II

(Niet-wetgevingshandelingen)

BESLUITEN

BESLUIT VAN DE RAAD

van 23 september 2013

betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie

(2013/488/EU)

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 240, lid 3,

Gezien Besluit 2009/937/EU van de Raad van 1 december 2009 houdende vaststelling van zijn reglement van orde [1], en met name artikel 24,

Overwegende hetgeen volgt:

(1) Teneinde de werkzaamheden van de Raad op alle gebieden die de verwerking van geclassificeerde/gerubriceerde informatie (hierna: „gerubriceerde informatie") vereisen, verder tot ontplooiing te brengen, is het passend een integraal beveiligingssysteem voor de bescherming van gerubriceerde informatie op te zetten dat de Raad, het secretariaat-generaal daarvan en de lidstaten bestrijkt.

(2) Dit besluit moet worden toegepast telkens als de Raad, zijn voorbereidende instanties en het secretariaat-generaal van de Raad (hierna: „SGR") gerubriceerde EU-informatie (hierna: „EUCI") verwerken.

(3) In overeenstemming met de nationale wet- en regelgeving en in de mate die voor het functioneren van de Raad vereist is, moeten de lidstaten, wanneer hun bevoegde instanties, personeel of contractanten EUCI verwerken, voldoen aan dit besluit, zodat ieder ervan verzekerd is dat EUCI een gelijkwaardig beschermingsniveau krijgt.

(4) De Raad, de Commissie en de Europese Dienst voor extern optreden (EDEO) zijn gehouden gelijkwaardige beveiligingsnormen toe te passen voor de bescherming van EUCI.

(5) De Raad onderstreept dat het van belang is om, waar passend, het Europees Parlement en andere instellingen, organen of instanties van de Europese Unie te betrekken bij de beginselen, normen en regels voor de bescherming van gerubriceerde informatie die noodzakelijk zijn voor de bescherming van de belangen van de Europese Unie en haar lidstaten.

(6) De Raad dient een passend kader vast te stellen voor het delen van EUCI van de Raad met andere instellingen, organen of instanties van de Europese Unie, al naar het geval, overeenkomstig dit besluit en de vigerende interinstitutionele regelingen.

(7) De krachtens titel V, hoofdstuk 2, van het Verdrag betreffende de Europese Unie (VEU) opgerichte organen en instanties van de Unie, Europol en Eurojust zijn verplicht in het kader van hun interne organisatie de in dit besluit vervatte basisbeginselen en minimumnormen voor de bescherming van EUCI toe te passen indien deze verplichting is opgenomen in de handeling waarbij zij zijn opgericht.

(8) De toepassing van de door de Raad ter bescherming van EUCI vastgestelde beveiligingsvoorschriften bij crisisbeheersingsoperaties in het kader van titel V, hoofdstuk 2, VEU door het daarbij betrokken personeel is verplicht indien deze verplichting is opgenomen in de handeling van de Raad waarbij deze operaties worden ingesteld.

(9) De speciale vertegenwoordigers van de Europese Unie en de leden van hun teams zijn verplicht de door de Raad ter bescherming van EUCI vastgestelde beveiligingsvoorschriften toe te passen indien deze verplichting in de toepasselijke handeling van de Raad is opgenomen.

(10) Dit besluit laat de artikelen 15 en 16 van het Verdrag betreffende de werking van de Europese Unie (VWEU) en de instrumenten ter uitvoering daarvan onverlet.

(11) Dit besluit laat de bestaande werkwijzen van de lidstaten inzake het informeren van hun nationale parlementen over de werkzaamheden van de Europese Unie onverlet.

[1] PB L 325 van 11.12.2009, blz. 35.

(12) Teneinde te waarborgen dat de beveiligingsvoorschriften voor de bescherming van EUCI tijdig worden toegepast met het oog op de toetreding van de Republiek Kroatië tot de Europese Unie, dient dit besluit in werking te treden op de datum waarop het wordt bekendgemaakt,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Doel, toepassingsgebied en definities

1. Bij dit besluit worden de grondbeginselen en minimumnormen inzake beveiliging ter bescherming van EUCI vastgesteld.

2. Deze grondbeginselen en minimumnormen gelden voor de Raad en het SGR en moeten door de lidstaten overeenkomstig hun eigen wet- en regelgeving worden nageleefd, opdat alle partijen erop kunnen rekenen dat een gelijkwaardig niveau van bescherming voor EUCI wordt geboden.

3. Voor de toepassing van dit besluit gelden de definities in aanhangsel A.

Artikel 2

Definitie van EUCI, rubriceringen en markeringen

1. „Gerubriceerde EU-informatie" (EUCI): informatie of materiaal met een bepaalde EU-rubricering, waarvan openbaarmaking zonder machtiging de belangen van de Europese Unie of van één of meer van haar lidstaten in meerdere of mindere mate kan schaden.

2. Voor EUCI worden de volgende rubriceringen gehanteerd:

a) TRÈS SECRET UE/EU TOP SECRET: informatie en materiaal waarvan de openbaarmaking zonder machtiging de wezenlijke belangen van de Europese Unie of van één of meer van haar lidstaten uitzonderlijk ernstig kan schaden;

b) SECRET UE/EU SECRET: informatie en materiaal waarvan de openbaarmaking zonder machtiging de wezenlijke belangen van de Europese Unie of van één of meer van haar lidstaten ernstig kan schaden;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informatie en materiaal waarvan de openbaarmaking zonder machtiging de wezenlijke belangen van de Europese Unie of van één of meer van haar lidstaten kan schaden;

d) RESTREINT UE/EU RESTRICTED: informatie en materiaal waarvan de openbaarmaking zonder machtiging nadelig kan zijn voor de belangen van de Europese Unie of van één of meer van haar lidstaten.

3. EUCI krijgt een rubricering overeenkomstig lid 2. Daarnaast kan zij markeringen krijgen waarmee de gebieden waarop zij betrekking heeft worden aangeduid, de opsteller wordt geïdentificeerd, de verspreiding of het gebruik wordt beperkt of de geschiktheid voor vrijgave wordt aangegeven.

Artikel 3

Rubriceringsbeheer

1. De bevoegde instanties zorgen ervoor dat EUCI naar behoren wordt gerubriceerd en duidelijk als gerubriceerde informatie wordt aangemerkt, en dat de rubriceringsgraad ervan slechts zolang als nodig wordt behouden.

2. Zonder dat de opsteller er schriftelijk in heeft toegestemd, wordt EUCI niet lager gerubriceerd of gederubriceerd, noch wordt een in artikel 2, lid 3, bedoelde markering gewijzigd of verwijderd.

3. De Raad stelt een beveiligingsbeleid inzake het genereren van EUCI vast, met inbegrip van een praktische rubriceringsgids.

Artikel 4

Bescherming van gerubriceerde informatie

1. EUCI wordt beschermd in overeenstemming met dit besluit.

2. De houder van enigerlei vorm van EUCI is verantwoordelijk voor de bescherming ervan in overeenstemming met dit besluit.

3. Door de lidstaten in de structuren of netwerken van de Europese Unie ingevoerde gerubriceerde informatie met een nationale rubricering, wordt door de Raad en het SGR in overeenstemming met de voorschriften voor EUCI beschermd op het niveau dat volgens de in aanhangsel B vervatte concordantietabel van rubriceringen overeenstemt met het nationale niveau.

4. Het is mogelijk dat gebundelde EUCI een beschermingsniveau vereist dat overeenstemt met een hogere rubriceringsgraad dan die van de componenten ervan.

Artikel 5

Beheer van beveiligingsrisico's

1. Risico's voor EUCI worden beheerd als een proces. Dit proces wordt gericht op het bepalen van de bekende beveiligingsrisico's, het vaststellen van beveiligingsmaatregelen om deze risico's tot een aanvaardbaar niveau te beperken conform de grondbeginselen en minimumnormen van dit besluit, en toepassing van deze maatregelen in overeenstemming met het begrip „verdediging in de diepte" (hierna: „defense in depth") zoals omschreven in aanhangsel A. De doeltreffendheid van deze maatregelen wordt constant geëvalueerd.

2. De beveiligingsmaatregelen ter bescherming van EUCI, gedurende de gehele bestaanscyclus ervan, staan in verhouding tot de rubricering, de vorm en de omvang van de informatie of het materiaal, de locatie en constructie van de faciliteiten waar de EUCI is ondergebracht en de lokaal beoordeelde dreiging of kwaadwillige en/of criminele activiteiten, met name spionage, sabotage en terrorisme.

3. In de rampenplannen wordt rekening gehouden met de noodzaak om EUCI in noodsituaties te beschermen, teneinde toegang en openbaarmaking zonder machtiging of aantasting van de integriteit of beschikbaarheid te voorkomen.

4. In de bedrijfscontinuïteitsplannen worden preventie- en herstelmaatregelen opgenomen, om de gevolgen van ernstige storing of incidenten voor de verwerking en opslag van EUCI zo gering mogelijk te houden.

Artikel 6

Uitvoering van dit besluit

1. Indien nodig keurt de Raad, op aanbeveling van het Beveiligingscomité, een beveiligingsbeleid goed dat maatregelen ter uitvoering van dit besluit omvat.

2. Het Beveiligingscomité kan op zijn niveau beveiligingsrichtlijnen aannemen ter aanvulling of ondersteuning van dit besluit en het door de Raad goedgekeurde beveiligingsbeleid.

Artikel 7

Personeelsgerelateerde beveiliging

1. Personeelsgerelateerde beveiliging is de toepassing van maatregelen die ervoor moeten zorgen dat toegang tot EUCI uitsluitend wordt verleend:

— op basis van het „need-to-know"-principe,

— aan personen die in voorkomend geval op het vereiste niveau een beveiligingsonderzoek hebben ondergaan, en

— zijn geïnstrueerd over hun taken.

2. De procedures inzake veiligheidsmachtiging voor personen zijn van dien aard dat kan worden bepaald of een persoon, gelet op zijn loyaliteit en betrouwbaarheid, toegang kan worden verleend tot EUCI.

3. Eenieder die bij het SGR op grond van zijn taken toegang moet hebben tot EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger, dan wel deze moet verwerken, wordt slechts toegelaten indien hij is voorzien van de veiligheidsmachtiging die aan de rubricering beantwoordt. Deze personen moeten door het tot aanstelling bevoegde gezag van het SGR worden gemachtigd om toegang te krijgen tot EUCI tot een bepaald niveau en tot een bepaalde datum.

4. Het in artikel 15, lid 3, bedoelde personeel van de lidstaten dat uit hoofde van zijn taken toegang moet kunnen hebben tot EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger, dient daartoe voorzien te zijn van een veiligheidsmachtiging die aan de rubricering beantwoordt of anderszins ambtshalve, in overeenstemming met de nationale wet- en regelgeving naar behoren te zijn gemachtigd.

5. Degene wie toegang wordt verleend tot EUCI wordt voorafgaandelijk, en vervolgens met regelmatige tussenpozen, geïnstrueerd over zijn verantwoordelijkheid ter bescherming van EUCI overeenkomstig dit besluit, en dient deze verantwoordelijkheid te bevestigen.

6. De bepalingen ter uitvoering van dit artikel staan in bijlage I.

Artikel 8

Fysieke beveiliging

1. Fysieke beveiliging is de toepassing van fysieke en technische beschermingsmaatregelen om toegang zonder machtiging tot EUCI te voorkomen.

2. Met de fysieke beveiligingsmaatregelen wordt beoogd het binnendringen met list of geweld te verhinderen, acties waarvoor geen toestemming is verleend te ontraden, te verhinderen en op te sporen en op basis van het „need-to-know"-principe en ten aanzien van toegang tot EUCI onderscheid tussen personeelsleden mogelijk te maken. Deze maatregelen worden op een risicobeheerproces gebaseerd.

3. Fysieke beveiligingsmaatregelen worden ingesteld voor alle locaties, gebouwen, bureaus, ruimten, andere zones waarin EUCI wordt verwerkt of opgeslagen, alsmede zones waar communicatie- en informatiesystemen, zoals gedefinieerd in artikel 10, lid 2, zijn ondergebracht.

4. Zones waar EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger wordt opgeslagen, worden overeenkomstig bijlage II als beveiligde zones vastgesteld en door de bevoegde beveiligingsinstantie goedgekeurd.

5. Voor de bescherming van EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger worden uitsluitend goedgekeurde apparatuur en voorzieningen gebruikt.

6. De bepalingen ter uitvoering van dit artikel staan in bijlage II.

Artikel 9

Beheer van gerubriceerde informatie

1. Het beheer van gerubriceerde informatie houdt in dat administratieve maatregelen voor het controleren van EUCI gedurende de gehele bestaanscyclus ervan worden toegepast, teneinde de in de artikelen 7, 8 en 10 bedoelde maatregelen aan te vullen, en daarbij te helpen voorkomen dat en vaststellen of die informatie al dan niet opzettelijk in gevaar of verloren raakt. Die maatregelen hebben met name betrekking op het genereren, registreren, kopiëren, vertalen, het verlagen van de rubricering, het derubriceren en het vervoeren en vernietigen van EUCI.

2. Informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger wordt vóór verspreiding en bij ontvangst voor beveiligingsdoeleinden geregistreerd. De bevoegde instanties in het SGR en in de lidstaten zetten met dit doel een registratiesysteem op. Informatie met rubricering TRÈS SECRET UE/EU TOP SECRET wordt in speciaal daarvoor bestemde registers geregistreerd.

3. De diensten en werkruimten waar EUCI wordt verwerkt of opgeslagen, worden regelmatig door de bevoegde beveiligingsinstantie geïnspecteerd.

4. EUCI wordt als volgt tussen de diensten en werkruimten buiten fysiek beveiligde zones overgebracht:

a) EUCI wordt in de regel overgedragen met elektronische middelen, beschermd door encryptieproducten die overeenkomstig artikel 10, lid 6, zijn goedgekeurd;

b) indien geen gebruik wordt gemaakt van de onder a) bedoelde middelen, wordt EUCI overgebracht:

   i) op elektronische dragers (zoals USB-sticks, cd's, harde schijven) beschermd door encryptieproducten die overeenkomstig artikel 10, lid 6, zijn goedgekeurd, of

   ii) in alle overige gevallen, op de wijze die door de bevoegde beveiligingsinstantie is voorgeschreven in overeenstemming met de desbetreffende beschermingsmaatregelen in bijlage III.

5. De bepalingen ter uitvoering van dit artikel staan in de bijlagen III en IV.

Artikel 10

Bescherming van EUCI die in communicatie- en informatiesystemen wordt verwerkt

1. Informatieborging (hierna: „Information Assurance — IA") op het gebied van communicatie- en informatiesystemen is de overtuiging dat die systemen de erin opgenomen informatie zullen beschermen en zullen functioneren zoals nodig en wanneer nodig, onder de controle van legitieme gebruikers. Doeltreffende IA waarborgt passende niveaus van vertrouwelijkheid, integriteit, beschikbaarheid, onweerlegbaarheid en authenticiteit. IA is op een risicobeheerproces gebaseerd.

2. „Communicatie- en informatiesystemen" (hierna: „CIS") zijn systemen waarmee informatie in elektronische vorm kan worden verwerkt. Een communicatie- en informatiesysteem omvat alle functionele bestanddelen die voor het functioneren ervan vereist zijn, waaronder infrastructuur, organisatie, personeel en informatiebronnen. Dit besluit geldt voor communicatie- en informatiesystemen die EUCI verwerken.

3. CIS verwerken EUCI overeenkomstig het IA-concept.

4. Alle CIS worden aan een homologatieprocedure onderworpen. Met de homologatie wordt beoogd de verzekering te verkrijgen dat alle toepasselijke beveiligingsmaatregelen zijn getroffen en dat het niveau van bescherming van de EUCI en van het CIS overeenkomstig dit besluit voldoende wordt geacht. In de homologatieverklaring worden de maximaal toegelaten rubriceringsgraad van de informatie die door een CIS mag worden verwerkt, en de voorwaarden daarvoor vastgesteld.

5. CIS die informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en hoger verwerken, worden met beveiligingsmaatregelen beschermd opdat de informatie niet in gevaar raakt door onopzettelijke elektromagnetische emissies („TEMPEST-beveiligingsmaatregelen"). Deze beveiligingsmaatregelen dienen in verhouding te staan tot het risico op misbruik en de rubriceringsgraad van de gegevens.

6. Encryptieproducten die de EUCI moeten beschermen worden als volgt goedgekeurd:

a) de vertrouwelijkheid van informatie met rubricering SECRET UE/EU SECRET en hoger wordt beschermd door encryptieproducten die door de Raad, als overheid voor de goedkeuring van encryptieproducten (hierna: „Crypto Approval Authority — CAA"), op voorstel van het Beveiligingscomité zijn goedgekeurd;

b) de vertrouwelijkheid van informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of RESTREINT UE/EU RESTRICTED wordt beschermd door encryptieproducten die door de secretaris-generaal van de Raad (hierna: „de secretaris-generaal"), als CAA, op voorstel van het Beveiligingscomité zijn goedgekeurd.

Niettegenstaande punt b), kan de vertrouwelijkheid van EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of RESTREINT UE/EU RESTRICTED binnen nationale systemen van de lidstaten worden beschermd door encryptieproducten die door de CAA van een lidstaat zijn goedgekeurd.

7. Bij overdracht van EUCI met elektronische middelen worden goedgekeurde encryptieproducten gebruikt. Niettemin kunnen in noodgevallen of in geval van specifieke technische configuraties, zoals bepaald in bijlage IV, specifieke procedures worden toegepast.

8. De bevoegde instanties van het SGR en van de lidstaten stellen respectievelijk de volgende IA-functies in:

a) een IA-overheid (hierna: „IAA");

b) een TEMPEST-overheid (hierna: „TA");

c) een overheid voor de goedkeuring van encryptieproducten (hierna: „CAA — Crypto Approval Authority");

d) een overheid voor de verdeling van encryptieproducten (hierna: „CDA — Crypto Distribution Authority").

9. Voor ieder systeem stellen de bevoegde instanties van het SGR en van de lidstaten respectievelijk de volgende functies in:

a) een homologatieoverheid;

b) een operationele IAA.

10. De bepalingen ter uitvoering van dit artikel staan in bijlage IV.

Artikel 11

Industriële beveiliging

1. Industriële beveiliging is de toepassing van maatregelen om de bescherming van EUCI door contractanten of subcontractanten tijdens precontractuele onderhandelingen en tijdens de volledige looptijd van gerubriceerde opdrachten te waarborgen. In het kader van dergelijke opdrachten mag geen toegang worden verleend tot informatie met rubricering TRÈS SECRET UE/EU TOP SECRET.

2. Het SGR kan opdrachten plaatsen voor taken die toegang tot of verwerking of opslag van EUCI behelzen of vereisen door industriële of andere entiteiten die zijn ingeschreven in een lidstaat of in een derde staat die overeenkomstig artikel 13, lid 2, onder a) en b), een overeenkomst heeft gesloten of een administratieve regeling heeft getroffen.

3. Het SGR zorgt er als aanbestedende overheid voor dat aan de in dit besluit en in de gerubriceerde opdrachten vervatte minimumnormen voor industriële beveiliging is voldaan bij het plaatsen van gerubriceerde opdrachten bij industriële of andere entiteiten.

4. De nationale beveiligingsinstantie (National Security Authority, hierna: „NSA"), de aangewezen beveiligingsinstantie (Designated Security Authority, hierna: „DSA") of een andere bevoegde overheidsinstantie van elke lidstaat draagt er, in de mate dat zulks mogelijk is volgens de nationale wet- en regelgeving, zorg voor dat contractanten en subcontractanten die op hun grondgebied zijn geregistreerd, alle maatregelen nemen die nodig zijn voor de bescherming van EUCI tijdens precontractuele onderhandelingen en de uitvoering van een gerubriceerde opdracht.

5. In elke lidstaat zorgt de NSA, de DSA of een andere bevoegde overheidsinstantie overeenkomstig de nationale wet- en regelgeving ervoor dat in de betrokken lidstaat geregistreerde contractanten of subcontractanten die deelnemen aan gerubriceerde opdrachten of onderaanneming waarvoor toegang vereist is tot informatie met de rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET binnen hun gebouwen, tijdens de uitvoering van de opdrachten of in de precontractuele fase beschikken over een veiligheidsmachtiging voor een vestiging (Facility Security Clearance, hierna: „FSC"), in overeenstemming met de dienovereenkomstige rubricering.

6. Personeel van contractanten of subcontractanten dat voor de uitvoering van een gerubriceerde opdracht toegang moet hebben tot als CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET gerubriceerde informatie krijgt van de NSA/DSA of een andere bevoegde overheidsinstantie een persoonlijke veiligheidsmachtiging (PVM) overeenkomstig de nationale wet- en regelgeving en de minimumbeveiligingsvoorschriften van bijlage I.

7. De bepalingen ter uitvoering van dit artikel staan in bijlage V.

Artikel 12

Delen van EUCI

1. De Raad bepaalt onder welke voorwaarden hij EUCI die in zijn bezit is, kan delen met andere instellingen, organen of instanties van de Europese Unie. Daartoe kan een adequaat kader worden opgezet, onder meer door interinstitutionele of andere daartoe vereiste regelingen te treffen.

2. Dit kader moet de garantie bieden dat EUCI wordt beschermd in overeenstemming met de bijbehorende rubriceringsgraad en volgens basisbeginselen en minimumnormen die gelijkwaardig zijn aan die welke in dit besluit zijn neergelegd.

Artikel 13

Uitwisseling van gerubriceerde informatie met derde staten en internationale organisaties

1. Indien de Raad bepaalt dat het noodzakelijk is EUCI uit te wisselen met een derde staat of een internationale organisatie, wordt daartoe een adequaat kader opgezet.

2. Om dat kader tot stand te brengen en wederzijdse voorschriften voor de bescherming van de uitgewisselde gerubriceerde informatie vast te stellen,

a) sluit de Europese Unie met derde landen of internationale organisaties overeenkomsten betreffende beveiligingsprocedures voor de uitwisseling en bescherming van gerubriceerde informatie (hierna: „overeenkomsten voor de beveiliging van informatie"), of

b) kan de secretaris-generaal namens het SGR een administratieve regeling treffen overeenkomstig punt 17 van bijlage VI indien de rubriceringsgraad van vrij te geven EUCI in het algemeen niet hoger is dan RESTREINT UE/EU RESTRICTED.

