Sveriges internationella överenskommelser

ISSN 1102-3716

Utgiven av Utrikesdepartementet

SÖ 2007: 2

Nr 2
Generellt säkerhetsskyddsavtal med Frankrike rörande ömsesidigt utbyte och skydd av hemliga uppgifter
Stockholm den 16 mars 2006

Regeringen beslutade den 1 september 2005 att underteckna avtalet. Regeringen beslutade den 18 maj 2006 att lämna underrättelse till Frankrike om svenskt godkännande. Underrättelse lämnades den 1 juni 2006. Avtalet trädde i kraft den 1 februari 2007.

Generellt säkerhetsskyddsavtal mellan Konungariket Sveriges regering och Republiken Frankrikes regering rörande ömsesidigt utbyte och skydd av hemliga uppgifter.

INLEDNING

Konungariket Sveriges regering
och
Republiken Frankrikes regering,
i föreliggande avtal kallade parterna,

i syfte att säkerställa skyddet av de hemliga uppgifter som via godkända kanaler delges mellan de båda länderna eller till organisationer inom handel eller industri i något av de båda länderna, med hänsyn till rikets säkerhet och i enlighet med säkerhetskraven i del 4 av ramavtalet mellan Frankrike, Italien, Spanien, Storbritannien, Sverige och Tyskland om åtgärder för att underlätta omstrukturering och drift av den europeiska försvarsindustrin som undertecknades den 27 juli 2000 i Farnborough och som här benämns "ramavtalet"

har kommit överens om följande:

ARTIKEL 1

Definitioner

För tydlighetens skull definieras följande termer:

1.1 **"Hemliga uppgifter"** avser information och materiel oavsett form, slag eller överföringsmetod, som har placerats, eller som är under färdigställande och avses att placeras, i informationssäkerhetsklass med hänsyn till rikets säkerhet och som i enlighet med parternas nationella lagstiftning och föreskrifter skall skyddas mot överträdelser, förstörelse, obehörig förändring, missbruk, röjande, förlust eller åtkomst av obehörig person eller varje annan form av obehörigt röjande.

1.2 **"Materiel"** omfattar maskin, utrustning, vapen eller dokument, hel eller till delar, antingen i färdigt skick eller under färdigställande.

1.3 **"Dokument"** avser dokumenterad information oberoende av fysisk form eller beskaffenhet bland annat skrivet material (däribland skrivelser, ritningar och planer), medier för elektronisk lagring (bland annat hårddiskar, disketter, chips, magnetband, CDskivor), fotografier och videoinspelningar samt optisk eller elektronisk återgivning av sådana.

1.4 **"Kontraktspart"** avser fysisk eller juridisk person med rättslig förmåga att ingå kontraktsförbindelse.

1.5 **"Kontrakt"** avser det rättsliga dokument som har upprättats mellan två eller flera kontraktsparter som fastställer och definiera rättigheter och skyldigheter mellan parterna.

1.6 **"Hemligt kontrakt"** ett kontrakt som innehåller eller rör hemliga uppgifter.

1.7 **"NSM/VSM"** avser nationell säkerhetsmyndighet/verkställande säkerhetsmyndighet med behörighet att tillse kontroll över och tillämpning av detta generella säkerhetsskyddsavtal (GSA).

1.8 **"Upprättande part"** avser den part, också offentlig eller privat organisation under landets jurisdiktion, där den hemliga uppgiften har sitt ursprung.

1.9 **"Mottagande part"** avser den part, också offentlig eller privat organisation under dess jurisdiktion, till vilken den hemliga uppgiften förmedlas.

ARTIKEL 2

Jämförelsetabell

2.1 Vid tillämpningen av detta avtals bestämmelser skall informationssäkerhetsklasserna med respektive motsvarighet i de båda länderna vara följande:

REPUBLIKEN FRANKRIKE	**KONUNGARIKET SVERIGE**	
	Försvarsmyndigheter	**Övriga myndigheter**
TRES SECRET DEFENSE	HEMLIG/TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET
SECRET DEFENSE	HEMLIG/SECRET	HEMLIG (Not 2)
CONFIDENTIEL DEFENSE	HEMLIG/CONFIDENTIAL	HEMLIG (Not 2)
(Not 1)	HEMLIG/RESTRICTED	–

(Not 1) Republiken Frankrike skall hantera och skydda uppgifter från Konungariket Sverige betecknade "HEMLIG/RESTRICTED" i enlighet med gällande nationella lagar och föreskrifter vad avser icke säkerhetsklassade, men skyddade uppgifter som åsatts beteckningen "DIFFUSION RESTREINTE". Konungariket Sverige skall hantera och skydda icke säkerhetsklassade uppgifter från Republiken Frankrike som har åsatts beteckningen "DIFFUSION RESTREINTE", i enlighet med gällande nationella lagar och föreskrifter vad avser skydd av uppgifter betecknade "HEMLIG/RESTRICTED",

(Not 2) Uppgifter från Konungariket Sverige endast märkta "HEMLIG" skall hanteras såsom "CONFIDENTIEL DEFENSE" av Republiken Frankrike om inget annat har angivits av upprättande part.

2.2 Parterna skall skydda de uppgifter de utbyter eller som har utbytts mellan offentliga och privata organisationer inom ramen för bestämmelserna i detta GSA, i enlighet med nationella lagar och föreskrifter.

2.3 Information för begränsad spridning och för vilken särskild behörighetskontroll krävs får utbytas, dock skall parterna då gemensamt bestämma vilka säkerhetsåtgärder som skall vidtas.

