennisname van bijzondere informatie door niet geautoriseerden;
c. *Rubriceren:* bepalen van het rubriceringsniveau en -duur van de bijzondere informatie op basis van de te verwachten nadelige gevolgen voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries als (een deel van) deze informatie bekend wordt bij niet geautoriseerden;
d. *Rubriceringsniveau:* aanduiding van de verwachte nadelige gevolgen aan de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries als (een deel van) de informatie bekend wordt bij niet geautoriseerden;
e. *Rubriceringsambtenaar:* ambtenaar bevoegd tot het vaststellen van rubriceringen, hiertoe aangewezen door de secretaris-generaal;
f. *Vaststeller van de rubricering:* minister, staatssecretaris, secretaris-generaal of een door de secretaris-generaal aangewezen rubriceringsambtenaar;
g. *Rijksdienst:* alle organisatieonderdelen waarvoor de ministeriële verantwoordelijkheid onverkort geldt.
h. *Zorgdrager:* degene die bij of krachtens de wet belast is met de zorg voor de archiefbescheiden.

Artikel 2 Plaatsbepaling en reikwijdte

1. Dit voorschrift met de bijbehorende toelichting en bijlage 1 geldt voor de Rijksdienst, waartoe gerekend worden de ministeries met de daaronder ressorterende diensten, bedrijven en instellingen.

2. Op de beveiliging van bijzondere informatie zijn de bepalingen van dit voorschrift als aanvulling op het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR 2007) en het Beveiligingsvoorschrift Rijk 2013 (BVR 2013) van toepassing.

3. Bijzondere informatie die krachtens een internationaal verdrag of overeenkomst is verkregen, behoudt de toegekende rubricering en wordt beveiligd volgens het overeenkomstige nationale beveiligingsniveau. Voor zover voor de beveiliging van dergelijke informatie als gevolg van het verdrag of de overeenkomst afwijkende of verdergaande beveiligingsbepalingen bestaan worden deze bepalingen toegepast.

Artikel 3 Beveiligingsbeleid

Het beveiligingsbeleid dat door de secretaris-generaal wordt vastgesteld omvat ten minste de ministeriële uitgangspunten voor de beveiliging van, de toegang tot, het omgaan met en verwerken van bijzondere informatie zoals bedoeld in dit voorschrift en de wijze waarop:
a. het ministerie informatie rubriceert;
b. de secretaris-generaal vooraf toestemming verleent voor het verwerken van bijzondere informatie;
c. het ministerie toezicht uitoefent op de beveiliging van bijzondere informatie.

Artikel 4 Rubriceringen

1. Informatie waarvan de geheimhouding vanwege het belang van de Staat, zijn bondgenoten of van één of meer ministeries is geboden, moet worden voorzien van een passend niveau van rubricering.

2. Bijzondere informatie wordt als volgt gerubriceerd:
   a. Staatsgeheim ZEER GEHEIM (afgekort Stg.ZG)
      Indien kennisname door niet geautoriseerden zeer ernstige schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten
   b. Staatsgeheim GEHEIM (afgekort Stg.G)
      Indien kennisname door niet geautoriseerden ernstige schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten
   c. Staatsgeheim CONFIDENTIEEL (afgekort Stg.C)
      Indien kennisname door niet geautoriseerden schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten
   d. Departementaal VERTROUWELIJK (afgekort Dep.V.).
      Indien kennisname door niet geautoriseerden schade kan toebrengen aan de belangen van één of meerdere ministeries.

3. De opsteller van de informatie doet een voorstel tot rubricering en brengt deze aan op de informatie. De vaststeller van de inhoud van de informatie stelt tevens de rubricering vast.

Artikel 5 Herzien en beëindigen van de rubricering

1. Rubriceringen worden verbonden aan een maximum tijdsverloop of aan een bepaalde gebeurtenis. Na die periode of na die gebeurtenis weegt de vaststeller voor bijzondere informatie af of herziening, dan wel beëindiging van de rubricering, aan de orde is.

2. Van het eerste lid van deze bepaling kan worden afgeweken in die gevallen waarin de rubricering betrekking heeft op:
   a. Bijzondere informatie die krachtens een internationaal verdrag of overeenkomst is verkregen;
   b. Staatsgeheimen die door de wet als zodanig zijn aangewezen.

3. Uitsluitend de vaststeller van de rubricering is bevoegd de rubricering te herzien of te beëindigen.

4. Bij overbrenging van bijzondere informatie naar een rijksarchiefbewaarplaats als bedoeld in de Archiefwet 1995 vervalt de rubricering, tenzij de zorgdrager, na advies van de algemene rijksarchivaris, bepaalt dat deze gehandhaafd dan wel herzien moet worden.

Artikel 6 Eisen aan de beveiliging

1. Bijzondere informatie wordt zodanig beveiligd dat:
   a. alleen personen die daartoe zijn geautoriseerd deze kunnen behandelen of inzien voor zover dit noodzakelijk is voor een goede uitoefening van hun taak en
   b. dat inbreuken op de beveiliging worden gedetecteerd en gedegen onderzoek naar (mogelijke) inbreuken mogelijk is.

2. De beveiliging is ingericht op basis van risicomanagement.

3. Bijzondere informatie die krachtens een internationaal verdrag of een internationale overeenkomst is verkregen wordt uitsluitend verwerkt nadat de autoriteit, die krachtens het betreffende verdrag verantwoordelijk is voor de beveiligingsregels ter bescherming van bijzondere informatie, haar goedkeuring aan de beveiliging heeft gegeven.

Artikel 7 Buiten de rijksdienst brengen van bijzondere informatie

1. Bij het buiten de rijksdienst brengen van bijzondere informatie, anders dan op grond van een wettelijke verplichting tot openbaarmaking, blijven de eisen aan de beveiliging en het toezicht daarop onverkort van kracht.

2. Bijzondere informatie die krachtens een internationaal verdrag of een internationale overeenkomst is verkregen wordt uitsluitend na voorafgaande toestemming van het land of de internationale organisatie van herkomst doorgegeven aan externe partijen.

Artikel 8 Compromittering van bijzondere informatie

1. Elke ambtenaar is verplicht de Beveiligingsambtenaar (BVA) onmiddellijk mededeling te doen van een inbreuk op de beveiliging die redelijkerwijs kan leiden, dan wel vermoedelijk of vaststaand heeft geleid, tot compromittering van bijzondere informatie.