3. De in lid 2 bedoelde informatiebeveiligingovereenkomst of administratieve regeling bevat bepalingen die ervoor zorgen dat door derde staten of internationale organisaties ontvangen EUCI wordt beschermd in overeenstemming met haar rubriceringsgraad en volgens minimumnormen die niet minder streng zijn dan die welke in dit besluit zijn vastgelegd.

4. Het besluit tot vrijgave van EUCI, afkomstig van de Raad, aan een derde staat of een internationale organisatie wordt per geval door de Raad genomen, naargelang van de aard en de inhoud van die informatie, de noodzaak dat de ontvanger er kennis van neemt en het nut dat de Europese Unie van de vrijgave heeft. Gerubriceerde informatie die niet afkomstig is van de Raad wordt door het SGR slechts met schriftelijke toestemming van de opsteller vrijgegeven. Indien de opsteller niet te bepalen is, beslist de Raad op eigen verantwoordelijkheid.

5. Evaluatiebezoek wordt georganiseerd om de doeltreffendheid van de door een derde staat of een internationale organisatie genomen maatregelen ter beveiliging van de verstrekte of uitgewisselde EUCI te verifiëren.

6. De bepalingen ter uitvoering van dit artikel staan in bijlage VI.

Artikel 14

Schending van de beveiliging en in gevaar brengen van EUCI

1. De beveiliging wordt geschonden als gevolg van een handeling die of een verzuim dat in strijd is met de beveiligingsvoorschriften van dit besluit.

2. EUCI raakt in gevaar wanneer, ten gevolge van een inbreuk op de beveiligingsvoorschriften, de informatie geheel of gedeeltelijk aan onbevoegden is bekendgemaakt.

3. Een schending of vermoedelijke schending van de beveiligingsvoorschriften wordt onmiddellijk aan de bevoegde beveiligingsinstantie gemeld.

4. Indien bekend of redelijkerwijs aan te nemen is dat EUCI in gevaar of verloren is geraakt, doet de NSA of een andere bevoegde instantie overeenkomstig de toepasselijke wetten en voorschriften het nodige om:

a) de opsteller daarvan in kennis te stellen;

b) ervoor te zorgen dat de zaak wordt onderzocht door personeel dat niet rechtstreeks met de schending te maken heeft, teneinde de toedracht vast te stellen;

c) de eventuele schade te beoordelen die aan de belangen van de Europese Unie of van de lidstaten is berokkend;

d) herhaling te voorkomen, en

e) de bevoegde instanties in kennis te stellen van de stappen die zijn ondernomen.

5. Eenieder die verantwoordelijk is voor schending van de beveiligingsvoorschriften van dit besluit, stelt zich bloot aan disciplinaire maatregelen, overeenkomstig de geldende regelgeving. Eenieder die verantwoordelijk is voor het in gevaar of verloren raken van EUCI, stelt zich bloot aan disciplinaire maatregelen en/of strafvervolging, in overeenstemming met de geldende wet- en regelgeving.

Artikel 15

Verantwoordelijkheid voor de uitvoering

1. De Raad neemt de nodige maatregelen om de algehele consistentie bij de toepassing van dit besluit te verzekeren.

2. De secretaris-generaal neemt de nodige maatregelen om ervoor te zorgen dat bij de verwerking of de opslag van EUCI en andere gerubriceerde informatie dit besluit in de werkruimten van de Raad en binnen het SGR wordt toegepast door de ambtenaren en andere personeelsleden van het SGR, het bij het SGR gedetacheerde personeel en de contractanten van het SGR.

3. De lidstaten nemen, in overeenstemming met hun nationale wet- en regelgeving, alle passende maatregelen om ervoor te zorgen dat bij de verwerking of de opslag van EUCI dit besluit wordt nageleefd door:

a) de personeelsleden van de permanente vertegenwoordigingen van de lidstaten bij de Europese Unie, en de leden van de nationale delegaties die bijeenkomsten van de Raad of zijn voorbereidende instanties bijwonen, of deelnemen aan andere werkzaamheden van de Raad;

b) hun andere personeelsleden die bij de nationale overheid in dienst of gedetacheerd zijn, hetzij op hun eigen grondgebied, hetzij daarbuiten;

c) eenieder die in de lidstaten ambtshalve naar behoren gemachtigd is om toegang te krijgen tot EUCI, en

d) hun contractanten, hetzij op hun eigen grondgebied, hetzij daarbuiten.

Artikel 16

Organisatie van de beveiliging binnen de Raad

1. In het kader van zijn rol bij het waarborgen van de algehele consistentie bij de toepassing van dit besluit, hecht de Raad zijn goedkeuring aan:

a) de in artikel 13, lid 2, onder a), bedoelde overeenkomsten;

b) besluiten waarbij machtiging wordt verleend tot of toegestemd wordt in vrijgave van EUCI, van oorsprong in of in het bezit van de Raad, aan derde staten en internationale organisaties, met inachtneming van het beginsel van toestemming van de bron;

c) een door het Beveiligingscomité aanbevolen jaarlijks programma van evaluatiebezoeken aan de diensten en werkruimten van de lidstaten en aan de organen, instanties en entiteiten van de Europese Unie die dit besluit of de beginselen daarvan toepassen, en van evaluatiebezoeken aan derde staten en internationale organisaties, om de doeltreffendheid van de ter bescherming van EUCI genomen maatregelen te verifiëren, en

d) het in artikel 6, lid 1, bedoelde beveiligingsbeleid.

2. De secretaris-generaal is de beveiligingsinstantie van het SGR. In die hoedanigheid wordt door hem:

a) het beveiligingsbeleid van de Raad gevoerd en bewaakt;

b) met de NSA's van de lidstaten samengewerkt in alle beveiligingskwesties met betrekking tot de bescherming van gerubriceerde informatie die de werkzaamheden van de Raad raakt;

c) aan ambtenaren, andere personeelsleden en gedetacheerde nationale deskundigen van het SGR, toegang verleend tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger, overeenkomstig artikel 7, lid 3;

d) in voorkomend geval, onderzoek gelast in gevallen waarin gerubriceerde informatie die in het bezit is of afkomstig is van de Raad, in gevaar of verloren is geraakt of het vermoeden daaromtrent bestaat, en wordt de bevoegde beveiligingsinstanties om hulp verzocht bij het onderzoek;

e) de beveiliging ter bescherming van gerubriceerde informatie in de werkruimten van het SGR periodiek aan inspectie onderworpen;

f) periodiek een evaluatiebezoek verricht om een beeld te krijgen van de regeling inzake beveiliging van EUCI in de organen, instanties en entiteiten van de Unie die dit besluit of de beginselen daarvan toepassen;

g) samen en in overeenstemming met de betrokken NSA, periodiek een evaluatie verricht van de regeling inzake beveiliging ter bescherming van EUCI in de diensten en werkruimten van de lidstaten;

h) ervoor gezorgd dat over de beveiligingsmaatregelen indien nodig coördinatie plaatsvindt met de bevoegde instanties van de lidstaten die verantwoordelijk zijn voor de bescherming van gerubriceerde informatie en, in voorkomend geval, derde staten of internationale organisaties, onder meer met betrekking tot de aard van de bedreigingen voor de beveiliging van EUCI en de middelen om zich daartegen te beschermen, en

i) de in artikel 13, lid 2, onder b), bedoelde administratieve regeling getroffen.

Bij het vervullen van deze taken wordt de secretaris-generaal bijgestaan door de dienst Beveiliging van het SGR.

3. Voor de toepassing van artikel 15, lid 3, moeten de lidstaten:

a) een NSA zoals vermeld in aanhangsel C aanwijzen die verantwoordelijk is voor de regeling inzake beveiliging ter bescherming van EUCI opdat:

i) EUCI die in het bezit is van nationale departementen, entiteiten of organisaties, hetzij publiek hetzij particulier, in het binnenland of het buitenland, overeenkomstig dit besluit beschermd zijn;

ii) de regeling inzake beveiliging ter bescherming van EUCI periodiek wordt geïnspecteerd of geëvalueerd;

iii) alle personen die werkzaam zijn bij een nationale overheid of van een contractant en aan wie toegang kan worden verleend tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger, passend zijn gescreend of anderszins ambtshalve, in overeenstemming met de nationale wet- en regelgeving, naar behoren zijn gemachtigd;

iv) de beveiligingsprogramma's worden opgezet die noodzakelijk zijn om het risico dat EUCI in gevaar of verloren raakt, tot een minimum te beperken;

v) beveiligingskwesties met betrekking tot EUCI worden gecoördineerd met andere bevoegde nationale instanties, zoals de in dit besluit genoemde instanties, en

vi) gevolg wordt gegeven aan een gerechtvaardigd verzoek om een veiligheidsonderzoek, in het bijzonder uitgaande van de op grond van titel V, hoofdstuk 2, VEU opgerichte organen, instanties en entiteiten van de Unie, de op grond van titel V, hoofdstuk 2, VEU ingestelde EU-operaties, en de speciale vertegenwoordigers van de EU (SVEU's) en hun teams die dit besluit of de beginselen daarvan toepassen;

b) ervoor zorgen dat hun bevoegde instanties hun regering, en langs die weg de Raad, van informatie en advies dienen over de aard van de bedreigingen voor de beveiliging van EUCI en de middelen om zich daartegen te beschermen.

Artikel 17

Beveiligingscomité

1. Een beveiligingscomité wordt ingesteld. Het onderzoekt en beoordeelt alle beveiligingskwesties die binnen het toepassingsgebied van dit besluit vallen, en doet in voorkomend geval aanbevelingen aan de Raad.

2. Het beveiligingscomité bestaat uit vertegenwoordigers van de NSA's van de lidstaten; zijn vergaderingen worden bijgewoond door een vertegenwoordiger van de Commissie en van de EDEO. Het wordt voorgezeten door de secretaris-generaal of diens aangewezen vertegenwoordiger. Het komt op instructie van de Raad of op verzoek van de secretaris-generaal of een NSA bijeen.

In gevallen waarin agendapunten betrekking hebben op organen, instanties en entiteiten van de Europese Unie die dit besluit of de beginselen daarvan toepassen, kunnen hun vertegenwoordigers op de vergadering worden uitgenodigd.

3. Het beveiligingscomité regelt zijn werkzaamheden in die zin dat het aanbevelingen over specifieke beveiligingsgebieden kan verstrekken. Het stelt een deskundigengroep voor het deelgebied IA-kwesties en in voorkomend geval voor andere deelgebieden in. Het stelt het mandaat voor deze deelgebieden vast en ontvangt verslagen over de desbetreffende activiteiten, indien nodig vergezeld van aanbevelingen voor de Raad.

Artikel 18

Vervanging van voorgaande besluiten

1. Besluit 2011/292/EU van de Raad [1] wordt ingetrokken en vervangen door dit besluit.

2. Alle in overeenstemming met Besluit 2001/264/EG van de Raad [2] en Besluit 2011/292/EU gerubriceerde EUCI blijft beschermd overeenkomstig de bepalingen dienaangaande in onderhavig besluit.

Artikel 19

Inwerkingtreding

Dit besluit treedt in werking op de dag van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Gedaan te Brussel, 23 september 2013.

Voor de Raad
De voorzitter
V. JUKNA

[1] Besluit 2011/292/EU van de Raad van 31 maart 2011 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-gegevens (PB L 141 van 27.5.2011, blz. 17).

[2] Besluit 2001/264/EG van de Raad van 19 maart 2001 tot vaststelling van beveiligingsvoorschriften van de Raad (PB L 101 van 11.4.2001, blz. 1).

BIJLAGEN

BIJLAGE I

Personeelsgerelateerde beveiliging

BIJLAGE II

Fysieke beveiliging

BIJLAGE III

Beheer van gerubriceerde informatie

BIJLAGE IV

Bescherming van in CIS verwerkte EUCI

BIJLAGE V

Industriële beveiliging

BIJLAGE VI

Uitwisseling van gerubriceerde informatie met derde staten en internationale organisaties

BIJLAGE I

PERSONEELSGERELATEERDE BEVEILIGING

I. INLEIDING

1. Deze bijlage bevat bepalingen ter uitvoering van artikel 7. Ze legt de criteria vast aan de hand waarvan kan worden bepaald of aan een persoon, rekening houdend met zijn loyaliteit en betrouwbaarheid, toegang tot gerubriceerde EU-informatie (hierna: „EUCI") mag worden verleend, alsook de onderzoeks- en administratieve procedures die daartoe moeten worden gevolgd.

II. HET VERLENEN VAN TOEGANG TOT EUCI

2. Een persoon wordt alleen toegang tot gerubriceerde informatie verleend indien:

a) zijn noodzaak tot kennisname is vastgesteld;

b) hij is geïnstrueerd over de beveiligingsvoorschriften en -procedures voor de bescherming van EUCI en hij zijn verantwoordelijkheid in verband met de bescherming van dergelijke informatie heeft bevestigd, en

c) in het geval van als CONFIDENTIEL UE/EU CONFIDENTIAL of hoger gerubriceerde informatie:

— hem een PVM voor het passende niveau is verleend of hij anderszins uit hoofde van zijn functie daartoe naar behoren is gemachtigd in overeenstemming met de nationale wet- en regelgeving, of

— in het geval van ambtenaren van het SGR, andere personeelsleden of gedetacheerde nationale deskundigen, hem door het tot aanstelling bevoegde gezag van het SGR tot een bepaald niveau en tot een bepaalde datum toegang tot EUCI is verleend overeenkomstig de punten 16 tot en met 25 hieronder.

3. Elke lidstaat en het SGR bepalen in hun structuren de functies waarvoor toegang tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger is vereist en verlangen daartoe een veiligheidsmachtiging voor het passende niveau.

III. EISEN INZAKE PERSOONLIJKE VEILIGHEIDSMACHTING

4. De nationale beveiligingsinstanties (hierna: „NSA's") of andere bevoegde nationale instanties zijn er, na ontvangst van een naar behoren gemotiveerd verzoek, verantwoordelijk voor dat hun onderdanen voor wie toegang tot als CONFIDENTIEL UE/EU CONFIDENTIAL of hoger gerubriceerde informatie vereist is, aan een veiligheidsonderzoek worden onderworpen. De onderzoeksnormen dienen in overeenstemming te zijn met de nationale wet- en regelgeving, zodat een PVM kan worden afgegeven of de verzekering kan worden gegeven dat de betrokkene toegang mag hebben tot EUCI, waar passend.

5. Mocht de betrokkene op het grondgebied van een andere lidstaat of een derde staat verblijven, dan verzoeken de bevoegde nationale instanties om bijstand van de bevoegde instantie van de staat van verblijf, in overeenstemming met de nationale wet- en regelgeving. De lidstaten helpen elkaar bij het verrichten van het veiligheidsonderzoek, in overeenstemming met de nationale wet- en regelgeving.

6. Wanneer de nationale wet- en regelgeving zulks toestaat, mogen NSA's of andere bevoegde nationale autoriteiten onderzoeken doen naar niet-onderdanen die toegang vragen tot als CONFIDENTIEL UE/EU CONFIDENTIAL of hoger gerubriceerde informatie. De onderzoeksnormen zijn in overeenstemming met de nationale wet- en regelgeving.

Criteria voor het veiligheidsonderzoek

7. De loyaliteit en de betrouwbaarheid van een persoon ten behoeve van een veiligheidsmachtiging voor toegang tot als CONFIDENTIEL UE/EU CONFIDENTIAL of hoger gerubriceerde informatie worden vastgesteld door middel van een veiligheidsonderzoek. De bevoegde nationale instantie maakt een algemene beoordeling aan de hand van de bevindingen van een dergelijk veiligheidsonderzoek. De belangrijkste criteria die voor dat doel worden gehanteerd, moeten — voor zover mogelijk krachtens de nationale wet- en regelgeving — betrekking hebben op de vraag of die persoon:

a) enigerlei handeling heeft gepleegd of getracht te plegen op het vlak van spionage, terrorisme, sabotage, verraad of opruiing, dan wel hiertoe heeft samengezworen met één of meer anderen of één of meer anderen heeft geholpen bij of aangezet tot het plegen van dergelijke handelingen;

b) zich inlaat of heeft ingelaten met spionnen, terroristen of saboteurs, dan wel met personen die redelijkerwijs als zodanig verdacht zijn, of zich inlaat of heeft ingelaten met vertegenwoordigers van organisaties of buitenlandse mogendheden, met inbegrip van buitenlandse inlichtingendiensten, die de beveiliging van de Europese Unie en/of de lidstaten kunnen bedreigen, tenzij deze contacten werden toegestaan in het kader van officiële werkzaamheden;

c) lid is of is geweest van enige organisatie die met gewelddadige, subversieve of andere onwettige middelen onder meer tracht de regering van een lidstaat omver te werpen, de grondwettelijke orde van een lidstaat te veranderen of de vorm of het beleid van de regering ervan te veranderen;

d) voorstander is of voorstander is geweest van een onder c) omschreven organisatie of nauwe banden heeft gehad met leden van een dergelijke organisatie;

e) opzettelijk substantiële, met name beveiligingsgevoelige informatie heeft achtergehouden, verkeerd heeft weergegeven of vervalst, dan wel opzettelijk heeft gelogen bij het invullen van een beveiligingsvragenlijst voor het personeel of tijdens een beveiligingsgesprek;

f) veroordeeld is wegens een strafbaar feit of strafbare feiten;

g) aan alcohol verslaafd is of is geweest, drugs gebruikt of heeft gebruikt, dan wel geneesmiddelen misbruikt of heeft misbruikt;

h) gedrag vertoont of heeft vertoond dat hem mogelijk kwetsbaar kan maken voor druk of chantage;

i) in woorden of daden blijk heeft gegeven van oneerlijkheid, gebrek aan loyaliteit of onbetrouwbaarheid;

j) ernstig of herhaaldelijk inbreuk gemaakt heeft op de beveiligingsvoorschriften, dan wel getracht heeft of erin geslaagd is niet toegestane activiteiten ten aanzien van communicatie- en informatiesystemen uit te voeren, en

k) gevoelig kan zijn voor druk (bv. door het bezit van één of meer niet-EU-nationaliteiten of via verwanten of anderen in zijn omgeving die op hun beurt kwetsbaar zouden kunnen zijn voor buitenlandse inlichtingendiensten, terreurgroepen of andere subversieve organisaties, of personen wier doelstellingen de veiligheidsbelangen van de Europese Unie en/of de lidstaten kunnen bedreigen).

8. In voorkomend geval en rekening houdend met de nationale wet- en regelgeving, kan de financiële en medische achtergrond van een persoon tijdens het veiligheidsonderzoek eveneens als relevant worden beschouwd.

9. In voorkomend geval en rekening houdend met de nationale wet- en regelgeving, kunnen het karakter, het gedrag en de levenssituatie van de echtgeno(o)t(e), partner of naaste familieleden tijdens het veiligheidsonderzoek eveneens als relevant worden beschouwd.

Onderzoeksvereisten voor toegang tot EUCI

Initiële toekenning van een veiligheidsmachtiging

10. De initiële veiligheidsmachtiging voor toegang tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET is gebaseerd op een veiligheidsonderzoek dat ten minste de jongste vijf jaar bestrijkt, dan wel de periode vanaf de leeftijd van achttien jaar, indien deze korter is, en dat het volgende omvat:

a) het invullen van een nationale vragenlijst voor beveiliging van personen voor het niveau van EUCI waartoe de betrokkene toegang kan vragen. De ingevulde vragenlijst wordt toegestuurd aan de bevoegde beveiligingsinstantie;

b) identiteitscontrole/staatsburgerschap/nationaliteitssituatie — de datum, de geboorteplaats en de identiteit van de betrokkene moeten worden gecontroleerd. De situatie in verband met burgerschap en/of nationaliteit in heden en verleden van de betrokkene moet worden vastgesteld. Dit houdt onder meer een beoordeling in van iedere vorm van kwetsbaarheid voor druk vanuit het buitenland, bijvoorbeeld naar aanleiding van een vroeger verblijf of contacten in het verleden, en

c) verificatie van wat nationaal en lokaal over de betrokkene is geboekstaafd — de informatie van het nationale beveiligingsregister en het nationale strafregister, indien voorhanden, en/of andere, vergelijkbare overheids- en politie-informatie moeten worden gecontroleerd. Ook de informatie van wetshandhavingsinstanties met een wettelijke bevoegdheid in de plaats waar de betrokkene heeft verbleven of in loondienst is geweest, moet worden gecontroleerd.

11. De initiële veiligheidsmachtiging voor toegang tot informatie met rubricering TRÈS SECRET UE/EU TOP SECRET vindt plaats op basis van een veiligheidsonderzoek dat ten minste de jongste tien jaar bestrijkt, dan wel de periode vanaf de leeftijd van achttien jaar, indien deze korter is. Indien gesprekken worden gevoerd als bedoeld in punt e) hieronder, moet het onderzoek ten minste de afgelopen zeven jaar bestrijken, dan wel de periode vanaf de leeftijd van achttien jaar, indien deze korter is. Naast de in punt 7 bedoelde criteria worden, voordat een PVM op het niveau TRÈS SECRET UE/EU TOP SECRET wordt verleend, ook de onderstaande elementen onderzocht voor zover mogelijk volgens nationale wet- en regelgeving; en deze elementen kunnen ook voorafgaand aan de verlening van een PVM op het niveau van CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET worden onderzocht, indien nationale wet- en regelgeving zulks voorschrijven:

a) financiële situatie — er dient informatie te worden vergaard over de financiële situatie van de betrokkene om na te gaan of er naar aanleiding van ernstige financiële moeilijkheden kwetsbaarheid voor buitenlandse of binnenlandse druk bestaat of om een verklaring te vinden voor eventuele welstand van onduidelijke herkomst;

b) onderwijs — er dient informatie te worden vergaard over de onderwijsachtergrond van de betrokkene op scholen, universiteiten en andere onderwijsinstellingen die hij sinds zijn achttiende verjaardag, of gedurende een periode die de onderzoekende instantie passend acht, heeft bezocht;

c) werkkring — er dient informatie te worden vergaard betreffende de huidige en vroegere werkzaamheden van de betrokkene, waarbij verwezen wordt naar bronnen als bescheiden over zijn arbeidsverleden, rapporten over zijn prestaties en doelmatigheid bij het werk, alsmede werkgevers of meerderen;

d) militaire dienst — indien van toepassing: de legerdienst van de betrokkene alsmede de aard van het ontslag daaruit, dienen te worden nagegaan, en

e) sollicitatiegesprekken — indien de nationale wetgeving hierin voorziet en zulks toelaat, wordt met de betrokkene een gesprek of een aantal gesprekken gevoerd. Er worden ook gesprekken gevoerd met andere personen die, gezien hun positie, een onafhankelijk oordeel over de achtergrond van de betrokkene en over zijn activiteiten, loyaliteit en betrouwbaarheid kunnen verstrekken. Indien het in de betreffende lidstaat gebruikelijk is de onderzochte persoon om referenties te vragen, dient met de betreffende personen een gesprek plaats te vinden, tenzij er goede redenen zijn om zulks niet te doen.