ARTIKEL 3

Behöriga säkerhetsmyndigheter

3.1 De myndigheter som ansvarar för att säkerställa tillämpningen av och tillsynen över avtalet i respektive land är:

FÖR REPUBLIKEN FRANKRIKE:
Secretariat Général de la Défense Nationale
51, Boulevard de la Tour-Maubourg
75700 - Paris - 07SP

FÖR KONUNGARIKET SVERIGE:
Försvarsmaktens högkvarter
Militära säkerhetstjänsten
Tegeluddsvägen 64
S-107 85 STOCKHOLM

3.2 De myndigheter som här har angivits skall meddela varandra om förändringar inom den egna organisationen eller underordnad organisation med ansvar för särskilda områden inom ramen för detta GSA.

ARTIKEL 4

Begränsningar för användning och delgivning

4.1 Mottagande part skall, i enlighet med nationella lagar och föreskrifter, vidta alla åtgärder för att hindra röjande eller användning av samtliga hemliga uppgifter som har tillsänts dem med undantag för de ändamål och med de begränsningar som har angivits av, eller gjorts för, upprättande part.

4.2 Mottagande part skall, i enlighet med nationella lagar och föreskrifter, vidta alla åtgärder för att förhindra att de hemliga uppgifter eller det material som har tillhandahållits inom ramen för bestämmelserna i detta GSA på något sätt delges tredje land eller internationell organisation, utan ett skriftligt förhandsgodkännande från upprättande part.

ARTIKEL 5

Skydd av hemliga uppgifter

5.1 Upprättande part skall:

a. Säkerställa att mottagande part är informerad om uppgifternas klassning och om de villkor för delgivning eller de begränsningar för användning som gäller

b. Säkerställa att dokumenten är vederbörligen märkta.

c. Säkerställa att mottagande part har blivit upplyst om eventuella efterföljande förändringar av klassning.

5.2 Mottagande part skall:

a. I enlighet med, och såsom föremål för nationell lagstiftning och föreskrifter, tillse att alla uppgifter och allt material som mottagits från den andra parten får samma säkerhetsskydd som mottagande parts egna hemliga uppgifter eller eget hemligt material med jämförbar klassning.

b. Säkerställa att hemliga uppgifter åsätts beteckning motsvarande den egna nationella klassningen enligt artikel 2.1 ovan.

c. Säkerställa att klassningen inte ändras, utom i de fall skriftligt tillstånd har lämnats av upprättande part.

5.3 1 syfte att uppnå och bibehålla jämförbar säkerhetsnivå, skall varje NSM/VSM, på anmodan av den andra partens NSM/VSM tillhandahålla ytterligare information om de säkerhetsbestämmelser som tillämpas för att

skydda hemliga uppgifter, och skall för detta ändamål underlätta för besök från behöriga säkerhetsmyndigheter.

ARTIKEL 6

Behörighet att ta del av hemliga uppgifter

6.1 Behörighet att ta del av hemliga uppgifter skall begränsas till de personer som för sin tjänst har behov av att ta del av uppgifterna, och som har säkerhetsklarerats av någon av parternas NSM/VSM, i enlighet med gällande nationella lagar och föreskrifter och på en nivå motsvarande uppgifternas klassning.

6.2 Behörighet att ta del av hemliga uppgifter på nivån TRES SECRET DEFENSE / HEMLIG/TOP SECRET till en person som innehar medborgarskap endast i en eller båda av parterna kan ges utan förhandsgodkännande från upprättande part.

6.3 Behörighet att ta del av hemliga uppgifter på nivån SECRET DEFENSE / HEMLIG/SECRET och CONFIDENTIEL DEFENSE / HEMLIG/CONFIDENTIAL till en person som är medborgare endast i en part kan ges utan förhandsgodkännande från upprättande part. Denna bestämmelse är tillämplig också vad gäller medborgare i något av ramavtalets länder.

6.4 Behörighet att ta del av hemliga uppgifter på nivån SECRET DEFENSE / HEMLIG/SECRET och CONFIDENTIEL DEFENSE / HEMLIG/CONFIDENTIAL till en person med dubbelt medborgarskap i en av parterna och i ett annat EU land kan ges utan förhandstillstånd från upprättande part.

6.5 Annan behörighet än sådan som omfattas av artiklarna 6.1 till 6.4 skall hanteras i enlighet med samrådsförfarandet enligt artikel 6.6 nedan.

6.6 Behörighet att ta del av hemliga uppgifter på nivån SECRET DEFENSE / HEMLIG/SECRET och CONFIDENTIEL DEFENSE / HEMLIG/CONFIDENTIAL, till person som inte innehar medborgarskap enligt paragraferna 6.2–6.3 ovan, kan ges efter samråd med upprättande part. I dessa fall skall samrådsförfarandet mellan behöriga säkerhetsmyndigheter följa vad som anges i punkterna a–d nedan:

a. Förfarandet skall inledas före starten av, eller när så är lämpligt, under ett projekts, programs eller kontrakts löptid.

b. Uppgifterna skall begränsas till den eller de omfrågades medborgarskap.

c. Den part som mottar sådan framställan skall undersöka om det finns skäl att ge behörighet till de hemliga uppgifterna.

d. Sådant samråd skall handläggas skyndsamt, med syfte att uppnå samsyn. När detta inte är möjligt skall upprättande parts beslut godtas.

6.7 Emellertid skall parterna, i syfte att göra det lättare att ge behörighet att ta del av den här typen av hemliga uppgifter, om möjligt, komma överens i projektsäkerhetsskyddsinstruktioner (PSI) eller annan lämplig dokumentation som godkänts av NSM/VSM, om att sådana behörighetsbegränsningar kan vara mindre stränga eller är överlödiga.

