MINISTERIE VAN DEFENSIE

Directie Juridische Zaken
Afdeling Wet- en Regelgeving

Onderwerp:
Regeling gedragsregels gebruik e-mail en internetvoorzieningen Defensie

Nummer: C/2009007689

DE STAATSSECRETARIS VAN DEFENSIE

BESLUIT:

Artikel 1 Doel van de regeling

1. Deze regeling geeft de wijze aan waarop bij Defensie en door het bij Defensie werkzame personeel wordt omgegaan met de e-mail en internetvoorzieningen van Defensie. Deze regeling omvat gedragsregels ten aanzien van verantwoord gebruik van de e-mail en internetvoorzieningen van Defensie en geeft op uitputtende wijze regels over de wijze waarop controle door de werkgever op de naleving van gedragsregels inzake het e-mail en internetgebruik plaatsvindt.

2. De in de artikelen 5 en 6 van deze regeling beschreven controle op persoonsgegevens bij gebruik van de e-mail en internetvoorzieningen van Defensie heeft als doel de handhaving van de naleving van de in de artikelen 3 en 4 van deze regeling opgenomen gedragsregels.

3. Deze regeling laat onverlet wettelijke bevoegdheden, zoals die van instanties als politie, Koninklijke marechaussee of openbaar ministerie op het terrein van strafvordering of zoals die van inlichtingen- en veiligheidsdiensten op het terrein van nationale veiligheid.

4. Deze regeling staat er niet aan in de weg dat de commandant der strijdkrachten terzake van het gebruik en controle van de e-mail en internetvoorzieningen van Defensie in het kader van militair-operationeel optreden specifieke regels kan stellen. Deze regeling staat er voorts niet aan in de weg dat de directeur militaire inlichtingen- en veiligheidsdienst specifieke regels kan stellen ten aanzien van het bij deze dienst werkzame personeel.

5. Deze regeling is niet van toepassing op het internet- of e-mailgebruik in het kader van internet op de legeringskamer of in het kader van welfare.

Artikel 2 Algemene uitgangspunten

1 De controle op de naleving van de in deze regeling opgenomen gedragsregels inzake het gebruik van de e-mail en internetvoorzieningen van Defensie zal overeenkomstig deze regeling worden uitgevoerd.

2 Er dient een juiste balans te bestaan tussen controle op verantwoord e-mail en internetgebruik en bescherming van privacy van werknemers bij het gebruik van de e-mail en internetvoorzieningen van Defensie.

3. Op een natuurlijk persoon te herleiden gegevens gerelateerd aan gebruik van e-mail en internetvoorzieningen van Defensie kunnen ten behoeve van de in artikel 5 van deze regeling beschreven controle niet langer worden gebruikt dan maximaal 6 maanden te rekenen vanaf het moment waarop het dataverkeer plaatsvindt.

4. Op een natuurlijk persoon te herleiden gegevens gerelateerd aan gebruik van e-mail en internetvoorzieningen van Defensie kunnen ten behoeve van de in artikel 6 van deze regeling beschreven controle langer dan zes maanden worden gebruikt indien wordt besloten tot zo'n controle en voorzover dat noodzakelijk is voor die controle, met een maximale termijn, te rekenen vanaf het moment waarop het dataverkeer plaatsvindt, van:
- 5 jaar indien de mogelijke overtreding van de gedragsregels informatie betreft welke als stg. confidentieel of hoger is gerubriceerd;
- 3 jaar indien de mogelijke overtreding van de gedragsregels informatie betreft welke als departementaal vertrouwelijk is gerubriceerd;
- 1 jaar in overige gevallen.

5. Iedere gebruiker van de e-mail en internetvoorzieningen van Defensie is persoonlijk verantwoordelijk voor de onder zijn of haar account verrichte handelingen.

Artikel 3 E-mailgebruik

1 De e-mailvoorzieningen van Defensie zijn voor de uitoefening van de dienst bestemde voorzieningen, die ook als zodanig gebruikt moeten worden.

2. Privé-gebruik van de e-mailvoorzieningen van Defensie is incidenteel toegestaan indien dit, zowel inhoudelijk als naar kwantiteit, niet belastend is voor de dagelijkse werkzaamheden en de goede dagelijkse gang van zaken.