12. Indien nodig en in overeenstemming met de nationale wet- en regelgeving kan extra onderzoek worden verricht om alle relevante informatie die beschikbaar is over een persoon te kunnen uitwerken en alle negatieve informatie te kunnen bevestigen dan wel ontkrachten.

Hernieuwing van een veiligheidsmachtiging

13. Na de initiële toekenning van een veiligheidsmachtiging wordt deze, mits de betrokkene ononderbroken bij een nationale overheid of het SGR werkzaam is geweest en nog steeds toegang tot EUCI dient te hebben, opnieuw bezien met het oog op hernieuwing; dit gebeurt na een termijn van ten hoogste vijf jaar voor een machtiging voor het niveau TRÈS SECRET UE/EU TOP SECRET, en tien jaar voor een machtiging voor het niveau SECRET UE/EU SECRET en CONFIDENTIEL UE/EU CONFIDENTIAL; deze termijn gaat in op de datum van kennisgeving van de uitkomst van het laatste veiligheidsonderzoek waarop de machtiging gebaseerd is. Alle veiligheidsonderzoeken met het oog op de hernieuwing van een PVM hebben betrekking op de periode die sinds het vorige onderzoek is verstreken.

14. Voor de hernieuwing van de veiligheidsmachtiging worden de in de punten 10 en 11 vermelde elementen onderzocht.

15. Het verzoek om hernieuwing wordt tijdig ingediend, rekening houdend met de gemiddelde termijn die voor het veiligheidsonderzoek nodig is. Wanneer de bevoegde NSA of een andere bevoegde nationale instantie evenwel het betrokken verzoek om hernieuwing en de overeenkomstige beveiligingsvragenlijst voor het verstrijken van de veiligheidsmachtiging heeft ontvangen, maar het noodzakelijke veiligheidsonderzoek niet voor het verstrijken van de veiligheidsmachtiging is afgerond, kan de bevoegde nationale overheid de geldigheid van de bestaande veiligheidsmachtiging met maximaal twaalf maanden verlengen, wanneer de nationale wet- en regelgeving zulks toestaan. Indien het veiligheidsonderzoek aan het einde van deze periode van twaalf maanden nog niet is voltooid, dient de betrokkene taken uit te oefenen waarvoor geen veiligheidsmachtiging vereist is.

Machtigingsprocedures in het SGR

16. Voor ambtenaren en andere personeelsleden van het SGR zendt de Veiligheidsautoriteit van het SGR de ingevulde vragenlijst voor de veiligheid van personen toe aan de NSA van de lidstaat waarvan de betrokkene onderdaan is, met het verzoek een veiligheidsonderzoek uit te voeren voor het niveau van EUCI waartoe toegang van de betrokkene noodzakelijk zal zijn.

17. Indien een persoon een veiligheidsmachtiging voor toegang tot EUCI heeft aangevraagd, en het SGR de beschikking krijgt over informatie over de betrokkene die voor het veiligheidsonderzoek van belang is, stelt het SGR de desbetreffende NSA hiervan in overeenstemming met de regels en voorschriften ter zake in kennis.

18. Nadat het veiligheidsonderzoek is afgesloten, brengt betrokken NSA de beveiligingsinstantie van het SGR op de hoogte van de uitkomst ervan, met gebruikmaking van het door het Beveiligingscomité voor de briefwisseling voorgeschreven standaardmodel.

a) Wanneer het veiligheidsonderzoek tot de zekerheid leidt dat er geen informatie bekend is die doet twijfelen aan de loyaliteit en betrouwbaarheid van de betrokkene, kan het tot aanstelling bevoegde gezag van het SGR hem een veiligheidsmachtiging voor toegang tot EUCI geven en tot een bepaalde datum toegang verlenen tot EUCI tot op het relevante niveau.

b) Wanneer het veiligheidsonderzoek niet tot die zekerheid leidt, stelt het tot aanstelling bevoegde gezag van het SGR de betrokkene daarvan in kennis; deze kan vragen om door het tot aanstelling bevoegde gezag te worden gehoord. Het tot aanstelling bevoegde gezag mag de bevoegde NSA alle aanvullende verduidelijkingen vragen die de overheid, volgens de nationale wet- en regelgeving, mag verstrekken. Indien de uitkomst wordt bevestigd, wordt geen machtiging voor toegang tot EUCI verleend.

19. Voor het veiligheidsonderzoek en de resultaten van het veiligheidsonderzoek gelden de in de betrokken lidstaat van toepassing zijnde wet- en regelgeving, ook wat de mogelijkheden tot beroep betreft. Tegen besluiten van het tot aanstelling bevoegde gezag van het SGR kan beroep worden aangetekend in overeenstemming met het statuut van de ambtenaren van de Europese Unie en de regeling die van toepassing is op de andere personeelsleden van de Europese Unie, vastgesteld in Verordening (EEG, Euratom, EGKS) nr. 259/68 [1] (hierna: „het statuut").

20. Nationale deskundigen die bij het SGR worden gedetacheerd voor een functie waarvoor toegang tot EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en hoger is vereist, leggen een geldig certificaat van veiligheidsmachtiging voor personen (CPVM) voor toegang tot EUCI aan de Veiligheidsautoriteit van het SGR over alvorens hun taak aan te vatten; op basis daarvan geeft het tot aanstelling bevoegde gezag een machtiging voor toegang tot EUCI af.

21. Het SGR aanvaardt de door een andere EU-instelling, een ander EU-orgaan of een andere EU-instantie verleende machtiging voor toegang tot EUCI, mits deze geldig blijft. De machtiging bestrijkt elke taak die de betrokkene in het SGR op zich neemt. De EU-instelling, het EU-orgaan of de EU-instantie waar de betrokkene in dienst treedt, geeft de bevoegde NSA kennis van de wijziging van werkgever.

22. Indien de periode waarin een persoon in dienst is, niet begint binnen twaalf maanden na de kennisgeving van de uitkomst van het veiligheidsonderzoek aan het tot aanstelling bevoegde gezag van het SGR, of indien de betrokkene zijn dienst voor een periode van twaalf maanden heeft onderbroken en gedurende die tijd niet bij het SGR of in een functie bij een nationale overheid van een lidstaat heeft gewerkt, wordt deze uitkomst naar de betrokken NSA verwezen voor de bevestiging dat die nog steeds geldig en passend is.

[1] Verordening (EEG, Euratom, EGKS) nr. 259/68 van de Raad van 29 februari 1968 tot vaststelling van het Statuut van de ambtenaren van de Europese Gemeenschappen en de Regeling welke van toepassing is op de andere personeelsleden van deze Gemeenschappen, alsmede van bijzondere maatregelen welke tijdelijk op de ambtenaren van de Commissie van toepassing zijn (PB L 56 van 4.3.1968, blz. 1).

23. Indien een persoon een veiligheidsmachtiging voor toegang tot EUCI is verleend, en het SGR de beschikking krijgt over informatie dat er in verband met die persoon een beveiligingsrisico bestaat, stelt het SGR, overeenkomstig de regels en voorschriften ter zake, de desbetreffende NSA hiervan in kennis en kan het de toegang tot de EUCI opschorten of de machtiging voor toegang tot de EUCI intrekken.

24. Wanneer de NSA het SGR in kennis stelt van de intrekking van een overeenkomstig punt 18, onder a), gegeven verzekering voor een persoon die over een machtiging voor toegang tot EUCI beschikt, kan het tot aanstelling bevoegde gezag van het SGR de NSA elke toelichting vragen die de instantie volgens de nationale wet- en regelgeving mag verstrekken. Indien de negatieve informatie wordt bevestigd, wordt de machtiging ingetrokken en wordt de betrokkene de toegang tot EUCI en tot functies waar dergelijke toegang mogelijk is of waar hij de beveiliging in gevaar zou kunnen brengen, ontzegd.

25. Elke beslissing om een machtiging voor toegang tot EUCI van een ambtenaar of ander personeelslid van het SGR in te trekken of op te schorten, alsook waar nodig de redenen daarvoor, worden meegedeeld aan de betrokkene, die kan vragen om door het tot aanstelling bevoegde gezag te worden gehoord. Voor door een NSA verstrekte informatie gelden de in de betrokken lidstaat van toepassing zijnde wetten en voorschriften, ook wat de mogelijkheden tot beroep betreft. Tegen besluiten van het tot aanstelling bevoegde gezag van het SGR kan beroep worden aangetekend in overeenstemming met het statuut.

Aantekeningen van veiligheidsmachtigingen en van machtigingen

26. De aantekeningen betreffende CPVM's en machtigingen die met het oog op toegang tot als CONFIDENTIEL UE/EU CONFIDENTIAL of hoger gerubriceerde informatie aan personen worden verleend, worden respectievelijk door de lidstaat en het SGR bewaard. Deze aantekeningen bevatten ten minste het niveau van de EUCI waartoe een persoon toegang kan worden verleend, de datum van verlening van de veiligheidsmachtiging en de geldigheidsduur ervan.

27. De bevoegde beveiligingsinstantie kan een certificaat van veiligheidsmachtiging voor personen (CVMP) afgeven met daarop het niveau van de EUCI waartoe de persoon toegang kan worden verleend (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger), de geldigheidsduur van de betrokken PVM voor toegang tot EUCI of machtiging voor toegang tot EUCI en de datum waarop de geldigheid van het certificaat zelf afloopt.

Vrijstellingen van de eis inzake veiligheidsmachtiging voor personen

28. De toegang tot EUCI door personen in de lidstaten die uit hoofde van hun functie daartoe naar behoren zijn gemachtigd, wordt vastgesteld in overeenstemming met de nationale wet- en regelgeving. Die personen worden geïnstrueerd over hun beveiligingsverplichtingen in verband met de bescherming van EUCI.

IV. BEVEILIGINGSOPLEIDING EN BEVEILIGINGSBESEF

29. Alle personen aan wie een veiligheidsmachtiging is verleend, bevestigen schriftelijk dat zij kennis dragen van hun plichten met betrekking tot de bescherming van EUCI en van de gevolgen indien EUCI wordt gecompromitteerd. Een aantekening van deze schriftelijke bevestiging wordt naargelang van het geval door de lidstaat of het SGR bewaard.

30. Eenieder die gemachtigd is om toegang te hebben tot of die moet omgaan met EUCI, dient vanaf het begin bewust te worden gemaakt van en regelmatig geïnstrueerd te worden over de dreigingen voor de beveiliging en moet iedere toenadering of activiteit die hij verdacht of ongewoon vindt, onmiddellijk aan de desbetreffende beveiligingsinstanties melden.

31. Alle personen die geen taken meer vervullen waarvoor toegang tot EUCI vereist is, dienen er bewust van te worden gemaakt dat hun plichten met betrekking tot de bescherming van EUCI blijven bestaan, en dienen zulks in voorkomend geval schriftelijk te bevestigen.

V. UITZONDERLIJKE OMSTANDIGHEDEN

32. Wanneer de nationale wet- en regelgeving het toestaan, kunnen nationale ambtenaren op grond van een door een bevoegde instantie van een lidstaat afgegeven veiligheidsmachtiging voor toegang tot nationale gerubriceerde informatie in afwachting van de afgifte van een PVM voor toegang tot EUCI, tijdelijk toegang krijgen tot EUCI tot het niveau in de concordantietabel in aanhangsel B, wanneer deze tijdelijke toegang in het belang van de Europese Unie noodzakelijk is. De NSA's laten het Beveiligingscomité weten in welke gevallen de nationale wet- en regelgeving een dergelijke tijdelijke toegang tot EUCI niet toestaan.

33. Het tot aanstelling bevoegde gezag van het SGR kan om dringende en naar behoren gemotiveerde redenen van dienstbelang en in afwachting van de voltooiing van het volledige veiligheidsonderzoek, na raadpleging van de NSA van de lidstaat waarvan de betrokkene onderdaan is en afhankelijk van de uitkomst van een eerste controle of er geen negatieve informatie bekend is, ambtenaren en andere personeelsleden van het SGR voor een specifieke functie tijdelijk toegang tot EUCI verlenen. Deze tijdelijke toegang wordt voor maximaal zes maanden verleend en geldt niet voor informatie met rubricering TRÈS SECRET UE/EU TOP SECRET. Alle personen aan wie tijdelijke toegang is verleend, bevestigen schriftelijk dat zij kennis dragen van hun plichten met betrekking tot de bescherming van EUCI en van de gevolgen indien EUCI wordt gecompromitteerd. Een aantekening van deze schriftelijke bevestiging wordt door het SGR bewaard.

34. Wanneer een persoon een functie krijgt toegewezen waarvoor een veiligheidsmachtiging nodig is van één niveau hoger dan die waarover hij op dat moment beschikt, kan deze nieuwe functie op voorlopige basis worden toegewezen, mits:

a) de dwingende noodzaak van toegang tot EUCI van een hogere rubriceringsgraad schriftelijk door de meerdere van de betrokkene wordt bevestigd;

b) de toegang wordt beperkt tot specifieke onderdelen van de EUCI die nodig zijn voor de functie;

c) de persoon in het bezit is van een geldige PVM of machtiging voor toegang tot EUCI;

d) er stappen zijn ondernomen om machtiging voor het voor de functie vereiste toegangsniveau te verkrijgen;

e) uit controles door de bevoegde instantie genoegzaam is gebleken dat de betrokkene de beveiligingsvoorschriften niet ernstig of herhaaldelijk heeft overtreden;

f) de toewijzing van de functie aan de betrokkene is goedgekeurd door de bevoegde instantie, en

g) van de verleende uitzondering een aantekening, met inbegrip van een beschrijving van de informatie waartoe toegang werd verleend, wordt bewaard door het verantwoordelijke register of subregister.

35. Deze procedure wordt gebruikt voor eenmalige toegang tot EUCI met een rubriceringsgraad die één niveau hoger ligt dan waarvoor de betrokkene is gescreend. Deze procedure mag niet bij herhaling worden gebruikt.

36. In zeer uitzonderlijke omstandigheden, zoals bij missies in een vijandige omgeving of gedurende perioden van groeiende internationale spanning, wanneer noodmaatregelen zulks vereisen, vooral wanneer er levens kunnen worden gered, kunnen de lidstaten en de SG/HV of de plaatsvervangend secretaris-generaal schriftelijk toegang tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET verlenen aan personen die niet in het bezit zijn van de vereiste veiligheidsmachtiging, zulks onder de voorwaarde dat die toestemming absoluut noodzakelijk is en er geen gerede twijfel bestaat aan de loyaliteit en de betrouwbaarheid van de betrokkene. Een aantekening van deze toestemming, met een beschrijving van de informatie waartoe toegang werd verleend, wordt bewaard.

37. In geval van informatie met rubricering TRÈS SECRET UE/EU TOP SECRET dienen dergelijke noodmaatregelen beperkt te blijven tot onderdanen van de Europese Unie aan wie toegang is verleend tot het nationale equivalent van TRÈS SECRET UE/EU TOP SECRET of tot informatie met rubricering SECRET UE/EU SECRET.

38. Het Beveiligingscomité wordt op de hoogte gesteld van gevallen waarin de in de punten 36 en 37 genoemde procedure is gevolgd.

39. Wanneer de wetten en voorschriften van een lidstaat strengere regels opleggen ten aanzien van tijdelijke machtigingen, voorlopige toewijzingen, eenmalige toegang of toegang in dringende gevallen tot gerubriceerde informatie, worden de in dit deel beschreven procedures alleen gevolgd binnen de beperkingen in de nationale wet- en regelgeving ter zake.

40. Het Beveiligingscomité krijgt een jaarlijks verslag over het gebruik van de in dit deel beschreven procedures.

VI. HET BIJWONEN VAN BIJEENKOMSTEN IN DE RAAD

41. Met inachtneming van punt 28 kunnen personen aan wie is opgedragen deel te nemen aan vergaderingen van de Raad of van voorbereidende instanties van de Raad waarin als CONFIDENTIEL UE/EU CONFIDENTIAL of hoger gerubriceerde informatie wordt besproken, dit alleen doen als de status van de betrokkene met betrekking tot de veiligheidsmachtiging wordt bevestigd. Voor gedelegeerden dient een CVMP ander bewijs van een veiligheidsmachtiging door de desbetreffende instanties aan de dienst Beveiliging van het SGR te worden toegezonden, of in uitzonderingsgevallen door de betrokken gedelegeerde te worden overgelegd. Indien van toepassing kan een geconsolideerde lijst van namen worden gebruikt, met het relevante bewijs van veiligheidsmachtiging.

42. Wanneer om beveiligingsredenen een PVM voor toegang tot EUCI wordt ingetrokken van een persoon die voor zijn werk moet deelnemen aan vergaderingen van de Raad of van voorbereidende instanties van de Raad, stelt de bevoegde instantie het SGR daarvan op de hoogte.

VII. MOGELIJKE TOEGANG TOT EUCI

43. Koeriers en bewakings- en begeleidingspersoneel dienen voor de passende rubriceringsgraad te zijn gescreend of anderszins een passend onderzoek te hebben ondergaan overeenkomstig de nationale wet- en regelgeving, te worden geïnstrueerd over de beveiligingsprocedures ter bescherming van EUCI en over hun plicht om de hun toevertrouwde EUCI te beschermen.

BIJLAGE II

FYSIEKE BEVEILIGING

I. INLEIDING

1. Deze bijlage bevat bepalingen ter uitvoering van artikel 8. Er worden minimumvoorschriften vastgesteld voor de fysieke beveiliging van locaties, gebouwen, bureaus, ruimten en andere zones waar EUCI wordt verwerkt en opgeslagen, evenals zones waar CIS zijn ondergebracht.

2. Fysieke beveiligingsmaatregelen zijn bedoeld om de toegang zonder machtiging tot EUCI te voorkomen door:

   a) ervoor te zorgen dat EUCI op passende wijze wordt verwerkt en opgeslagen;

   b) op basis van het „noodzaak tot kennisname"-beginsel en, in voorkomend geval, van hun veiligheidsmachtiging een onderscheid tussen personeelsleden mogelijk te maken wat de toegang tot EUCI betreft;

   c) acties waarvoor geen toestemming is verleend af te schrikken, tegen te houden en op te sporen, en

   d) het door list of geweld binnendringen te verhinderen of te vertragen.

II. VEREISTEN EN MAATREGELEN INZAKE FYSIEKE BEVEILIGING

3. De fysieke beveiligingsmaatregelen worden geselecteerd op basis van de dreigingsbeoordeling door de bevoegde instanties. Het SGR en de lidstaten passen ieder een risicobeheerprocedure toe ter bescherming van EUCI in hun gebouwen, teneinde ervoor te zorgen dat een fysieke bescherming wordt geboden die overeenstemt met het ingeschatte risico. In de risicobeheerprocedure wordt rekening gehouden met alle relevante factoren, met name:

   a) de rubriceringsgraad van de EUCI;

   b) de vorm en omvang van de EUCI, waarbij in aanmerking moet worden genomen dat grote hoeveelheden of een compilatie van EUCI de toepassing van striktere beschermingsmaatregelen kunnen vergen;

   c) de omgeving en de structuur van de gebouwen of zones waar EUCI ondergebracht is, en

   d) de beoordeelde dreiging die uitgaat van inlichtingendiensten die zich richten op de Europese Unie of de lidstaten en van sabotage, terrorisme en subversieve of andere criminele activiteiten.

4. De bevoegde beveiligingsinstantie stelt aan de hand van het begrip „defence in depth" vast welke passende combinatie van fysieke beveiligingsmaatregelen moet worden getroffen. Deze maatregelen kunnen zijn:

   a) een afsluiting: een fysieke barrière ter verdediging van de grens van een zone die bescherming behoeft;

   b) indringerdetectiesystemen (intrusion detection systems, hierna: „IDS"): een IDS kan worden gebruikt om het beveiligingsniveau van de afsluiting te verhogen, of in lokalen en gebouwen om beveiligingspersoneel te vervangen of te ondersteunen;

   c) toegangscontrole: er kan toegangscontrole worden uitgeoefend voor een locatie, een gebouw of gebouwen op een locatie of voor zones of ruimten in een gebouw. De controle kan elektronisch of elektromechanisch worden verricht, door beveiligingspersoneel en/of een receptionist, of met enig ander fysiek hulpmiddel;

   d) beveiligingspersoneel: beveiligingspersoneel dat een opleiding heeft gekregen, onder toezicht werkt en, in voorkomend geval, een gedegen veiligheidsonderzoek heeft ondergaan, kan onder meer worden ingezet om personen af te schrikken die overwegen heimelijk binnen te dringen;

   e) gesloten tv-circuit (hierna: „CCTV"): een gesloten tv-circuit kan door beveiligingspersoneel worden gebruikt om incidenten en IDS-alarmen op grote locaties of aan de afsluitingen te controleren;

   f) beveiligingsverlichting: beveiligingsverlichting kan worden gebruikt om mogelijke indringers af te schrikken en biedt daarnaast de noodzakelijke verlichting voor effectieve bewaking die rechtstreeks door beveiligingspersoneel dan wel onrechtstreeks via een gesloten tv-circuit geschiedt, en

   g) alle andere passende fysieke maatregelen om ongeoorloofde toegang te ontmoedigen of op te sporen of om verlies of beschadiging van EUCI te voorkomen.

5. De bevoegde instantie kan worden gemachtigd om controles uit te voeren bij het in- en uitgaan, ter afschrikking van het ongeoorloofd binnenbrengen van materiaal in, of het ongeoorloofd verwijderen van EUCI uit een locatie of gebouw.

6. Als het risico bestaat dat EUCI van buitenaf wordt waargenomen, zelfs per ongeluk, worden passende maatregelen genomen om dit risico te voorkomen.

