51

AANBIEDINGSFORMULIER VOOR RNV

Van. Minister van Binnenlandse Zaken en Koninkrijksrelaties

Datum aanbieding: 24 september 2007	**Nummer:** 2943542/01
Hamerstuk: Nee	**Voorgaande behandeling:** N.v.t.

Korte titel:

Rapportage over de implementatie en evaluatie van het besluit Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie (Vir-bi).

Inhoud en doelstelling van het voorstel:

Het betreft een rapportage over de implementatie en evaluatie van het besluit Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie (Vir-bi).

De aanleiding voor dit rapport is de verplichting conform het Vir-bi van de minister van Binnenlandse Zaken en Koninkrijksrelaties om eens in de twee jaar aan de ministerraad te rapporteren over de beveiliging van bijzondere informatie binnen de rijksdienst.

De AIVD is beleidsverantwoordelijk voor het opstellen van deze rapportage. Vanuit het interdepartementaal gedeelde belang voor de toepassing en naleving van het Vir-bi is door de AIVD aansluiting gezocht bij het Coördinerend Beraad Integrale Beveiliging (CBIB), welke een werkgroep Vir-bi heeft ingesteld voor het uitvoeren van de inventarisatie naar de implementatie van het (Vir-bi) bij de ministeries. Hieraan gekoppeld is het uitvoeren van een evaluatie van het besluit.

Voorgesteld besluit:

Aanvaarding van de evaluatie en de bijbehorende aanbevelingen ten behoeve van doorgeleiding aande ministerraad

Interdepartementale afstemming

Gevolgen voor de Rijksbegroting Nee

Gevolgen voor administratieve lasten Nee

Overeenstemming met Justitie (wetgevingstoets en effecten analyse) N.v.t.

Aan EU-notificatieverplichting voldaan N.v t

Samenhang met int. Verplichtingen verdragen en / of Europese regelgeving N.v.t.

Ambtelijk voorbereid in CBIB, CVIN

Overeenstemming bereikt op ambtelijk niveau Ja
Overeenstemming bereikt met: AZ, BVK, BZK, BuZa, Def, EZ, Fi, Ju, LNV, OCW, SZW, V&I, V&W, VWS en VROM

Omschrijving geschilpunten

Afstemming met AZ / DG RVD Nee

Contactpersonen

[redacted]

Ministerie van **Binnenlandse Zaken** *en* **Koninkrijksrelaties**

Datum
29 augustus 2007

Ons kenmerk
2943542/01

Status

Onderdeel
AIVD

Auteur(s)

T (070) 320 44 00
F (070) 320 07 33

Postadres
Postbus 20010
2500 EA Den Haag

Beveiliging van bijzondere informatie binnen de rijksdienst

rapportage over de implementatie en evaluatie van het besluit Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie (Vir-bi)

Algemene Inlichtingen- en Veiligheidsdienst

Hoofdstuk 1. Inleiding

1.1 Doel van de rapportage

Artikel 16 van het besluit 'Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie' (Vir-bi) verplicht de minister van Binnenlandse Zaken en Koninkrijksrelaties periodiek de ministerraad over de beveiliging van bijzondere informatie binnen de rijksdienst te rapporteren.

De AIVD is beleidsverantwoordelijk voor het opstellen van deze rapportage. Vanuit het interdepartementaal gedeelde belang voor de toepassing en naleving van het Vir-bi is door de AIVD aansluiting gezocht bij het Coördinerend beraad integrale beveiliging (CBIB), welke een werkgroep Vir-bi heeft ingesteld voor het uitvoeren van de inventarisatie naar de implementatie van het (Vir-bi) bij de ministeries. Hieraan gekoppeld is het uitvoeren van een evaluatie van het besluit.

De rapportage beoogt een goed en consistent niveau te bevorderen van beveiliging van bijzondere informatie (BI), waaronder staatsgeheimen. Tevens is het doel om te oordelen of het besluit werkbaar is en de ministeries in staat stelt hun verantwoordelijkheden voor de beveiliging van BI te nemen. Ook bevat dit rapport aanbevelingen voor de bevordering van de beveiliging van BI.

1.2 Opzet van het onderzoek

Voor het verzamelen van informatie heeft de werkgroep een vragenlijst opgesteld die als leidraad diende voor de gevoerde gesprekken. Door de werkgroep zijn interviews georganiseerd met beveiligingsambtenaren (BVA's) en andere betrokkenen van alle departementen. Deze opzet van de gesprekken en de gebruikte vragenlijst zijn besproken en goedgekeurd door het CBIB. Aan de geïnterviewden is het verzoek gedaan het verslag te laten accorderen door de secretaris-generaal.

Hoofdstuk 2. Inventarisatie van de implementatie van het Vir-bi.