6.8 När särskilda säkerhetsskäl föreligger, och upprättande part kräver att behörighet att ta del av hemliga uppgifter på nivån SECRET DEFENSE / HEMLIG/SECRET och CONFIDENTIEL DEFENSE / HEMLIG/CONFIDENTIAL skall begränsas endast till dem som innehar medborgarskap i någon part, skall sådana uppgifter åsättas beteckning med klassning och

en extra anteckning där det anges att uppgifterna endast får distribueras till Frankrike eller Sverige.

ARTIKEL 7

Förmedling av hemliga uppgifter

7.1 Hemliga uppgifter på nivån TRES SECRET DEFENSE / HEMLIG/ TOP SECRET får endast befordras mellan parterna med de officiella kanaler som finns för diplomatisk kurirpost. I enskilda fall och förutsatt att skriftligt ömsesidigt godkännande från båda parternas NSM finns kan dock befordran ske på annat sätt.

7.2 Hemliga uppgifter på nivån SECRET DEFENSE / HEMLIG/SECRET och CONFIDENTIEL DEFENSE / HEMLIG/CONFIDENTIAL skall förmedlas mellan parterna i enlighet med den upprättande partens nationella säkerhetsbestämmelser. Det normala befordringssättet skall vara genom de diplomatiska kanalerna, men i brådskande fall kan befordran ske på annat sätt under förutsättning att båda parterna lämnat sitt godkännande.

7.3 1 brådskande fall och när de diplomatiska kanalerna inte är ändamålsenliga, får hemliga uppgifter på nivån CONFIDENTIEL DEFENSE / HEMLIG/CONFIDENTIAL skickas med privata kurirföretag som är godkända av den ena partens NSM/VSM och förutsatt att följande kriterier uppfylls:

a. Att kurirföretaget är lokaliserat inom parternas territorium och har ett säkerhetsskyddsprogram för befordran av värdeförsändelser med kvittenssystem inklusive fortlöpande kontroll av att försändelsen är omhändertagen antingen med användning av kvittenser och leveranslistor eller elektroniskt spårnings- och uppföljningssystem.

b. Att kurirföretaget till avsändaren tillhandahåller och erhåller bevis för att försändelsen levererats, med hjälp av kvittenser och leveranslistor, eller genom kvittenser mot försändelsenummer.

c. Att kurirföretaget kan garantera att försändelsen lämnas till mottagaren vid ett visst klockslag och datum samt, under normala omständigheter, inom en 24 timmarsperiod.

d. Att kurirföretaget har möjlighet att anlita ombud eller underleverantör. Ansvaret för att uppfylla de ovannämnda kraven måste dock kvarstå hos kurirföretaget.

7.4 Hemliga uppgifter i enlighet med artikel 2.1 (not 1) skall förmedlas i enlighet med upprättande parts nationella säkerhetsskyddsbestämmelser, med den förutsättning att de stipulerar lägre krav än vad som föreskrivs i artiklarna 7.1 och 7.2.

7.5 Hemliga uppgifter på nivån SECRET DEFENSE / HEMLIG/SECRET och CONFIDENTIEL DEFENSE / HEMLIG/CONFIDENTIAL får överföras mellan de två parterna via säkra elektroniska eller elektromagnetiska förbindelser inom ramen för detta GSA. I sådana fall skall emellertid parternas behöriga säkerhetsmyndigheter komma överens om ett enskilt "arrangemang".

7.6 Hemliga uppgifter på nivån SECRET DEFENSE / HEMLIG/SECRET och CONFIDENTIEL DEFENSE / HEMLIG/CONFIDENTIAL får inte befordras elektroniskt i klartext. Endast kryptosystem som är godkända av parternas behöriga säkerhetsmyndigheter får användas för kryptering av hemliga uppgifter på nivån SECRET DEFENSE / HEMLIG/SECRET och

CONFIDENTIEL DEFENSE / HEMLIG/CONFIDENTIAL oavsett överföringsmetod.

7.7 För hemliga uppgifter i enlighet med artikel 2.1 (not 1) som överförs eller görs tillgängliga på elektronisk väg (exempelvis via direktuppkopplad datorlänk eller via ett öppet nät såsom Internet) skall statlig eller kommersiell krypteringsutrustning som godkänts av parternas behöriga säkerhetsmyndigheter användas. Förutsatt att parterna godkänner det får dock information i telefonsamtal, videokonferenser eller fax betecknad i enlighet med artikel 2.1 (not 1) överföras i klartext om godkänt krypteringssystem inte är tillgängligt.

7.8 När det rör sig om stora mängder hemliga uppgifter som skall överföras, bestäms transportmedel, väg och eskort för varje enskilt fall av parternas NSM/VSM gemensamt.

ARTIKEL 8

Besök

8.1 Varje part skall medge besök som innefattar att besökare tar del av hemliga uppgifter vid myndigheters lokaler och laboratorier samt vid kontraktsparts industrianläggningar, av civila eller militära företrädare för den andra parten eller kontraktstagares anställda, under förutsättning att besökaren har erforderlig säkerhetsklarering och behov av att ta del av uppgifterna. För besök där hemliga uppgifter förekommer vid anläggningar belägna inom den andra parten eller en kontraktstagares anläggningar, där behörighet att ta del av hemliga uppgifter på nivån TRES SECRET DEFENSE / HEMLIG/TOP SECRET är nödvändig, skall en formell framställan om att avlägga besök skickas med godkänd diplomatisk förbindelse.