2. De BVA laat, nadat hij op de hoogte is gebracht van een inbreuk op de beveiliging, onmiddellijk

(nood)maatregelen treffen om verdere inbreuk te voorkomen.

3. De BVA onderzoekt of compromittering van bijzondere informatie heeft plaatsgevonden; indien dit het geval is doet hij hiervan mededeling aan de secretaris-generaal en adviseert over de noodzaak tot het instellen van een commissie van onderzoek.

4. Indien de compromittering betrekking heeft op bijzondere informatie die is verkregen van een ander ministerie of krachtens internationaal verdrag of overeenkomst, doet de BVA bovendien mededeling aan dat betreffende ministerie of de krachtens het verdrag of de overeenkomst voor de beveiliging van die bijzondere informatie verantwoordelijke instantie.

Artikel 9 Commissie van onderzoek

1. Een commissie van onderzoek wordt ingesteld door de secretaris-generaal.

2. De commissie stelt een onderzoek in naar:
   a. de wijze waarop de compromittering heeft plaatsgevonden;
   b. de aard en de omvang van de schade aan de belangen van de Staat of zijn bondgenoten;
   c. de te nemen maatregelen om de schade te beperken en herhaling te voorkomen.

3. De commissie voert, indien de gecompromitteerde bijzondere informatie (mede) afkomstig is van een ander ministerie, haar onderzoek uit in overleg met de BVA van dat ministerie. In het geval dat de gecompromitteerde bijzondere informatie krachtens een internationaal verdrag of overeenkomst is verkregen voert de commissie haar onderzoek uit in samenwerking met de instantie die krachtens het verdrag of de overeenkomst verantwoordelijk is voor de beveiliging ervan.

4. De secretaris-generaal of een door hem aangewezen ambtenaar treft, op basis van de bevindingen van de commissie van onderzoek, maatregelen om de schade die de compromittering heeft toegebracht aan de veiligheid of andere gewichtige belangen van de Staat of zijn bondgenoten te beperken en herhaling van de compromittering te voorkomen.

5. Indien het de compromittering van een staatsgeheim betreft stelt de secretaris-generaal het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst in kennis van de uitkomsten van het onderzoek. Bij het ministerie van Defensie wordt de Militaire Inlichtingen- en Veiligheidsdienst op de hoogte gesteld van de uitkomsten van het onderzoek.

Artikel 10 Slotbepaling

1. Het Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie van 24 februari 2004 wordt ingetrokken.

2. Rubriceringen die zijn vastgesteld vóór inwerkingtreding van dit voorschrift worden uiterlijk tien jaar na vaststelling door de vaststeller onderzocht op de mogelijkheid om de rubricering te herzien of te beëindigen.

3. Dit besluit en de daarbij behorende bijlagen treden in werking met ingang van 1 juni 2013.

4. Dit besluit wordt aangehaald als: Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013).

5. Dit besluit zal met de toelichting in de Staatscourant worden geplaatst. Van de ter inzage legging van de bij dit besluit behorende bijlagen zal mededeling worden gedaan in de Staatscourant.

De Minister-President, Minister van Algemene Zaken,
M. Rutte.

BIJLAGE 1. UITGANGSPUNTEN EN MINIMUM NIVEAU BEVEILIGING

Deze bijlage beschrijft de uitgangspunten en het minimum beveiligingsniveau voor de beveiliging van bijzondere informatie. Bij de inrichting van een adequaat stelsel van beveiligingsmaatregelen voor de beveiliging van bijzondere informatie moet binnen het in de artikelen beschreven principe van risicomanagement worden uitgegaan van de volgende inrichtingsprincipes:

- Beveiliging in lagen: De beveiliging zal bestaan uit meerdere lagen, zodat er geen afhankelijkheid is van één beveiligingsmaatregel.
- Minste privilege: Alleen de autorisaties die iemand nodig heeft om zijn taak te kunnen vervullen, zullen worden toegekend;
- Zelf beschermende systemen: Ieder systeem beschouwt andere systemen als onvertrouwd totdat het tegendeel is bewezen en treft maatregelen om veilig informatie uit te kunnen wisselen met wel vertrouwde systemen indien deze communicatie via onvertrouwde systemen verloopt.
- Verificatie implementatie beveiliging: De maatregelen voor beveiliging van bijzondere informatie worden onder de verantwoordelijkheid van de BVA of de accreditatieautoriteit periodiek gecontroleerd.

Deze inrichtingprincipes moeten stringenter worden toegepast naarmate het niveau van de rubricering toeneemt.

Voor de volgende onderwerpen, die grotendeels afkomstig zijn uit de Code voor Informatiebeveiliging, zijn specifiek op bijzondere informatie toegesneden doelstellingen en eisen geformuleerd waaraan dient te worden voldaan. Waar aan de orde zijn daarbij ook maatregelen benoemd die ten minste deel uit moeten maken van de totale set van maatregelen om de vertrouwelijkheid van bijzondere informatie te waarborgen.
Hiermee is voor alle betrokkenen inzichtelijk gemaakt wat minimaal wordt verlangd op het gebied van beveiliging voor de verschillende rubriceringen op grond van dit voorschrift. Tevens is op efficiënte wijze de toepassing van een uniforme set van minimale maatregelen gedefinieerd waardoor waarborgen zijn gecreëerd voor een consistente beveiliging van bijzondere informatie.

1. Management van bedrijfsmiddelen

Doelstelling

Het handhaven van een adequaat, ordelijk en controleerbaar beheer van bedrijfsmiddelen waarop bijzondere informatie wordt verwekt.

Eis

Bedrijfsmiddelen waarop bijzondere informatie wordt verwerkt, dienen te zijn geregistreerd en aan een 'eigenaar" te zijn toegewezen. Daarbij is onderkend welke van deze bedrijfsmiddelen specifieke beveiligingsmaatregelen behoeven.

		Dep.V	Stg.C	Stg.G	Stg.ZG
A	Maatregel Registreer alle middelen en de personen aan wie deze zijn uitgereikt.			*V*	*V*
B	Maatregel Registreer de locatie/standplaats van alle middelen en de toewijzing aan een eigenaar.			*V*	*V*

2. Personen

Doelstelling

Organisaties moeten zekerstellen dat personen hun verantwoordelijkheden kennen en geschikt zijn voor de rol die zij vervullen evenals het beperken van de risico's van menselijk handelen.