7. Voor nieuwe voorzieningen worden fysieke beveiligingsvereisten en functiespecificaties reeds bij het plannen en ontwerpen vastgesteld. Voor bestaande voorzieningen worden fysieke beveiligingsvereisten in de hoogst mogelijke mate uitgevoerd.

III. UITRUSTING VOOR DE FYSIEKE BESCHERMING VAN EUCI

8. Bij de aanschaf van uitrusting (zoals beveiligingsopbergmiddelen, papierversnipperaars, deursloten, elektronische systemen voor toegangscontrole, indringerdetectiesystemen, alarmsystemen) voor de fysieke bescherming van EUCI ziet de bevoegde beveiligingsinstantie erop toe dat de uitrusting in overeenstemming is met de goedgekeurde technische normen en minimumvoorschriften.

9. De technische specificaties van uitrusting die bestemd is voor de fysieke bescherming van EUCI worden vastgelegd in beveiligingsrichtlijnen die door het Beveiligingscomité moeten worden goedgekeurd.

10. De beveiligingssystemen worden geregeld geïnspecteerd en de uitrusting wordt regelmatig onderhouden. Bij de onderhoudswerkzaamheden wordt met het resultaat van de inspecties rekening gehouden om te garanderen dat de uitrusting optimaal blijft werken.

11. De effectiviteit van individuele beveiligingsmaatregelen en van het gehele beveiligingssysteem wordt bij iedere inspectie getoetst.

IV. FYSIEK BESCHERMDE ZONES

12. Voor de fysieke bescherming van EUCI worden twee soorten fysiek beschermde zones, of de nationale equivalenten ervan, ingesteld:

    a) administratieve zones, en

    b) beveiligde zones (waaronder technisch beveiligde zones).

    In dit besluit slaan alle verwijzingen naar administratieve zones en beveiligde zones, waaronder technisch beveiligde zones, ook op de nationale equivalenten daarvan.

13. De bevoegde beveiligingsinstantie bepaalt dat een zone voldoet aan de eisen om te worden aangewezen als administratieve zone, beveiligde zone of technisch beveiligde zone.

14. Voor administratieve zones:

    a) wordt een duidelijk omschreven afscheiding ingesteld waar personen en indien mogelijk voertuigen kunnen worden gecontroleerd;

    b) wordt toegang zonder begeleiding alleen toegestaan aan personen die naar behoren door de bevoegde instantie gemachtigd zijn, en

    c) worden alle andere personen altijd begeleid of aan gelijkwaardige controles onderworpen.

15. Voor beveiligde zones:

    a) wordt een duidelijk omschreven, beschermde afscheiding ingesteld waar elk in- en uitgaan wordt gecontroleerd middels een pasje of een systeem van persoonsherkenning;

    b) wordt toegang zonder begeleiding alleen verleend aan personen die een veiligheidsonderzoek hebben ondergaan en specifiek gemachtigd zijn om de zone te betreden op basis van hun noodzaak tot kennisname, en

    c) worden alle andere personen altijd begeleid of aan gelijkwaardige controles onderworpen.

16. Wanneer het betreden van een beveiligde zone in de praktijk neerkomt op rechtstreekse toegang tot de gerubriceerde informatie die zich daar bevindt, zijn daarnaast de volgende aanvullende voorschriften van toepassing:

    a) de hoogste rubriceringsgraad van de informatie die normaal in de zone worden bewaard, wordt duidelijk aangegeven;

    b) alle bezoekers moeten een specifieke machtiging bezitten om de zone te betreden, moeten altijd worden begeleid en moeten passend gescreend zijn, tenzij het nodige wordt gedaan opdat dat geen toegang tot EUCI mogelijk is.

17. Beveiligde zones die tegen afluisteren zijn beschermd, worden als technisch beveiligde zones aangemerkt. Daarnaast zijn de volgende aanvullende voorschriften van toepassing:

    a) de zones worden uitgerust met IDS, worden afgesloten wanneer ze niet worden gebruikt en bewaakt wanneer ze in gebruik zijn. Sleutels worden gecontroleerd overeenkomstig afdeling VI;

    b) alle personen en goederen die deze zones binnenkomen, worden gecontroleerd;

    c) deze zones worden aan regelmatige fysieke en/of technische inspecties onderworpen, zoals vereist door de bevoegde beveiligingsinstantie. Die inspecties worden ook verricht nadat de zones door onbevoegden zijn betreden of indien dit wordt vermoed, en

    d) deze zones zijn vrij van ongeoorloofde communicatielijnen of telefoons of andere ongeoorloofde communicatieapparatuur en elektrische of elektronische apparatuur.

18. Niettegenstaande punt 17, onder d), moet communicatieapparatuur en elektrische en elektronische apparatuur van welke aard ook, voordat zij wordt gebruikt in zones waar vergaderingen plaatsvinden of werk wordt verricht in verband met informatie met rubricering SECRET UE/EU SECRET en hoger, wanneer de dreiging voor EUCI als hoog wordt beoordeeld, eerst door de bevoegde beveiligingsinstantie worden onderzocht om ervoor te zorgen dat geen begrijpelijke informatie door die apparatuur onbedoeld of op illegale wijze kan worden doorgegeven tot buiten de perimeter van de betrokken beveiligde zone.

19. Beveiligde zones waar niet op 24-uursbasis dienstdoend personeel aanwezig is, worden, in voorkomend geval, aan het eind van de normale werktijd geïnspecteerd, alsook buiten de normale werktijd met willekeurige tussenpozen, tenzij er een indringerdetectiesysteem is.

20. Beveiligde zones en technische beveiligde zones kunnen binnen een administratieve zone tijdelijk worden ingesteld voor een gerubriceerde vergadering of een soortgelijk doel.

21. Voor iedere beveiligde zone worden operationele beveiligingsprocedures opgesteld, waarbij het volgende wordt vastgesteld:

    a) het niveau van de EUCI die in die zone mag worden verwerkt en opgeslagen;

    b) de te handhaven bewakings- en beschermingsmaatregelen;

    c) de personen die op grond van hun noodzaak tot kennisname en veiligheidsmachtiging zonder begeleiding toegang mogen hebben tot de zone;

    d) in voorkomend geval, de procedures inzake begeleiding of inzake bescherming van EUCI wanneer aan anderen toegang tot de zone wordt verleend, en

    e) andere relevante maatregelen en procedures.

22. Binnen de beveiligde zones worden kluizen geïnstalleerd. De muren, vloeren, plafonds, ramen en afsluitbare deuren moeten door de bevoegde beveiligingsinstantie worden goedgekeurd en een gelijkwaardig beschermingsniveau bieden als de beveiligingsopbergmiddelen die zijn goedgekeurd voor de opslag van EUCI met dezelfde rubriceringsgraad.

V. FYSIEKE BEVEILIGINGSMAATREGELEN VOOR HET VERWERKEN EN OPSLAAN VAN EUCI

23. EUCI met rubricering RESTREINT UE/EU RESTRICTED mag worden verwerkt:

    a) in een beveiligde zone;

    b) in een administratieve zone, als de EUCI wordt beschermd tegen toegang door onbevoegden, of

    c) buiten een beveiligde of een administratieve zone, als de houder EUCI vervoert overeenkomstig de punten 28 tot en met 41 van bijlage III en heeft toegezegd zich te zullen houden aan de in de beveiligingsinstructies van de bevoegde beveiligingsinstantie opgenomen compenserende maatregelen ter bescherming van EUCI tegen toegang van onbevoegden.

24. EUCI met rubricering RESTREINT UE/EU RESTRICTED wordt opgeslagen in daarvoor geschikt afgesloten kantoormeubilair in een administratieve zone of een beveiligde zone. De informatie mag tijdelijk buiten een beveiligde of een administratieve zone worden opgeslagen, als de houder heeft toegezegd zich te zullen houden aan compenserende maatregelen volgens de beveiligingsinstructies van de bevoegde beveiligingsinstantie.

25. EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET mag worden verwerkt:

a) in een beveiligde zone;

b) in een administratieve zone, als de EUCI wordt beschermd tegen toegang door onbevoegden, of

c) buiten een beveiligde zone of een administratieve zone als de houder:

i) de EUCI vervoert overeenkomstig de punten 28 tot en met 41 van bijlage III;

ii) heeft toegezegd zich te zullen houden aan de in de beveiligingsinstructies van de bevoegde beveiligingsinstantie opgenomen compenserende maatregelen ter bescherming van EUCI tegen toegang van onbevoegden;

iii) de EUCI te allen tijde onder zijn persoonlijke controle houdt, en

iv) in het geval van documenten op papier, het desbetreffend register op de hoogte heeft gebracht.

26. EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET wordt in een beveiligde zone opgeslagen in hetzij een beveiligingsopbergmiddel, hetzij een kluis.

27. EUCI met rubricering TRÈS SECRET UE/EU TOP SECRET wordt verwerkt in een beveiligde zone.

28. EUCI met rubricering TRÈS SECRET UE/EU TOP SECRET wordt opgeslagen in een beveiligde zone, op één van de volgende manieren:

a) in een beveiligingsopbergmiddel overeenkomstig punt 8 met één of meer van de volgende aanvullende controles:

i) permanente bescherming of verificatie door beveiligingspersoneel of dienstdoend personeel in het bezit van een veiligheidsmachtiging;

ii) een goedgekeurd IDS in combinatie met interventiebeveiligingspersoneel, of

b) in een met een IDS uitgeruste kluis in combinatie met interventiebeveiligingspersoneel.

29. De voorschriften voor het vervoeren van EUCI buiten fysiek beveiligde zones staan in bijlage III.

VI. CONTROLE VAN SLEUTELS EN CODECOMBINATIES DIE WORDEN GEBRUIKT VOOR DE BESCHERMING VAN EUCI

30. De bevoegde beveiligingsinstantie stelt procedures vast voor het beheer van sleutels en codecombinaties voor kantoren, lokalen, kluizen en beveiligingsopbergmiddelen. Die procedures bieden bescherming tegen ongeoorloofde toegang.

31. De codecombinaties worden gememoriseerd door het kleinst mogelijke aantal personen die er kennis van moeten nemen. De codecombinaties van beveiligingsopbergmiddelen en kluizen waarin EUCI wordt opgeslagen, worden gewijzigd:

a) bij ontvangst van nieuwe opbergmiddelen;

b) in geval van een wijziging in het personeel dat de combinatie kent;

c) bij compromitteren of het vermoeden ervan;

d) wanneer een slot in onderhoud of in herstelling is geweest, en

e) ten minste om de twaalf maanden.

BIJLAGE III

BEHEER VAN GERUBRICEERDE INFORMATIE

I. INLEIDING

1. Deze bijlage bevat bepalingen ter uitvoering van artikel 9. Zij stelt de administratieve maatregelen vast voor het controleren van EUCI gedurende haar gehele levenscyclus teneinde het al dan niet opzettelijk compromitteren of verliezen van die informatie te helpen voorkomen en opsporen.

II. RUBRICERINGBEHEER

Rubriceringen en markeringen

2. Informatie wordt gerubriceerd wanneer zij bescherming behoeft wat hun vertrouwelijkheid betreft.

3. De opsteller van EUCI is verantwoordelijk voor het bepalen van de rubriceringsgraad, overeenkomstig de desbetreffende rubriceringrichtlijnen, en voor de eerste verspreiding van de informatie.

4. De rubriceringsgraad van EUCI wordt vastgesteld overeenkomstig artikel 2, lid 2, en onder verwijzing naar het beveiligingsbeleid dat de Raad overeenkomstig artikel 3, lid 3, moet vaststellen.

5. De rubricering wordt duidelijk en correct aangegeven, ongeacht of de EUCI in papieren, mondelinge, elektronische of enige andere vorm bestaat.

6. Afzonderlijke delen van een bepaald document (zoals bladzijden, punten, afdelingen, bijlagen, aanhangsels, aanhechtsels en bijvoegsels) kunnen verschillende rubriceringen vereisen en worden dienovereenkomstig gemarkeerd, ook wanneer zij elektronisch worden opgeslagen.

7. De rubricering die voor het gehele document of bestand geldt, is minstens van dezelfde graad als die van het hoogst gerubriceerde gedeelte ervan. Wanneer informatie uit diverse bronnen worden verzameld, wordt voor het eindproduct in zijn geheel nagegaan welke rubriceringsgraad het moet krijgen, aangezien hiervoor een hogere rubricering vereist kan zijn dan voor de onderdelen ervan.

8. Voor zover mogelijk worden documenten die delen met verschillende rubriceringsgraden bevatten, zo gestructureerd dat de delen met een verschillende rubriceringsgraad gemakkelijk kunnen worden herkend en, indien nodig, worden gescheiden.

9. De rubricering van een brief of een nota die bijvoegsels vergezelt, is van dezelfde graad als het hoogst gerubriceerde bijvoegsel. De bron geeft door middel van een passende markering duidelijk aan welke rubricering op die brief of nota moet worden toegepast indien deze gescheiden wordt van de bijvoegsels, bijvoorbeeld:

CONFIDENTIEL UE/EU CONFIDENTIAL:

Zonder aanhechtsel(s) RESTREINT UE/EU RESTRICTED

Markeringen

10. Ter aanvulling van een van de rubriceringen als bedoeld in artikel 2, lid 2, kan EUCI voorzien zijn van aanvullende markeringen zoals:

a) een identificatiemiddel om de bron aan te duiden;

b) waarschuwingsmarkeringen, codewoorden of afkortingen waarmee het activiteitengebied waarop het document betrekking heeft, een speciale verspreiding op basis van noodzaak tot kennisname of beperkingen voor het gebruik worden aangegeven;

c) markeringen inzake de geschiktheid voor vrijgave, of

d) in voorkomend geval, de datum of de specifieke gebeurtenis waarna het document lager gerubriceerd of gederubriceerd kan worden.

Afgekorte rubriceringen

11. Gestandaardiseerde afgekorte rubriceringen kunnen worden gebruikt om de rubriceringsgraad van afzonderlijke delen van een tekst aan te geven. Afkortingen komen niet in de plaats van de volledige rubriceringen.

12. De volgende standaardafkortingen mogen in gerubriceerde EU-documenten worden gebruikt ter aanduiding van de rubriceringsgraad van afdelingen of onderdelen van tekst van minder dan één bladzijde:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Het genereren van EUCI

13. Bij het genereren van een gerubriceerd EU-document:

a) wordt op elke bladzijde duidelijk de rubriceringsgraad aangegeven;

b) wordt elke bladzijde genummerd;

c) wordt het document voorzien van een referentienummer en een onderwerp, dat op zich geen gerubriceerde informatie is, tenzij het als zodanig wordt gemarkeerd;

d) wordt het document gedateerd, en

e) worden documenten met rubricering SECRET EU/EU SECRET en hoger op elke bladzijde van een exemplaarnummer voorzien, indien zij in meerdere exemplaren moeten worden verspreid.

14. Als het niet mogelijk is punt 13 toe te passen op EUCI, worden andere passende maatregelen genomen overeenkomstig de krachtens artikel 6, lid 2, op te stellen beveiligingsrichtlijnen.

Lagere rubricering en derubricering van EUCI

15. Bij het genereren geeft de bron waar mogelijk, en in het bijzonder voor als RESTREINT UE/EU RESTRICTED gerubriceerde informatie, aan of de EUCI op een bepaalde datum of na een bepaalde gebeurtenis lager gerubriceerd of gederubriceerd kan worden.

16. Het SGR beziet regelmatig de EUCI waarover het beschikt opnieuw om na te gaan of de rubriceringsgraad nog steeds van toepassing is. Het SGR stelt een regeling in om de rubriceringsgraad van EUCI waarvan het de opsteller is, ten minste om de vijf jaar opnieuw te bezien. Deze controle is niet nodig wanneer de opsteller vanaf het begin heeft aangegeven dat de informatie automatisch lager gerubriceerd of gederubriceerd zullen worden en dat zij dienovereenkomstig gemarkeerd zijn.

III. REGISTRATIE VAN EUCI VOOR BEVEILIGINGSDOELEINDEN

17. Voor iedere organisatorische entiteit binnen het SGR en binnen de nationale overheden van de lidstaten die met EUCI werkt, wordt een verantwoordelijk register aangewezen dat moet garanderen dat EUCI overeenkomstig dit besluit wordt verwerkt. De registers worden ingericht als beveiligde zones zoals omschreven in bijlage II.

18. Voor de toepassing van dit besluit wordt onder registratie voor beveiligingsdoeleinden (hierna: „registratie") verstaan: de toepassing van procedures waarbij de levenscyclus van materiaal, ook de verspreiding en de vernietiging ervan, wordt geregistreerd.

19. Alle materiaal met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en hoger wordt in speciaal daarvoor bestemde registers geregistreerd wanneer het bij een organisatorische overheid aankomt of deze entiteit verlaat.

20. Het centrale register binnen het SGR houdt aantekening van alle gerubriceerde informatie die door de Raad en het SGR worden vrijgegeven aan derde staten en internationale organisaties, en van alle gerubriceerde informatie die worden ontvangen van derde staten of internationale organisaties.

21. In het geval van een CIS kunnen de registratieprocedures worden doorlopen door middel van processen binnen het CIS zelf.

22. De Raad stelt een beveiligingsbeleid inzake de registratie van EUCI voor beveiligingsdoeleinden vast.

Registers voor TRÈS SECRET UE/EU TOP SECRET

23. Er wordt in de lidstaten en bij het SGR een register aangewezen dat optreedt als de centrale instantie voor het ontvangen en verzenden van informatie met rubricering TRÈS SECRET UE/EU TOP SECRET. In voorkomend geval kunnen subregisters worden aangewezen die zulke informatie voor registratiedoeleinden verwerken.

24. Deze subregisters mogen geen TRÈS SECRET UE/EU TOP SECRET-documenten rechtstreeks overdragen aan andere subregisters van hetzelfde centrale TRÈS SECRET UE/EU TOP SECRET-register, noch naar buiten toe overdragen, zonder uitdrukkelijke schriftelijke toestemming van dit centrale register.

IV. KOPIËREN EN VERTALEN VAN GERUBRICEERDE EU-DOCUMENTEN

25. Documenten met rubricering TRÈS SECRET UE/EU TOP SECRET worden niet zonder voorafgaande schriftelijke toestemming van de bron gekopieerd of vertaald.

26. Indien de bron van documenten met rubricering SECRET UE/EU SECRET of lager geen waarschuwingsmarkeringen met betrekking tot het kopiëren of vertalen heeft aangebracht, kunnen deze documenten op instructie van de houder worden gekopieerd of vertaald.

27. De beveiligingsmaatregelen die voor het originele document gelden, zijn ook van toepassing op de kopieën en vertalingen ervan.

V. VERVOER VAN EUCI

28. Voor het vervoer van EUCI gelden de beschermende maatregelen van de punten 30 tot en met 41. Wanneer EUCI op elektronische dragers wordt vervoerd, kunnen onverminderd artikel 9, lid 4, onderstaande beschermende maatregelen worden aangevuld met passende technische tegenmaatregelen — die door de bevoegde beveiligingsinstantie worden voorgeschreven — om het risico op verlies of compromitteren zo klein mogelijk te maken.

29. De bevoegde beveiligingsinstantie in het SGR en in de lidstaten geven overeenkomstig dit besluit instructies over het vervoer van EUCI.

Binnen een gebouw of op zichzelf staande groep van gebouwen

30. EUCI die binnen een gebouw of een op zichzelf staande groep van gebouwen wordt vervoerd, wordt bedekt om te voorkomen dat de inhoud ervan wordt waargenomen.

31. Binnen een gebouw of een op zichzelf staande groep van gebouwen wordt informatie met rubricering TRÈS SECRET UE/EU TOP SECRET vervoerd in een beveiligde envelop met daarop alleen de naam van de geadresseerde.

Binnen de Europese Unie

32. EUCI die tussen gebouwen en locaties binnen de Europese Unie wordt vervoerd, wordt zodanig verpakt dat zij wordt beschermd tegen ongeoorloofde openbaarmaking.

33. Het vervoer van informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET binnen de Europese Unie geschiedt op de volgende wijze:

a) per militaire koerier, overheidskoerier of diplomatieke koerier, naargelang het geval;

b) in handbagage, op voorwaarde dat:

i) de drager de EUCI niet uit handen geeft, tenzij zij wordt opgeslagen conform de voorschriften van bijlage II;

ii) de EUCI niet onderweg wordt geopend of op openbare plaatsen gelezen;

iii) de persoon geïnstrueerd wordt over zijn verantwoordelijkheden inzake de beveiliging, en

iv) de persoon zo nodig een koerierspas krijgt;

c) postdiensten of commerciële koeriersdiensten, op voorwaarde dat:

i) zij door de desbetreffende NSA zijn goedgekeurd overeenkomstig de nationale wet- en regelgeving, en

ii) zij adequate beschermingsmaatregelen toepassen overeenkomstig de minimumvoorschriften die moeten worden vastgelegd in de krachtens artikel 6, lid 2, op te stellen beveiligingsrichtlijnen.

Bij vervoer van een lidstaat naar een andere wordt het bepaalde onder c) beperkt tot informatie tot en met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL.

34. Informatie met rubricering RESTREINT UE/EU RESTRICTED mag ook door postdiensten of commerciële koeriersdiensten worden vervoerd. Voor het vervoer van dergelijke informatie is geen koerierspas vereist.

35. Materiaal met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET (bv. uitrustingen of onderdelen van machines) dat niet kan worden vervoerd met de in punt 33 bedoelde middelen, wordt overeenkomstig bijlage V als vracht vervoerd door commerciële vervoersondernemingen.

36. Het vervoer van informatie met rubricering TRÈS SECRET UE/EU TOP SECRET tussen gebouwen of locaties binnen de Europese Unie geschiedt per militaire koerier, overheidskoerier of diplomatieke koerier, naargelang het geval.

Vanuit de Europese Unie naar het grondgebied van een derde staat

37. EUCI die vanuit de Europese Unie naar het grondgebied van een derde staat wordt vervoerd, wordt zodanig verpakt dat zij wordt beschermd tegen ongeoorloofde openbaarmaking.