In dit hoofdstuk wordt ingegaan op de stand van de implementatie van het Vir-bi bij de rijksoverheid. Deze wordt besproken aan de hand van vijf aandachtsgebieden, te weten de aard en omvang van BI, het beleid voor informatiebeveiliging, de functionarissen voor informatiebeveiliging, de incidenten en het beveiligingsbewustzijn. Voor de duidelijkheid wordt eerst aangegeven wat de betekenis is van enkele begrippen.

Bijzondere informatie (BI): Informatie die als "staatsgeheim" of als "departementaal vertrouwelijk" is gerubriceerd. In geval van staatsgeheimen kan kennisname door niet gerechtigden schade hebben voor de belangen van de Staat of van zijn bondgenoten en nadeel in geval van departementaal vertrouwelijk voor de belangen van één of meer ministeries.

Rubriceren: Het vaststellen en aangeven dat een gegeven bijzondere informatie is en het bepalen van de mate van beveiliging die voor deze informatie noodzakelijk is (het bepalen van het rubriceringsniveau). Hoe groter de mogelijke nadelige gevolgen bij ongerechtigde kennisname, des te hoger het rubriceringsniveau.

Rubriceringsniveaus: Er worden vier rubriceringsniveaus onderscheiden. Aan elk niveau is een aantal exclusiviteitseisen verbonden, waarbij elk hoger niveau een strengere beveiliging met zich meebrengt. De vier niveaus zijn, in oplopende volgorde: departementaal vertrouwelijk; staatsgeheim (stg.) confidentieel; stg. geheim en stg. zeer geheim.

Exclusiviteitseisen: Een samenhangend pakket van eisen waaraan de beveiliging van BI moet voldoen om met voldoende zekerheid de vertrouwelijkheid (exclusiviteit) van informatie te beschermen.

Coördinerend Beraad Integrale Beveiliging (CBIB): Het CBIB is een coördinerend overleg over de beveiligingsaspecten binnen de rijksdienst. Alle ministeries hebben hier zitting in.

2.1 Aard en omvang

Uit de gesprekken blijkt dat van alle overheidsinformatie op de departementen, de BI slechts een klein deel vormt. Echter op enkele departementen of delen daarvan is meer BI aanwezig. Hierbij gaat het om de ministeries van Defensie, Buitenlandse Zaken, Algemene Zaken, Justitie en Binnenlandse Zaken en Koninkrijksrelaties.

Tevens is geconstateerd dat van alle bijzondere informatie er per niveau minder is naarmate de rubricering hoger is. Voor meerdere departementen vormt de documentenstroom rond de ministerraad het grootste deel van de BI voor de staatsgeheime niveaus.

2.2 Beleid

De meeste ministeries beschikken over een vastgesteld actueel departementaal beleid met betrekking tot de bescherming van bijzondere informatie dat voldoet aan de relevante regelgeving en als afdoende is beoordeeld door onafhankelijke deskundigen. De departementale auditdiensten hebben bevonden dat dit beleid voldoet. Voor de overige ministeries geldt dat actualisering van het beleid loopt om aan de relevante regelgeving te voldoen.

Een trend is om het structureel onafhankelijk toezicht op de beveiliging van bijzondere informatie onderdeel te laten uitmaken van de departementale P&C-cyclus.

2.3 Departementale organisatie

Ieder ministerie beschikt over een Beveiligingsambtenaar (BVA). De bevoegdheden van de BVA zijn in lijn met de verantwoordelijkheden die het Vir-bi hieraan toekent.

Onafhankelijk toezicht wordt uitgevoerd door de departementale auditdiensten.

2.4 Incidenten

De afgelopen jaren zijn er enkele grote incidenten in de media gekomen over gevoelige informatie. In enkele gevallen betrof het BI (zoals de lekkende AIVD tolk), vaker anderszins gevoelige maar ongerubriceerde informatie (bij voorbeeld de documenten door NOVA aangetroffen in het vuilnis van het Kabinet der Koningin of de "stralende stemmachines"). In dit soort gevallen is er geen sprake van incidenten in de zin van het Vir-bi, maar kan er nog steeds politieke of publicitaire relevantie zijn.

Veel incidenten betreffen verlies of diefstal van goederen waarbij de schade niet bestaat uit inbreuken op de vertrouwelijkheid van informatie. Bij diefstal of verlies van gegevensdragers zijn de verloren gegevens doorgaans geen BI. Wanneer gegevensdragers wel BI bevatten, wordt het risico op verspreiding of lekken van de informatie beheerst door het gebruik van door het Nationaal Bureau voor Verbindingsbeveiliging (een afdeling van de AIVD) goedgekeurde versleutelingsproducten.

Door de ministeries genoemde incidenten zijn conform het Vir-bi onderzocht en hebben zonodig tot optimalisatie van de beveiliging geleid.