8.2 All besökande personal skall följa värdpartens säkerhetsbestämmelser. Hemliga uppgifter som delges, eller som besökarna ges behörighet att ta del av, skall behandlas som om de tillhandahållits den part som besökarna tillhör, och skall skyddas därefter.

8.3 För besök där hemliga uppgifter förekommer vid statliga anläggningar tillhörande den andra parten eller kontraktstagares anläggningar, och behov finns av att ta del av hemliga uppgifter på nivåerna SECRET DEFENSE / HEMLIG/SECRET eller CONFIDENTIEL DEFENSE / HEMLIG/CONFIDENTIAL, skall följande förfarande tillämpas:

a. I enlighet med följande bestämmelser, förbereds sådana besök i direktkontakt mellan avsändande anläggning och den anläggning som skall besökas.

b Följande krav måste också uppfyllas i samband med dessa besök:

1) Besöket skall ha ett officiellt syfte.

2) Anläggning som besöks skall ha erhållit erforderlig säkerhetsklarering.

3) Före ankomsten till sådan anläggning som avses ovan måste bekräftelse på besökarens säkerhetsklarering direkt tillhandahållas den mottagande anläggningen utfärdat av den säkerhetsansvarige vid den sändande anläggningen. För att styrka sin identitet måste besökaren ha ID kort eller pass som uppvisas för de säkerhetsansvariga i den mottagande anläggningen.

8.4 Besök där hemliga uppgifter i enlighet med artikel 2.1 (not 1) förekom-

mer kan också ordnas direkt mellan den avsändande anläggningen och den anläggning som skall besökas.

8.5 Säkerhetsansvarig ansvarar för:

a. vid den avsändande anläggningen, att kontrollera med sin NSM/VSM att företag eller anläggning som besöks har erforderlig säkerhetsklarering,

b. att både den avsändande anläggningen och den anläggning som skall besökas är överens om att det finns behov av att göra besöket.

8.6 Säkerhetsansvarig vid den anläggning som skall besökas skall tillse att register förs över alla besökare med uppgifter om namn, den organisation de företräder, sista giltighetsdatum för personell säkerhetsklarering, datum för besöket eller besöken och namn på de personer eller den person som man har besökt. Dessa register skall bevaras i minst två år.

8.7 NSM/VSM i mottagande part har rätt att begära förhandsmeddelande från sina företag beträffande besök längre än 21 dagar. Det tillkommer behörig säkerhetsmyndighet att ge tillstånd, men de skall, om säkerhetsproblem uppstår, rådgöra med behörig säkerhetsmyndighet i besökarens land.

ARTIKEL 9

Kontrakt

9.1 Part som tecknar, eller bemyndigar kontraktspart i sitt land att teckna kontrakt som berör hemliga uppgifter med kontraktstagare i den andra parten, skall i förväg erhålla intyg från det andra landets NSM/VSM om att den förslagna kontraktsparten är säkerhetsklarerad på erforderlig nivå och har ändamålsenligt säkerhetsskydd för att på lämpligt sätt skydda hemliga uppgifter. Med intyget följer ett ansvar för att den klarerade kontraktsparten följer gällande nationella säkerhetsbestämmelser och att detta kontrolleras av avsändande NSM/VSM.

9.2 Den avsändande partens NSM/VSM skall meddela all relevant information om det hemligstämplade kontraktet till mottagande parts NSM/VSM i syfte att möjliggöra erforderlig säkerhetsuppföljning.

9.3 Till hemliga kontrakt skall tillägg eller bilaga bifogas med riktlinjer om säkerhetskrav och klassificering för det som kontraktet avser. I riktlinjerna skall det anges vilka hemliga aspekter som kontraktet har eller medför samt specifik informationssäkerhetsklass för det som kontraktet avser. Information om ändringar i detta avseende skall lämnas när och på det sätt som krävs och upprättande part skall eddela mottagande part när del av eller all information inte längre skall vara placerad i en informationssäkerhetsklass.

ARTIKEL 10

Ömsesidiga säkerhetsåtgärder avseende företag

10.1 Varje NSM/VSM skall efter framställan från den andra parten meddela säkerhetsstatus för en företagsanläggning belägen i det egna landet. Varje NSM/VSM skall också efter framställan från den andra parten lämna information om säkerhetsklarering vad avser en fysisk person i form av ett intyg. Dessa intyg kallas i det som följer säkerhetsklarering gällande företag och lokaler (FSQ respektive personell säkerhetsklarering (PSC).

10.2 På förfrågan skall NSM/VSM lämna besked om säkerhetsklarering för det företag eller den fysiska personen som är föremål för framställan samt

tillhandahålla intyg om säkerhetsklarering i de fall företaget eller den fysiska personen redan erhållit klarering. Om företaget eller personen inte är säkerhetsklarerad, eller om klareringen avser en lägre säkerhetsklass än den framställan gäller, skall meddelande skickas om att intyg om säkerhetsklarering inte omedelbart kan utfärdas, men att om den andra partens NSM/VSM så begär, kommer framställan om säkerhetsklarering att behandlas. När ärendet är färdigbehandlat meddelas beslut i frågan till framställande myndighet.

10.3 Om någon av parternas NSM/VSM återkallar eller vidtar åtgärder för att återkalla en personell säkerhetsklarering eller behörighet för medborgare i den andra parten, skall skälen för en sådan åtgärd meddelas den andra parten.

10.4 Om någon av parternas NSM/VSM får kännedom om information av ofördelaktigt slag om en redan säkerhetsklarerad fysisk person skall denna information samt uppgifter om vilka åtgärder man avser vidta eller som har vidtagits meddelas den andra parten.