Eis

Elk persoon die frequent gaat werken met bijzondere informatie, dient voorafgaand aan indiensttreding een aan zijn functievervulling gerelateerd betrouwbaarheidsonderzoek te ondergaan. Voor het bepalen of een functie als vertrouwensfunctie moet worden aangewezen, dient de betreffende leidraad aanwijzen vertrouwensfuncties van de AIVD (civiele sector) en MIVD (militaire sector) te worden gevolgd.
Bij beëindiging of wijziging van het dienstverband waarin gewerkt is met bijzondere informatie, wordt zeker gesteld dat de geheimhoudingsplicht geborgd is.

Van elk persoon die frequent werkt met bijzondere informatie moet geborgd zijn dat deze over een aan zijn functievervulling gerelateerd, actueel betrouwbaarheidsonderzoek beschikt.

		Dep.V	Stg.C	Stg.G	Stg.ZG
A	Maatregel Personen die hebben te maken met bijzondere informatie, dienen een geheimhoudingsverklaring te ondertekenen. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.	*V*	*V*	*V*	*V*
B	Maatregel Personen die frequent hebben te maken met bijzondere informatie dienen tevens te beschikken over een passende verklaring.	VOG[1]	VGB[2]	VGB[2]	VGB[2]
C	Maatregel 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.	*V*	*V*	*V*	*V*

1 Verklaring omtrent het gedrag
2 Verklaring van geen bezwaar conform de Wet op de veiligheidsonderzoeken

3. Fysieke en omgevingsbeveiliging

Doelstelling

Het waarborgen van toereikende weerstand tegen (pogingen tot) ongeautoriseerde fysieke toegang van locaties, gebouwen en ruimtes (waaronder kluizen) waar zich bijzondere informatie bevindt.

Eis

Voor elke locatie, gebouw en ruimte waar zich bijzondere informatie bevindt, dient systematisch de beveiligingsmaatregelen in beeld te zijn gebracht voor fysieke toegangsbeheersing. Hierbij is ten minste voorzien in:
- Het aanbrengen van zonering c.q. compartimentering.
- Het detecteren van ongeautoriseerde toegangen of pogingen daartoe.
- Het regelen van een ordelijk toegangsbeleid en sleutelbeheer.
- Het uitoefenen door bewakingspersoneel van toezicht buiten reguliere werktijden.
- Het toewijzen van ruimten waar met bijzondere informatie mag worden gewerkt.

Ten aanzien van zonering kunnen de diverse beveiligingszones worden onderkend, waarbij om toegang te krijgen tot ruimtes waarin bijzondere informatie wordt verwerkt, steeds zwaardere beveiligingsmaatregelen worden getroffen.

		Dep.V	Stg.C	Stg.G	Stg.ZG
A	Maatregel Bijzondere informatie wordt zodanig behandeld en opgeslagen dat er een positief beveiligingsrendement[1] is, op basis van schadeacceptatie en het dreigingsprofiel.	*V*	*V*	*V*	*V*
B	Maatregel Tempestmaatregelen conform Beleidsadvies Compromitterende straling (VBV 32000).		*V*	*V*	*V*
C	Maatregel Tegengaan van afluisteren, zicht op en reflectie van informatie (bv via beeld-schermen of spiegelende oppervlakten).		*V*	*V*	*V*
D	Maatregel 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.	*V*	*V*	*V*	*V*
E	Maatregel Bezoekers worden begeleid wanneer zij ruimten waarin bijzondere informatie aanwezig is, betreden.		*V*	*V*	*V*
F	Maatregel Bezoekers 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.).			*V*	*V*

1 Zie hiervoor toelichting artikel 3 onder b.

4. Logische toegangsbeveiliging

Doelstelling

Het waarborgen van een beheerste en gecontroleerde toegang tot ICT-voorzieningen waarin zich bijzondere informatie bevindt.

Eisen

Voorzie in procedures en regels voor toegangsrechten tot en monitoring van netwerkdiensten, besturingssystemen en applicaties waar zich gerubriceerde informatie bevindt.

Voorzie in een stelsel van logische toegangsbeveiligingsmaatregelen dat is gerelateerd aan de relevante dreiging en het rubriceringniveau.

		Dep.V	Stg.C	Stg.G	Stg.ZG
A	Maatregel Toegang tot een account wordt na een aantal direct achtereenvolgende foutieve inlogpogingen geblokkeerd.	5	3	3	3
B	Maatregel Toegang tot systemen kan op groepsniveau worden bepaald.	*V*	*V*	*V*	niet toegestaan
C	Maatregel Toegang tot bijzondere informatie wordt op individueel niveau bepaald.			*V*	*V*

5. Levenscyclus ICT-voorzieningen

Doelstelling

Het waarborgen van een passend niveau van beveiliging gedurende de gehele levenscyclus van ICT-voorzieningen waarin bijzondere informatie wordt verwerkt.

Eis

Voorafgaand aan verwerving, ontwikkeling, onderhoud en afstoot van informatiesystemen waarin bijzondere informatie wordt verwerkt, dienen de dreigingen en risico's in beeld te zijn gebracht.

		Dep.V	Stg.C	Stg.G	Stg.ZG
A	Maatregel Gedurende de gehele levenscyclus van een systeem worden periodieke audits, inspecties, reviews en tests uitgevoerd om te controleren of de beveiligingsmaatregelen effectief zijn. Deze controles worden uitgevoerd door deskundige specialisten die beschikken over de juiste onderzoeksmiddelen en beproefde onderzoeksmethoden.	Self assess-ment	Self assess-ment	Onafhankelijke deskundige	Onafhankelijke deskundige
B	Maatregel De verantwoordelijkheden en procedures voor het adequaat beheer en juist gebruik van de ICT-voorzieningen waarin bijzondere informatie wordt verwerkt, zijn vastgesteld.	*V*	*V*	*V*	*V*
C	Maatregel Voor het beheer van ICT-voorzieningen is het beveiligingsniveau in overeenstemming met de risico's.	*V*	*V*	*V*	*V*
D	Maatregel Bij uitbesteding van (delen van) de dienstverlening dient een zelfde beveiligingsniveau te worden gerealiseerd als geldt bij de interne dienstverlening.	*V*	*V*	*V*	*V*

6. Verzending van gerubriceerde informatie

Doelstelling

Het waarborgen van een wederzijds verenigbaar beveiligingsniveau voor de vertrouwelijkheid van bijzondere informatie.