2.5 Beveiligingsbewustzijn

Het onderhouden van beveiligingsbewustzijn vraagt voortdurende aandacht van de ministeries. Op veel ministeries worden activiteiten ontplooid om dit bewustzijn bij de medewerkers te vergroten. Aandacht voor de omgang met BI is hierbij een onderdeel van een bredere aanpak. Er bestaat een duidelijke behoefte aan het onderling uitwisselen van best practices en ervaringen (zie de evaluatie).

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties beziet of het mogelijk is rijksbrede instrumenten hiervoor in te zetten. Hierbij valt te denken aan instrumenten die ook worden gebruikt om het bewustzijn rond het thema integriteit te bevorderen, aangezien er raakvlakken zijn met het informatiebeveiligingsthema.

Hoofdstuk 3. Evaluatie van het Vir-bi

Het vorige hoofdstuk betrof de rapportage over de stand van de beveiliging van bijzondere informatie binnen de rijksdienst conform Vir-bi artikel 16.1. Dit hoofdstuk gaat in op de ervaringen met de werkbaarheid van het besluit. In het onderzoek is gevraagd naar de praktische toepasbaarheid van de artikelen en andere verbeterpunten.

Onderstaand worden de onderzoeksresultaten behandeld in de volgorde van de hoofdstukken van het besluit. Daarbij zijn aanbevelingen opgenomen over hoe om te gaan met de gesignaleerde verbeterpunten.

> *Geadviseerd wordt om in lijn met de aanbevelingen van dit onderzoek en reeds bekende technische en tekstuele verbeterpunten een revisie van het besluit uit te laten voeren. Daarbij kan hernieuwd aansluiting worden gezocht bij het besluit voorschrift informatiebeveiliging rijksdienst 2007(VIR2007) en het besluit beveiligingsvoorschift rijksdienst 2005.*

3.1 Rubriceringen

Het rubriceringsniveau departementaal vertrouwelijk is in 2004 met de inwerkingtreding van het Vir-bi voor het eerst geïntroduceerd. Dit vierde niveau wordt door een aantal ministeries als een verrijking ervaren en sluit aan op hun behoefte. Aandachtspunt is een goed werkbaar kader om tot een juiste rubricering van informatie te komen. Met name voor de nieuwe rubricering "departementaal vertrouwelijk" bestaat bij veel ministeries behoefte aan meer handreikingen.

Een gesignaleerd punt bij het toekennen van een rubricering is dat het niet altijd duidelijk is welke rubricering van toepassing is in welke situatie. Het verschil tussen de niveaus is niet duidelijk. Om het zekere voor het onzekere te nemen worden stukken bovendien soms hoger gerubriceerd dan nodig is. Dit is inefficiënt want het brengt extra verplichtingen en inspanningen met zich mee die onnodig zijn. Bovendien vermindert dit de acceptatie van een door een ander aangebrachte rubricering, waardoor de voorgeschreven maatregelen minder strikt of niet worden toegepast.

Specifiek wordt de rubricering van de besluitenlijst van de ministerraad (dit geldt expliciet niet voor de notulen) door meerdere departementen genoemd als te hoog. Algemene Zaken herkent dit niet als een probleem.

> *Voorgesteld wordt om het CBIB op te dragen meer duidelijkheid te verschaffen over de toekenning van de juiste rubricering en structureel de uitwisseling van ervaringen te bevorderen en informatie teneinde de interpretatieruimte te verkleinen.*

3.2 Exclusiviteitseisen

Een gesignaleerd knelpunt is dat de vereiste maatregelen ter beveiliging van hoog gerubriceerde stukken belemmerend gevonden worden voor een effectieve en efficiënte omgang ermee. Enkele departementen gaven aan dat snelle communicatie van gerubriceerde documenten nodig kan zijn maar onpraktisch is. Bijvoorbeeld wanneer regelmatig meerdere hooggerubriceerde documenten snel tussen twee locaties moeten worden verzonden, wordt het niet haalbaar gevonden om ze fysiek te versturen. Door enkele departementen is opgemerkt dat er een behoefte is aan meer ondersteuning (in de vorm van bijvoorbeeld goedgekeurde ICT-produkten en technische adviezen) van het Nationaal Bureau voor Verbindingbeveiliging (het NBV).

Voorgesteld wordt om het CBIB op te dragen om structureel rijksbreed ervaringen en informatie uit te laten wisselen om zo tot praktische en verantwoorde oplossingen te komen voor de geconstateerde belemmeringen.