38. Het vervoer van informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET vanuit de Europese Unie naar het grondgebied van een derde staat geschiedt op één van de volgende wijzen:

a) per militaire of diplomatieke koerier;

b) in handbagage, op voorwaarde dat:

i) het pakket een officieel zegel draagt of in een verpakking zit waarop is aangegeven dat het om een officiële zending gaat die niet aan een douane- of beveiligingscontrole dient te worden onderworpen;

ii) de persoon een koerierspas bij zich heeft die het pakket identificeert en hem machtigt het te vervoeren;

iii) de drager de EUCI niet uit handen geeft, tenzij zij wordt opgeslagen conform de voorschriften van bijlage II;

iv) de EUCI niet onderweg wordt geopend of op openbare plaatsen gelezen, en

v) de persoon geïnstrueerd wordt over zijn verantwoordelijkheden inzake de beveiliging.

39. Het vervoer van informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET die door de Europese Unie wordt vrijgegeven aan een derde staat of een internationale organisatie, moet in overeenstemming zijn met de desbetreffende bepalingen van een overeenkomst voor de beveiliging van informatie of een administratieve regeling overeenkomstig artikel 13, lid 2, onder a) en b).

40. Informatie met rubricering RESTREINT UE/EU RESTRICTED mag ook door postdiensten of commerciële koeriersdiensten worden vervoerd.

41. Het vervoer van informatie met rubricering TRÈS SECRET UE/EU TOP SECRET vanuit de Europese Unie naar het grondgebied van een derde staat geschiedt per militaire of diplomatieke koerier.

VI. VERNIETIGING VAN EUCI

42. Gerubriceerde EU-documenten die niet langer nodig zijn, mogen worden vernietigd onverminderd de geldende regels en voorschriften inzake archivering.

43. Documenten die volgens artikel 9, lid 2, moeten worden geregistreerd, worden door het verantwoordelijke register vernietigd op instructie van de houder of van een bevoegde instantie. De logboeken en andere informatie betreffende de registratie worden dienovereenkomstig bijgewerkt.

44. De vernietiging van documenten met rubricering SECRET UE/EU SECRET of TRÈS SECRET UE/EU TOP SECRET vindt plaats in het bijzijn van een getuige die gemachtigd is voor ten minste de rubriceringsgraad van het document dat wordt vernietigd.

45. Zowel de registrator als de getuige, als de aanwezigheid van deze laatste vereist is, ondertekenen een vernietigingscertificaat, dat wordt bewaard in het register. In het register worden vernietigingscertificaten van documenten met rubricering TRÈS SECRET UE/EU TOP SECRET gedurende minstens tien jaar en van documenten met rubriceringsgraad CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET gedurende minstens vijf jaar bewaard.

46. Om te voorkomen dat gerubriceerde documenten geheel of gedeeltelijk worden gereconstrueerd worden deze documenten, ook die met rubricering RESTREINT UE/EU RESTRICTED, vernietigd volgens methoden die voldoen aan EU-normen of gelijkwaardige normen, of methoden die door de lidstaten zijn goedgekeurd volgens nationale technische normen.

47. Vernietiging van voor EUCI gebruikte digitale opslagmedia geschiedt overeenkomstig punt 37 van bijlage IV.

48. In noodgevallen of indien er een imminent gevaar van openbaarmaking zonder machtiging is, wordt de EUCI door de houder derwijze vernietigd dat deze niet in haar geheel, noch ten dele kan worden gereconstrueerd. De bron en het register van oorsprong worden op de hoogte gebracht van de noodvernietiging van geregistreerde EUCI.

VII. EVALUATIEBEZOEKEN

49. De term „evaluatiebezoek" wordt hierna gebruikt voor:

a) iedere inspectie of evaluatiebezoek overeenkomstig artikel 9, lid 3, en artikel 16, lid 2, onder e), f) en g), of

b) ieder evaluatiebezoek overeenkomstig artikel 13, lid 5,

ter evaluatie van de doeltreffendheid van de maatregelen ter bescherming van EUCI.

50. Evaluatiebezoeken moeten onder meer:

a) waarborgen dat de in dit besluit neergelegde vereiste minimumnormen voor de bescherming van EUCI worden nageleefd;

b) het belang benadrukken van beveiliging en doelmatig risicobeheer binnen de geïnspecteerde entiteiten;

c) tegenmaatregelen aanbevelen om de specifieke gevolgen van de aantasting van de vertrouwelijkheid, integriteit of beschikbaarheid van gerubriceerde informatie te matigen, en

d) de lopende opleidings- en bewustmakingsprogramma's die door de beveiligingsinstanties met betrekking tot beveiliging worden uitgevoerd, versterken.

51. Voor het eind van ieder kalenderjaar neemt de Raad het in artikel 16, lid 1, onder c), bedoelde programma van evaluatiebezoeken voor het volgende jaar aan. De concrete data van ieder evaluatiebezoek worden in overeenstemming met het EU-orgaan of de EU-instantie in kwestie, de betrokken lidstaat, de derde staat of de internationale organisatie in kwestie vastgesteld.

Uitvoering van evaluatiebezoeken

52. Er worden evaluatiebezoeken verricht om de desbetreffende regels, voorschriften en procedures in de bezochte entiteit te controleren en na te gaan of de werkwijzen van de entiteit stroken met de basisbeginselen en minimumnormen die zijn vastgelegd in dit besluit en in de bepalingen betreffende de uitwisseling van gerubriceerde informatie met die entiteit.

53. De evaluatiebezoeken verlopen in twee fasen. Voorafgaand aan het bezoek zelf wordt, zo nodig, een voorbereidende vergadering met de betrokken entiteit belegd. Na deze voorbereidende vergadering stelt het evaluatieteam in overleg met de betrokken entiteit een gedetailleerd programma van evaluatiebezoeken op dat alle aspecten van de beveiliging omvat. Het evaluatieteam dient toegang te hebben tot iedere locatie waar EUCI wordt verwerkt, en met name tot de registers en CIS-points of presence.

54. Evaluatiebezoeken bij de nationale overheden van de lidstaten en van derde staten en bij internationale organisaties worden uitgevoerd in volledige samenwerking met de functionarissen van de bezochte entiteit, derde staat of internationale organisatie.

55. Evaluatiebezoeken aan de EU-agentschappen, instanties en entiteiten die dit besluit of de beginselen daarvan toepassen, worden verricht met de bijstand van deskundigen van de NSA op het grondgebied waarvan het orgaan of de instantie is gevestigd.

56. Voor evaluatiebezoeken aan EU-organen, instanties en entiteiten die dit besluit of de beginselen daarvan toepassen, alsook aan derde staten en internationale organisaties, kunnen bijstand en bijdragen van NVI-deskundigen worden verlangd overeenkomstig de gedetailleerde regeling die door het Beveiligingscomité moet worden vastgesteld.

Verslagen

57. Aan het eind van het evaluatiebezoek worden de belangrijkste conclusies en aanbevelingen aan de bezochte entiteit voorgelegd. Vervolgens wordt er een verslag opgesteld van het evaluatiebezoek. Indien corrigerende maatregelen en aanbevelingen zijn voorgesteld, moet het verslag voldoende nadere informatie bevatten ter ondersteuning van de getrokken conclusies. Het verslag moet aan de bevoegde instantie van de bezochte entiteit worden toegezonden.

58. Ten aanzien van evaluatiebezoeken bij de nationale overheden van de lidstaten geldt onderstaande:

a) het ontwerpevaluatieverslag wordt toegezonden aan de betrokken NSA, zodat kan worden nagegaan of het feitelijk correct is en het geen informatie bevat die hoger is gerubriceerd dan RESTREINT UE/EU RESTRICTED, en

b) de evaluatieverslagen worden, tenzij de NSA van de betrokken lidstaat zich tegen een algemene verspreiding verzet, toegezonden aan het Beveiligingscomité. Het verslag krijgt de rubricering RESTREINT UE/EU RESTRICTED.

Onder de verantwoordelijkheid van de dienst Beveiliging van het SGR wordt op gezette tijden een verslag opgesteld met, voor een specifieke periode, de lessen die uit de evaluatiebezoeken in de lidstaten zijn getrokken en door het Beveiligingscomité zijn bestudeerd.

59. Het verslag van evaluatiebezoeken aan derde staten en internationale organisaties wordt toegezonden aan het Beveiligingscomité. Het verslag krijgt ten minste de rubricering RESTREINT UE/EU RESTRICTED. Alle corrigerende maatregelen worden tijdens een vervolgbezoek geverifieerd en aan het Beveiligingscomité gerapporteerd.

60. Van evaluatiebezoeken aan EU-organen, instanties en entiteiten die dit besluit of de beginselen daarvan toepassen, worden de verslagen van de evaluatiebezoeken aan het Beveiligingscomité toegezonden. Het ontwerpverslag van het evaluatiebezoek wordt toegezonden aan het betrokken orgaan of de betrokken instantie, zodat kan worden nagegaan of het inhoudelijk correct is en geen informatie bevat die hoger zijn gerubriceerd dan RESTREINT UE/EU RESTRICTED. Alle corrigerende maatregelen worden tijdens een vervolgbezoek geverifieerd en aan het Beveiligingscomité gerapporteerd.

61. De beveiligingsinstantie van het SGR verricht geregelde inspecties van organisatorische entiteiten in het SGR, en wel voor de in punt 50 beschreven doelen.

Controlelijst

62. De beveiligingsinstantie van het SGR (dienst Beveiliging) stelt een controlelijst op met de punten die tijdens een evaluatiebezoek moeten worden geverifieerd. Deze controlelijst wordt toegezonden aan het Beveiligingscomité.

63. De informatie ter aanvulling van de controlelijst wordt, in het bijzonder tijdens het bezoek verkregen bij de voor het beveiligingsbeheer bevoegde functionarissen van de entiteit die wordt geïnspecteerd. Zodra de controlelijst met de gedetailleerde antwoorden is aangevuld, wordt hij in overleg met de geïnspecteerde entiteit gerubriceerd. De lijst maakt geen deel uit van het inspectieverslag.

BIJLAGE IV

BESCHERMING VAN IN CIS VERWERKTE EUCI

I. INLEIDING

1. Deze bijlage bevat bepalingen ter uitvoering van artikel 10.

2. Onderstaande IA-eigenschappen en -concepten zijn essentieel voor de beveiliging en de correcte werking van operaties met CIS.

Authenticiteit: de garantie dat informatie echt en ongewijzigd is en van bonafide bronnen afkomstig zijn.

Beschikbaarheid: op verzoek van een gemachtigde entiteit toegankelijk en bruikbaar zijn.

Vertrouwelijkheid: de informatie wordt niet vrijgegeven aan niet-gemachtigde personen, entiteiten of processen.

Integriteit: de nauwkeurigheid en de volledigheid van de informatie en de functionele bestanddelen worden gewaarborgd.

Onweerlegbaarheid: het vermogen om te bewijzen dat een actie of gebeurtenis heeft plaatsgevonden, zodat deze niet vervolgens kan worden ontkend.

II. BEGINSELEN VAN INFORMATION ASSURANCE

3. De onderstaande bepalingen vormen de basis voor de beveiliging van alle CIS die voor het verwerken van EUCI worden gebruikt. In de beveiligingsbeleidsmaatregelen en beveiligingsrichtlijnen inzake IA moeten uitgebreide voorschriften voor de uitvoering van deze bepalingen worden vastgelegd.

Beheer van beveiligingsrisico's

4. Beheer van beveiligingsrisico's is een integraal onderdeel van het omschrijven, ontwikkelen, exploiteren en onderhouden van een CIS. Risicobeheer (beoordeling, behandeling, aanvaarding en communicatie) verloopt als een zich herhalend proces, gezamenlijk uitgevoerd door vertegenwoordigers van de eigenaren van systemen, projectinstanties, exploitanten en beveiligingsgoedkeuringsinstanties, met gebruikmaking van een risicobeoordelingsprocedure die zichzelf heeft bewezen en transparant en volledig begrijpelijk is. De reikwijdte van het CIS en zijn functionele bestanddelen wordt aan het begin van de risicobeheerprocedure duidelijk afgebakend.

5. De bevoegde instanties bezien de mogelijke dreigingen voor CIS en zorgen voor bijgewerkte en nauwkeurige dreigingsbeoordelingen die weergeven hoe de operationele omgeving van dat moment is. Zij werken voortdurend hun kennis inzake kwetsbaarheden bij en herzien op gezette tijden de kwetsbaarheidsbeoordeling, met het oog op aanpassing aan de veranderende informatietechnologie (IT)-omgeving.

6. De behandeling van beveiligingsrisico's is erop gericht een reeks beveiligingsmaatregelen toe te passen die een bevredigend evenwicht oplevert tussen de verlangens van de gebruikers, de kosten en het resterende beveiligingsrisico.

7. De door de bevoegde SAA bepaalde specifieke eisen, reikwijdte en gedetailleerdheid voor de homologatie van een CIS stemmen overeen met het ingeschatte risico, rekening houdend met alle relevante factoren, waaronder de rubriceringsgraad van de in het CIS verwerkte EUCI. Homologatie houdt mede een formele verklaring betreffende het resterende risico in en aanvaarding van dat resterende risico door een verantwoordelijke instantie.

Beveiliging gedurende de levenscyclus van het CIS

8. Beveiliging is gedurende de gehele levenscyclus van het CIS — vanaf de ingebruikname tot de buitengebruikstelling — een vereiste.

9. De rol en interactie van iedere bij een CIS betrokken partij in verband met de beveiliging ervan wordt voor iedere fase van de levenscyclus vastgesteld.

10. Alle CIS, inclusief de maatregelen voor de technische en niet-technische beveiliging ervan, worden tijdens de homologatieprocedure aan beveiligingstests onderworpen om ervoor te zorgen dat het passende niveau van IA wordt bereikt en om na te gaan of zij correct zijn geïmplementeerd, geïntegreerd en geconfigureerd.

11. Beveiligingsbeoordelingen, inspecties en evaluaties worden op gezette tijden verricht tijdens de werking en het onderhoud van een CIS en wanneer zich uitzonderlijke omstandigheden voordoen.

12. De beveiligingsdocumentatie voor een CIS evolueert gedurende de levenscyclus van dat CIS als een integrerend deel van het proces van wijzigings- en configuratiebeheer.

Beste praktijken

13. Het SGR en de lidstaten ontwikkelen samen optimale toepassingen voor de bescherming van in CIS verwerkte EUCI. Richtlijnen inzake optimale toepassing beschrijven technische, fysieke, organisatorische en procedurele beveiligingsmaatregelen voor CIS, waarvan is aangetoond dat zij doeltreffend zijn in het bestrijden van dreigingen en kwetsbaarheden.

14. De bescherming van in CIS verwerkte EUCI steunt op de lering die door de bij IA betrokken entiteiten, zowel binnen als buiten de EU, is getrokken.

15. De verspreiding en de daaropvolgende toepassing van beste praktijken dragen bij aan het bereiken van een zelfde niveau van IA voor de diverse CIS waarin EUCI wordt verwerkt en die door het SGR en de lidstaten worden gebruikt.

Verdediging in de diepte

16. Om het risico voor CIS tot een minimum te beperken, wordt een reeks technische en niet-technische beveiligingsmaatregelen genomen, in de vorm van meerdere verdedigingslagen. Deze lagen omvatten:

    a) *afschrikking:* beveiligingsmaatregelen die vijandelijke plannen om het CIS aan te vallen, moeten ontraden;

    b) *preventie:* beveiligingsmaatregelen die een aanval op het CIS moeten verhinderen of tegenhouden;

    c) *detectie:* beveiligingsmaatregelen die moeten ontdekken dat het CIS wordt aangevallen;

    d) *veerkracht:* beveiligingsmaatregelen die het effect van een aanval tot een zo klein mogelijke reeks informatie of onderdelen van CIS moeten beperken en verdere schade moeten voorkomen, en

    e) *herstel:* beveiligingsmaatregelen die weer tot een veilige situatie voor het CIS moeten leiden.

    Aan de hand van een risicobeoordeling wordt bepaald hoe streng die beveiligingsmaatregelen moeten zijn.

17. De NSA of een andere bevoegde instantie ziet er tevens op toe dat:

    a) vermogens voor verdediging tegen cyberaanvallen worden ingezet om te reageren op bedreigingen die wellicht de organisatorische en nationale grenzen overschrijden, en

    b) de reacties gecoördineerd worden en informatie over deze bedreigingen, incidenten en de ermee verband houdende risico's worden gedeeld (computernoodhulpdiensten).

Minimaliteitsbeginsel en „least privilege"

18. Ter vermijding van onnodige risico's worden uitsluitend de functies, apparaten en diensten geactiveerd die essentieel zijn voor het vervullen van de operationele eisen.

19. Gebruikers van een CIS en geautomatiseerde processen krijgen alleen de toegang, voorrechten of machtigingen die zij nodig hebben voor het uitvoeren van hun taken, zodat schade ten gevolge van ongelukken, vergissingen of ongeoorloofd gebruik van CIS-middelen beperkt blijft.

20. De door een CIS uitgevoerde registratieprocedures worden indien nodig geverifieerd als onderdeel van de homologatieprocedure.

Besef van informatieborging

21. De eerste verdedigingslaag voor de beveiliging van CIS bestaat in bewustwording met de risico's en de beschikbare beveiligingsmaatregelen. Vooral alle leden van het personeel dat betrokken is bij de levenscyclus van CIS, met inbegrip van de gebruikers, moeten inzien:

    a) dat beveiligingsfouten ernstige schade kunnen berokkenen aan de CIS;

    b) dat interconnectiviteit en onderlinge afhankelijkheid kunnen leiden tot schade voor anderen, en

    c) dat zij individuele verantwoordelijkheid en aansprakelijkheid dragen voor de beveiliging van CIS overeenkomstig hun functies binnen de systemen en processen.

22. Al het betrokken personeel, onder meer het hogere kader en de CIS-gebruikers, moeten verplicht een IA-opleiding en -bewustmakingstraining volgen, zodat goed wordt begrepen waar de verantwoordelijkheden inzake beveiliging liggen.

Evaluatie en goedkeuring van IT-beveiligingsproducten

23. De vereiste graad van vertrouwen in de beveiligingsmaatregelen, gedefinieerd als een niveau van IA, wordt bepaald aan de hand van de resultaten van de risicobeheersprocedure en het beveiligingsbeleid en de beveiligingsrichtlijnen in kwestie.

24. Het niveau van IA wordt geverifieerd middels internationaal erkende of nationaal goedgekeurde processen en technologieën. Dit omvat in de eerste plaats evaluatie, controles en audits.

25. Encryptieproducten voor de bescherming van EUCI worden geëvalueerd en goedgekeurd door een CAA van een lidstaat.

26. Deze encryptieproducten moeten, voordat zij worden aanbevolen voor goedkeuring door de Raad of de SG/HV, overeenkomstig artikel 10, lid 6, zijn onderworpen aan een succesvolle tweede evaluatie door een naar behoren gekwalificeerde instantie (AQUA) van een lidstaat die niet betrokken is bij het ontwerp of de vervaardiging van de apparatuur. Hoe uitvoerig een en ander tijdens een tweede evaluatie moet worden bekeken, hangt af van het beoogde maximale rubriceringsniveau van de EUCI die door deze producten moet worden beschermd. De Raad stelt een beveiligingsbeleid inzake de evaluatie en goedkeuring van encryptieproducten vast.

27. Wanneer zulks om specifieke operationele redenen gerechtvaardigd is, kan de Raad, respectievelijk de SG/HV in voorkomend geval, op aanbeveling van het Beveiligingscomité, afwijken van de vereisten in de punten 25 en 26 van deze bijlage en een tijdelijke goedkeuring voor een specifieke periode verlenen overeenkomstig de procedure van artikel 10, lid 6.

28. De Raad kan op voorstel van het Beveiligingscomité zijn goedkeuring hechten aan het proces van evaluatie, selectie en goedkeuring van encryptieproducten van een derde land of internationale organisatie of deze encryptieproducten volgens dezelfde procedure geschikt bevinden voor de aan dat derde land of deze internationale organisatie vrijgegeven EUCI.

29. Een AQUA is een CAA van een lidstaat, die op basis van door de Raad vastgestelde criteria is geaccrediteerd voor het uitvoeren van de tweede evaluatie van encryptieproducten voor de bescherming van EUCI.

30. De Raad stelt een beveiligingsbeleid vast inzake de kwalificatie en goedkeuring van IT-beveiligingsproducten die geen encryptieproducten zijn.

Overdracht binnen beveiligde en administratieve zones

31. Niettegenstaande het bepaalde in dit besluit kan, wanneer de overdracht van EUCI beperkt is tot beveiligde of administratieve zones, op basis van het resultaat van een risicobeheerprocedure en behoudens goedkeuring van de SAA, gebruik worden gemaakt van onversleutelde toezending of van versleuteling op een lager niveau.

Beveiligde interconnectie van CIS

32. In dit besluit wordt onder een interconnectie verstaan: een rechtstreekse koppeling van twee of meer IT-systemen, met als doel het gezamenlijke gebruik van informatie en andere bronnen van informatie (bv. communicatie), in één of meer richtingen.

33. Een CIS beschouwt ieder gekoppeld IT-systeem als niet-vertrouwd en activeert beschermende maatregelen om de uitwisseling van gerubriceerde informatie te controleren.

34. Alle interconnecties van CIS aan een ander IT-systeem voldoen aan onderstaande basisvereisten:

a) de zakelijke of operationele vereisten voor dergelijke interconnecties worden door de bevoegde instanties vastgelegd en goedgekeurd;

b) de interconnecties worden aan een procedure inzake risicobeheersing en homologatie onderworpen en behoeven de goedkeuring van de SAA's, en

c) de perimeters van alle CIS worden opgezet met voorzieningen om de grenzen te beschermen (Boundary Protection Services, hierna BPS).

35. Er wordt geen interconnectie tot stand gebracht tussen een gehomologeerde CIS en een onbeschermd of openbaar netwerk, behalve indien voor dat doel in het CIS goedgekeurde BPS werden opgezet om de grenzen te beschermen tussen het CIS en het onbeschermde of openbare netwerk. De beveiligingsmaatregelen voor dergelijke interconnecties worden getoetst door de bevoegde IAA en goedgekeurd door de bevoegde SAA.

    Wanneer het onbeschermde of openbare netwerk alleen als drager wordt gebruikt en de informatie versleuteld is met een overeenkomstig artikel 10 goedgekeurd encryptieproduct, wordt een dergelijke koppeling niet gezien als een interconnectie.

36. De rechtstreekse interconnectie of de interconnectie in cascade van een CIS dat gehomologeerd is om informatie met rubricering TRÈS SECRET UE/EU TOP SECRET te verwerken en een onbeschermd of openbaar netwerk, is verboden.

