Sveriges internationella överenskommelser

ISSN 1102-3716

Utgiven av Utrikesdepartementet

SÖ 2007: 66

Nr 66
Generellt säkerhetsskyddsavtal med Storbritannien och Nordirland om skydd av information utväxlad mellan de båda länderna om förvarssamarbete, forskning, produktion och anskaffning
London den 13 september 2002

Regeringen beslutade den 29 augusti 2002 att underteckna avtalet. Avtalet trädde i kraft vid undertecknandet, den 13 september 2002.

Översättning

Generellt säkerhetsskyddsavtal mellan Konungariket Sveriges regering, företrädd av dess försvarsminister, och Förenade Konungariket Storbritannien och Nordirlands regering, företrädd av statssekreteraren för försvaret, om skydd av information utväxlad mellan de båda länderna om försvarssamarbete, forskning, produktion och anskaffning

Innehållsförteckning

Inledning

Konungariket Sveriges regering, företrädd av dess försvarsminister, och Förenade Konungariket Storbritannien och Nordirlands regering, företrädd av statssekreteraren för försvaret, även kallade *parterna* för de syften som avses i detta avtal, har i den nationella säkerhetens intresse kommit överens om följande bestämmelser som anges i detta generella säkerhetsskyddsavtal (GSA), som önskar trygga skyddet av hemlig information som överförs för försvarssamarbete, forskning, produktion och anskaffning mellan de båda länderna eller till kommersiella och industriella företag i ettdera av de båda länderna genom godkända kanaler. Detta GSA ska också genomföra de säkerhetsskyddsbestämmelser som ingår i ramavtalet mellan Republiken Frankrike, Republiken Italien, Konungariket Spanien, Förenade Konungariket Storbritannien och Nordirland, Konungariket Sverige och Förbundsrepubliken Tyskland om åtgärder för att underlätta omstrukturering och drift av den europeiska försvarsindustrin, som undertecknades i Farnborough den 27 juli 2000, nedan kallat *ramavtalet*.

Detta GSA täcker inte utväxling av nukleär, biologisk och kemisk information (NBC) hänförlig till utrustning som vanligen benämns *massförstörelsevapen* (WMD).

Detta GSA ersätter avtalet mellan Sveriges försvarsminister och statssekreteraren för försvaret i Storbritannien om skydd av sekretessbelagd information som utbyts för försvarsändamål, forskning, produktion och anskaffning mellan de båda länderna, daterat den 16 juni 1998.

1. Allmän bestämmelse

Parternas åtaganden i detta GSA ska tolkas i enlighet med deras respektive nationella lagar och bestämmelser.

2. Informationssäkerhetsklasser

Informationssäkerhetsklasserna och deras motsvarigheter i de båda länderna är följande:

Storbritannien	Sverige
UK SECRET	HEMLIG/SECRET
UK CONFIDENTIAL	HEMLIG/CONFIDENTIAL
UK RESTRICTED	HEMLIG/RESTRICTED

De svenska tilläggen SECRET, CONFIDENTIAL och RESTRICTED ska tolkas som den säkerhetsskyddshantering som ska ges den utväxlade hemliga informationen. Om den svenska beteckningen är HEMLIG utan angivande av extra säkerhetsskyddshantering, måste den hemliga informationen ges en säkerhetsskyddshantering på nivån UK SECRET.

Som allmän regel gäller att de ovannämnda nivåerna ska betraktas som likvärdiga. Exempelvis ska ett dokument betecknat UK CONFIDENTIAL som överförs till Sverige förmedlas, behandlas, lagras och placeras på ett sätt som ger samma skydd som för ett svenskt dokument betecknat HEMLIG/CONFIDENTIAL.

3. Definitioner

Följande termer definieras för tydlighets skull:

hemlig information: uppgifter (dvs. kunskap som kan överföras i någon form) eller material som fordrar skydd mot otillåtet röjande, som har åsatts informationssäkerhetsklass.

säkerhetsskyddsavtal: ett avtal som innehåller eller omfattar hemlig information.

mottagare: kontraktstagare, anläggning eller annan enhet som mottar materialet från överlåtaren för vidare sammansättning, användning, vidareförädling eller annat ändamål. Termen omfattar inte transportörer eller agenter.

överlåtare: person eller enhet som är ansvarig för att tillhandahålla mottagaren material.

kontrakt: en överenskommelse som rättsligt binder två eller flera parter och som skapar och definierar verkställbara rättigheter och skyldigheter mellan parterna.

leverantör: en fysisk eller juridisk person som är behörig att ingå avtal med rättsligt bindande verkan.

dokument: dokumenterad information oberoende av fysisk form eller beskaffenhet, exempelvis skrivet och tryckt material (däribland skrivelser, ritningar och planer), medier för elektronisk lagring (bland annat hårddiskar,

disketter, chip, magnetband, cd-skivor), fotografier och videoinspelningar samt optisk eller elektronisk återgivning av sådana.

anläggning: installation, verk, fabrik, laboratorium, kontor, universitet eller annan utbildningsanstalt eller företag (med tillhörande lagerlokaler, lageromräden, nyttigheter och beståndsdelar som ingår i dessa på grund av sin funktion eller lokalisering) samt offentlig myndighet eller enhet.

material: föremål eller ämnen från vilka information kan hämtas. Termen omfattar dokument, utrustning, vapen eller komponenter.

nationell säkerhetsskyddsmyndighet/verkställande säkerhetsskyddsmyndighet (NSA/DSA): officiell myndighet eller enhet som av en part har utsetts att ansvara för samordning samt genomförande av nationellt säkerhetsskydd.

upprättande part: den part som genererar den hemliga informationen på uppdrag av NSA/DSA.

mottagande part: den part till vilken hemlig information överförs på uppdrag av NSA/DSA.

säkerhetsskyddsansvarig: den person som utsetts av en NSA/DSA att tillse att säkerhetsskyddsföreskrifterna tillämpas i en offentlig anläggning eller i en leverantörs lokaler.