Voorgesteld wordt om bij de behoeftebepaling voor technische hulpmiddelen afstemming te zoeken met alle departementen. Hiervoor dient aansluiting gezocht te worden bij het CBIB vanuit het oogpunt van beveiliging, maar ook bij de belangendragers voor de informatievoorziening, verenigd in het Interdepartementaal Overleg Directeuren Informatievoorziening (IODI). Een bredere bevraging van het NBV zal wel kunnen leiden tot een grotere vraag van meer departementen en een bredere aansturing en financiering noodzakelijk maken. Bezien wordt hoe deze vorm te geven.

Een gesignaleerd knelpunt is dat bij sommige departementen weinig kennis bestaat over welke maatregelen vereist zijn voor de correcte omgang met gerubriceerde documenten. De eisen worden ervaren als moeilijk en ontoegankelijk. Tevens is bij sommige departementen weinig kennis over de bestaande mogelijkheden en voorzieningen voor een correcte omgang met gerubriceerde informatie. Bij enkele departementen is er behoefte aan advies en informatie bij de implementatie van het Vir-bi. Vervolgens worden ook weer weinig documenten gerubriceerd om de 'moeilijke' maatregelen te vermijden. Een document is dan niet gerubriceerd maar er wordt wel vertrouwelijk mee omgegaan.

De voorgestelde kennisuitwisseling in het CBIB draagt tevens bij aan het verbeteren van de kennis van departementen waar weinig met bijzondere informatie wordt gewerkt.

3.3 Organisatie

Bij meerdere departementen is gebleken dat de eigen verantwoordelijkheid van het departement en afwijkingsmogelijkheden van de exclusiviteitseisen in het Vir-bi onbekend zijn. Daardoor wordt het Vir-bi als dwingend en weinig flexibel ervaren.

Tijdens de uitvoering van de evaluatie is hier bij departementen meer duidelijk over geworden.

Voorgesteld wordt om het CBIB op te dragen om structureel rijksbreed ervaringen en informatie uit te laten wisselen om zo de kennis over dit onderwerp op peil te brengen en te houden.

Bij enkele departementen is de behoefte aangegeven om maatregelen te treffen die misschien niet de exclusiviteitseisen volgen maar wel leiden tot een betere beveiliging. Risicoanalyse en risicomanagement zouden meer aandacht mogen krijgen. Doel hierbij is het bepalen van optimale, werkbare beveiliging gebaseerd op risicomanagement.

Voorgesteld wordt het Vir-bi doelstellingen in plaats van beveiligingseisen te laten bevatten.

Organisaties buiten de rijksdienst (bijvoorbeeld de KLPD, gemeenten en waterschapen) zijn niet gehouden aan het Vir-bi en de daarin gestelde eisen. Enkele departementen hebben aangegeven dat er behoefte is aan het vormgeven van 'ketenverantwoordelijkheid' voor het delen van bijzondere informatie met andere overheden en niet overheidsorganisaties.

Voorgesteld wordt om in lijn met het VIR 2007 onder verantwoordelijkheid van het CBIB te komen tot een voorstel om risicomanagement en ketenverantwoordelijkheid vorm te geven.

3.4 Overige opmerkingen

Er zijn enkele inhoudelijke vragen gesignaleerd die in het huidige besluit niet worden benoemd. Zo is onduidelijk hoe om te gaan met ongerubriceerde verspreidde concepten die later als gerubriceerde documenten worden vastgesteld. Onduidelijk is tevens hoe oude gegevensdragers vernietigd kunnen worden.

Ten aanzien van de beleidsverantwoordelijkheid is door een departement voorgesteld dat het besluit voor de bescherming van bijzondere informatie het beste bij hetzelfde organisatieonderdeel kan worden gepositioneerd als de verantwoordelijkheid voor de bescherming van reguliere informatie. Tevens is geopperd te bezien of de status van ministerraadbesluit gewenst is of dat er een wet op de informatiebeveiliging zou moeten komen. Door een departement worden bepaalde verplichtingen als onnodig ervaren en niet uitgevoerd . Deze vloeien deels voort uit internationale verplichtingen. De verhouding van de regeling tot deze verplichtingen is een punt van aandacht.

Voorgesteld wordt om het CBIB op te dragen deze onderwerpen te adresseren en hierover best practices uit te laten wisselen.

Hoofdstuk 4 Conclusies

Rijksbreed krijgt de bescherming van bijzondere informatie de nodige aandacht. Desalniettemin is er ruimte voor verbetering.

Departementen die minder met BI werken kunnen profiteren van de ervaring van departementen die daar meer mee te maken hebben. Structurele uitwisseling van deze kennis en ervaring draagt bij aan een verdere toename van kennis en expertise en een uniforme rijksbrede interpretatie van het besluit. Aanbevolen wordt het CBIB in deze behoefte te laten voorzien.

Daarnaast wordt voorgesteld om het bestaande besluit op basis van de bovenstaande aanbevelingen te herzien.