Eisen

Er dient te zijn voorzien in een passende set van verenigbare maatregelen indien bijzondere informatie het ministerie verlaat.

De vertrouwelijkheid van informatie moet tijdens (elektronisch) transport buiten gecontroleerd gebied gehandhaafd blijven

		Dep.V	Stg.C	Stg.G	Stg.ZG
A	Maatregel Digitale verzending van bijzondere informatie dient met ministerieel goedgekeurde cryptografische middelen te geschieden. De ministeriële goedkeuring vindt plaats op basis van advies van de Werkgroep Bijzondere Informatiebeveiliging (WBI) of diens rechtsopvolger over de beveiligingswaarde van de cryptografische middelen.		*V*	*V*	*V*
B	Maatregel Digitale verzending van informatie die krachtens een internationaal verdrag of een internationale overeenkomst is verkregen, dient met door de verstrekkende instantie goedgekeurde cryptografische middelen te worden verzonden.			*V*	*V*
C	Maatregel Fysieke verzending van bijzondere informatie dient te geschieden met ministerieel goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.	*V*	*V*	*V*	*V*
D	Maatregel 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.		*V*	*V*	nvt
E	Maatregel Nationale verzending uitsluitend via een overheidskoerier.				*V*
F	Maatregel Internationale verzending uitsluitend als diplomatieke koeringszending of militair transport.				*V*
G	Maatregel Zowel digitaal als niet digitaal is er een onweerlegbare bevestiging van ontvangst.		*V*	*V*	*V*
H	Maatregel Beveiligingsrelevante handelingen worden geregistreerd.	*V*	*V*	*V*	*V*
I	Maatregel 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.			*V*	*V*
J	Maatregel Elk document moet tenminste bij verspreiding voorzien zijn van: • Rubriceringsniveau; • Rubriceringsduur; • Bladzijdenummering en totaal aantal bladzijden waaruit het document bestaat;	*V*	*V*	*V*	*V*
K	Maatregel Elk document wordt voorzien van: • Exemplaarnummer.		*V*	*V*	*V*
L	Maatregel Van alle exemplaren van bijzondere documenten worden de volgende gegevens vastgelegd: • Exemplaarnummer; • Maker; • Ontvanger.		*V*	*V*	*V*
M	Maatregel Er worden niet meer kopieën van bijzondere informatie gemaakt dan strikt noodzakelijk.		*V*	*V*	*V*

TOELICHTING OP DE ARTIKELEN VIRBI 2013

Artikel 1 Begripsbepalingen

Onder a:
Dit voorschrift gebruikt de term informatie onafhankelijk van het gebruikte medium en onafhankelijk of de informatie is vastgesteld. Het voorschrift betreft dus informatie in ruste (bijvoorbeeld opgenomen in documenten of databases), in bewerking (bijvoorbeeld in het geheugen van een computer) of in communicatie (telefoongesprekken, vergaderingen, datacommunicatie, andere elektromagnetische signalen.
Kennisname van bijzondere informatie dient beperkt te blijven tot geautoriseerde personen. Autorisatie vraagt om een expliciete en aantoonbare toestemming, waarbij de eisen aan de autorisatieprocedure met het rubriceringsniveau toenemen. Het is bij het verlenen van autorisatie niet voldoende dat een beoogde ontvanger over een verklaring van geen bezwaar van het juiste niveau beschikt. Er dient een afzonderlijke afweging gemaakt te worden over de functionele noodzaak tot kennisname door de betrokken persoon.

Onder b:
In de toelichting op de artikelen 8 en 9 wordt nader ingegaan op compromittering.

Onder c:
Voordat aan informatie een rubricering en rubriceringsduur kan worden toegekend, worden eerst afwegingen gemaakt over de te voorziene nadelige gevolgen die met een redelijke kans op kunnen treden; dit is nader uitgewerkt in de toelichting op artikel 4. De betekenis van de rubriceringsduur is nader uitgewerkt in de toelichting bij artikel 5, lid 1.

Onder d:
Er bestaan vier rubriceringsniveaus. De rubriceringen verschillen in de ernst van de nadelige gevolgen die zijn voorzien bij ongeautoriseerde kennisname. De toelichting op artikel 4 gaat hier nader op in.

Onder e:
De secretaris-generaal kan rubriceringsambtenaren aanwijzen die namens hem de rubricering vast kunnen stellen. In de regel zijn dit de hogere lijnfunctionarissen, de BVA en zijn plaatsvervanger of andere inhoudelijk deskundigen.

Onder h:
Op grond van artikel 23, eerste lid van de Archiefwet 1995 dragen de ministers zorg voor de archiefbescheiden die niet zijn overgebracht naar een rijksarchiefbewaarplaats. Als zorgdrager heeft de minister de bevoegdheid bij overbrenging beperkingen aan de openbaarheid te stellen.

Artikel 2 Plaatsbepaling en reikwijdte

Lid 1:
De artikelen bevatten op hoofdlijnen de werkwijze voor de behandeling van bijzondere informatie en de wijze van rubriceren. De uitwerking heeft dezelfde zeggingskracht en geeft nadere aanwijzingen over de inrichting van de rubricering en de verwerking van bijzondere informatie.

Tot de Rijksdienst behoren alle organisatieonderdelen waarvoor de ministeriële verantwoordelijkheid onverkort geldt. Het VIRBI 2013 heeft geen directe werking buiten de Rijksdienst (publieke en private partijen), waaronder ook zelfstandige bestuursorganen. Het kan echter noodzakelijk zijn om bijzondere informatie buiten de Rijksdienst te brengen. Het voorschrift staat dit alleen toe als voldoende zekerheid bestaat dat de informatie in overeenstemming met dit voorschrift wordt beveiligd. Centraal staat hierbij het waarborgen van de vertrouwelijkheid middels proportionele maatregelen. In het ministeriële beveiligingsbeleid (artikel 3) dient dit verder te worden uitgewerkt. Regels voor het buiten de rijksdienst brengen van bijzondere informatie worden gegeven in artikel 7.