3. Het is niet toegestaan:
a. de e-mail-voorzieningen van Defensie te gebruiken indien het gebruik schadelijk is voor het dienstbelang, daaronder in ieder geval begrepen het ongeautoriseerd verspreiden van vertrouwelijke informatie alsmede gebruik waarbij de inhoud van dreigende, intimiderende, beledigende, seksueel getinte of racistische aard is;

b. e-mail geautomatiseerd door te zenden naar een e-mailadres dat niet door Defensie ter beschikking is gesteld;

c. gerubriceerde informatie danwel informatie met een overeenkomstige internationale rubricering zonder een overeenkomstig het Defensie Beveiligingsbeleid door de beveiligingsautoriteit goedgekeurde voorvercijfering te sturen naar een e-mailadres waarbij de verzending via het publieke internet plaatsvindt of over een niet publiek netwerk dat niet voldoet aan de eisen van beveiliging die behoren bij de rubricering van de informatie;

d. zonder toestemming van de beveiligingsautoriteit naar een e-mailadres dat niet door Defensie ter beschikking is gesteld een e-mailbericht te sturen met de merkingen ”Intern Beraad” of “Intern Gebruik Defensie”;

e. zonder toestemming van de beveiligingsautoriteit een e-mailbericht te versturen aan alle of vrijwel alle gebruikers van de Defensie e-mailvoorzieningen ten einde overbelasting van de e-mail en internetvoorzieningen van Defensie te voorkomen;

f. het e-mailsysteem te gebruiken voor kettingbrieven.

Artikel 4 Internetgebruik

1 De internetvoorzieningen van Defensie zijn voor de uitoefening van de dienst bestemde voorzieningen, die ook als zodanig gebruikt moeten worden.

2. Privé-gebruik van de internetvoorzieningen van Defensie is incidenteel toegestaan indien dit, zowel inhoudelijk als naar kwantiteit, niet belastend is voor de dagelijkse werkzaamheden en de goede dagelijkse gang van zaken.

3. Het is niet toegestaan:
a. de internetvoorzieningen van Defensie te gebruiken indien dit gebruik schadelijk is voor het dienstbelang, daaronder in ieder geval begrepen het ongeautoriseerd verspreiden van vertrouwelijke informatie, het plaatsen van voor het dienstbelang schadelijke informatie op weblogs en forums alsmede gebruik waarbij de inhoud van dreigende, intimiderende, beledigende, seksueel getinte of racistische aard is;

b. niet door Defensie geautoriseerde programmatuur te downloaden van internetsites, tenzij de beveiligingsautoriteit daarvoor schriftelijk toestemming heeft verleend.

Artikel 5 Niet persoonsgerichte controle e-mail en internet

1. In het kader van systeem- en netwerkbeveiliging en ter voorkoming en detectie van overtreding van de gedragsregels, bedoeld in de artikelen 3 en 4, kan het e-mail- en internetgebruik op geautomatiseerde wijze en niet-persoonsgericht worden gecontroleerd.

2. Het op geautomatiseerde wijze en niet-persoonsgerichte controleren betreft:
a.het controleren op schadelijke bestandsformats en virushandtekeningen;
b.het controleren op het automatisch doorzenden van e-mailberichten naar een e-mailadres dat niet door Defensie ter beschikking is gesteld;
c. het controleren op het downloaden van programmatuur;
d.het ten behoeve van kosten- en capaciteitsbeheersing analyseren van verkeersgegevens van e-mail en internetgebruik;
e.het door middel van content scanning controleren achteraf van e-mailberichten en internetverkeer op racistische en seksueel getinte inhoud of het ongeautoriseerd verspreiden van vertrouwelijke informatie.

3. De controle, bedoeld in het tweede lid, onderdeel e, is gericht op trefwoorden en grafische bestanden met bepaalde eigenschappen. Controle van het internetverkeer kan tevens plaats vinden aan de hand van namen van bezochte sites.

4. De controle, bedoeld in het tweede lid, onderdeel e, op racistische en seksueel getinte inhoud vindt slechts steekproefsgewijs en op basis van toestemming van de secretaris-generaal plaats aan de hand van de door de secretaris-generaal vastgestelde trefwoorden, grafische bestanden danwel sites.

5. De controle, bedoeld in het tweede lid, onderdeel e, op het ongeautoriseerd verspreiden van vertrouwelijke informatie vindt slechts plaats in het kader van een huishoudelijk onderzoek aan de hand van de door de secretaris-generaal vastgestelde trefwoorden, grafische bestanden danwel sites.