10.5 Om någon av parternas NSM/VSM får kännedom om information som ger anledning att ifrågasätta ett företags säkerhetsklareringen, skall sådan information så snart som möjligt meddelas den andra parten så att en utredning kan inledas.

10.6 Varje NSM/VSM förbehålls rätten att begära att den andra partens NSM/VSM omprövar en säkerhetsklarering gällande ett företag förutsatt att skälen till att omprövning begärs bifogas framställan. Efter omprövning skall framställande NSM/VSM meddelas resultatet av denna.

10.7 Om den ena partens NSM/VSM så begär skall den andra partens NSM/VSM medverka i omprövningar och utredningar gällande säkerhetsklareringar.

ARTIKEL 11

Förlust eller skada

11.1 Om någon av parterna upptäcker eller misstänker att hemliga uppgifter har förlorats eller blivit röjda skall den andra partens NSM/VSM omedelbart informeras.

11.2 Den part som upptäckt eller misstänker att hemliga uppgifter har förlorats eller blivit röjda skall omedelbart genomföra en utredning (med stöd från den andra parten om så är nödvändigt) i enlighet med tillämpliga nationella lagar och föreskrifter i respektive land.

Den part som leder utredningen skall, så snart möjligt, informera den andra partens NSM/VSM om omständigheterna, resultatet av utredningen, åtgärder som vidtagits och vad som gjorts för att rätta till det inträffade.

ARTIKEL 12

Övrigt

12.1 Tillämpningen av detta avtal skall normalt sett inte medföra några särskilda kostnader.

12.2 Eventuella kostnader skall bäras av vardera parten inom ramen för befintlig budget.

12.3 Varje part och myndigheterna i respektive land skall underlätta för personal från den andra parten att utföra tjänster och utöva rättigheter på dess

territorium i enlighet med bestämmelserna i detta GSA.

12.4 Skulle behov uppstå skall parternas behöriga säkerhetsmyndigheter samråda om särskilda tekniska aspekter av tillämpningen av detta GSA och får, från fall till fall, gemensamt överenskomma om att utfärda säkerhetsbestämmelser som tillägg till detta GSA.

ARTIKEL 13

Slutbestämmelser

13.1 Detta avtal ersätter Överenskommelse mellan Republiken Frankrikes regering och Konungariket Sveriges regering rörande visst utbyte av sekretesskyddad information, undertecknad i Stockholm den 22 oktober 1973.

13.2 Avtalets löptid är obegränsad. Detta GSA skall träda ikraft på den första dagen i andra månaden efter det att ett sista meddelande mellan parterna har mottagits, som anger att nödvändiga nationella åtgärder för ikraftträdandet har vidtagits.

13.3 Detta GSA får hävas gemensamt eller ensidigt sex månader efter det att skriftlig meddelande därom har lämnats till den andra parten. Båda parterna förblir ansvariga för skyddet av samtliga hemliga uppgifter som har utbytts inom ramen för detta GSA.

13.4 Vaje part skall utan dröjsmål meddela den andra parten ändringar i den nationella lagstiftningen eller nationella bestämmelser som påverkar skyddet av hemliga uppgifter inom ramen för detta GSA. Om så är fallet, skall parterna samråda för att överväga möjliga ändringar i detta GSA. Under tiden skall hemliga uppgifter skyddas såsom här beskrivs.

13.5 Avtalets bestämmelser får ändras förutsatt att skriftligt medgivande från båda parter föreligger. Sådana ändringar skall träda i kraft i enlighet med punkt 13.2 ovan.

13.6 Tvister om tolkning eller tillämpning av avtalets bestämmelser skall lösas endast i samråd mellan representanter för de båda parterna utan inblandning av tredje part eller internationell domstol.

Till bekräftelse härav har undertecknande, därtill vederbörligen bemyndigade av respektive regering, undertecknat detta GSA.

Undertecknat i Stockholm den 16 mars 2006 i två exemplar, varav ett på svenska och ett på franska, där båda texterna äger lika giltighet.

För Konungariket Sveriges regering
Helena Lindberg

För Republiken Frankrikes regering
Denis Delbourg

Accord général de sécurité entre le Gouvernement du Royaume de Suède et le Gouvernement de la République française concernant l'échange et la protection réciproque d'informations classifiées.

PREAMBULE

Le Gouvernement de Royaume de Suède et le Gouvernement de la République française;

Ci-après dénommés les Parties,

souhaitant garantir la protection des informations classifiées entre les deux Etats ou transmises à des organismes commerciaux et industriels de 1'un des deux Etats par des voies approuvées ; dans l'intérêt de la sécurité nationale et ayant à l'esprit les dispositions relatives à la sécurité des informations classifiées figurant au chapitre 4 de l'Accord cadre conclu entre la République française, la République fédérale d'Allemagne, le royaume d'Espagne, la République italienne, le royaume de Suède et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord relatif aux mesures visant à faciliter la restructuration et le fonctionnement de l'industrie européenne de défense, fait à Farnborough le 27 juillet 2000 et ci-après dénommé "Accord cadre" ;

Sont convenus des dispositions suivantes

ARTICLE 1

Définitions

Les termes suivants sont définis par souci de clarté

1.1 **"Informations classifiées"** fait référence aux informations et aux matériels, quels qu'en soient la forme, la nature ou le mode de transmission, qu'ils soient élaborés ou en cours d'élaboration, auquel un degré de classification ou de protection a été attribué et qui, dans l'intérêt de la sécurité nationale et conformément aux lois et réglementations nationales des Parties, nécessitent une protection contre toute violation, destruction, détournement, modification non autorisée, divulgation, perte, accès par une personne non autorisée ou tout autre type de compromission.