Lid 2:
Het VIRBI 2013 is het raamwerk in aanvulling op het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR 2007) en BVR 2013. Het geeft de regels voor de Rijksdienst voor de beveiliging van bijzondere informatie.
Het VIR 2007 geeft de regels voor de informatiebeveiliging voor de Rijksdienst. Het is een raamwerkregeling in de zin dat de werkwijze om tot een verantwoorde beveiliging te komen bepaald is, zonder een minimaal beveiligingsniveau voor de Rijksdienst op te leggen. Het BVR 2013 geeft de regels voor de integrale beveiliging voor de Rijksdienst.

Waar het VIR betrekking heeft op de gehele beveiliging van informatiesystemen, is alleen de vertrouwelijkheid van informatie het onderwerp van het VIRBI 2013. Dit houdt in dat voor de bescherming van de integriteit en beschikbaarheid van de informatie in informatiesystemen afwegingen in overeenstemming met het VIR gemaakt moeten worden. Dit geldt ook voor de bescherming van de vertrouwelijkheid van informatie die niet is gerubriceerd.

Lid 3:
Bijzondere informatie van internationale herkomst behoudt zijn oorspronkelijke rubricering. Dit houdt in dat de oorspronkelijke rubricering niet vervangen mag worden door een Nederlandse rubricering. Op dergelijke bijzondere informatie is primair niet het VIR-BI, maar een internationaal verdrag van toepassing. In dergelijke verdragen is opgenomen dat, behoudens enkele uitzonderingen, de nationale regelgeving wordt gevolgd:

1. Het VIRBI 2013. Het ministerie draagt zelf zorg voor een afdoende beveiliging en verantwoording.
2. Het internationaal verdrag kan een aantal uitzonderingen geven. Deze komen neer op een uiterst beperkte ruimte voor risicomanagement en gescheiden verwerking van nationale en internationale bijzondere informatie.
3. Toestemming voor ontvangst, beheer, verwerking en verdere verspreiding van dergelijke informatie dient verkregen te worden van de Security Accreditation Authority (SAA). De Secretaris-generaal van het ministerie is de SAA voor civiele omgevingen en de beveiligingsautoriteit van het ministerie van Defensie voor defensieomgevingen. Deze zijn verantwoordelijk om voorafgaand aan een toestemmingverlening (accreditatie), te (laten) onderzoeken of de beveiliging van de informatie voor wat betreft de bescherming van de internationale belangen aan de vereisten voldoet. De National Security Authority (NSA), respectievelijk civiel en militair, voert de controle op de beveiliging uit en verzorgt de verdere afhandeling naar de internationale organisaties. Het ministerie blijft zelf verantwoordelijk voor een afdoende beveiliging van de nationale belangen (voor zowel beschikbaarheid, integriteit als de vertrouwelijkheid). De 'Information Assurance'-functies die door de EU en NATO worden onderscheiden, zijn en worden met het instellingsbesluit van de Werkgroep Bijzondere Informatiebeveiliging (WBI) of haar rechtsopvolger toegewezen (IA-autoriteit, Tempest-autoriteit, Crypto Approval-autoriteit en Cryptodistributie-autoriteit).

Met betrekking tot NAVO en EU informatie wordt de volgende vergelijkingstabel gehanteerd om tot het vergelijkbaar nationaal niveau te komen:

Nederland	NAVO	EU
Dep. VERTROUWELIJK	NATO RESTRICTED	RESTREINT UE/EU RESTRICTED
Stg. CONFIDENTIEEL	NATO CONFIDENTIAL	CONFIDENTIEL UE/EU CONFIDENTIEL
Stg. GEHEIM	NATO SECRET	SECRET UE/EU SECRET
Stg. ZEER GEHEIM	COSMIC TOP SECRET	TRÈS SECRET UE/EU TOP SECRET

Met betrekking tot informatie die bilateraal uit andere landen wordt ontvangen, wordt dit conform de bilaterale overeenkomst behandeld. Indien er geen bilaterale overeenkomst is, kan middels de bovenstaande tabel een vergelijkbaar nationaal niveau bepaald worden voor de beveiliging, in afstemming met de eigenaar van de informatie.

Het kan noodzakelijk zijn om aan informatie gelijktijdig zowel nationale als internationale rubriceringen toe te kennen. Indien bijvoorbeeld documenten zijn samengesteld met informatie uit verschillende bronnen met verschillende rubriceringen dan behoudt de informatie iedere oorspronkelijke rubricering van de broninformatie.

Artikel 3 Beveiligingsbeleid

Dit artikel geeft met betrekking tot bijzondere informatie aanvullende bepalingen ten opzichte van de eisen die het VIR 2007 in artikel 3 aan het beveiligingsbeleid stelt. Het ministeriële beleid geeft de aanwijzingen voor de wijze waarop de medewerkers met bijzondere informatie omgaan; het VIRBI 2013 geeft de kaders voor dit ministerieel beleid.

Het VIRBI 2013 bevat, ten opzichte van het VIR 2007, drie aanvullende onderwerpen voor het beleid. De onderwerpen hebben betrekking op de wijze waarop het ministerie informatie rubriceert, de wijze waarop de secretaris-generaal vooraf toestemming verleent voor het verwerken van bijzondere informatie en de wijze waarop het ministerie toezicht uitoefent op de beveiliging van bijzondere informatie. De onderwerpen kunnen onderdeel uitmaken van een integraal beleidsdocument of afzonderlijk worden vastgelegd.

Onder a:

Dit omvat zowel de wijze waarop binnen het ministerie tot rubricering wordt besloten als de te hanteren criteria om tot de juiste rubricering te komen. Belangrijk is hierbij af te wegen dat naarmate het rubriceringsniveau van informatie hoger ligt, de beveiligingseisen toenemen, waarmee de beperkingen door en de kosten van de beveiliging ook navenant toe kunnen nemen.