4. Behöriga säkerhetsmyndigheter

Ansvariga myndigheter för försvarsrelaterat säkerhetsskydd är:

För Storbritannien
Director of Defence Security (D Def Sy)
Ministry of Defence
(Direktören för försvarets säkerhetsskydd, Försvarsministeriet)
St Giles Court
1-13 St Giles High Street
London, WC2H 8LD

För Sverige
NSA i Sverige med det högsta ansvaret för försvarsrelaterat säkerhetsskydd:
Försvarsmakten
Högkvarteret
Militära underrättelse- och säkerhetstjänsten (MUST)
SE-107 85 STOCKHOLM
Sverige
DSA i Sverige ansvarig för försvarsrelaterad industriell säkerhet är:
Försvarets materielverk
Säkerhetsskydd
SE-115 88 STOCKHOLM
Sverige

5. Begränsningar i fråga om användning och delgivning

5.1 Part får inte utan föregående skriftligt tillstånd av upprättande part tillkännage, delge eller tillåta tillkännagivande eller delgivning av hemlig information, som är relaterad till ett program, till en annan regering eller in-

ternationell organisation eller någon enhet som inte deltar i programmet.

5.2 Mottagande part får inte utan föregående samråd offentligen delge, använda eller tillåta användning av hemlig information, utom för de ändamål och med de begränsningar som angivits av upprättande part eller på dennas vägnar.

5.3 Ingenting i detta GSA ska tolkas som ett bemyndigande att tillkännage, använda, utväxla eller delge information som omfattas av upphovsrätt förrän särskilt skriftligt tillstånd har erhållits av rättsinnehavaren, oberoende av om denne är en av parterna eller tredje part.

6. Skydd av hemlig information

6.1 Upprättande part ska tillse att mottagande part informeras om

a) informationens informationssäkerhetsklass och andra villkor för dess tillkännagivande eller begränsningar i fråga om användning och att informationen är märkt på detta sätt, samt

b) eventuella senare ändringar av informationssäkerhetsklass.

6.2. Mottagande part ska

a) i enlighet med sina nationella lagar och bestämmelser, ge information som mottagits från den andra parten samma säkerhetsskydd som ges hemlig information på samma nivå hos upprättande part,

b) tillse att hemlig information åsätts dess egen informationssäkerhetsklass i enlighet med avsnitt 2 ovan, samt

c) tillse att informationssäkerhetsklasserna inte ändras utan skriftligt tillstånd av upprättande part eller på dennas vägnar.

6.3 För att uppnå och bibehålla likvärdigt säkerhetsskydd ska parternas NSA/DSA efter anmodan lämna varandra upplysningar om sina bestämmelser och rutiner och sina riktlinjer avseende skydd av hemlig information och ska i detta syfte underlätta besök från varandras behöriga säkerhetsmyndigheter.

7. Behörighet till hemlig information

7.1 Rätt att ta del av hemlig information ska vara förbehållen personer som har behov av den i tjänsten och som har genomgått säkerhetsprövning av NSA/DSA hos mottagande part eller av NSA/DSA i en part i ramavtalet i enlighet med dennas nationella bestämmelser för den nivå som motsvarar informationssäkerhetsklassen hos den information som ska delges.

7.2 I enlighet med artikel 23 i ramavtalet gäller följande.

7.2.1 Tillstånd att ta del av hemlig information betecknad UK CONFIDENTIAL / HEMLIG/CONFIDENTIAL och UK SECRET / HEMLIG/SECRET vad gäller en person som är medborgare endast i en part i ramavtalet får ges utan upprättande parts förhandstillstånd.

7.2.2 Tillstånd att ta del av hemlig information betecknad UK CONFIDENTIAL / HEMLIG/CONFIDENTIAL och UK SECRET / HEMLIG/SECRET vad gäller en person som är medborgare i en av parterna och i en annan medlemsstat i EU ska beviljas utan upprättande parts förhandstillstånd. Vid behörighet att ta del av hemlig information som inte följer av denna punkt ska det samrådsförfarande tillämpas som anges i 7.2.3 nedan.

7.2.3 Rätt att ta del av information betecknad UK CONFIDENTIAL /

HEMLIG/CONFIDENTIAL och UK SECRET / HEMLIG/SECRET vad gäller en person som inte har medborgarskap som anges i 7.2.1 och 7.2.2 ovan ska göras till föremål för föregående samråd med upprättande part. Det samrådsförfarande som gäller sådana personer ska ske på det sätt som anges under a - d nedan.

a) Samrådsförfarandet ska inledas innan ett projekt eller ett program har satts igång eller, om det är lämpligare, under arbetets gång.

b) Informationen ska begränsas till de berörda personernas nationalitet.

d) En part som mottar en sådan begäran ska pröva om delgivning av dess hemliga information till icke-godkända medborgare kan godtas.

e) Sådant samråd ska beredas skyndsamt med målet att uppnå konsensus. Om detta inte är möjligt, ska upprättande parts beslut godtas.

8. Överföring av sekretessbelagd information

8.1 Hemlig information med den brittiska beteckningen UK CONFIDENTIAL/UK SECRET och den svenska beteckningen HEMLIG/CONFIDENTIAL/HEMLIG/SECRET ska överföras mellan de båda länderna i enlighet med upprättande parts säkerhetsskyddsbestämmelser. Den normala vägen ska vara via de diplomatiska kanalerna mellan de båda parterna, men andra överföringssätt får användas, såsom genom personligt överlämnande eller via säkra kommunikationsmedel (kryptering), om de är godtagbara för båda parterna.