Digitale opslagmedia

37. Digitale opslagmedia worden vernietigd volgens procedures die de bevoegde beveiligingsinstantie heeft goedgekeurd.

38. Digitale opslagmedia worden hergebruikt, lager gerubriceerd of gederubriceerd conform overeenkomstig artikel 6, lid 2, vast te stellen richtsnoeren voor beveiliging.

Noodgevallen

39. Niettegenstaande het bepaalde in dit besluit mogen de hieronder beschreven specifieke procedures worden toegepast in noodgevallen, zoals dreigende of uitgebroken crises, conflicten, oorlogssituaties of in uitzonderlijke operationele omstandigheden.

40. EUCI mag met toestemming van de bevoegde instantie door middel van voor een lager rubriceringniveau goedgekeurde encryptieproducten of zonder versleuteling worden overgedragen, indien vertraging schade zou veroorzaken die duidelijk zwaarder weegt dan de schade ten gevolge van de verspreiding van het gerubriceerde materiaal en indien:

    a) de zender en de ontvanger niet over de vereiste encryptieapparatuur beschikken of helemaal geen encryptieapparatuur hebben, en

    b) het gerubriceerde materiaal niet op tijd met andere middelen kan worden verstuurd.

41. Gerubriceerde informatie die in de in punt 39 bedoelde omstandigheden wordt overgedragen, mag geen tekenen of aanwijzingen dragen die haar onderscheiden van ongerubriceerde informatie of informatie die beschermd kan worden door een beschikbaar encryptieproduct. Ontvangers worden onverwijld langs andere wegen op de hoogte gebracht van het rubriceringniveau.

42. Indien gebruik wordt gemaakt van punt 39, wordt nadien een verslag opgesteld voor de bevoegde instantie en het Beveiligingscomité.

III. FUNCTIES EN INSTANTIES OP HET GEBIED VAN INFORMATION ASSURANCE

43. In de lidstaten en in het SGR worden onderstaande functies op het gebied van IA ingesteld. Deze functies vereisen geen afzonderlijke organisatorische entiteiten. Ze hebben afzonderlijke mandaten. Deze functies en de ermee samengaande verantwoordelijkheden kunnen echter in één organisatorische entiteit worden ondergebracht of geïntegreerd dan wel in meerdere organisatorische entiteiten worden gesplitst, als maar wordt vermeden dat belangen of taken botsen.

Information Assurance Authority (IA-overheid)

44. De IAA is verantwoordelijk voor:

    a) het ontwikkelen van beveiligingsbeleidsmaatregelen en beveiligingsrichtlijnen inzake IA en het toezien op de doeltreffendheid en pertinentie ervan;

    b) het beschermen en beheren van technische informatie over encryptieproducten;

    c) het garanderen dat IA-maatregelen die zijn geselecteerd voor de bescherming van EUCI, voldoen aan het beleid inzake de geschiktheid en selectie van die maatregelen;

    d) het garanderen dat encryptieproducten worden geselecteerd overeenkomstig het beleid inzake de geschiktheid en selectie ervan;

    e) het coördineren van opleiding en voorlichting inzake IA;

    f) het overleg met de provider van het systeem, de beveiligingsmedewerkers en de vertegenwoordigers van gebruikers over beveiligingsbeleidsmaatregelen en beveiligingsrichtlijnen inzake IA, en

    g) het garanderen dat er in het deskundigendeelgebied van het Beveiligingscomité passende deskundigheid beschikbaar is voor IA-kwesties.

TEMPEST-overheid

45. De TEMPEST-overheid (hierna: „TA") is ervoor verantwoordelijk dat CIS in overeenstemming is met het beleid en de richtlijnen van TEMPEST. Zij keurt tegenmaatregelen van TEMPEST voor installaties en producten goed voor de bescherming van EUCI tot een bepaald rubriceringniveau in haar operationele omgeving.

Overheid voor de goedkeuring van encryptieproducten

46. De overheid voor de goedkeuring van encryptieproducten (Crypto Approval Authority, hierna: „CAA") is ervoor verantwoordelijk dat encryptieproducten voldoen aan het nationale cryptobeleid of het cryptobeleid van de Raad. De CAA verleent aan een encryptieproduct goedkeuring voor de bescherming van EUCI tot een bepaald rubriceringniveau in haar operationele omgeving. Wat de lidstaten betreft, is de CAA voorts verantwoordelijk voor het evalueren van encryptieproducten.

Cryptodistributieoverheid

47. De cryptodistributieoverheid (Crypto Distribution Authority, hierna: „CDA") is verantwoordelijk voor:

a) het beheer van en de verantwoording voor encryptiemateriaal van de EU;

b) de naleving van passende procedures en de instelling van kanalen voor verslaglegging over, en veilige verwerking, opslag en verspreiding van al het encryptiemateriaal van de EU, en

c) de overdracht van encryptiemateriaal van de Europese Unie aan of van personen of diensten die er gebruik van maken.

Homologatieoverheid

48. De homologatieoverheid (Security Accreditation Authority, hierna SAA) voor ieder systeem is verantwoordelijk voor:

a) het garanderen dat CIS het toepasselijke beveiligingsbeleid en de beveiligingsrichtlijnen naleven, door het afgeven van een goedkeuringsverklaring voor CIS voor de verwerking van EUCI tot een bepaald rubriceringniveau in zijn operationele omgeving, met de voorwaarden voor de homologatie, en de criteria volgens welke hergoedkeuring nodig is;

b) het instellen van een procedure voor beveiligingshomologatie, overeenkomstig het desbetreffende beleid, met duidelijke goedkeuringsvoorwaarden voor CIS die onder haar gezag staan;

c) het opstellen van een strategie voor beveiligingshomologatie waarin de mate van gedetailleerdheid voor de homologatie wordt aangegeven, afhankelijk van het vereiste niveau van IA;

d) het bestuderen en goedkeuren van documentatie over beveiliging, inclusief risicobeheer en verklaringen over resterende risico's, systeemgebonden specificatie van beveiligingseisen (hierna: „SSB"), documenten ten bewijze van de beveiligingsimplementatie en operationele beveiligingsprocedures (hierna: „OB's"), en het garanderen dat die documentatie strookt met de regels en beleidsmaatregelen van de Raad inzake beveiliging;

e) het controleren van de implementatie van beveiligingsmaatregelen met betrekking tot het CIS, en wel via het uitvoeren of steunen van beveiligingsbeoordelingen, -inspecties of -toetsingen;

f) het vaststellen van beveiligingseisen (bijvoorbeeld machtigingsgraad van het personeel) voor gevoelige posten in verband met het CIS;

g) het onderschrijven van de selectie van goedgekeurde encryptie- en TEMPEST-producten die worden gebruikt om een CIS te beveiligen;

h) het goedkeuren, of indien nodig, het deelnemen aan de gezamenlijke goedkeuring van de interconnectie van een CIS met andere CIS, en

i) overleg met de provider van het systeem, de beveiligingsmedewerkers en vertegenwoordigers van de gebruikers over beveiligingsrisicobeheer, in het bijzonder het resterende risico, en de voorwaarden voor de goedkeuringsverklaring.

49. De SAA van het SGR is verantwoordelijk voor de homologatie van alle CIS die binnen het SGR functioneren.

50. De bevoegde SAA van een lidstaat is verantwoordelijk voor de homologatie van CIS en componenten van CIS die binnen de bevoegdheid van die lidstaat functioneren.

51. Een gemeenschappelijk beveiligingshomologatieorgaan (hierna: „VAO") is verantwoordelijk voor het accrediteren van CIS binnen de bevoegdheid van de IVA van het SGR en van de IVA van de lidstaten. Het bestaat uit een vertegenwoordiger van de IVA van iedere lidstaat en de vergaderingen worden bijgewoond door een vertegenwoordiger van de IVA van de Commissie. Andere entiteiten met een aansluiting op een CIS wordt verzocht de vergadering bij te wonen waarin dat systeem wordt besproken.

Het VAO wordt voorgezeten door een vertegenwoordiger van de IVA van het SGR. Het neemt besluiten met eenparigheid van stemmen van de IVA-vertegenwoordigers van instellingen, lidstaten en andere entiteiten met aansluitingen op het CIS. Het brengt periodiek verslag over zijn werkzaamheden uit aan het Beveiligingscomité en stelt dit in kennis van alle homologatieverklaringen.

Operationele instantie voor information assurance

52. De operationele IA-overheid voor ieder systeem is verantwoordelijk voor:

a) het ontwikkelen van beveiligingsdocumentatie die strookt met het beveiligingsbeleid en de beveiligingsrichtlijnen, in het bijzonder de SSB met inbegrip van de verklaring inzake het resterend risico, de OB's en het versleutelingsplan in de CIS-homologatieprocedure;

b) het deelnemen aan de selectie en het testen van de systeemspecifieke maatregelen, apparatuur en software voor de technische beveiliging, teneinde toezicht te houden op de implementatie ervan en ervoor te zorgen dat deze veilig worden geïnstalleerd, geconfigureerd en onderhouden overeenkomstig de beveiligingsdocumentatie;

c) het deelnemen aan de selectie van TEMPEST-beveiligingsmaatregelen en -apparatuur indien dat volgens de SSB nodig is en ervoor zorgen dat deze veilig worden geïnstalleerd en onderhouden, in samenwerking met de TA;

d) het toezien op de uitvoering en toepassing van de OB's en, in voorkomend geval, het overdragen van operationele verantwoordelijkheden voor beveiliging aan de eigenaar van het systeem;

e) het beheer van en het werken met encryptieproducten, de bewaring van versleutelde en gecontroleerde informatie en, indien nodig, het genereren van cryptografische variabelen;

f) het uitvoeren van evaluaties en tests van beveiligingsanalysen, in het bijzonder teneinde de door de IVA verlangde risicoverslagen op te stellen;

g) het aanbieden van CIS-specifieke IA-opleidingen, en

h) het implementeren en toepassen van CIS-specifieke beveiligingsmaatregelen.

BIJLAGE V

INDUSTRIËLE BEVEILIGING

I. INLEIDING

1. Deze bijlage bevat bepalingen ter uitvoering van artikel 11. De bijlage bevat algemene beveiligingsbepalingen die voor industriële of andere entiteiten gelden in precontractuele onderhandelingen en gedurende de levenscyclus van gerubriceerde opdrachten die het SGR gunt.

2. De Raad stelt richtsnoeren inzake industriële beveiliging vast waarin in het bijzonder uitvoerige vereisten worden geformuleerd inzake VMV's, memoranda over de beveiligingsaspecten (MBA's), bezoeken, overdracht en vervoer van EUCI.

II. BEVEILIGINGSELEMENTEN IN EEN GERUBRICEERDE OPDRACHT

Gids voor rubricering (GBR)

3. Alvorens een aanbesteding uit te schrijven of een gerubriceerde opdracht te gunnen, bepaalt het SGR als aanbestedende instantie welke rubricering wordt gegeven aan informatie die aan inschrijvers en contractanten moeten worden verstrekt, en welke rubricering wordt gegeven aan informatie die de contractant zal genereren. Voor dat doel stelt het SGR een GBR op die bij de uitvoering van de opdracht moet worden gebruikt.

4. Voor het bepalen van de rubricering van de diverse onderdelen van een gerubriceerde opdracht gelden onderstaande beginselen:

a) bij het opstellen van een GBR houdt het SGR rekening met alle ter zake doende beveiligingsaspecten, zoals de rubricering die is gegeven aan verstrekte informatie waarvan het gebruik voor de opdracht is goedgekeurd door de bron van de informatie;

b) de algehele rubriceringsgraad van de opdracht kan niet lager zijn dan de hoogste rubricering van een van haar onderdelen, en

c) indien nodig neemt het SGR contact op met de NSA/DSA's van de lidstaten of enige andere bevoegde beveiligingsinstantie als zich wijzigingen voordoen met betrekking tot de rubricering van door of aan contractanten verstrekte informatie tijdens de uitvoering van een opdracht, en wanneer verdere wijzigingen in de GBR worden aangebracht.

Memorandum over de beveiligingsaspecten (MBA)

5. De specifieke beveiligingseisen voor de opdracht worden beschreven in een MBA. Het MBA bevat in voorkomend geval de GBR en maakt integraal deel uit van een gerubriceerde opdracht of opdracht in onderaanneming.

6. Het MBA bevat bepalingen die de contractant en/of de subcontractant verplichten zich te houden aan de minimumbeveiligingsnormen in dit besluit. Niet-naleving van deze minimumnormen kan voldoende reden zijn voor opzegging van de opdracht.

Programma-/projectbeveiligingsinstructies (PBI)

7. Afhankelijk van het toepassingsgebied van programma's of projecten waarvoor toegang tot of verwerking of opslag van EUCI nodig is, kan de aanbestedende instantie die het programma of het project zal beheren, specifieke PBI opstellen. De PBI moeten worden goedgekeurd door de NSA/DSA's van de lidstaten of een andere bevoegde beveiligingsinstantie die deelneemt aan de PBI, en kunnen nadere beveiligingsvoorschriften bevatten.

III. VEILIGHEIDSMACHTIGING VOOR EEN VESTIGING (VMV)

8. Een VMV wordt verleend door de NSA of DSA of een andere bevoegde instantie van een lidstaat en toont overeenkomstig de nationale wetten en regelgeving aan dat een industriële of andere entiteit binnen haar vestigingen in staat is EUCI te beschermen op het vereiste rubriceringsniveau (CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET). Voordat aan een contractant of subcontractant of mogelijke contractant of subcontractant EUCI mag worden verstrekt of toegang tot EUCI mag worden verleend, wordt de machtiging overgelegd aan het SGR, als aanbestedende instantie.

9. Wanneer de betrokken NSA of DSA een VMV afgeeft, zal zij op zijn minst:

a) de integriteit van de industriële of andersoortige entiteit evalueren;

b) de verantwoordelijkheid evalueren, evenals de controle of de ontvankelijkheid voor ongewenste invloed, die als een beveiligingsrisico kan worden beschouwd;

c) nagaan of de industriële of andere entiteit in de vestiging een beveiliging heeft geïnstalleerd die alle passende beveiligingsmaatregelen omvat die nodig zijn voor het beschermen van informatie of materiaal met rubriceringsgraad CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET, overeenkomstig de in dit besluit vastgelegde vereisten;

d) nagaan of de personeelsbeveiligingsstatus van management, eigenaars en werknemers die toegang moeten hebben tot informatie van de rubriceringsgraad CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET, voldoet aan de in dit besluit vastgelegde vereisten, en

e) nagaan of de industriële of andere entiteit een vestigingsbeveiligingsfunctionaris (VBF) heeft benoemd die tegenover het management verantwoordelijk is voor het doen naleven van de beveiligingsverplichtingen in de entiteit.

10. In voorkomend geval deelt het SGR, als aanbestedende instantie, de NSA/DSA of een andere bevoegde beveiligingsinstantie mee dat in de precontractuele fase of voor de uitvoering van de opdracht een VMV vereist is. Een VMV of een BMP wordt verlangd in de precontractuele fase waarin EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET moet worden verstrekt in het stadium van de offertes.

11. De aanbestedende instantie kent geen gerubriceerde toe opdracht aan een geselecteerde inschrijver zonder van de NSA/DSA of een andere bevoegde beveiligingsinstantie van de lidstaat waar de contractant of subcontractant is geregistreerd, een bevestiging te hebben ontvangen dat er, indien zulks vereist is, een VMV is afgegeven.

12. De NSA/DSA of een andere bevoegde beveiligingsinstantie die een VMV heeft afgegeven brengt het SGR, de aanbestedende instantie, op de hoogte van wijzigingen die de VMV betreffen. Bij onderaanneming worden de NSA/DSA of een andere bevoegde beveiligingsinstantie op de hoogte gebracht.

13. Intrekking van een VMV door de NSA/DSA of andere bevoegde nationale beveiligingsinstantie biedt het SGR, de aanbestedende instantie, voldoende redenen om een gerubriceerde opdracht te beëindigen of een inschrijver uit te sluiten van mededinging.

IV. GERUBRICEERDE OPDRACHTEN EN ONDERAANNEMING

14. Wanneer in de precontractuele fase EUCI wordt verstrekt aan een inschrijver, bevat de uitnodiging tot inschrijving een bepaling die de inschrijver die uiteindelijk geen offerte doet, of die niet wordt geselecteerd, verplicht alle gerubriceerde documenten binnen een bepaalde termijn terug te zenden.

15. Zodra een gerubriceerde opdracht of opdracht in onderaanneming is gegund, deelt het SGR, als aanbestedende instantie, de NSA/DSA of een andere bevoegde beveiligingsinstantie van de contractant of subcontractant de beveiligingsbepalingen van de gerubriceerde opdracht mee.

16. Wanneer zulke opdrachten aflopen, deelt het SGR, als aanbestedende dienst (en/of, bij onderaanneming, de NSA/DSA of een andere bevoegde beveiligingsinstantie, naargelang het geval) dit mee aan de NSA/DSA of een andere bevoegde beveiligingsinstantie van de lidstaat waar de contractant of subcontractant is geregistreerd.

17. Als algemene regel geldt dat de contractant of subcontractant alle EUCI die hij in zijn bezit heeft, na voltooiing van de gerubriceerde opdracht of onderaanneming moet terugbezorgen aan de aanbestedende instantie.

18. In het MBA worden specifieke bepalingen opgenomen voor het verwijderen van EUCI tijdens de uitvoering van een opdracht of bij de voltooiing ervan.

19. Wanneer de contractant of subcontractant gemachtigd is EUCI te houden na voltooiing van een opdracht, blijven de minimumnormen van dit besluit van toepassing en wordt de vertrouwelijkheid van EUCI door de contractant of subcontractant beschermd.

20. De voorwaarden waaronder een contractant een beroep kan doen op subcontractanten worden in de aanbesteding en de opdracht omschreven.

21. Een contractant krijgt van het SGR, de aanbestedende instantie, toestemming voordat hij delen van een gerubriceerde opdracht uitbesteedt aan een onderaannemer. Industriële of andere entiteiten die geregistreerd zijn in een land dat geen lidstaat van de Europese Unie is en geen informatiebeveiligingsovereenkomst met de Europese Unie heeft, mogen niet als subcontractant worden ingeschakeld.

22. Het is de verantwoordelijkheid van de contractant te garanderen dat alle onderaannemingsactiviteiten verlopen in overeenstemming met de minimumnormen van dit besluit en de contractant mag geen EUCI doorgeven aan een subcontractant zonder voorafgaande schriftelijke toestemming van de aanbestedende instantie.

23. Wat betreft EUCI die door de contractant of subcontractant wordt gegenereerd of verwerkt, oefent de aanbestedende instantie de rechten van de bron uit.

V. BEZOEKEN IN VERBAND MET GERUBRICEERDE OPRACHTEN

24. Wanneer het SGR of personeel van contractanten of subcontractanten voor de uitvoering van een gerubriceerde opdracht in elkaars ruimten toegang vragen tot als CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET gerubriceerde informatie, worden in overleg met de NSA/DSA's of een andere bevoegde beveiligingsinstantie bezoeken georganiseerd. In het kader van specifieke projecten kunnen de NSA/DSA's echter ook een procedure overeenkomen waarmee zulke bezoeken rechtstreeks kunnen worden georganiseerd.

25. Alle bezoekers beschikken over een passende BMP en hebben een „need-to-know" voor toegang tot de EUCI met betrekking tot de opdracht van het SGR.

26. Bezoekers krijgen uitsluitend toegang tot de EUCI die verband houdt met het doel van het bezoek.

VI. OVERDRACHT EN VERVOER VAN EUCI

27. Op de overdracht van EUCI met elektronische middelen zijn artikel 10 en bijlage IV van toepassing.

28. Op het vervoer van EUCI is bijlage III van toepassing, overeenkomstig de nationale wet- en regelgeving.

29. Wat het vervoer van gerubriceerd materiaal als vracht betreft, worden bij de opstelling van regeling inzake beveiliging de volgende beginselen toegepast:

a) de beveiliging wordt tijdens alle fasen van het vervoer gewaarborgd, van het punt van oorsprong tot de eindbestemming;

b) de mate van bescherming die aan een zending wordt verleend, wordt bepaald door de hoogste rubriceringsgraad van het materiaal dat zij bevat;

c) er wordt een VMV op het passende niveau verkregen voor de ondernemingen die het vervoer verzorgen. In dat geval moeten de personeelsleden die de zending verwerken, in overeenstemming met bijlage I een veiligheidsonderzoek ondergaan;

d) vóór iedere grensoverschrijdende verplaatsing van materiaal met rubriceringsgraad CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET stelt de verzender een vervoerplan op, dat wordt goedgekeurd door de betrokken NSA's/DSA's of een andere bevoegde beveiligingsinstantie;

e) de reizen geschieden zoveel mogelijk zonder onderbreking, en worden zo snel als de omstandigheden toelaten uitgevoerd, en

f) waar mogelijk leiden de routen alleen door lidstaten. Routen door niet-lidstaten worden alleen gevolgd met toestemming van de NSA/DSA of een andere bevoegde beveiligingsinstantie van de staat van de verzender en de staat van de geadresseerde.

VII. OVERDRACHT VAN EUCI NAAR CONTRACTANTEN IN DERDE STATEN

30. EUCI wordt overgedragen aan contractanten en subcontractanten in derde staten overeenkomstig de beveiligingsmaatregelen die zijn overeengekomen door het SGR, als aanbestedende dienst, en de NSA/DSA van de derde staat in kwestie waar de contractant is geregistreerd.

VIII. ALS RESTREINT UE/EU RESTRICTED GERUBRICEERDE INFORMATIE

31. Samen, waar nodig, met de NSA/DSA van de lidstaat, is het SGR, als aanbestedende instantie, op basis van contractuele bepalingen gerechtigd inspecties te verrichten van vestigingen van contractanten/subcontractanten om na te gaan of, zoals in de opdracht wordt vereist, de beveiligingsmaatregelen ter zake zijn getroffen voor de bescherming van EUCI van het niveau RESTREINT UE/EU RESTRICTED.

32. Voor zover dat nodig is volgens de nationale wet- en regelgeving, worden NSA's/DSA's of andere bevoegde beveiligingsinstanties door het SGR, als aanbestedende dienst, in kennis gesteld van opdrachten of opdrachten in onderaanneming die informatie met rubricering RESTREINT UE/EU RESTRICTED bevatten.