Onder b:
Het belang dat met bijzondere informatie gemoeid is, maakt een expliciete afweging op centraal niveau noodzakelijk om reeds op voorhand te waarborgen dat de informatieverwerking zorgvuldig geschiedt. Daarom wordt in het beleid vastgelegd hoe vooraf toestemming wordt gegeven voor het verwerken van bijzondere informatie. Onder verwerken wordt verstaan elke handeling of elk geheel van handelingen met betrekking tot informatie, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Mandatering van toestemmingverlening is mogelijk en kan voor verschillende rubriceringsniveaus verschillend worden ingevuld.

Voor bijzondere informatie en informatiesystemen wordt, onder andere ten behoeve van die centrale afweging, in het ministeriële integrale beveiligingsbeleid beschreven op welke wijze bepaald wordt met welke dreigingen (onderkend of voorspelbaar) en welke risico's (voorstelbaar) rekening gehouden moet worden. Alsmede hoe dit overzicht van dreigingen en risico's actueel gehouden wordt.

Voor internationale bijzondere informatie geldt een andere procedure. Voordat dergelijke informatie mag worden verwerkt is in lijn met artikel 6 lid 3 van dit voorschrift, tevens toestemming nodig van de NSA.

Onder c:
Behalve de initiële toestemming voor de verwerking van bijzondere informatie stelt het VIRBI 2013 in de bijlage ook eisen aan het toezicht tijdens de verwerking. Hierbij wordt een minimale frequentie van toezicht gegeven die hoger is naarmate het rubriceringsniveau ook hoger ligt. Ook worden voor Stg. Confidentieel en hoger gerubriceerde informatie eisen gesteld aan de administratie met betrekking tot kennisname.
Zoals in het BVR 2013, artikel 5, lid 1, is vastgelegd is het lijnmanagement verantwoordelijk voor de integrale beveiliging van hun dienstonderdeel. De BVA heeft namens de secretaris-generaal de centrale toezichthoudende rol (BVR 2013, artikel 4, lid 3). De voor het toezicht noodzakelijke onafhankelijke toetsing kan door derden (bijvoorbeeld de auditfunctie van de Rijksdienst) worden ingevuld.

Nadere invulling van de toewijzing van verantwoordelijkheden voor ketens van informatiesystemen

Het VIR bepaalt dat de verantwoordelijkheid voor ketens van informatiesystemen aan lijnmanagers wordt toegewezen. Het VIRBI 2013 stelt eisen aan de beveiliging van bijzondere informatie, ook die in ketens wordt verwerkt.

De functionaris onder wiens verantwoordelijkheid de bijzondere informatie wordt verwerkt zorgt er voor en ziet erop toe dat de beveiliging van de bijzondere informatie in overeenstemming met de eisen wordt ingericht, ook door de lijnmanagers die verantwoordelijk zijn voor de ketens van informatiesystemen voordat de bijzondere informatie daarin wordt opgenomen. Ook waar delen van ketens zich buiten de rijksdienst bevinden dient zekerheid te bestaan dat aan de beveiligingseisen is voldaan.

Artikel 4 Rubriceringen

In de Wet bescherming staatsgeheimen is in de titel aangegeven dat Staatsgeheimen gegevens betreffen waarvan de geheimhouding door het belang van de Staat wordt geboden. In artikel IIA van de Wet bescherming staatsgeheimen is opgenomen dat onder de veiligheid van de Staat ook wordt verstaan de veiligheid van diens bondgenoten. Informatie waarvan de geheimhouding is geboden door het belang van één of meerdere ministeries en niet als Staatsgeheim is gerubriceerd, wordt als Departementaal Vertrouwelijk gerubriceerd.

De inschaling van de rubricering wordt op basis van twee criteria bepaald: schade en belang.

Schade

De mate van schade aan een belang is mede bepalend voor de hoogte van de rubricering. Uitgegaan is van de volgende criteria in oplopende volgorde:
a. Schade: beperkte nadelige invloed;
b. Ernstige schade: nadelige invloed, korte termijn geen alternatieven;
c. Zeer ernstige schade: onmisbaar, geen alternatieven mogelijk.

Belang

De mate van vitaliteit van de belangen voor de Staat of haar bondgenoten of een belang van een of meerdere ministeries is mede bepalend voor de hoogte van de rubricering. Voor de bepaling van de (vitale) belangen van de Staat en/of haar bondgenoten is aangesloten op de vijf onderscheiden vitale belangen in de Strategie Nationale Veiligheid (Tweede Kamer, vergaderjaar 2006–2007, 30 821, nr. 3), die de basis is voor de Rijksbrede aanpak van de nationale veiligheid. Deze vitale belangen zijn als volgt gedefinieerd:
a. territoriale veiligheid: het ongestoord functioneren van Nederland als onafhankelijke staat, en in het bijzonder de territoriale integriteit van het grondgebied en de internationale positie;
b. fysieke veiligheid: het ongestoord functioneren van de mens in Nederland en zijn omgeving;
c. economische veiligheid: het ongestoord functioneren van Nederland als een effectieve en efficiënte economie;
d. ecologische veiligheid: het beschikken over voldoende zelfherstellend vermogen van de leefomgeving bij aantasting;
e. sociale en politieke stabiliteit: het ongestoorde voortbestaan van een maatschappelijk klimaat waarin groepen mensen goed met elkaar kunnen samenleven binnen de kaders van de democratische rechtstaat en gedeelde kernwaarden.

Belang van een of meerdere ministeries betreffen het ongestoord functioneren van het ministerie in de uitvoering van haar taken of ter realisatie van haar doelen.
Conform de transitietabel in de toelichting bij artikel 2, wordt bijzondere informatie gerubriceerd door NAVO en EU beveiligd volgens het overeenkomstige nationale beveiligingsniveau.

Een rubricering kan aangevuld worden door een of meerdere merkingen. Hiermee kan een specifieke beperking van de kring van gerechtigden worden aangegeven. Merkingen staan echter los van de rubricering van de informatie en dit onderwerp is daarom niet opgenomen in deze regeling.

Lid 2, onder a, b en c:
Benadrukt wordt de aansluiting met artikel 98 en verder van het Wetboek van Strafrecht, dat de strafbaarheid regelt van misdrijven met betrekking tot staatsgeheimen, zoals het ongeautoriseerd toegang proberen te verkrijgen tot of het onzorgvuldig behandelen van staatsgeheimen. Artikel 98 en verder van het Wetboek van Strafrecht hanteert de term ‘een inlichting’; de in het VIRBI 2013 gebruikte term ‘informatie’ sluit de term ‘een inlichting’ in.