8.2 I enlighet med artikel 25 i ramavtalet och dess bilaga får i brådskande fall, dvs. endast när diplomatisk kurirpost inte uppfyller dessa krav, hemlig information betecknad UK CONFIDENTIAL / HEMLIG/CONFIDENTIAL överföras med anlitande av privata kurirföretag, under förutsättning att följande krav är uppfyllda:

a) Kurirföretaget är lokaliserat inom parternas territorium och har ett säkerhetsskyddsprogram för transport av värdeförsändelser, med kvittenssystem inkluderande fortlöpande kontroll av att försändelsen är omhändertagen antingen med användning av kvittenser och leveranslistor eller elektroniskt spårnings- och uppföljningssystem.

b) Kurirföretaget ska tillhandahålla och ge avsändaren ett mottagningsbevis på leveranslista eller tillhandahålla kvittens som överensstämmer med numret på försändelsen.

c) Kurirföretaget garanterar att försändelsen lämnas till mottagaren före ett bestämt klockslag och datum inom en 24-timmarsperiod.

d) Kurirföretaget har rätt att anlita ett ombud eller en underleverantör. Ansvaret för att uppfylla de ovannämnda kraven måste dock kvarstå hos kurirföretaget.

8.3 Hemlig information betecknad UK RESTRICTED / HEMLIG/RESTRICTED ska överföras mellan parterna i enlighet med upprättande parts nationella bestämmelser, vilket kan innefatta anlitande av privata kurirföretag.

8.4 I enlighet med artikel 25 i ramavtalet och dess bilaga får hemlig information betecknad UK CONFIDENTIAL / HEMLIG/CONFIDENTIAL och UK SECRET / HEMLIG/SECRET inte överföras elektroniskt i klartext. Endast signalskyddssystem som godkänts av parternas NSA/DSA får användas för kryptering av hemlig information betecknad UK CONFIDENTIAL / HEMLIG/CONFIDENTIAL och UK SECRET / HEMLIG/SECRET obero-

ende av överföringssätt. Hemlig information betecknad UK RESTRICTED / HEMLIG/RESTRICTED får överföras eller nås på elektronisk väg (exempelvis genom punkt-till-punkt-förbindelser) via ett allmänt nätverk såsom Internet, med användning av officiella eller kommersiella kryptoutrustningar som ömsesidigt godkänts av de behöriga nationella myndigheterna. Emellertid får telefonsamtal, videokonferenser eller faxöverföringar som innehåller hemlig information betecknad UK RESTRICTED / HEMLIG/RESTRICTED ske i klartext, om ett godkänt signalskyddssystem inte är tillgängligt.

8.5 När stora mängder av hemlig information ska överföras, ska transportsättet, vägen och eskorten (i förekommande fall) gemensamt bestämmas i varje särskilt fall av parternas behöriga myndigheter.

9. Besök

9.1 Parterna ska bevilja civila och militära företrädare från den andra parten eller dennes leverantörers anställda tillstånd till besök, som innefattar tillgång till hemlig information, i sina statliga anläggningar, organ och laboratorier och i industrianläggningar som tillhör leverantörer, om besökarna är placerade i säkerhetsklass och har behov av att ta del av informationen i tjänsten.

9.2 Besökare är skyldiga att följa värdpartens säkerhetsskyddsbestämmelser. Hemlig information som lämnats ut till eller gjorts tillgänglig för en besökare ska betraktas såsom delgiven till den part som är ansvarig för besökaren och ska skyddas i enlighet därmed.

9.3 I enlighet med artikel 26 i ramavtalet och dess bilaga om besök som berör hemlig information i offentliga anläggningar tillhörande den andra parten eller i en leverantörs anläggningar där tillgång till hemlig information betecknad UK CONFIDENTIAL / HEMLIG/CONFIDENTIAL och UK SECRET / HEMLIG/SECRET krävs, ska följande förfarande tillämpas.

1) Enligt följande bestämmelser ska sådana besök avtalas direkt mellan den sändande anläggningen och den mottagande anläggningen.

2) För dessa besök ska följande krav också vara uppfyllda:

a) Besöket görs i ett officiellt syfte.

b) Leverantörsägda anläggningar som ska besökas måste vara godkända ur säkerhetssynpunkt.

c) Före ankomsten måste bekräftelse på besökarens säkerhetsprövning lämnas direkt till den mottagande anläggningen av den säkerhetsansvarige vid den sändande anläggningen i överenskommen form. För att styrka sin identitet måste besökaren ha ID-kort eller pass, som uppvisas för de säkerhetsansvariga i den mottagande anläggningen.

9.4 De säkerhetsskyddsansvariga vid den sändande anläggningen

a) är skyldiga att försäkra sig hos sina NSA/DSA om att den anläggning som ska besökas är godkänd ur säkerhetssynpunkt, och

b) är, tillsammans med de säkerhetsskyddsansvariga i den mottagande anläggningen, skyldiga att komma överens om att besöket är nödvändigt.

9.5 Den säkerhetsskyddsansvarige i en anläggning som ska besökas eller, i förekommande fall, en statlig anläggning, ska tillse att alla besökare antecknas med namn, den organisation de företräder, dagen för utgången av säkerhetsprövningens giltighetstid, dagen eller dagarna för besöket samt uppgift om vilka personer som har besökts. Dokumentationen ska bevaras i minst fem år.

9.6 NSA/DSA i den mottagande parten har rätt att begära förhandsmeddelande från sina anläggningar när det gäller besök om besöket varar längre än 21 dagar. Det tillkommer vederbörande NSA/DSA att ge tillstånd, men de ska, om säkerhetsproblem uppstår, rådgöra med NSA/DSA från besökarens land.

9.7 Besök som berör hemlig information betecknad UK RESTRICTED / HEMLIG/RESTRICTED ska också avtalas direkt mellan den sändande och den mottagande anläggningen.

10. Kontrakt

10.1 När upprättande part avser att göra en beställning, eller bemyndigar en leverantör i sitt land att göra en beställning, som innefattar hemlig information betecknad UK CONFIDENTIAL / HEMLIG/CONFIDENTIAL eller högre, hos en leverantör i det andra landet, ska den i förväg begära en försäkran från NSA/DSA i det andra landet, som utvisar att den avsedda leverantören är godkänd ur säkerhetssynpunkt upp till den erforderliga nivån och även har tillräckliga säkerhetsanordningar för att ge hemlig information erforderligt skydd. I försäkran ska det ingå att den säkerhetsgodkända leverantörens säkerhetsuppträdande ska överensstämma med nationella säkerhetsskyddsbestämmelser och övervakas av dennes NSA/DSA.