1.2 **"Matériel"** inclut tout composant ou équipement ou arme ou document qu'il soit achevé ou en cours d'élaboration.

1.3 **"Document"** signifie toutes les informations enregistrées quelles que soient leur forme physique ou leurs caractéristiques, par exemple matériel écrit ou imprimé (notamment lettre, dessin, plan), supports informatiques (notamment disque dur, disquette, puce, bande magnétique, CD), enregistrements photographiques ou magnétoscopiques, reproduction optique ou électronique de ces informations.

1.4 **"Contractant"** signifie une personne physique ou une personne morale disposant du pouvoir juridique de conclure des contrats.

1.5 **"Contrat"** signifie un acte légal conclu entre deux ou plusieurs Contractants et créant et définissant les droits et les obligations applicables entre les parties.

1.6 **"Contrat elassé"** signifie un Contrat qui contient ou implique des Informations classifiées.

1.7 **"ANS/ASD"** signifie les Autorités nationales de sécurité/Autorités de sécurité désignées qui sont les autorités compétentes chargées du contrôle et de la mise en œuvre du présent Accord Général de Sécurité (AGS).

1.8 **"Partie d'origine"** signifie la Partie, y compris tout autre organisme public/privé placé sous sa juridiction, fournissant les Informations classiflées.

1.9 **"Partie destinataire"** signifie la Partie, y compris tout autre organisme public/privé placé sous sa juridiction, à laquelle les Informations classiflées sont transmises.

ARTICLE 2

Tableau d'équivalences

2.1 Aux fins des présentes dispositions, les classifications de sécurité et leurs équivalents dans les deux Etats sont les suivants :

ROYAUME DE SUEDE	**REPUBLIQUE FRANÇAISE,**	
Autorites de defense	**Autres Autorites**	
HEMLIG/TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	TRES SECRET DEFENSE
HEMLIG/SECRET	HEMLIG (Nota 2)	SECRET DEFENSE
HEMLIG/CONFIDENTIAL	HEMLIG (Nota 2)	CONFIDENTIEL DEFENSE
HEMLIG/RESTRICTED	–	(Nota 1)

Le Royaume de Suède traite et protége les informations non classifiées mais revêtues d'une mention telle que "DIFFUSION RESTREINTE" transmises par la République française selon ses lois et réglementations nationales en vigueur relatives à la protection des informations "HEMLIG/RESTRICTED".

(Nota 1) La République Française traite et protége les informations portant la mention "HEMLIG/RESTRICTED" transmises par le Royaume de Suède selon ses lois et réglementations nationales en vigueur relatives aux informations protégées mais non classifiées telles que les informations revêtues de la mention "DIFFUSION RESTREINTE".

(Nota 2) Sauf contre-indication de la Partie d'origine, les informations transmises par le Royaume de Suède revêtues de la seule mention "HEMLIG" sont traitées par la République française comme "CONFIDENTIEL DEFENSE".

2.2 Les Parties protègent les informations échangées entre elles et/ou entre des organismes publics ou privés selon les dispositions du présent AGS et en accord avec leurs propres lois et réglementations nationales.

2.3 Des informations exigeant une distribution limitée et des contrôles d'accès spécifiques peuvent être échangées. Dans ce cas, les mesures de sécurité à appliquer sont déterminées d'un commun accord entre les Parties.

ARTICLE 3

Autorités de Sécurité Compétentes

3.1 Les Autorités gouvernementales chargées de garantir la mise en œuvre et le contrôle du présent AGS dans chacun des Etats sont :

POUR LE ROYAUME DE SUEDE
Försvarsmaktens högkvarter
Militära säkerhetstjänsten
Tegeluddsvägen 64
S 107 85 Stockholm

POUR LA REPUBLIQUE FRANÇAISE:,
Secrétariat Général de la Défense Nationale
51, Boulevard de la Tour Maubourg
75700 - Paris - 07SP

3.2 Les Autorités susmentionnées s'infonnent réciproquement de tout changement éventuel les concernant, ainsi que des organismes subordonnés responsables des domaines spécifiques, conformément aux dispositions du présent AGS.

ARTICLE 4

Restrictions en matière d'utilisation et de divulgation

4.1 Conformément à leurs législation et réglementation nationales, les Parties destinataires ne divulguent ni n'utilisent, ni ne pennettent la divulgation ou l'utilisation de toute Information classifiée qui leur est communiquée, excepté à des fins et compte tenu des restrictions indiquées par ou au nom de la Partie d'origine.

4.2 Conformément à sa législation et réglementation nationales, la Partie destinataire ne transmet à un quelconque Etat tiers, ou organisation internationale, une quelconque Information classifiée ou un quelconque Matériel, fourni en vertu des dispositions du présent AGS, ni ne divulgue publiquement une quelconque Information classifiée sans l'accord écrit préalable de la Partie d'origine.

ARTICLE 5

Protection des Informations classifiées

5.1 La Partie d'origine :

a. s'assure que la Partie destinataire est informée de la classification des Informations et de toute condition de communication ou restriction imposée à leur utilisation

b. s'assure que les documents sont dûment marqués ;

c. s'assure que la Partie destinataire est informée de tout changement de classification ultérieur.