Lid 2, onder d:
Departementaal Vertrouwelijk gerubriceerde informatie betreft primair het belang van één of meerdere ministeries. De maatschappelijke consequenties als gevolg van ongeautoriseerde kennisname blijven voor dit rubriceringniveau beperkt in tijd en omvang.

Lid 3:
Het vaststellen van rubricering gebeurt expliciet met het vaststellen van de inhoud of de informatie. En eveneens (mondeling) bij vergaderingen of andere gesprekken. Daarnaast kunnen databases en informatiesystemen door de (proces)eigenaar in zijn geheel gerubriceerd worden, waarmee dit ook geldt voor de opgenomen/ingevoerde informatie.

In de conceptfase wordt de informatie behandeld conform het niveau van beveiliging gekoppeld aan het voorstel tot rubricering van de steller, totdat het definitieve niveau van rubricering is bepaald door degene die de inhoud vaststelt, waarna de beveiliging conform het vastgestelde rubriceringsniveau wordt behandeld.

Artikel 5 Herzien en beëindigen van de rubricering

De geheimhouding van bijzondere informatie is noodzakelijk voor een specifieke periode of verbonden aan een bepaalde gebeurtenis, maar zal niet automatisch vervallen. De rubricering wordt daarom altijd aangevuld met een maximum tijdsverloop of bepaalde gebeurtenis, na dit tijdsverloop of de bepaalde gebeurtenis dient de noodzaak tot en de hoogte van de rubricering opnieuw te worden

vastgesteld. Hiermee wordt enerzijds voorkomen dat informatie onnodig lang beveiligd wordt en anderzijds wordt de geheimhouding van informatie geborgd zolang dit noodzakelijk is. Er kan eventueel een verzoek worden ingediend, door personen die geautoriseerd zijn om kennis te nemen van die informatie, bij de vaststeller van de rubricering van de informatie, om te voorkomen dat informatie onnodig gerubriceerd blijft.

Bij een verzoek in het kader van de Wet Openbaarheid Bestuur (WOB) wordt op grond van artikel 5 de rubricering opnieuw beoordeeld. De rubricering van de informatie of delen daarvan moet (en) worden beëindigd als de belangen niet onder de uitzonderingsgronden van de WOB vallen. Informatie die wordt vrijgegeven op basis van een dergelijk verzoek kan immers niet langer gerubriceerd zijn. Indien delen niet worden gederubriceerd, moeten deze onleesbaar worden gemaakt in, dan wel verwijderd uit het vrij te geven document.

Bijzondere informatie die krachtens een internationaal verdrag of overeenkomst is verkregen en Staatsgeheimen die door de wet als zodanig zijn aangewezen, vallen buiten dit regime.
Bijzondere informatie die krachtens een internationaal verdrag is verkregen, heeft per definitie een niet Nederlandse rubricering. De informatie dient overeenkomstig de in het verdrag overeengekomen beveiligingsregime te worden beveiligd. Indien de informatie niet meer nodig is, kan deze worden teruggestuurd of worden vernietigd.
Informatie die door de wet als zodanig is aangewezen, valt eveneens buiten het gestelde in het eerste lid van dit artikel. De Kernenergiewet en het Geheimhoudingsbesluit Kernenergiewet, KB 17 juni 1971 zijn hiervan voorbeelden.

Uitsluitend de vaststeller van de rubricering is bevoegd de rubricering te herzien of te beëindigen. De vaststelling is functie- en niet persoonsgebonden. De vaststeller van de informatie blijft ook na reorganisaties (onderbrengen bij een ander deel van of buiten de Rijksdienst) of overdracht van functies naar een ander deel van of buiten de Rijksdienst, de zorgplicht houden voor de bijzondere informatie, tenzij expliciet vóór een dergelijke reorganisatie of functieoverdracht is bepaald dat de zorgplicht ook over gaat. Indien de zorgplicht niet over gaat, zal de zorgdrager bij een voornemen of plicht tot herziening of beëindiging van de rubricering overleg voeren met de nieuwe procesverantwoordelijke waar de organisatie of functie is ondergebracht.

Omdat uitsluitend de oorspronkelijke rubriceerder mag herrubriceren, behoudt afgeleid werk de oorspronkelijke rubricering van het gebruikte bronmateriaal, tenzij in overeenstemming met de oorspronkelijke rubriceerder een andere rubricering kan worden vastgesteld. Het is dus niet zonder meer toegestaan om uittreksels of overzichten lager te rubriceren dan het bronmateriaal dat hiervoor gebruikt is. Uitsluitend de SG van het ministerie dat de oorspronkelijke rubricering heeft vastgesteld kan functionarissen mandateren om de rubricering te herzien.

Lid 4 is vooral bedoeld als herinnering. In de Archiefwet 1995 (artikel 14) is bepaald dat archiefbescheiden die in een archiefbewaarplaats berusten, behoudens het bepaalde in de artikelen 15, 16 en 17, openbaar zijn. De rubricering vervalt dus bij overbrenging naar een rijksarchiefbewaarplaats, tenzij de zorgdrager besluit dat de rubricering ook in de archiefbewaarplaats geldt, gelet op de belangen die in artikel 15, eerste lid van de Archiefwet 1995 staan opgesomd. Bij overbrenging is het op grond van de Archiefwet 1995 de zorgdrager, i.c. de minister, die de beperkingen aan de openbaarheid vaststelt, na advies van de algemene rijksarchivaris. Relevant is in dergelijke gevallen de eisen aan de beveiliging die de zorgdrager (eigenaar van de informatie) stelt ook expliciet kenbaar te maken. De beheerder van de archiefbewaarplaats is eveneens gehouden aan het VIR 2007 en, voor zover het bijzonder informatie betreft, het VIRBI 2013.

Artikel 6 Eisen aan de beveiliging

Lid 2:
Bij gebruik van de afwijkingsruimte gegeven in het tweede lid dienen in de verantwoording van de afwijking de beveiligingsdoelstellingen te worden meegewogen, conform het principe ‘pas toe of leg uit’.