10.2 Vederbörande NSA/DSA är skyldig att tillse att leverantörer som får beställningar till följd av dessa förfrågningar före kontraktets ingående är medvetna om följande bestämmelser och skyldigheter:

10.2.1 Definitionen av termen hemlig information och likvärdiga nivåer för informationssäkerhetsklasser hos de båda parterna enligt denna uppgörelse.

10.2.2 Namnen på de båda ländernas myndigheter som är behöriga att ge tillstånd till utlämnande av, och samordning av skyddet av, hemlig information som berör ett kontrakt.

10.2.3 Kanaler som får användas för överföring av hemlig information mellan de berörda myndigheterna och/eller leverantörerna.

10.2.4 Förfaranden och mekanismer för att meddela eventuella förändringar gällande hemlig information, antingen när det gäller informationssäkerhetsklass eller att skydd inte längre behövs.

10.2.5 Formaliteter för beviljande av besökstillstånd, tillträde eller inspektion för personer från det ena landet i företag i det andra landet som omfattas av ett kontrakt.

10.2.6 Att leverantören förbinder sig att inte lämna ut hemlig information till andra personer än sådana som är placerade i säkerhetsklass med avseende på rätt att ta del av informationen, som har behov av den i tjänsten och som är anställda eller anlitade för att genomföra ett kontrakt.

10.2.7 Att leverantören förbinder sig att inte lämna ut hemlig information eller tillåta att sådan information delges till personer som inte är säkerhetsprövade för att ta del av den.

10.2.8 Att leverantören är skyldig att omedelbart meddela sin NSA/DSA om inträffad eller misstänkt förlust eller röjande av hemlig information som hör till ett kontrakt.

10.3 Den behöriga säkerhetsskyddsmyndigheten i upprättande part ska överlämna två kopior av de relevanta delarna av ett säkerhetsskyddsavtal till mottagande parts behöriga säkerhetsskyddsmyndighet för att möjliggöra

erforderlig säkerhetsskyddsövervakning.

10.4 Varje kontrakt ska innehålla anvisningar om säkerhetsskyddsbestämmelserna och informationssäkerhetsklasserna för varje aspekt eller del av ett kontrakt. För Sveriges del ska dessa anvisningar anges i särskilda relevanta säkerhetsskyddsdokument. För Storbritanniens del ska dessa anvisningar täckas av särskilda säkerhetsskyddsklausuler och i en skrivelse om säkerhetsskyddsaspekter (SAL). I anvisningarna måste identifieras varje hemlig aspekt av ett kontrakt, eller varje hemlig aspekt som kommer att genereras av kontraktet, och åsättas en särskild informationssäkerhetsklass. Ändringar i krav, aspekter eller delar ska meddelas om och när så är nödvändigt och upprättande part ska meddela mottagande part när information inte längre är placerad i informationssäkerhetsklass.

11. Ömsesidiga säkerhetsskyddsarrangemang för industrin

11.1 Vardera NSA/DSA ska på begäran av den andra parten lämna upplysningar om säkerhetsläget för ett företags lokaler i sitt land. Vardera NSA/DSA ska också på begäran lämna upplysningar om säkerhetsprövning för sina medborgare. Dessa upplysningar benämns *säkerhetsklarering för anläggningar* respektive *intyg om säkerhetsprövning*.

11.2 NSA/DSA ska på begäran fastställa status för säkerhetsklarering för ett företag eller en säkerhetsprövning för en person och översända intyg om detta, om företaget eller personen redan är klarerad respektive säkerhetsprövad. Om företaget eller personen saknar intyg om säkerhetsklarering eller säkerhetsprövning eller om klareringen eller säkerhetsprövningen gäller en lägre informationssäkerhetsklass än den som har begärts, ska upplysningar sändas med innebörd att intyg om säkerhetsklarering respektive säkerhetsprövning inte omedelbart kan utfärdas, men att åtgärder håller på att vidtas för att behandla framställningen. Om prövningen ger godkänt resultat, ska intyg om säkerhetsklarering respektive säkerhetsprövning utfärdas.

11.3 För ett företag som av NSA/DSA i det land där det är registrerat bedöms stå under ägande, kontroll eller inflytande av tredje land, vars syften inte är förenliga med den berörda regeringens syften, får säkerhetsklarering inte utfärdas, och begärande NSA/DSA ska underrättas.

11.4 Om endera NSA/DSA får kännedom om ofördelaktiga uppgifter om en person för vilken ett intyg om säkerhetsprövning har utfärdats, ska den meddela den andra NSA/DSA uppgifternas karaktär och de åtgärder den avser att vidta eller har vidtagit. Endera NSA/DSA får begära omprövning av ett intyg om säkerhetsprövning som tidigare har lämnats av den andra NSA/DSA, under förutsättning att framställningen motiveras. Den begärande NSA/DSA ska underrättas om resultatet av omprövningen och om därav föranledda åtgärder.

11.5 Om uppgifter framkommer som väcker tvivel om ett godkänt företags lämplighet att fortsätta att få tillgång till hemlig information i det andra landet, ska närmare detaljer om dessa uppgifter ofördröjligen framföras till den berörda NSA/DSA för att möjliggöra en utredning.

11.6 Om endera NSA/DSA upphäver eller vidtar åtgärder för att dra in ett intyg om säkerhetsprövning eller upphäver eller vidtar åtgärder för att dra in ett tillstånd att ta del av hemlig information som har beviljats en medborgare i det andra landet med stöd av en säkerhetsprövning, ska den andra parten

underrättas och delges motiven för dessa åtgärder.