5.2 La Partie destinataire

a. conformément à ses lois et réglementations nationales, accorde à toute Information et à tout Matériel reçu de l'autre Partie le niveau de protection

de sécurité qui est attribué aux Informations et Matériel classifiés bénéficiant d'une classification équivalente et transmises par la Partie destinataire

b. s'assure que les Informations classifiées sont pourvues de la mention de leur propre classification nationale équivalente, conformément à l'Article 2.1 ci-dessus ;

c. s'assure que les classifications ne sont pas modifiées, excepté en cas d'autorisation écrite de la Partie d'origine.

5.3 Afin d'atteindre et de conserver des niveaux de sécurité comparables, chaque ANS/ASD fournit, sur demande, à l'autre ANS/ASD des informations sur ses réglementations de sécurité, procédures et pratiques de protection des Informations classifiées et facilite, à ces fins, les contacts et les visites entre leurs Autorités de sécurité compétentes respectives.

ARTICLE 6

Accès aux Informations classifiées

6.1 L'accès aux Informations classifiées est limité aux personnes ayant le "besoin d'en connaître", et qui ont été préalablement habilitées par l'une ou l'autre des ANS/ASD des Parties, en accord avec les lois et réglementations nationales, au niveau de classification approprié selon les Informations à connaître.

6.2 L'accès aux Informations classifiées de niveau HEMLIG/TOP SECRET / TRES SECRET DEFENSE par une personne ayant exclusivement la nationalité d'une Partie au présent AGS peut être accordé sans l'autorisation préalable de la Partie d'origine.

6.3 L'accès aux Informations classifiées de niveau HEMLIG/SECRET / SECRET DEFENSE et de niveau HEMLIG/CONFIDENTIAL / CONFIDENTIEL DEFENSE par une personne ayant exclusivement la nationalité des Parties peut être accordé sans l'autorisation préalable de la Partie d'origine. Cette disposition s'applique également aux ressortissants des Parties à "l'Accord cadre".

6.4 L'accès aux Informations classifiées de niveau HEMLIG/SECRET / SECRET DEFENSE et de niveau HEMLIG/CONFIDENTIAL / CONFIDENTIEL DEFENSE par une personne ayant la double nationalité de l'une des Parties et d'un Etat de l'Union européenne peut être accordé sans autorisation préalable de la Partie d'origine.

6.5 Tout autre accès non couvert par les paragraphes 6.1 à 6.4 est soumis au processus de consultation décrit au paragraphe 6.6 ci-dessous.

6.6 L'accès aux Informations classifiées de niveau HEMLIG/SECRET / SECRET DEFENSE et de niveau HEMLIG/CONFIDENTIAL / CONFIDENTIEL DEFENSE par une personne n'ayant pas la nationalité décrite aux paragraphes 6.2–6.3 ci-dessus fait l'objet d'une consultation préalable avec la Partie d'origine. Le processus de consultation entre les Autorités de sécurité compétentes au sujet de telles personnes est décrit aux alinéas a.-d. comme suit :

a. le processus est lancé avant le début ou, le cas échéant, pendant un projet/programme ou Contrat ;

b. les informations sont limitées à la nationalité des personnes concernées

c. une Partie recevant une telle notification détermine si l'accès à ses

Informations classifiées est acceptable ou non ;

d. de telles consultations sont traitées d'urgence afin de parvenir à un consensus. Dans les cas où cela s'avère impossible, la décision de la Partie d'origine est acceptée.

6.7 Cependant, afin de simplifier l'accès à ces Informations classifiées, les Parties s'efforcent de parvenir à un accord dans le cadre des Instructions de sécurité du programme (ISP) ou dans tout autre document approuvé par les ANS/ASD, de manière à ce que ces restrictions d'accés soient moins rigoureuses ou ne soient pas exigées.

6.8 Pour des raisons de sécurité particulières, lorsque la Partie d'origine exige que l'accés à des Informations classifiées de niveau HEMLIG/SECRET / SECRET DEFENSE et de niveau HEMLIG/CONFIDENTIAL / CONFIDENTIEL DEFENSE soit limité aux seules personnes ayant exclusivement la nationalité des parties, ces informations porteront la mention de leur classification et un avertissement supplémentaire “Spécial – France/Suède”.

ARTICLE 7

Transmission des Informations classifiées

7.1 Les Informations classifiées de niveau HEMLIG/TOP SECRET / TRES SECRET DEFENSE sont uniquement transmises entre les Parties par la voie diplomatique. Cependant, au cas par cas, d'autres dispositions peuvent être prises si elles sont mutuellement approuvées par écrit entre les ANS des Parties.

7.2 Les Informations classifiées de niveau HEMLIG/SECRET / SECRET DEFENSE et de niveau HEMLIG/CONFIDENTIAL / CONFIDENTIEL DEFENSE sont transmises entre les deux Parties conformément aux réglementations nationales relatives à la sécurité de la Partie d'origine. La voie normale est la voie diplomatique, mais d'autres dispositions peuvent être établies en cas d'urgence si elles sont acceptées d'un commun accord entre les deux Parties.

7.3 En cas d'urgence, c'est-à-dire uniquement lorsque l'utilisation de la voie diplomatique ne peut répondre aux exigences, les Informations classiflées de niveau HEMLIG/CONFIDENTIAL / CONFIDENTIEL DEFENSE peuvent être transmises via des sociétés commerciales de messagerie, à condition que les critères suivants soient satisfaits :

a. la société de messagerie est implantée sur le territoire des Parties et a mis en place un programme de sécurité et de protection pour la prise en charge d'articles de valeur avec un service de signature, incluant une surveillance et un enregistrement permanents permettant de déterminer à tout moment qui en a la charge, soit par un système de registre de signatures et de pointage, soit par un système électronique de suivi et d'enregistrement

b. la société de messagerie doit obtenir et fournir à l'expéditeur un justificatif de livraison sur le registre de signatures et de pointage, ou doit obtenir un reçu portant les numéros des colis ;

c. la société de messagerie doit garantir que l'expédition sera livrée au destinataire avant une date et une heure données dans un délai de 24 heures dans des circonstances normales

d. la société de messagerie peut confier la tâche à un agent ou à un sous-traitant étant entendu que la responsabilité de l'exécution des obligations ci-dessus incombe toujours à la société de messagerie.