Onder risicomanagement wordt verstaan het in een inzichtelijk afwegingsproces bepalen van de beveiligingsmaatregelen, waarbij de maatregelen proportioneel, efficiënt en effectief zijn in relatie tot de belangen, de reële dreigingen en onderkende risico’s. Hierbij wordt ook inzichtelijk gemaakt welke restrisico’s worden geaccepteerd. Met betrekking tot de dreiging van specifieke tegenstanders, hun capaciteiten en modus operandi kan de BVA informatie aanreiken. Een deel van de informatie betrekt de BVA van de AIVD, de MIVD, de NCTV en andere niet voor een ieder toegankelijke bronnen die op dit terrein een taak hebben. Het geheel wordt zo opgezet dat verantwoording afgelegd kan worden over de gemaakte keuzes en het bereikte beveiligingsniveau. In de bijlage worden de eisen die aan de

vertrouwelijkheid worden gesteld nader benoemd. Specifiek voor de beveiliging van bijzondere informatie geldt dat voor de toepassing en naleving van de eis van vertrouwelijkheid (exclusiviteit) een dusdanige set van maatregelen zijn toegepast dat de risico's die de verwerking en de aard van de te beschermen bijzondere informatie met zich meebrengen, adequaat zijn afgedekt. Dit wordt aangeduid als een positief beveiligingsrendement.

Lid 3 geeft aan dat er op basis van internationale verdragen of internationale overeenkomsten beperkingen bestaan waardoor voor de beveiliging van betreffende bijzondere informatie verantwoording aan een andere autoriteit verschuldigd is. Het betreft hier de NSA.

Artikel 7 Buiten de rijksdienst brengen van bijzondere informatie

Het kan noodzakelijk zijn om bijzondere informatie buiten de rijksdienst te brengen. Hiervan is sprake zodra de informatie ter beschikking wordt gesteld aan mensen of instanties waarop het VIRBI 2013 niet van toepassing is, dus zodra zij buiten de reikwijdte gesteld in artikel 2 lid 1 van dit voorschrift vallen. De lijnmanager die verantwoordelijk is voor de informatie dient zorg te dragen voor een toereikende beveiliging en te voorzien in de mogelijkheid en bevoegdheid om toezicht en controle hierop uit te oefenen, alvorens de betreffende bijzondere informatie buiten de rijksdienst wordt gebracht. Bijzondere informatie wordt uitsluitend buiten de rijksdienst gebracht indien de secretaris-generaal, of de door hem aangewezen ambtenaar, vooraf toestemming heeft verleend. Bij structurele informatieoverdracht naar externe partijen kan door het ministerie een generieke regeling worden getroffen, waarmee de voorwaarden centraal worden vastgelegd.
Daar waar noodzakelijkerwijs informatie door omstandigheden direct buiten de Rijksdienst moet worden gebracht, wordt achteraf verantwoording afgelegd over de noodzaak en de getroffen maatregelen.

Artikel 8 Compromittering van bijzondere informatie

De BVA of de aangewezen beveiligingscoördinatoren (BVR 2013), zijn het eerste en centrale aanspreekpunt bij mogelijke incidenten met bijzondere informatie. De BVA kan verschillende meldingen aan elkaar relateren, heeft de mogelijkheden om een goede eerste inschatting te maken van de aard en omvang van een eventueel incident, heeft op grond van het BVR 2013 directe toegang tot de secretaris-generaal en de bevoegdheid om aanwijzingen te geven voor de eerste schadebeperkende en beveiligingsherstellende maatregelen.
Waar het staatsgeheimen betreft, informeert de BVA, indien bij eerste beschouwing daadwerkelijk sprake lijkt te zijn van een ongeautoriseerde kennisname, direct de secretaris-generaal. Deze bepaalt aan de hand van de situatie en op advies van de BVA de wijze waarop het verdere onderzoek naar het incident dient te worden ingevuld.
Waar de BVA het eerste en centrale aanspreekpunt binnen het ministerie vormt, heeft de AIVD deze rol voor de gehele rijksdienst met uitzondering van het ministerie van Defensie. Centrale melding van vermoedelijke en feitelijke ongeautoriseerde kennisname maakt het mogelijk om trends en verbanden te ontdekken binnen deze meldingen.
Waar andere partijen schade kunnen krijgen als gevolg van de (vermoedelijke) ongeautoriseerde kennisname van bijzondere informatie worden deze partijen geïnformeerd en betrokken bij het onderzoek. Voor internationale informatie geldt dat de NSA medezeggenschap heeft over het onderzoek.

Artikel 9 Commissie van onderzoek

Deze commissie bestaat uit één of meer ambtenaren die met het uitvoeren van onderzoeken ervaring hebben, die niet betrokken zijn bij de compromittering en die niet onmiddellijk ondergeschikt zijn aan bij de compromittering betrokken ambtenaren. De commissie is gerechtigd kennis te nemen van de informatie die op de compromittering betrekking heeft en de bij de compromittering betrokken ambtenaren, alsmede de ambtenaar die de rubricering heeft vastgesteld, te horen. Het rapport van bevindingen dient te worden beoordeeld op de noodzaak tot rubricering.

Voordat een interne commissie van onderzoek van start gaat wordt expliciet de afweging gemaakt of sprake is van een strafbaar feit in welk kader aangifte vereist is. Er wordt dan geen zelfstandig intern onderzoek opgestart, wel wordt direct bepaald in overleg met de opsporingsinstantie of en zo ja, welke gegevens veilig gesteld moeten worden en op welke wijze dit gebeurt.

Het is van belang om ten behoeve van het uitvoeren van dergelijke onderzoeken gebruik te kunnen maken van expertise op Rijksniveau. De BVA's kunnen dan een beroep doen op hun collega's om hen

bij te staan en te ondersteunen in een dergelijk onderzoek.
De Algemene Inlichtingen- en Veiligheidsdienst of de Militaire Inlichtingen- en Veiligheidsdienst kunnen de commissie bij haar onderzoek terzijde staan.

Artikel 10 Slotbepaling

Lid 2:

Reeds bestaande gerubriceerde informatie hoeft niet als gevolg van de inwerkingtreding van het VIRBI 2013 opnieuw te worden beoordeeld en gerubriceerd. Dit wordt uiterlijk 10 jaar na vaststelling door de vaststeller of diens rechtsopvolger onderzocht.

De Minister-President, Minister van Algemene Zaken,
M. Rutte.