11.7 Vardera NSA/DSA får med en motiverad framställning begära att den andra NSA/DSA omprövar ett intyg om säkerhetsklarering för anläggningar. Den begärande NSA/DSA ska efter omprövningen underrättas om resultatet av denna och delges de omständigheter som styrker ett eventuellt beslut.

11.8 Vardera NSA/DSA ska på begäran av den andra parten samarbeta vid omprövningar och utredningar avseende säkerhetsprövning och säkerhetsklarering av anläggningar.

12. Förlust eller röjande

12.1 I händelse av säkerhetsöverträdelse som innebär förlust av hemligt material, eller misstanke om att hemlig information har röjts, ska mottagande parts NSA/DSA omedelbart underrätta upprättande parts NSA/DSA.

12.2 Mottagande part ska omedelbart genomföra en utredning (med biträde av upprättande part om så begärs) i enlighet med sina gällande bestämmelser om säkerhetsskydd. Mottagande part ska så snart det är möjligt underrätta upprättande part om omständigheterna, om vilka åtgärder som vidtagits samt om resultatet av utredningen.

13. Kostnader

Alla kostnader som uppkommit vid tillämpning av bestämmelserna i detta GSA ska betalas av respektive part.

14. Ändringar

Bestämmelserna i detta GSA får ändras med parternas ömsesidiga skriftliga tillstånd.

15. Tvister

Tvister om tolkningen eller tillämpningen av detta GSA ska lösas genom samråd mellan parterna eller med någon annan ömsesidigt godtagbar metod.

16. Ikraftträdande

Detta GSA träder i kraft dagen för den sista underskriften.

17. Uppsägning och översyn

17.1 Detta GSA ska förbli i kraft tills det skriftligen sägs upp av någon av parterna med sex månaders varsel. Parterna ska förbli ansvariga efter uppsägningen för skyddet av all hemlig information som utbytts med stöd av bestämmelserna i detta GSA.

17.2 Likaledes ska hemlig information som utbytts med stöd av detta GSA skyddas, även om överföringen har skett efter det att någon av parterna har sagt upp detta GSA.

17.3 I fall av uppsägning ska utestående frågor söka lösas genom samråd mellan de båda parterna.

17.4 Detta GSA ska ses över av parterna gemensamt inom tio år efter dess ikraftträdande.

Föregående text utgör den överenskommelse som har träffats mellan Konungariket Sveriges försvarsminister och Förenade konungariket Storbritannien och Nordirlands statssekreterare för försvaret om de frågor som avses i överenskommelsen.

Detta GSA har undertecknats i två original på engelska språket.

För Konungariket Sveriges försvarsminister
Expeditionschef i Försvarsdepartementet
Ingvar Åkesson

För Förenade konungariket Storbritannien och Nordirlands statssekretare för försvaret
Generaldirektör för säkerhet och sekretesskydd i försvarsministeriet
Gloria Craig

London den 13 september 2002

GENERAL SECURITY ARRANGEMENT

between

THE GOVERNMENT OF THE UNITED KINGDOM

OF GREAT BRITAIN AND NORTHERN IRELAND

REPRESENTED BY THE

THE SECRETARY OF STATE FOR DEFENCE

and

THE GOVERNMENT OF SWEDEN

REPRESENTED BY THE

MINISTER FOR DEFENCE

OF THE KINGDOM OF SWEDEN

CONCERNING

THE PROTECTION OF

CLASSIFIED INFORMATION EXCHANGED

FOR THE PURPOSE OF DEFENCE CO-OPERATION,

RESEARCH, PRODUCTION, AND PROCUREMENT

BETWEEN THE TWO COUNTRIES

LIST OF CONTENTS Pag

INTRODUCTION

The Government of the United Kingdom of Great Britain and Northern Ireland represented by the Secretary of State for Defence and the Government of Sweden represented by the Minister for Defence of the Kingdom of Sweden, also referred to as the Participants for the purpose of this Arrangement have, in the interests of national security, established the following arrangements which are set out in this General Security Arrangement (GSA), wishing to ensure the protection of Classified Information transferred for the purposes of defence co-operation, research, production and procurement between the two countries or to commercial and industrial organisations in either of the two countries, through approved channels. This GSA will also implement the security provisions incorporated in the Framework Agreement between the French Republic, the Federal Republic of Germany, the Italian Republic, the Kingdom of Spain, the Kingdom of Sweden and the United Kingdom of Great Britain and Northern Ireland concerning Measures to Facilitate the Restructuring and Operation of the European Defence industry signed at Farnborough on 27 July 2000, hereafter referred to as "the Framework Agreement".

This GSA does not cover the exchange of Nuclear, Biological or Chemical (NBC) information related to equipment commonly referred to as Weapons of Mass Destruction (WMD).

This GSA replaces the GSA between the Secretary of State for Defence of the United Kingdom of Great Britain and Northern Ireland and The Minister for Defence of the Kingdom of Sweden concerning The Protection of Classified Information Exchanged For the Purpose of Defence Research, Production and Procurement Between the Two Countries dated 16 June 1998.

1. GENERAL PROVISION

Each Participants commitments under this GSA are to be interpreted in accordance with their respective domestic laws and regulations.

2. SECURITY CLASSIFICATIONS

The **security classifications** and their equivalents in the two countries are:

IN THE UNITED KINGDOM	IN SWEDEN
UK SECRET	HEMLIG / SECRET
UK CONFIDENTIAL	HEMLIG / CONFIDENTIAL
UK RESTRICTED	HEMLIG / RESTRICTED

The additional Swedish marking SECRET, CONFIDENTIAL and RESTRICTED is to be interpreted as the afforded level of protective security handling of the exchanged Classified Information. If the Swedish classification is HEMLIG, without the additional level of protective security handling, the Classified Information must be safeguarded on the security handling level of UK SECRET.

As a general rule, the levels referred to above are to be considered as equivalent. For example a UK CONFIDENTIAL document passed to Sweden is to be transmitted, handled, stored and located in a manner which will afford the same protection as that given to a Swedish HEMLIG/CONFIDENTIAL document.