Artikel 6 Persoonsgerichte inhoudelijke controle

1. Onverminderd bestaande plichten tot melding van incidenten of gebeurtenissen wordt een melding gedaan aan de secretaris-generaal indien een controle als bedoeld in het tweede lid nodig wordt geacht voor de beoordeling in hoeverre de in deze regeling beschreven gedragsregels zijn of worden overtreden.

2. De secretaris-generaal kan bij zwaarwegende redenen besluiten tot een persoonsgerichte inhoudelijke controle achteraf van de door die gebruiker verrichte verwerkingen met de e-mail en internetvoorzieningen van Defensie.

Artikel 7

1. Werknemers ten aanzien van wie is geconstateerd dat zij zich niet aan deze regeling houden, worden door de leidinggevende op hun gedrag aangesproken.

2. Overtreding van een in deze regeling vervatte gedragsregel kan leiden tot een sanctie overeenkomstig de geldende rechtspositionele en tuchtrechtelijke regelgeving. Deze bepaling laat handhaving van strafrechtelijke bepalingen door de daartoe bevoegde instanties onverlet.

Artikel 8 Rechten van betrokkenen

De onderhavige regeling doet geen afbreuk aan de in de Algemene verordening gegevensbescherming omschreven rechten, zoals onder andere het in artikel 15 van deze verordening omschreven recht om zich tot de werkgever te wenden om inzage te verkrijgen in de hem betreffende persoonsgegevens en het in artikel 16 van deze verordening omschreven recht de werkgever te verzoeken hem betreffende onjuiste persoonsgegevens te rectificeren.

Artikel 9 Overleg medezeggenschap

De onderhavige regeling wordt niet gewijzigd zonder overleg met de medezeggenschap.

Artikel 10

Deze regeling treedt in werking met ingang van de tweede dag na de dagtekening van de Staatscourant waarin de mededeling inzake publicatie in de serie Ministeriële Publicaties wordt gedaan.

Deze regeling zal worden gepubliceerd in de serie Ministeriële Publicaties. Van deze publicatie wordt mededeling gedaan in de Staatscourant.

´s-Gravenhage, 15 mei 2009

DE STAATSSECRETARIS VAN DEFENSIE

Drs. J.G. de Vries

Toelichting

Algemeen

De onderhavige regeling bevat regels inzake de wijze waarop bij Defensie en door het defensiepersoneel wordt omgegaan met de e-mail en internetvoorzieningen van Defensie. De regeling omvat gedragsregels ten aanzien van verantwoord gebruik van de e-mail en internetvoorzieningen van Defensie en geeft op uitputtende en uitvoerige wijze regels over de wijze waarop controle door de werkgever op naleving van dit gebruik kan worden uitgeoefend. Veel organisaties hebben een regeling inzake het gebruik door de werknemers van de e-mail en internetvoorzieningen van de werkgever. Hoewel binnen Defensie afzonderlijke interne voorschriften of bepalingen bestaan, ontbreekt op dit moment een uniforme defensiebrede regeling. De onderhavige regeling voorziet daarin; zij is geënt op een in april 2002 uitgebrachte Raamregeling voor het gebruik van e-mail en internet van het college bescherming persoonsgegevens.

De regeling ziet op de eerste plaats op de "reguliere" werksituatie. De in de regeling opgenomen gedragsregels zijn voorts van toepassing op het gebruik van e-mail en internetvoorzieningen van Defensie in het kader van militair-operationele omstandigheden. De situatie in die omstandigheden is echter niet (volledig) te vergelijken met een reguliere werksituatie. Het is immers zeer wel denkbaar dat bij militaire operaties uit veiligheidsoverwegingen er specifieke (stringentere) regels nodig zijn. De regeling staat er daarom niet aan in de weg dat de commandant der strijdkrachten terzake van het gebruik en controle van de e-mail en internetvoorzieningen van Defensie in het kader van militair-operationeel optreden specifieke (stringentere) regels stelt. Voorts staat deze regeling er niet aan in de weg dat de directeur MIVD specifieke (stringentere) regels stelt ten aanzien van het gebruik en controle van de e-mail en internetvoorzieningen van Defensie door het bij de MIVD werkzame personeel. Dit gelet op diens bijzondere zorgplicht voor de geheimhouding van daarvoor in aanmerking komende gegevens, bronnen en voor de veiligheid van de personen met wier medewerking gegevens worden verzameld.