33. Een VMV of een BMP voor contractanten of subcontractanten en hun personeel is niet vereist voor opdrachten van het SGR, die als RESTREINT UE/EU RESTRICTED gerubriceerde informatie bevatten.

34. Het SGR bestudeert, als aanbestedende dienst, de reacties op de uitnodigingen tot inschrijving voor opdrachten waarvoor toegang tot als RESTREINT UE/EU RESTRICTED gerubriceerde informatie nodig is, ongeacht eventuele vereisten met betrekking tot VMV of BMP uit hoofde van nationale wet- en regelgeving.

35. De voorwaarden voor uitbesteding in onderaanneming door de contractant zijn in overeenstemming met het bepaalde in punt 21.

36. Wanneer een opdracht de verwerking van informatie met rubricering RESTREINT UE/EU RESTRICTED in een door een contractant geëxploiteerd CIS behelst, zorgt het SGR, als aanbestedende dienst, ervoor dat in het contract of de onderaanneming de nodige technische en administratieve eisen worden gespecificeerd met betrekking tot de homologatie van het CIS in overeenstemming met het ingeschatte risico, rekening houdend met alle belangrijke factoren. Hoe ver de homologatie van een dergelijke CIS reikt, wordt door de aanbestedende dienst en de betrokken NSA/DSA bepaald.

BIJLAGE VI

UITWISSELING VAN GERUBRICEERDE INFORMATIE MET DERDE STATEN EN INTERNATIONALE ORGANISATIES

I. INLEIDING

1. Deze bijlage bevat bepalingen ter uitvoering van artikel 13.

II. KADERS VOOR DE UITWISSELING VAN GERUBRICEERDE INFORMATIE

2. Wanneer de Raad bepaalt dat het nodig is om voor een lange termijn gerubriceerde informatie uit te wisselen,

— wordt een informatiebeveiligingsovereenkomst gesloten, of

— wordt een administratieve regeling getroffen,

overeenkomstig artikel 13, lid 2, en deel III en IV, op basis van een aanbeveling van het Beveiligingscomité.

3. Wanneer ten behoeve van een EVDB-operatie gegenereerde EUCI moet worden verstrekt aan derde staten of internationale organisaties die aan die operatie deelnemen, en wanneer geen van de in punt 2 bedoelde kaders bestaat, wordt de uitwisseling van EUCI met de bijdragende derde staat of internationale organisatie overeenkomstig deel V geregeld door:

— een kaderovereenkomst inzake deelname;

— een ad-hocovereenkomst inzake deelname, of

— bij het ontbreken daarvan, een ad hoc administratieve regeling.

4. Bij het ontbreken van een kader als bedoeld in de punten 2 en 3, en wanneer het besluit wordt genomen om EUCI op een uitzonderlijke ad-hocbasis vrij te geven aan een derde staat of een internationale organisatie conform afdeling VI, wordt de betrokken derde staat of de internationale organisatie om schriftelijke verzekering verzocht om te garanderen dat deze alle vrijgegeven EUCI zal beschermen overeenkomstig de grondbeginselen en minimumnormen in dit besluit.

III. INFORMATIEBEVEILIGINGSOVEREENKOMSTEN

5. Informatiebeveiligingsovereenkomsten bevatten de grondbeginselen en minimumnormen voor de uitwisseling van gerubriceerde informatie tussen de Europese Unie en een derde staat of internationale organisatie.

6. Informatiebeveiligingsovereenkomsten bevatten ook een technische uitvoeringsregeling, waarover overeenstemming moet worden bereikt tussen de bevoegde beveiligingsinstanties van de relevante EU-instellingen en de bevoegde beveiligingsinstantie van de derde staat of de internationale organisatie in kwestie. Deze regeling is afgestemd op het niveau van bescherming dat wordt geboden door de beveiligingsvoorschriften, -structuren en -procedures in de derde staat of binnen de internationale organisatie in kwestie. Ze worden goedgekeurd door het Beveiligingscomité.

7. Uit hoofde van een informatiebeveiligingsovereenkomst wordt geen EUCI uitgewisseld via elektronische middelen, tenzij daarin uitdrukkelijk is voorzien in de overeenkomst of de overeenkomstige technische uitvoeringsregeling.

8. Wanneer de Raad een informatiebeveiligingsovereenkomst sluit, wordt er bij elke partij een register aangewezen als het belangrijkste punt langs waar gerubriceerde informatie binnenkomt of uitgaat.

9. Ter beoordeling van de doeltreffendheid van de beveiligingsvoorschriften, -structuren en -procedures in de derde staat of binnen de internationale organisatie in kwestie, worden in overleg met de betrokken derde staat of internationale organisatie evaluatiebezoeken afgelegd. Zulke evaluatiebezoeken verlopen overeenkomstig de bepalingen in kwestie van bijlage III en houden een evaluatie in van:

a) het regelgevingskader voor de bescherming van gerubriceerde informatie;

b) specifieke kenmerken van het beveiligingsbeleid en de manier waarop de beveiliging in de derde staat of bij de internationale organisatie is georganiseerd, en de eventuele gevolgen die een en ander heeft voor het niveau van de gerubriceerde informatie die kan worden uitgewisseld;

c) de vigerende beveiligingsmaatregelen en -procedures, en

d) de veiligheidsmachtigingsprocedures voor het vrij te geven niveau van EUCI.

10. Het team dat namens de Europese Unie een evaluatiebezoek aflegt, beoordeelt of de beveiligingsvoorschriften en -procedures in de derde staat of binnen de internationale organisatie in kwestie toereikend zijn voor de bescherming van EUCI op een gegeven niveau.

11. De bevindingen van die bezoeken worden vermeld in een verslag op basis waarvan het Beveiligingscomité het maximumniveau bepaalt van de EUCI die met de derde partij in kwestie op papier of in voorkomend geval in elektronische vorm mag worden uitgewisseld, alsook de specifieke voorwaarden voor uitwisseling met deze partij.

12. Alles zal in het werk worden gesteld om een volledig beveiligingsevaluatiebezoek af te leggen aan de derde staat of internationale organisatie in kwestie, voordat het Beveiligingscomité de uitvoeringsregeling goedkeurt, teneinde de aard en de doeltreffendheid van het bestaande beveiligingssysteem te bepalen. Mocht dit niet mogelijk zijn, dan krijgt het Beveiligingscomité van de dienst Beveiliging van het SGR een zo volledig mogelijk verslag, op basis van de informatie waarover deze beschikt, waarin het Beveiligingscomité wordt geïnformeerd over de toepasselijke beveiligingsvoorschriften en over de manier waarop de beveiliging in de derde staat of binnen de internationale organisatie in kwestie is georganiseerd.

13. Het verslag over het evaluatiebezoek of, bij gebreke daaraan, het in punt 12 bedoelde verslag wordt toegezonden aan het Beveiligingscomité, dat het bevredigend moet achten alvorens er daadwerkelijk EUCI aan de derde staat of de internationale organisatie in kwestie wordt vrijgegeven.

14. De bevoegde beveiligingsinstanties van de instellingen en organen van de Unie delen de derde staat of internationale organisatie mede vanaf welke datum de Unie bij machte is om uit hoofde van de overeenkomst EUCI vrij te geven, alsook tot welk maximumniveau de EUCI in papieren vorm of met elektronische middelen kan worden uitgewisseld.

15. Indien nodig worden follow-upevaluatiebezoeken verricht, meer bepaald als:

a) het niveau van EUCI dat kan worden vrijgegeven, dient te worden verhoogd, of

b) de Unie kennis is gegeven van fundamentele wijzigingen in de beveiligingsregeling van de derde staat of internationale organisatie die van invloed kunnen zijn op de wijze waarop zij EUCI beschermt, of

c) er een ernstig incident is geweest waarbij EUCI zonder machtiging openbaar is gemaakt.

16. Zodra de informatiebeveiligingsovereenkomst van kracht is en er met de betrokken derde staat of internationale organisatie gerubriceerde informatie wordt uitgewisseld, kan het Beveiligingscomité besluiten het maximumniveau waarop EUCI op papier of in elektronische vorm mag worden uitgewisseld te wijzigen, met name naar aanleiding van een vervolgevaluatiebezoek.

IV. ADMINISTRATIEVE REGELING

17. Indien het nodig is om met derde staten of internationale organisaties voor een lange termijn informatie uit te wisselen waarvan de rubriceringsgraad als algemene regel niet hoger is dan RESTREINT UE/EU RESTRICTED, en wanneer het Beveiligingscomité heeft vastgesteld dat de partij in kwestie geen voldoende ontwikkeld beveiligingssysteem heeft om een informatiebeveiligingsovereenkomst te sluiten, mag de SG/HV, na goedkeuring door de Raad, namens het SGR een administratieve regeling treffen met de daarvoor aangewezen instanties van de derde staat of de internationale organisatie in kwestie.

18. Indien om dringende operationele redenen snel een kader voor de uitwisseling van gerubriceerde informatie moet worden opgezet, kan de Raad bij wijze van uitzondering besluiten dat er een administratieve regeling wordt getroffen voor de uitwisseling van informatie met een hogere rubriceringsgraad.

19. Een administratieve regeling heeft in de regel de vorm van een briefwisseling.

20. Een evaluatiebezoek als bedoeld in punt 9 wordt afgelegd en het verslag of, bij gebreke daarvan, het in punt 12 bedoelde verslag wordt toegezonden aan het Beveiligingscomité, dat het bevredigend moet achten alvorens er daadwerkelijk EUCI aan de derde staat of de internationale organisatie in kwestie wordt vrijgegeven.

21. Uit hoofde van een administratieve regeling wordt geen EUCI uitgewisseld via elektronische middelen, tenzij daarin uitdrukkelijk is voorzien in de regeling.

V. UITWISSELING VAN GERUBRICEERDE INFORMATIE IN DE CONTEXT VAN EVDB-OPERATIES

22. Deelname van derde staten of internationale organisaties aan EVDB-operaties worden geregeld bij kaderovereenkomsten inzake deelname. Deze overeenkomsten bevatten bepalingen betreffende de vrijgave van ten behoeve van EVDB-operaties gegenereerde EUCI aan de bijdragende derde staten of internationale organisaties. De hoogste rubriceringsgraad van EUCI die mag worden uitgewisseld, is RESTREINT UE/EU RESTRICTED voor burgerlijke EVDB-operaties en CONFIDENTIEL UE/EU CONFIDENTIAL voor militaire EVDB-operaties, tenzij anders is bepaald in het gemeenschappelijk optreden waarbij iedere EVDB-operatie wordt ingesteld.

23. Voor een specifieke EVDB-operatie gesloten ad-hocovereenkomsten inzake deelname bevatten bepalingen betreffende de vrijgave van ten behoeve van die operatie gegenereerde EUCI aan de bijdragende derde staat of internationale organisatie. De hoogste rubriceringsgraad van EUCI die mag worden uitgewisseld, is RESTREINT UE/EU RESTRICTED voor burgerlijke EVDB-operaties en CONFIDENTIEL UE/EU CONFIDENTIAL voor militaire EVDB-operaties, tenzij anders is bepaald in het gemeenschappelijk optreden waarbij iedere EVDB-operatie wordt ingesteld.

24. Indien er geen informatiebeveiligingsovereenkomst is gesloten en in afwachting van de sluiting van een overeenkomst inzake deelname kan de vrijgave van ten behoeve van de operatie gegenereerde EUCI aan een derde land of internationale organisatie die aan de operatie deelneemt, geregeld worden in een administratieve regeling waartoe de hoge vertegenwoordiger kan toetreden, of in een besluit tot ad-hocvrijgave overeenkomstig afdeling VI. EUCI wordt alleen uitgewisseld uit hoofde van een dergelijke regeling zolang de deelneming van de derde staat of internationale organisatie nog wordt overwogen. De hoogste rubriceringsgraad van EUCI die mag worden uitgewisseld, is RESTREINT UE/EU RESTRICTED voor burgerlijke EVDB-operaties en CONFIDENTIEL UE/EU CONFIDENTIAL voor militaire EVDB-operaties, tenzij anders is bepaald in het gemeenschappelijk optreden waarbij iedere EVDB-operatie wordt ingesteld.

25. Ten aanzien van gerubriceerde informatie die moeten worden opgenomen in kaderovereenkomsten inzake deelname, in ad-hocovereenkomsten inzake deelname en in ad hoc administratieve regelingen bedoeld in de punten 22 tot en met 24, wordt bepaald dat de derde staat of de internationale organisatie in kwestie ervoor zorgt dat het naar een operatie uitgezonden personeel EUCI zal beschermen overeenkomstig de beveiligingsvoorschriften van de Raad en overeenkomstig nadere instructies van de bevoegde instanties, waaronder de commandostructuur van de operatie.

26. Indien vervolgens een informatiebeveiligingsovereenkomst wordt gesloten tussen de Europese Unie en een bijdragende derde staat of internationale organisatie, vervangt de informatiebeveiligingsovereenkomst, wat betreft het uitwisselen en verwerken van EUCI, de bepalingen over de uitwisseling van gerubriceerde informatie als neergelegd in een eventuele kaderovereenkomst inzake deelname, ad-hocovereenkomst inzake deelname of ad hoc administratieve regeling.

27. Elektronische uitwisseling van EUCI wordt niet toegestaan op basis van een kaderovereenkomst inzake deelname, een ad-hocovereenkomst inzake deelname of een ad hoc administratieve regeling met een derde staat of een internationale organisatie, tenzij daarin in de overeenkomst of regeling in kwestie uitdrukkelijk wordt voorzien.

28. Ten behoeve van een EVDB-operatie gegenereerde EUCI mag worden bekendgemaakt aan personeel dat door derde staten of internationale organisaties bij die operatie gedetacheerd is, overeenkomstig de punten 22 tot en met 27. Wanneer aan dat personeel toegang tot EUCI wordt verleend in werkruimten of in CIS van een EVDB-operatie, moeten maatregelen worden getroffen (zoals registratie van bekendgemaakte EUCI) om het risico van verlies of compromittering te verkleinen. Dergelijke maatregelen worden opgesteld in de desbetreffende plannings- of missiedocumenten.

29. Indien er geen informatiebeveiligingsovereenkomst is gesloten, kan in geval van specifieke en onmiddellijke operationele noodzaak de vrijgave van EUCI aan de ontvangende staat op het grondgebied waarvan een EVDB-operatie wordt uitgevoerd, geregeld worden in een administratieve regeling waartoe de hoge vertegenwoordiger kan toetreden. In deze mogelijkheid wordt voorzien in het gemeenschappelijk optreden waarin de EVDB-operatie wordt vastgesteld. Onder dergelijke omstandigheden wordt alleen EUCI vrijgegeven die ten behoeve van de EVDB-operatie wordt gegenereerd en die niet hoger is gerubriceerd dan RESTREINT UE/EU RESTRICTED, tenzij in het besluit waarbij de EVDB-operatie wordt ingesteld een hogere rubriceringsgraad is opgenomen. In het kader van een dergelijke administratieve regeling dient de ontvangende staat zich ertoe te verbinden EUCI te beschermen overeenkomstig met minimumnormen die niet minder streng zijn dan die van dit besluit.

30. Indien er geen informatiebeveiligingsovereenkomst is gesloten, kan de vrijgave van EUCI aan de betrokken derde staten en internationale organisaties, andere dan die welke aan een GVDB-operatie deelnemen, geregeld worden in een administratieve regeling waartoe de hoge vertegenwoordiger kan toetreden. Indien nodig worden deze mogelijkheid, alsmede de voorwaarden waaronder daarvan gebruik kan worden gemaakt, nader gepreciseerd in het besluit waarbij de EVDB-operatie wordt opgezet. Onder dergelijke omstandigheden wordt alleen EUCI vrijgegeven die ten behoeve van de EVDB-operatie wordt gegenereerd en die niet hoger is gerubriceerd dan RESTREINT UE/EU RESTRICTED, tenzij in het besluit waarbij de EVDB-operatie wordt ingesteld een hogere rubriceringsgraad is vastgesteld. In het kader van een dergelijke administratieve regeling dient de betrokken derde staat of internationale organisatie zich ertoe te verbinden EUCI te beschermen overeenkomstig met minimumnormen die niet minder streng zijn dan die van dit besluit.

31. Er zijn geen uitvoeringsregelingen of evaluatiebezoeken vereist alvorens de bepalingen betreffende de vrijgave van EUCI in de context van de punten 22, 23 en 24 worden uitgevoerd.

VI. UITZONDERLIJKE AD-HOCVRIJGAVE VAN EUCI

32. Indien er geen kader bestaat overeenkomstig de afdelingen III tot en met V, en wanneer de Raad of een van zijn voorbereidende instanties vaststelt dat zich een uitzonderlijke noodzaak voordoet om EUCI vrij te geven aan een derde staat of een internationale organisatie, moet het SGR:

a) voor zover mogelijk, met de beveiligingsinstanties van de derde staat of de internationale organisatie in kwestie nagaan of de beveiligingsvoorschriften, -structuren en -procedures van die staat of organisatie van die aard zijn dat aan hen vrijgegeven EUCI wordt beschermd volgens normen die niet minder streng zijn dan die van dit besluit, en

b) het Beveiligingscomité verzoeken om op basis van de beschikbare informatie een aanbeveling te doen betreffende het vertrouwen dat kan worden gesteld in de beveiligingsvoorschriften, -structuren en -procedures van de derde staat of de internationale organisatie waaraan de EUCI moet worden vrijgegeven.

33. Indien het Beveiligingscomité aanbeveelt de EUCI vrij te geven, wordt de zaak voorgelegd aan het Comité van permanente vertegenwoordigers (Coreper), dat een besluit neemt over de vrijgave.

34. Indien het beveiligingscomité aanbeveelt de EUCI niet vrij te geven, worden:

a) aangelegenheden inzake het GBVB/EVDB besproken door het Politiek en Veiligheidscomité, dat een aanbeveling doet voor een besluit van het Coreper;

b) alle andere aangelegenheden besproken door het Coreper, dat vervolgens een besluit neemt.

35. Wanneer zulks passend wordt geacht en indien de bron vooraf schriftelijk toestemming verleent, kan het Coreper besluiten dat de gerubriceerde informatie slechts gedeeltelijk mag worden vrijgegeven of pas nadat zij een lagere rubricering heeft gekregen of gederubriceerd is, of dat de vrij te geven informatie wordt opgesteld zonder vermelding van de bron of de oorspronkelijke EU-rubricering.

36. Nadat tot vrijgave van EUCI is besloten, verzendt het SGR het betrokken document, met daarop een markering inzake de geschiktheid voor vrijgave die vermeldt aan welke derde staat of internationale organisatie het is vrijgegeven. Voorafgaand aan of op het moment van de daadwerkelijke vrijgave, zegt de derde partij in kwestie schriftelijk toe dat zij de EUCI die zij ontvangt, zal beschermen overeenkomstig de grondbeginselen en minimumnormen van dit besluit.

VII. BEVOEGDHEID OM EUCI VRIJ TE GEVEN AAN DERDE STATEN OF INTERNATIONALE ORGANISATIES

37. Indien er overeenkomstig punt 2 een kader bestaat voor de uitwisseling van gerubriceerde informatie met een derde staat of een internationale organisatie, neemt de Raad een besluit waarbij de SG/HV wordt gemachtigd om, met inachtneming van het beginsel inzake toestemming van de bron, EUCI vrij te geven aan de derde staat of internationale organisatie in kwestie. De secretaris-generaal kan deze machtiging delegeren aan hoge ambtenaren van het SGR.

38. Indien overeenkomstig punt 2, eerste streepje, een informatiebeveiligingsovereenkomst is afgesloten, kan de Raad een besluit nemen waarbij de hoge vertegenwoordiger gemachtigd wordt tot vrijgave van EUCI die haar oorsprong vindt in de Raad op het gebied van het gemeenschappelijk buitenlands en veiligheidsbeleid, na de instemming te hebben verkregen van de opsteller van daarin opgenomen bronnenmateriaal, aan de betrokken derde staat of internationale organisatie. De hoge vertegenwoordiger kan deze machtiging delegeren aan hoge ambtenaren van de EDEO of aan SVEU's.

39. Indien er overeenkomstig punt 2 of punt 3 een kader bestaat voor de uitwisseling van gerubriceerde informatie met een derde staat of een internationale organisatie, wordt de hoge vertegenwoordiger gemachtigd om EUCI vrij te geven, overeenkomstig het gemeenschappelijk optreden waarbij de EVDB-operatie wordt opgezet en met inachtneming van het beginsel inzake toestemming van de bron. De hoge vertegenwoordiger kan deze machtiging delegeren aan hoge ambtenaren van de EDEO, aan bevelhebbers van EU-operaties, strijdkrachten of missies, of aan de hoofden van EU-missies.