3. **DEFINITIONS**

The following terms are defined in the interests of clarity:

"Classified Information" means any information (namely, knowledge that can be communicated in any form) or Material determined to require protection against unauthorised disclosure which has been so designated by security classification.

"Classified Contract" means a Contract, which contains or involves Classified Information.

"Consignee" means the Contractor, Facility or other organisation receiving the Material from the Consignor either for further assembly, use, processing or other purposes. It does not include carriers or agents.

"Consignor" means the individual or organisation responsible for supplying Material to the Consignee.

"Contract" means an agreement between two or more parties creating and defining enforceable rights and obligations between the parties.

"Contractor" means an individual or legal entity possessing the legal capacity to undertake Contracts.

"Document" means any recorded information regardless of physical form or characteristics, e.g. written or printed matter (inter alia letter, drawing, plan), computer storage media (inter alia fixed disk, diskette, chip, magnetic tape, CD), photograph and video recording, optical or electronic reproduction of them.

"Facility" means an installation, plant, factory, laboratory, office, university or other educational institution or commercial premises (including any associated warehouse, storage areas, utilities and components which when related by function and location, form an operating entity), or any government department and establishment.

"Material" means any item or substance from which information can be derived. This includes Documents, equipment, weapons or components.

"National Security Authority (NSA) / Designated Security Authority (DSA)" means the government department, authority or agency designated by a Participant as being responsible for the co-ordination and implementation of national security policy.

"Originating Participant" means the Participant initiating the Classified Information as represented by the NSA / DSA.

"Recipient Participant" means the Participant to which the Classified Information is transmitted as represented by the NSA / DSA.

"Security Official" means an individual designated by a NSA/DSA to implement security requirements at a Government establishment or Contractor's premises.

4. COMPETENT SECURITY AUTHORITIES

The Government Authorities responsible for Defence Security in each country are:

FOR THE UNITED KINGDOM

Director of Defence Security (D Def Sy)
Ministry of Defence
St Giles Court
1-13 St Giles High Street
London, WC2H 8LD

FOR THE KINGDOM OF SWEDEN

The NSA in Sweden with overall responsibility for Defence Security is:

Försvarsmakten
(The Swedish Armed Forces) Headquarters
Military Intelligence and Security (MUST)
SE-107 86 STOCKHOLM
Sweden

The DSA in Sweden responsible for Industrial Defence Security is:

Försvarets Materielverk
(The Swedish Defence Materiel Administration)
Security
SE-115 88 STOCKHOLM
Sweden

5. RESTRICTIONS ON USE AND DISCLOSURE

5.1 The Participants will not release, disclose or permit the release or disclosure of Classified Information related to a programme to another government or international organisation, or any entity not participating in the programme, without prior written consent of the Originating Participant.

5.2 The Recipient Participant will not, without prior consultation, publicly disclose, use, or permit the use of any Classified Information except for purposes and within any limitations stated by or on behalf of the Originating Participant.

5.3 Nothing in this GSA will be taken as an authority for, or to govern the release, use, exchange or disclosure of information in which intellectual property rights exist, until the specific written authorisation of the owner of these rights has first been obtained, whether the owner is one of the Participants or a third party.

6. **PROTECTION OF CLASSIFIED INFORMATION**

6.1 The Originating Participant will ensure that the Recipient Participant is informed of:

a. The classification of the information and of any conditions of release or limitations on its use, and that documents are so marked.

b. Any subsequent change in classification.

6.2 The Recipient Participant will:

a. In accordance with its national laws and regulations, afford information received from the other Participant a level of security protection that is afforded to Classified Information of an equivalent classification originated by the Recipient Participant

b. Ensure that Classified Information is marked with its own classification in accordance with Section 2 above.

c. Ensure that classifications are not altered, except as authorised in writing by or on behalf of the Originating Participant.

6.3 In order to achieve and maintain comparable standards of security, each NSA/DSA will, on request, provide to the other information about its security standards, procedures and practices for safeguarding Classified Information, and will for this purpose facilitate visits by the Competent Security Authorities of the other Participant.

7. **ACCESS TO CLASSIFIED INFORMATION**

7.1 Access to Classified Information will be limited to those persons who have a "need to know", and who have been granted a security clearence by the recipient NSA/DSA or by the NSA/DSA of a Framework Agreement Party, in accordance with their national standards, to the level appropriate to the classification of the information to be accessed.

7.2 In accordance with Article 23 of the Framework Agreement:

7.2.1 Access to Classified Information at the UK CONFIDENTIAL/ HEMLIG/CONFIDENTIAL and UK SECRET / HEMLIG/SECRET levels by a person holding the sole nationality of a Party to the Framework Agreement may be granted without prior authorisation of the Originating Participant.

7.2.2 Access to Classified Information at the UK CONFIDENTIAL / HEMLIG/ CONFIDENTIAL and UK SECRET / HEMLIG/SECRET levels by a person holding the dual nationality of one of the Participants and another European Union country may be granted without prior authorisation of the Originating Participant. Access not covered by this paragraph will follow the consultation process described in paragraph 7.2.3 below.

7.2.3 Access to Classified Information at the UK CONFIDENTIAL / HEMLIG/ CONFIDENTIAL and UK SECRET / HEMLIG/SECRET levels by a person not holding the nationality described in paragraphs 7.2.1 and 7.2.2 above will be subject to prior consultation with the Originating Participant. The consultation process concerning such persons will be as described in sub-paragraphs a-d below.

a. The consultation process will be initiated before the start or, as appropriate, in the course of a project/programme.

b. The information will be limited to the nationality of the persons concerned.

d. A Participant receiving such notification will examine whether access to its Classified Information by non-approved nationals is acceptable or not.

e. Such consultations will be given urgent consideration with the objective of reaching consensus. Where this is not possible the Originating Participant's decision will be accepted

8. TRANSMISSION OF CLASSIFIED INFORMATION

8.1 Classified Information at the UK CONFIDENTIAL/UK SECRET and Swedish HEMLIG/CONFIDENTIAL / HEMLIG/SECRET levels will be transmitted between the two countries in accordance with the national security regulations of the Originating Participant. The normal route will be through official diplomatic Government-to-Government channels, but other arrangements may be established, such as hand carriage, secure communications (encryption), if mutually acceptable to both Participants.