De scope van de regeling betreft de e-mail en internetvoorzieningen van Defensie. Daarbij doet het er niet toe waar gebruik van de e-mail en internetvoorzieningen van Defensie wordt gemaakt. Wanneer door een Defensiemedewerker op een plek buiten Defensie gebruik wordt gemaakt van de e-mail en internetvoorzieningen van Defensie (denk aan het gebruik van een BlackBerry van Defensie) dan is de onderhavige regeling derhalve van toepassing. Voorts doet het er voor de toepasselijkheid van deze regeling en de daarin geregelde controle niet toe of het gebruik van de Defensie-voorzieningen voor privédoeleinden geschiedt (hetgeen overigens ingevolge deze regeling slechts incidenteel is toegestaan). De regeling is dan ook van toepassing indien e-mail met een privékarakter wordt gewisseld via de voorzieningen van Defensie. De regeling ziet echter niet op het gebruik door een defensiemedewerker van eigen privé e-mail en internetvoorzieningen. Voorts bevat de regeling in artikel 1, vijfde lid, een bijzondere bepaling met betrekking tot het internet- of e-mailgebruik in het kader van internet op de legeringskamer of in het kader van welfare (voorzieningen ten behoeve van het uitgezonden personeel met het oog op het kunnen onderhouden van contacten met het thuisfront gedurende de missie). Omdat deze voorzieningen naar hun aard en doel voor privédoeleinden zijn bestemd, is in de regeling bepaald dat deze hierop niet van toepassing is. Daarbij kan worden opgemerkt dat ingevolge (militair) ambtenaarrechtelijke bepalingen ook dan een (militair) ambtenaar zich dient te onthouden van het openbaren van gedachten of gevoelens indien door de uitoefening daarvan de goede vervulling van zijn functie of de goede functionering van de openbare dienst, voor zover deze in verband staat met zijn functievervulling, niet in redelijkheid zou zijn verzekerd.

De regeling betreft een uniforme en defensiebrede regeling. Een en ander betekent dat, behoudens de in artikel 1, vierde lid, opgenomen mogelijkheid voor de commandant der strijdkrachten en de directeur MIVD, er door de afzonderlijke dienstonderdelen van Defensie geen (aanvullende) regels meer (dienen te) worden gesteld. Eventuele in het verleden door de afzonderlijke dienstonderdelen uitgevaardigde interne voorschriften of bepalingen dienen door deze dienstonderdelen te worden gewijzigd cq ingetrokken voor zover deze betrekking hebben op het onderwerp van deze Regeling gedragsregels gebruik e-mail en internetvoorzieningen Defensie.

Uitputtende regeling controle werkgever op gebruik e-mail en internetvoorzieningen Defensie
De regeling bestaat in wezen uit twee elementen. Allereerst omvat de regeling gedragsregels ten aanzien van een verantwoord gebruik van de e-mail en internetvoorzieningen van Defensie. Hiermee wordt dan ook, voor zover het gaat om gebruik van e-mail en internetvoorzieningen van Defensie, uitvoering gegeven aan aanbeveling 2 (blz. 25) van het rapport van de commissie Lemstra (belast met onderzoek naar oorzaken van het lekken van vertrouwelijke informatie) om gedragsregels op te stellen op het punt van het niet-lekken van vertrouwelijke informatie.
Daarnaast beschrijft de regeling uitputtend en uitvoerig wat mogelijk is terzake van de controle van de e-mail en internetvoorzieningen van Defensie door de werkgever Defensie ten behoeve van de naleving van de in de regeling opgenomen gedragsregels. Uit de formulering van artikel 1, tweede lid, artikel 5, eerste lid en artikel 6, eerste lid, vloeit voort dat de controle dient te zijn gerelateerd aan de handhaving van de in deze regeling omschreven gedragsregels en de systeem- en netwerkbeveiliging.
De uitputtende regeling laat uiteraard de reguliere sociale controle onverlet. Indien in de werkomgeving direct geconstateerd wordt (zonder dat hiervoor de nadere technische handelingen, bedoeld in artikel 5 en 6 nodig zijn) dat niet conform de gedragsregels wordt gehandeld dan kan dit ook in zo'n geval leiden tot een sanctie overeenkomstig de geldende rechtspositionele en tuchtrechtelijke regelgeving. Uiteraard laat deze regeling voorts onverlet wettelijke bevoegdheden van instanties, zoals opsporingsdiensten (zie ook de toelichting bij artikel 6).