Aanhangsels

Aanhangsel A

Definities

Aanhangsel B

Concordantie van de rubriceringen

Aanhangsel C

Lijst van nationale beveiligingsinstanties (NSA's)

Aanhangsel D

Lijst van afkortingen

Aanhangsel A

DEFINITIES

In dit besluit wordt verstaan onder:

„Homologatie": het proces dat leidt tot de formele verklaring van de instantie voor beveiligingshomologatie (SAA) dat een systeem mag functioneren met een bepaald rubriceringniveau, in een specifieke beveiligingsmodus in zijn operationele omgeving en op een aanvaardbaar risiconiveau, nadat is vastgesteld dat er een goedgekeurde reeks technische, fysieke, organisatorische en procedurele beveiligingsmaatregelen is ingebouwd;

„Kritisch bestanddeel": alles wat van waarde is voor een organisatie, haar bedrijfsactiviteiten en de continuïteit daarvan, met inbegrip van informatiebronnen ter ondersteuning van de opdracht van de organisatie;

„Machtiging voor toegang tot EUCI": een besluit van het tot aanstelling bevoegde gezag van het SGR op grond van een van een bevoegde instantie verkregen verzekering dat een functionaris van het SGR, een ander personeelslid of een gedetacheerde nationale deskundige, mits zijn noodzaak tot kennisname is vastgesteld en hij op passende wijze in kennis is gesteld van zijn verantwoordelijkheden, tot op een bepaald niveau CONFIDENTIEL UE/EU CONFIDENTIAL of hoger) en tot een bepaalde datum toegang is verleend tot EUCI;

„CIS-levenscyclus": de volledige bestaansduur van een CIS, inhoudende ingebruikname, conceptie, planning, behoefteanalyse, ontwerp, ontwikkeling, testen, implementatie, in bedrijf zijn, onderhoud en buitengebruikstelling;

„Gerubriceerde opdracht": een overeenkomst tussen het SGR en een contractant voor de levering van goederen, de uitvoering van werken of de verrichting van diensten waarvan de uitvoering de toegang tot of het genereren van EUCI vereist of behelst;

„Gerubriceerde onderaanneming": een overeenkomst tussen een contractant van het SGR en een andere contractant (de subcontractant) voor de levering van goederen, de uitvoering van werken of de verrichting van diensten waarvan de uitvoering de toegang tot of het genereren van EUCI vereist of behelst;

„Communicatie- en informatiesysteem" (CIS) — zie artikel 10, lid 2;

„Contractant": een natuurlijke persoon of een rechtspersoon die handelingsbekwaam is om overeenkomsten te sluiten;

„Encryptiemateriaal": encryptiealgoritmen, hard- en softwaremodules voor encryptie en encryptieproducten, inclusief nadere informatie betreffende de implementatie en bijbehorende documentatie en bedieningsmateriaal;

„Encryptieproduct": een product waarvan de functie er hoofdzakelijk en in de eerste plaats in bestaat aan de hand van één of meer encryptiemechanismen een beveiligingsdienst te verlenen (vertrouwelijkheid, integriteit, beschikbaarheid, echtheid, onweerlegbaarheid);

„EVDB-operatie": een militaire of civiele crisisbeheersingsoperatie uit hoofde van titel V, hoofdstuk 2 van het VEU;

„Derubricering": de opheffing van een rubricering;

„Verdediging in de diepte": de toepassing van een reeks beveiligingsmaatregelen in de vorm van meerdere verdedigingslagen;

„Aangewezen beveiligingsinstantie" (Designated Security Authority — DSA): een instantie onder het gezag van de nationale beveiligingsinstantie (NSA) van een lidstaat die tot taak heeft industriële of andere entiteiten te informeren over alle aspecten van het nationaal beleid inzake industriële beveiliging, en leiding te geven en bijstand te verlenen bij de uitvoering ervan. De NSA of een andere bevoegde instantie kan de rol van DSA op zich nemen;

„Document": opgeslagen informatie, ongeacht de fysieke vorm of de kenmerken daarvan;

„Rubricering verlagen": verlaging van het rubriceringsniveau;

„Gerubriceerde EU-informatie" (EUCI) — zie artikel 2, lid 1;

„Veiligheidsmachtiging voor een vestiging" (VMV): een administratieve beslissing van een NVI of AVI waaruit blijkt dat de vestiging vanuit beveiligingsoogpunt een afdoend niveau van bescherming biedt voor EUCI met een bepaalde rubriceringsgraad;

„Verwerking" van EUCI: alle mogelijke handelingen waaraan EUCI tijdens de gehele levenscyclus kan worden onderworpen. Hiertoe behoren het genereren, verwerken, vervoeren, rubricering verlagen, declassificeren en vernietigen van de informatie. Met betrekking tot CIS behoren hiertoe ook het verzamelen, tonen, overdragen en opslaan ervan;

„Houder": een naar behoren gemachtigde persoon van wie de noodzaak tot kennisname vaststaat en die EUCI in zijn bezit heeft en derhalve voor de bescherming daarvan verantwoordelijk is;

„Industriële of andere entiteit": een entiteit die betrokken is bij de levering van goederen, de uitvoering van werken of de verlening van diensten; het kan hierbij gaan om entiteiten die actief zijn op het gebied van industrie, handel, diensten, wetenschappen, onderzoek, onderwijs of ontwikkeling, of om een zelfstandige;

„Industriële beveiliging" — zie artikel 11, lid 1;

„Information assurance" — zie artikel 10, lid 1;

„Interconnectie" — zie bijlage IV, punt 32;

„Beheer van gerubriceerde informatie" — zie artikel 9, lid 1;

„Materiaal": een document, gegevensdrager of enigerlei onderdeel van machines of uitrustingen die zijn of worden vervaardigd;

„Bron": de instelling, het orgaan of de instantie of de lidstaat van de Europese Unie, een derde staat of een internationale organisatie onder het gezag waarvan gerubriceerde informatie is gegenereerd en/of ingevoerd in de structuren van de Europese Unie;

„Personeelsgerelateerde beveiliging" — zie artikel 7, lid 1;

„Persoonlijke veiligheidsmachtiging" (PVM): een verklaring van een bevoegde instantie van een lidstaat, die wordt afgelegd na de voltooiing van een veiligheidsonderzoek door de bevoegde instanties van die lidstaat, waarbij wordt bevestigd dat de betrokkene tot een bepaalde datum toegang mag hebben tot EUCI tot een bepaald niveau (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger);

„Certificaat van veiligheidsmachtiging voor personen" (CVMP): een door een bevoegde instantie afgegeven certificaat waarin wordt bevestigd dat de betrokkene gescreend is en in het bezit is van een geldige veiligheidsmachtiging voor personen of machtiging van het tot aanstelling bevoegde gezag voor toegang tot EUCI, en dat de rubriceringsgraad vermeldt van EUCI waartoe hij toegang mag hebben (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger), alsook de geldigheidsduur van de BMP en de datum waarop de geldigheid van het certificaat zelf afloopt;

„Fysieke beveiliging" — zie artikel 8, lid 1;

„Programma-/projectbeveiligingsinstructie" (PBI): een lijst van beveiligingsprocedures die op een specifiek programma/project worden toegepast om de beveiligingsprocedures te standaardiseren. Het kan gedurende de gehele looptijd van het programma/project worden herzien;

„Registratie" — zie bijlage III, punt 18;

„Overblijvend risico": het risico dat blijft bestaan nadat er beveiligingsmaatregelen zijn genomen, aangezien niet alle dreigingen worden tegengegaan en niet alle kwetsbaarheden kunnen worden weggenomen;

„Risico": de mogelijkheid dat een bepaalde dreiging de interne en externe kwetsbaarheden van een organisatie of een van de door haar gebruikte systemen zal uitbuiten en daarbij schade zal toebrengen aan de organisatie en haar materiële en immateriële kritische bestanddelen. Risico wordt gemeten als een combinatie van de waarschijnlijkheid dat dreigingen zich zullen voordoen en het effect daarvan;

— „Risicoaanvaarding": het besluit om erin te berusten dat er na de risicobehandeling een overblijvend risico blijft bestaan;

— „Risicobeoordeling": het in kaart brengen van dreigingen en kwetsbaarheden en het verrichten van de daarmee verband houdende risicoanalyse, d.w.z. de analyse van de waarschijnlijkheid en het effect;

— „Risicocommunicatie": houdt in dat er risicovoorlichtingscampagnes worden gevoerd, gericht op gebruikers van CIS, dat goedkeuringsinstanties over die risico's worden geïnformeerd en dat er verslag over wordt uitgebracht aan de exploitanten;

— „Risicobehandeling": het matigen, verwijderen, verkleinen (via een passende combinatie van technische, fysieke, organisatorische of procedurele maatregelen), overbrengen of onder toezicht houden van het risico;

„Memorandum over de beveiligingsaspecten" (MBA): een geheel van bijzondere, door de aanbestedende instantie uitgevaardigde contractvoorwaarden die een integrerend deel vormen van een gerubriceerde opdracht die de toegang tot of het genereren van EUCI behelst, en waarin de beveiligingseisen of de elementen van de opdracht die beveiligd moeten worden, worden genoemd;

„Gids voor rubricering" (GBR): een document waarin wordt bepaald welke elementen van een programma of opdracht gerubriceerd zijn en wat de toepasselijke rubriceringsgraden zijn. De GBR kan gedurende de looptijd van het programma of de opdracht worden uitgebreid en de informatie kan opnieuw of lager worden gerubriceerd; als er een GBR is, is het een onderdeel van het MBA;

„Veiligheidsonderzoek": de onderzoeksprocedures die de bevoegde instantie van een lidstaat overeenkomstig de nationale wet- en regelgeving uitvoert om zekerheid te krijgen dat er geen negatieve feiten bekend zijn waardoor de betrokkene niet in aanmerking zou komen voor een PVM of een machtiging voor toegang tot EUCI tot op een bepaald niveau (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger);

„Beveiligingsmodus": de vaststelling van de voorwaarden waaronder een CIS functioneert, op basis van de rubricering van de verwerkte informatie en de machtigingsgraden, de formele goedkeuringen inzake toegang en de noodzaak tot kennisname van de gebruikers ervan. Er zijn vier modi voor het verwerken en overdragen van gerubriceerde informatie: de gededicaceerde modus, de system-highmodus, de compartimenteringsmodus en de multilevelmodus;

— „Gededicaceerde modus": een modus operandi waarbij alle personen die toegang hebben tot het CIS een machtiging hebben voor de hoogste graad van rubricering van de in het CIS verwerkte informatie, en tevens een gedeelde „noodzaak tot kennisname" voor alle in het CIS verwerkte informatie;

— „System-highmodus": een modus operandi waarbij alle personen die toegang hebben tot het CIS een machtiging hebben voor de hoogste graad van rubricering van de in het CIS verwerkte informatie, maar niet alle personen met toegang tot het CIS een gedeelde noodzaak tot kennisname hebben voor de in het CIS verwerkte informatie; toegang tot informatie kan worden gegeven door één persoon;

— „Compartimenteringsmodus": een modus operandi waarbij alle personen die toegang hebben tot het CIS een machtiging hebben voor de hoogste graad van rubricering van de in het CIS verwerkte informatie, maar niet alle personen met toegang tot het CIS een formele machtiging hebben voor toegang tot alle in het CIS verwerkte informatie; een formele machtiging houdt in dat er een formeel centraal beheer is van toegangscontrole, anders dan de bevoegdheid van een individueel persoon om toegang te verlenen;

— „Multilevelmodus": een modus operandi waarbij niet alle personen die toegang hebben tot het CIS een machtiging hebben voor de hoogste graad van rubricering van de in het CIS verwerkte informatie, en niet alle personen met toegang tot het CIS een gedeelde noodzaak tot kennisname hebben voor de in het CIS verwerkte informatie;

„Proces inzake het beheer van beveiligingsrisico's": het volledige proces van het vaststellen, onder controle houden en tot een minimum beperken van onzekere gebeurtenissen die de beveiliging van een organisatie of de door haar gebruikte systemen kunnen treffen. Het bestrijkt alle risicogebonden activiteiten, met inbegrip van beoordeling, behandeling, aanvaarding en communicatie;

„TEMPEST": het onderzoeken en bestuderen van en het toezicht houden op compromitterende elektromagnetische emissies en de maatregelen om ze te bestrijden;

„Dreiging": een mogelijke oorzaak van een ongewenst incident dat kan leiden tot schade aan een organisatie of de door haar gebruikte systemen; zulke dreigingen kunnen onopzettelijk op opzettelijk (kwaadwillig) zijn, en worden gekenmerkt door bedreigende elementen, mogelijke doelwitten en aanvalsmethoden;

„Kwetsbaarheid": een zwakte van eender welke aard die door één of meer dreigingen kan worden uitgebuit. Kwetsbaarheid kan bestaan in nalatigheid of kan verband houden met onvoldoende strenge, onvolledige of onsamenhangende controles en kan van technische, procedurele, fysieke, organisatorische of operationele aard zijn.

Aanhangsel B

CONCORDANTIE VAN DE RUBRICERINGEN

EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
België	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	zie voetnoot (1)
Bulgarije	Строго секретно	Секретно	Поверително	За служебно ползване
Tsjechië	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Denemarken	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Duitsland	STRENG GEHEIM	GEHEIM	VS (2) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Estland	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ierland	Top Secret	Secret	Confidential	Restricted
Griekenland	Άκρως Απόρρητο Afgekort: (ΑΑΠ)	Απόρρητο Afgekort: (ΑΠ)	Εμπιστευτικό Afgekort: (ΕΜ)	Περιορισμένης Χρήσης Afgekort: (ΠΧ)
Spanje	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Frankrijk	Très Secret Défense	Secret Défense	Confidentiel Défense	zie voetnoot (3)
Kroatië	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italië	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο Afgekort: (ΑΑΠ)	Απόρρητο Afgekort: (ΑΠ)	Εμπιστευτικό Afgekort: (ΕΜ)	Περιορισμένης Χρήσης Afgekort: (ΠΧ)
Letland	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litouwen	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hongarije	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ogħla Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted (4)
Nederland	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Oostenrijk	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polen	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Roemenië	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenië	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Slowakije	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Zweden ([5])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Verenigd Koninkrijk	UK TOP SECRET	UK SECRET	UK CONFIDENTIAL	UK RESTRICTED

([1]) Diffusion Restreinte/Beperkte Verspreiding is in België geen classificatiegraad. België behandelt en beschermt alle gegevens met rubricering „RESTREINT UE/EU RESTRICTED" op een niet minder stringente wijze dan door de normen en procedures in beveiligingsvoorschriften van de Raad van de Europese Unie wordt voorgeschreven.
([2]) Duitsland: VS = Verschlusssache (gerubriceerde gegevens).
([3]) Frankrijk maakt in zijn nationale systeem geen gebruik van de rubricering „RESTREINT". Frankrijk behandelt en beschermt alle gegevens met rubricering „RESTREINT UE/EU RESTRICTED" op een niet minder stringente wijze dan door de normen en procedures in de beveiligingsvoorschriften van de Raad van de Europese Unie wordt voorgeschreven.
([4]) Voor Malta kunnen de Maltese en de Engelse vermeldingen door elkaar worden gebruikt.
([5]) Zweden: de rubriceringen op de bovenste rij worden gebruikt door de defensieautoriteiten en die op de onderste rij door andere instanties.

Aanhangsel C

LIJST VAN NATIONALE BEVEILIGINGSINSTANTIES (NSA's)

BELGIË Nationale Veiligheidsoverheidsdienst FOD Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking Karmelietenstraat 15 1000 Brussel Tel. secretariaat: +32 25014542 Fax +32 25014596 E-mail: nvo-ans@diplobel.fed.be	**ESTLAND** National Security Authority (Nationale beveiligingsautoriteit) Ministerie van Defensie Sakala 1 EE-15094 Tallinn Tel. +372 717 0019, +372 7170117 Fax +372 7170213 E-mail: nsa@mod.gov.ee
BULGARIJE State Commission on Information Security 90 Cherkovna Str. 1505 Sofia Tel. +359 29333600 Fax +359 29873750 E-mail: dksi@government.bg Website: www.dksi.bg	**IERLAND** National Security Authority (Nationale veiligheidsautoriteit) Departement Buitenlandse Zaken 76 - 78 Harcourt Street Dublin 2 Tel. +353 14780822 Fax +353 14082959
TSJECHIË Národní bezpečnostní úřad (Nationale beveiligingsdienst) Na Popelce 2/16 150 06 Praag 56 Tel. +420 257283335 Fax +420 257283110 E-mail: czech.nsa@nbu.cz Website: www.nbu.cz	**GRIEKENLAND** Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ) Διεύθυνση Ασφαλείας και Αντιπληροφοριών ΣΤΓ 1020 -Χολαργός (Αθήνα) Τηλ.: +30 2106572045 (ώρες γραφείου) +30 2106572009 (ώρες γραφείου) Φαξ: +30 2106536279 +30 2106577612 Hellenic National Defence General Staff (HNDGS) Counter Intelligence and Security Directorate (NSA) 227-231 Holargos STG 1020 Athene Tel. +30 2106572045 +30 2106572009 Fax +30 2106536279 +30 2106577612
DENEMARKEN Politiets Efterretningstjeneste (Deense veiligheidsinlichtingendienst) Klausdalsbrovej 1 2860 Søborg Tel. +45 33148888 Fax +45 33430190 Forsvarets Efterretningstjeneste (Deense defensie-inlichtingendienst) Kastellet 30 2100 Kopenhagen Ø Tel. +45 33325566 Fax +45 33931320	**SPANJE** Autoridad Nacional de Seguridad Oficina Nacional de Seguridad Avenida Padre Huidobro s/n 28023 Madrid Tel. +34 913725000 Fax +34 913725808 E-mail: nsa-sp@areatec.com
DUITSLAND Bundesministerium des Innern Referat ATS III 3 Alt-Moabit 101 D 11014 Berlijn Tel. +49 30186810 Fax +49 30186811441 E-mail: oesIII3@bmi.bund.de	**FRANKRIJK** Secrétariat général de la défense et de la sécurité nationale Sous-direction Protection du secret (SGDSN/PSD) 51 Boulevard de la Tour-Maubourg 75700 Parijs 07 SP Tel. +33 171758177 Fax +33 171758200

KROATIË
Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb

Tel. +385 14681222
Fax +385 14686049
Website: www.uvns.hr

ITALIË
Presidenza del Consiglio dei Ministri
D.I.S. - U.C.Se.
Via di Santa Susanna, 15
00187 Rome

Tel. +39 0661174266
Fax +39 064885273

CYPRUS
ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία

Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministerie van Defensie
Minister's Military Staff
„Nationale veiligheidsinstantie (NVI)"
4 Emanuel Roidi street
1432 Nicosia

Tel. +357 22807569, +357 22807643, +357 22807764
Fax +357 22302351
E-mail: cynsa@mod.gov.cy

LETLAND
National Security Authority (Nationale veiligheidsautoriteit)
Constitution Protection Bureau of the Republic of Latvia
P.O. Box 286
Riga, LV-1001

Tel. +371 67025418
Fax +371 67025454
E-mail: ndi@sab.gov.lv

LITOUWEN
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania
(Nationale beveiligingsdienst)
Gedimino 40/1
LT-01110 Vilnius

Tel. +370 706 66701, +370 706 66702
Fax +370 706 66700
E-mail: nsa@vsd.lt

LUXEMBURG
Autorité nationale de Sécurité
(Nationale veiligheidsoverheidsdienst)
Boîte postale 2379
1023 Luxemburg

Tel. +352 24782210 centrale
+352 24782253 direct
Fax +352 24782243

HONGARIJE
Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
1024 Boedapest, Szilágyi Erzsébet fasor 11/B

Tel. +36 17952303
Fax +36 17950344
Postadres
1357 Boedapest, PO Box 2
E-mail: nbf@nbf.hu
Website: www.nbf.hu

MALTA
Ministry for Home Affairs and National Security
Postbus 146
Valletta

Tel. +356 21249844
Fax +356 25695321

NEDERLAND
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag

Tel. +31 703204400
Fax +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag

Tel. +31 703187060
Fax +31 703187522

OOSTENRIJK
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A1014 Wenen

Tel. +43 1531152594
Fax +43 1531152615
E-mail: ISK@bka.gv.at

POLEN Agencja Bezpieczeństwa Wewnętrznego — ABW (Bureau interne veiligheid) 2A Rakowiecka St. 00-993 Warschau Tel. +48 225857360 Fax +48 225858509 E-mail: nsa@abw.gov.pl Website: www.abw.gov.pl	**SLOWAKIJE** Národný bezpečnostný úrad (Nationale beveiligingsdienst) Budatínska 30 Postbus 16 850 07 Bratislava Tel. +421 268692314 Fax +421 263824005 Website: www.nbusr.sk
PORTUGAL Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300-342 Lissabon Tel. +351 213031710 Fax +351 213031711	**FINLAND** National Security Authority (Nationale veiligheidsautoriteit) Ministerie van Buitenlandse Zaken Postbus 453 FI-00023 Government Tel. +358 16055890 Fax +358 916055140 E-mail: NSA@formin.fi
ROEMENIË Oficiul Registrului Național al Informațiilor Secrete de Stat (Romanian NSA — ORNISS National Registry Office for Classified Information) Str. Mureș nr. 4, sector 1 012275 Boekarest Tel. +40 212245830 Fax +40 212240714 E-mail: nsa.romania@nsa.ro Website: www.orniss.ro	**ZWEDEN** Utrikesdepartementet (Ministerie van Buitenlandse Zaken) UD-RS SE-103 39 Stockholm Tel. +46 84051000 Fax +46 87231176 E-mail: ud-nsa@foreign.ministry.se
SLOVENIË Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 SI-1000 Ljubljana Tel. +386 14781390 Fax +386 14781399 E-mail: gp.uvtp@gov.si	**VERENIGD KONINKRIJK** UK National Security Authority Room 335, 3rd Floor 70 Whitehall Londen SW1A 2AS Tel. 1: +44 2072765645 Tel. 2: +44 2072765497 Fax +44 2072765651 E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk

Aanhangsel D

LIJST VAN AFKORTINGEN

Acroniem	Betekenis
AQUA	Appropriately Qualified Authority (naar behoren gekwalificeerde instantie)
BPS	Boundary Protection Services (voorzieningen om de grenzen te beschermen)
CAA	Crypto Approval Authority (overheid voor de goedkeuring van encryptieproducten)
CCTV	Closed Circuit Television (gesloten tv-circuit)
CDA	Crypto Distribution Authority (overheid voor de verdeling van encryptieproducten)
GBVB	Gemeenschappelijk buitenlands en veiligheidsbeleid
CIS	Communication and Information Systems handling EUCI (communicatie- en informatiesystemen die EUCI verwerken)
Coreper	Comité van permanente vertegenwoordigers
GBVB	Gemeenschappelijk buitenlands en veiligheidsbeleid
DSA	Designated Security Authority (aangewezen beveiligingsinstantie)
ECSD	European Commission Security Directorate (directoraat Veiligheid van de Europese Commissie)
EUCI	EU Classified Information (gerubriceerde EU-informatie)
SVEU	Speciale vertegenwoordiger van de EU
FSC	Facility Security Clearance (veiligheidsmachtiging voor een vestiging)
SGR	Secretariaat-generaal van de Raad
IA	Information Assurance (informatieborging)
IAA	Information Assurance Authority (IA-overheid)
IDS	Intrusion Detection System (indringerdetectiesysteem)
IT	Informatietechnologie
NSA	National Security Authority (nationale beveiligingsinstantie)
PVM	Persoonlijke veiligheidsmachtiging
CVMP	Certificaat van veiligheidsmachtiging voor personen
PSI	Programme/Project Security Instructions (programma-/projectbeveiligingsinstructies)
SAA	Security Accreditation Authority (homologatieoverheid)
VAO	Beveiligingshomologatieorgaan
MBA	Memorandum over de beveiligingsaspecten
OB's	Operationele beveiligingsprocedures
GBR	Gids voor rubricering
SSB	Systeemgebonden specificatie van beveiligingseisen
TA	TEMPEST Authority (TEMPEST-overheid)