8.2 In accordance with Article 25 and the Annex to the Framework Agreement in cases of urgency, i.e. only when the use of Government-to-Government diplomatic bag channels cannot meet the requirements, Classified Information at the UK CONFIDENTIAL / HEMLIG/CONFIDENTIAL level may be transmitted via private courier companies, provided that the following criteria are met:

a. The courier company is located within the territory of the Participants and has established a protective security programme for handling valuable items with a signature service, including a record of continuous accountability on custody through either a signature and tally record, or an electronic tracking/tracing system.

b. The courier company must obtain and provide to the Consignor proof of delivery on the signature and tally record, or it must obtain receipts against package numbers.

c. The courier company must guarantee that the consignment will be delivered to the Consignee by a specific time and date within a 24-hour period.

d. The courier company may charge a commissioner or sub-contractor. However, the responsibility for fulfilling the above requirements must remain with the courier company.

8.3 Classified Information at the UK RESTRICTED / HEMLIG RESTRICTED level will be transmitted between the Participants in accordance with the national regulations of the Originating Participant, which may include the use of private courier companies.

8.4 In accordance with Article 25 and the Annex to the Framework Agreement, Classified Information at the UK CONFIDENTIAL / HEMLIG/CONFIDENTIAL and UK SECRET / HEMLIG/SECRET levels must not be transmitted electronically in clear text. Only cryptographic systems approved by the Participants NSAs/DSAs will be used for the encryption of Classified Information at the UK CONFIDENTIAL / HEMLIG/CONFIDENTIAL and UK SECRET / HEMLIG/SECRET levels, irrespective of the method of transmission. Classified Information at the UK RESTRICTED / HEMLIG/RESTRICTED level may be transmitted or accessed electronically (e.g. by means of point-to-point computer links) via a public network like the Internet, using government or commercial encryption devices mutually accepted by the competent national authorities. However, telephone conversations, video conferencing or facsimile transmissions containing Classified Information at the UK RESTRICTED / HEMLIG/RESTRICTED level may be in clear text, if an approved encryption system is not available.

8.5 Where large volumes of Classified Information are to be transmitted, the means of transport, the route and the escort (if any) will be jointly determined on a case-by-case basis by the competent authorities of the Participants.

9. VISITS

9.1 Each Participant will permit visits involving access to Classified Information to its Government establishments, agencies and laboratories and contractor industrial facilities, by civilian or military representatives of the other Participant or by their contractor employees, provided that the visitor has an appropriate Personal Security Clearance and a "need to know".

9.2 All visiting personnel will comply with security regulations of the host Participant. Any Classified Information disclosed or made available to visitors will be treated as if supplied to the Participant sponsoring the visiting personnel, and will be protected accordingly.

9.3 In accordance with Article 26 and the Annex to the Framework Agreement for visits in the context of Classified Information to Government establishments of the other Participant or to facilities of a contractor where access to Classified Information at the UK CONFIDENTIAL / HEMLIG/CONFIDENTIAL and UK SECRET / HEMLIG/SECRET levels is required, the following procedure will apply:

1. Subject to the following provisions, such visits will be prepared directly between the sending facility and the facility to be visited.

2. For these visits the following prerequisites must also be met:

a. The visit will be for an official purpose.

b. Any facility of a contractor to be visited will have the appropriate Facility Security Clearance.

c. Prior to arrival, confirmation of the visitor's Personal Security Clearance must be provided directly to the facility to be visited by the security official of the sending facility, in the agreed format. To confirm identity the visitor must be in possession of an ID card or passport for presentation to the security authorities at the facility to be visited.

9.4 It is the responsibility of the security officials of:

a. the sending facility to ensure with their NSA/DSA that any company facility to be visited is in possession of an appropriate Facility Security Clearance;

b. both the sending facility and the facility to be visited to agree that there is a need for the visit.

9.5 The security official of a company facility to be visited or, where appropriate, a Government establishment must ensure that records are kept of all visitors, including their name, the organisation they represent, the date of expiry of the Personal Security Clearance, the date(s) of the visit(s) and the name(s) of the person(s) visited. Such records are to be retained for a period of no less than five years.

9.6 The NSA/DSA of the host Participant has the right to require prior notification from their facilities to be visited of visits of more than 21 days' duration. This NSA/DSA may then grant approval, but should a security problem arise it will consult with the NSA/DSA of the visitor.

9.7 Visits relating to Classified Information at the UK RESTRICTED / HEMLIG/RESTRICTED level will also be arranged directly between the sending facility and the facility to be visited.

10. CONTRACTS

10.1 When proposing to place, or authorising a Contractor in its country to place, a Contract involving Classified Information at the UK CONFIDENTIAL / HEMLIG CONFIDENTIAL level or above with a Contractor in the other country the Originating Participant will obtain prior assurance from the NSA/DSA of the other country that the proposed Contractor is security cleared to the appropriate level and also has suitable security safeguards to provide adequate protection for Classified Information. The assurance will carry a responsibility that the security conduct by the cleared Contractor will be in accordance with national security rules and regulations and monitored by his NSA/DSA.

10.2 The Competent Security Authority will ensure that Contractors that receive Contracts placed as a consequence of these pre-contract enquiries are aware of the following provisions and obligations:

10.2.1 The definition of the term "Classified Information" and of the equivalent levels of security classification of the two participants in accordance with the provisions of this Arrangement.

10.2.2 The names of the Government Authorities of each of the two countries empowered to authorise the release and to co-ordinate the safeguarding of Classified Information related to the Contract.

10.2.3 The channels to be used for the transfer of the Classified Information between the Government Authorities and/or Contractors involved.