Gedragsregels
In de artikelen 3 en 4 zijn de gedragsregels neergelegd ten aanzien van een verantwoord gebruik van de e-mail en internetvoorzieningen van Defensie. In deze artikelen wordt aangegeven dat de e-mail en internetvoorzieningen van Defensie voor de uitoefening van de dienst bestemde voorzieningen zijn, die ook als zodanig gebruikt moeten worden.Duidelijk zal zijn dat het gebruik voor niet Defensie gerelateerde handelsdoeleinden hier niet mee in overstemming is. Privé-gebruik van die voorzieningen is incidenteel toegestaan indien dit, zowel inhoudelijk als naar kwantiteit, niet belastend is voor de dagelijkse werkzaamheden en de goede dagelijkse gang van zaken. In genoemde artikelen wordt voorts bepaald dat het niet is toegestaan de e-mail en internetvoorzieningen van Defensie te gebruiken indien het gebruik schadelijk is voor het dienstbelang. Daarbij wordt aangegeven welke situaties daaronder in ieder geval worden begrepen. Voorts worden in artikel 3, tweede lid, onderdeel b tot en met f, meer uit beveiligingsoptiek regels gesteld. Buiten deze regels blijft overigens het Defensie beveiligingsbeleid van toepassing.

Controle op de gedragsregels
De hierboven reeds genoemde reguliere sociale controle buiten beschouwing latend, beschrijft de regeling uitputtend en uitvoerig wat mogelijk is terzake van de controle van de e-mail en internetvoorzieningen van Defensie door de werkgever Defensie ten behoeve van de naleving van de in de regeling opgenomen gedragsregels inzake het gebruik van de e-mail en internetvoorzieningen van Defensie. De regeling kent daarbij twee soorten van controle, de in artikel 5 geregelde niet persoonsgerichte controle en de in artikel 6 geregelde persoonsgerichte controle.

Controle artikel 5
In artikel 5 wordt de niet persoonsgerichte controle geregeld. De controle wordt geautomatiseerd uitgevoerd en is niet op een concrete persoon gericht. Ingevolge artikel 2 kunnen persoonsgegevens gerelateerd aan het gebruik van e-mail en internetvoorzieningen van Defensie ten behoeve van deze controle maximaal zes maanden worden gebruikt. Onder persoonsgegevens worden overigens tevens de inhoud van de e-mails begrepen. De geautomatiseerde controle zal in de praktijk door de bedrijfsgroep Informatievoorziening en -Technologie (IVENT) van het Commando DienstenCentra worden uitgevoerd. Deels vindt deze controle plaats uit oogpunt van systeembeveiliging en is deze al opgenomen in de dienstverlening van IVENT (controle, bedoeld in artikel 5, tweede lid, onder a tot en met d). De controle, bedoeld in onderdeel e betreft een controle achteraf op racistische of pornografische inhoud danwel het ongeautoriseerd verspreiden van vertrouwelijke informatie (lekken). IVENT welke reeds over de technische mogelijkheden beschikt deze controle uit te voeren, zal deze gaan verrichten conform de volgende systematiek. De controle op racistische of seksueel getinte inhoud vindt steekproefsgewijs plaats en op basis van toestemming van de secretaris-generaal (SG) aan de hand van door de SG vastgestelde trefwoorden, grafische bestanden danwel sites. De controle op het ongeautoriseerd verspreiden van vertrouwelijke informatie vindt conform de huidige situatie slechts plaats in het kader van een huishoudelijk onderzoek. Ingevolge de onderhavige regeling geschiedt de controle aan de hand van door de SG vastgestelde trefwoorden, grafische bestanden danwel sites. Over de uitkomst van de uitgevoerde controle wordt door IVENT periodiek (bijv. driemaandelijks) gerapporteerd aan de SG.