10.2.4 The procedures and mechanisms for communicating the changes that may arise in respect of Classified Information either because of changes in its security classification or because protection is no longer necessary.

10.2.5 The procedures for the approval of visits, access or inspection by personnel of one country to companies of the other country which are covered by the Contract.

10.2.6 An obligation that the Contractor will disclose the Classified Information only to a person who has previously been cleared for access, who needs to know, and is employed on, or engaged in, the carrying out of the Contract.

10.2.7 An obligation that the Contractor will not disclose the Classified Information or permit it to be disclosed to any person not cleared to have such access.

10.2.8 An obligation that the Contractor will immediately notify his NSA/DSA of any actual or suspected loss, leak or compromise of the Classified Information of this Contract.

10.3 The Competent Security Authority of the Originating Participant will pass two copies of the relevant parts of the Classified Contract to the Competent Security Authority of the Recipient Participant, to allow adequate security monitoring.

10.4 Each contract will contain guidance on the security requirements and on the classification of each aspect/element of the Contract. In Sweden this guidance will be set out in separate relevant security documents. In the UK the guidance will be contained in specific security clauses and in a Security Aspects Letter (SAL). The guidance must identify each classified aspect of the Contract, or any classified aspect which is to be generated by the contract, and allocate to it a specific security classification. Changes in the requirements or to the aspects/elements will be notified as and when necessary and the Originating Participant will notify the Recipient Participant when all the information has been declassified.

11 RECIPROCAL INDUSTRIAL SECURITY ARRANGEMENTS

11.1 Each NSA/DSA will notify the security status of a company site in its country when requested by the other Participant. Each NSA/DSA will also notify the security clearance status of one of its nationals when so requested. These notifications will be known as Facility Security Clearance and Personnel Security Clearance assurance respectively.

11.2 When requested the NSA/DSA will establish the security clearance status of the company/individual which is the subject of the enquiry and forward a Security Clearance assurance if the company/individual is already cleared. If the company/individual does not have a Security Clearance, or the clearance is at a lower security level than that which has

been requested, notification will be sent that the Security Clearance assurance cannot be issued immediately, but that action is being taken to process the request. Following successful enquiries a Security Clearance assurance will be provided.

11.3 A company which is deemed by the NSA/DSA, in the country in which it is registered, to be under the ownership, control or influence of a third country whose aims are not compatible with those of the host Participant is not eligible for a Facility Security Clearance assurance and the requesting NSA/DSA will be notified.

11.4 If either NSA/DSA learns of any adverse information about an individual for whom a Personnel Security Clearance assurance has been issued, it will notify the other NSA/DSA of the details and the action it intends to take, or has taken. Either NSA/DSA may request a review of any Personnel Security Clearance assurance that has been furnished earlier by the other NSA/DSA, provided that the request is accompanied by a reason. The requesting NSA/DSA will be notified of the results of the review and any subsequent action.

11.5 If information becomes available which raises doubts about the suitability of a cleared company to continue to have access to Classified Information in the other country then details of this information will be promptly notified to the NSA/DSA to allow an investigation to be carried out.

11.6 If either NSA/DSA suspends or takes action to revoke a Personnel Security Clearance, or suspends or takes action to revoke access which is granted to a national of the other country based upon a Personnel Security Clearance, the other Participant will be notified and given the reasons for such an action.

11.7 Each NSA/DSA may request the other to review any Facility Security Clearance assurances, provided that their request is accompanied by the reasons for seeking the review. Following the review, the requesting Authority will be notified of the results and will be provided with facts supporting any decisions taken.

11.8 If required by the other Participant each NSA/DSA will co-operate in reviews and investigations concerning Personnel or Facility Security Clearances.

12. LOSS OR COMPROMISE

12.1 In the event of a security infringement involving loss of classified material or suspicion that Classified Information has been disclosed to unauthorised persons, the NSA/DSA of the Recipient Participant will immediately inform the NSA/DSA of the Originating Participant.

12.2 An immediate investigation will be carried out by the Recipient Participant (with assistance from the Originating Participant if required) in accordance with the regulations in force in that country for the protection of Classified Information. The Recipient Participant will inform the Originating Participant about the circumstances, measures adopted and outcome of the investigation as soon as is practicable.

13. **COSTS**

Any costs incurred in the application of the provisions of this GSA will be borne by the Participant providing the services.

14. **AMENDMENT**

The provisions of this GSA may be amended with the mutual consent in writing of the Participants.

15. **DISPUTES**

Any dispute regarding the interpretation or application of this GSA will be resolved by consultation between the Participants or by any other mutually acceptable method of settlement.

16. **EFFECTIVE DATE**

This GSA becomes effective upon the date of the last signature.

17. **TERMINATION/REVIEW**

17.1 This GSA will remain in operation until terminated by either Participant giving the other six months written notice of termination. Both Participants will remain responsible after termination for the safeguarding of all Classified Information exchanged under the provisions of this GSA.

17.2 Similarly, any Classified Information which is exchanged under the cover of this GSA will also be safeguarded, even though its transfer may occur following notice by either of the Participants to terminate.

17.3 In the event of termination, solutions to any outstanding problems will be sought by consultation between the two Participants.

17.4 This GSA will be reviewed jointly by the Participants no later than ten years after its effective date.

The foregoing represents the understandings reached between the Secretary of State for Defence of the United Kingdom of Great Britain and Northern Ireland and the Minister for Defence of the Kingdom of Sweden upon the matters referred to therein.

This GSA is signed in two originals, in the English language.

FOR THE SECRETARY OF STATE FOR DEFENCE OF THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND	**FOR THE MINISTER FOR DEFENCE OF THE KINGDOM OF SWEDEN**
DIRECTOR GENERAL SECURITY AND SAFETY MINISTRY OF DEFENCE	**PERMANENT UNDER SECRETARY MINISTRY OF DEFENCE**
Signed	**Signed**
Date 13 September 2002	**Date** 13 september 2002
Place London	**Place** London

Edita Stockholm 2008