Procedure artikel 6
In artikel 6 wordt op uitputtende wijze de persoonsgerichte controle door de werkgever Defensie geregeld ter handhaving van de in deze regeling verwoorde gedragsregels. Indien voor de vaststelling in hoeverre de gedragsregels zijn overtreden een persoonsgerichte controle nodig is, kan ingevolge de onderhavige regeling binnen Defensie de SG bij zwaarwegende belangen besluiten tot zo'n controle. Vandaar dat in het eerste lid van artikel 6 is bepaald dat een melding wordt gedaan aan de SG indien een controle als bedoeld in het tweede lid, nodig wordt geacht voor de beoordeling in hoeverre de in deze regeling beschreven gedragsregels zijn of worden overtreden. Het woord "onverminderd" in het eerste lid brengt tot uitdrukking dat de melding aan de SG reeds kan voortvloeien uit bestaande voorschriften (in het bijzonder kan worden gedacht aan aanwijzing SG A/906 Melding bijzondere gebeurtenissen) en dat deze regeling aan die voorschriften overigens geen afbreuk doet. Indien de constatering van een (vermoedelijke) schending van de gedragsregels voortvloeit uit de door de IVENT uitgevoerde niet persoonsgerichte controle, bedoeld in artikel 5, geschiedt de melding aan de SG door IVENT. Indien anderszins een (vermoedelijke) schending van de gedragsregels wordt geconstateerd, kan de melding aan de SG geschieden via de commandantenlijn.

Het criterium "zwaarwegende redenen" strekt ertoe te waarborgen dat niet lichtvaardig tot een persoonsgerichte controle wordt overgegaan. In zijn algemeenheid is het niet goed mogelijk de zwaarwegende redenen te concretiseren, omdat veel zal afhangen van de omstandigheden van het geval. Om toch een indicatie te geven: gedacht moet worden aan een situatie waarin ofwel langs de weg van de niet-persoonsgerichte controle ofwel langs andere weg er een gereed vermoeden is dat een bepaalde persoon zich niet houdt aan de voor het gebruik van internet en e-mail geldende regels. Om zeker te stellen dat betrokkene zich inderdaad schuldig maakt aan laakbaar gedrag, te denken valt aan het doen van racistische uitlatingen of het ongeautoriseerd verspreiden van vertrouwelijke informatie, kan het noodzakelijk zijn over te gaan tot een persoonsgerichte inhoudelijke controle als bedoeld in artikel 6.

Uiteraard laat deze regeling onverlet wettelijke bevoegdheden, zoals die van instanties als politie, Koninklijke marechaussee of openbaar ministerie op het terrein van strafvordering of zoals die van inlichtingen- en veiligheidsdiensten op het terrein van nationale veiligheid. Indien bijvoorbeeld een bepaalde gedraging mogelijk ook een strafbaar feit oplevert dan kan uiteraard in het kader van een strafrechtelijk onderzoek door de daartoe bevoegde instanties worden opgetreden. Volledigheidshalve kan worden opgemerkt dat deze regeling voorts bestaande procedures inzake de afbakening tot strafrechtelijke onderzoeken onverlet laat. In het bijzonder kan daarbij worden gedacht aan Aanwijzing SG A/868 inzake een eenvormige procedure voor het instellen van huishoudelijke onderzoeken (ter voorkoming dat strafrechtelijke onderzoeken worden belemmerd). Een en ander betekent dat, wanneer de Koninklijke marechaussee een onderzoek wenst te verrichten naar een mogelijk strafbaar feit, het onderzoek door de SG wordt beëindigd danwel geschorst.

Sancties
Indien direct wordt vastgesteld danwel indien na een onderzoek als bedoeld in artikel 6 wordt vastgesteld dat de gedragsregels zijn overtreden, kan dit leiden tot een sanctie overeenkomstig de geldende rechtspositionele en tuchtrechtelijke regelgeving.

Bekendheid
Op het terrein van communicatie richting personeel van de regeling en de daarin vervatte gedragsregels zullen de nodige acties worden ondernomen. Naast de reguliere publicatie in de serie ministeriële publicaties zal aan de regeling in ieder geval de nodige bekendheid worden gegeven in de defensiekrant. Hiernaast zijn ook andere vormen van voorlichting mogelijk. Te denken valt aan bevordering van bewustwording van de gedragsregels via het Programma Beveiligingsbewustzijn van de beveiligingsautoriteit.

´s-Gravenhage, 15 mei 2009

DE STAATSSECRETARIS VAN DEFENSIE

Drs. J.G. de Vries