7.4 Les Informations telles que définies à l'Article 2.1 (Nota 1) sont transmises conformément aux réglementations nationales relatives à la sécurité de la Partie d'origine, étant entendu qu'elles sont moins restrictives que celles mentionnées aux paragraphes 7.1 et 7.2 ci-dessus.

7.5 Les Informations classifiées de niveau HEMLIG/SECRET / SECRET DEFENSE et de niveau HEMLIG/CONFIDENTIAL / CONFIDENTIEL DEFENSE peuvent être transmises entre les Parties par des moyens électroniques ou électromagnétiques sécurisés selon les dispositions du présent AGS. Cependant, dans ce cas, un "arrangement" séparé est conclu entre les Autorités de sécurité compétentes des Parties aux fins de préciser les conditions dans lesquelles s'effectue ce type de transmission.

7.6 Les Informations classifiées de niveau HEMLIG/SECRET / SECRET DEFENSE et de niveau HEMLIG/CONFIDENTIAL / CONFIDENTIEL DEFENSE ne doivent pas être transmises en clair par des moyens électroniques. Seuls des systémes cryptographiques approuvés par les Autorités de sécurité compétentes des Parties sont utilisés pour le cryptage d'lnformations classifiées de niveau HEMLIG/SECRET / SECRET DEFENSE et de niveau HEMLIG/CONFIDENTIAL / CONFIDENTIEL DEFENSE, quel que soit le mode de transmission.

7.7 Les Informations telles que définies à l'Article 2.1 (Nota 1) sont transmises ou récupérées par des moyens électroniques (par exemple des liaisons informatiques point à point ou via un réseau public comme Internet), en utilisant des dispositifs de cryptage gouvernementaux ou commerciaux acceptés d'un commun accord entre les Autorités de sécurité compétentes des Parties. Cependant, si les Parties l'acceptent, les conversations téléphoniques, les vidéoconférences ou les transmissions par télécopie contenant des Informations telles que déflnies à l'Article 2.1 (Nota 1) peuvent être effectuées en clair si un système de chiffrement approuvé n'est pas disponible.

7.8 Lorsque d'importants volumes d'informations classifiées doivent être transmis les moyens de transport, le trajet et l'escorte le cas échéant, sont déterminés d'un commun accord, au cas par cas, par les ANS/ASD des Parties.

ARTICLE 8

Visites

8.1 Chaque Partie autorise des visites impliquant Vaccés aux Informations classifiées de ses établissements, agences et laboratoires gouvernementaux ainsi que des établissements industriels des contractants, par des représentants civils ou militaires de l'autre Partie et par les employés d'un contractant à condition que le visiteur dispose d'une habilitation de sécurité individuelle et fasse êtat d'un besoin d'en connaître. Pour les visites effectuées dans le contexte des Informations classifiées aux établissements de l'autre Partie ou aux établissements d'un contractant pour lesquelles l'accès à des Informations classifiées de niveau HEMLIG/TOP SECRET / TRES SECRET DEFENSE est requis, il convient de présenter une demande formelle de visite par la voie diplomatique.

8.2 Tous les visiteurs se conforment aux réglementations de sécurité de la Partie d'accueil. Toutes les Informations classifiées communiquées ou mises à la disposition visiteurs sont traitées comme si elles étaient fournies à la Partie répondant des visiteurs et sont protégées en conséquence.

8.3 Pour les visites effectuées dans le contexte des Informations classifiées aux établissements de l'autre Partie ou aux établissements d'un contractant pour lesquelles l'accès à des Informations classifiées de niveau HEMLIG/ SECRET / SECRET DEFENSE ou de niveau HEMLIG/CONFIDENTIAL / CONFIDENTIEL DEFENSE est requis, la procédure suivante est applicable:

a. sous réserve des dispositions suivantes, de telles visites sont directement préparées entre l'établissement d'envoi et l'établissement d'accueil

b. ces visites sont également soumises aux conditions suivantes

1) la visite a un but officiel ;

2) tout établissement d'accueil dispose d'une habilitation de sécurité d'établissement appropriée ;

3) avant l'arrivée, une confirmation de l'habilitation de sécurité individuelle du visiteur est directement fournie à l'établissemenl d'accueil, par le responsable de la sécurité de l'établissement denvoi. Pour confirmer son identité, le visiteur doit être en possession d'une carte d'identité ou d'un passeport à présenter aux autorités de sécurité de l'établissement d'accueil.

8.4 Les visites relatives à des Informations telles que définies à l'Article 2.1 (Nota 1) sont également directement organisées entre l'établissement d'envoi et l'établissement d'accueil.

8.5 Il appartient au responsable de la sécurité :

a. de l'établissement d'envoi de vérifier auprès de son ANS/ASD que l'établissement d'accueil est en possession d'une habilitation de sécurité appropriée ;

b. des établissements d'envoi et d'accueil de se mettre d'accord sur la nécessité de la visite.

8.6 Le responsable de la sécurité de l'établissement d'accueil ou, le cas échéant, d'un établissement gouvernemental, doit s'assurer que tous les visiteurs sont inscrits sur un registre, avec leur nom, l'organisation qu'ils représentent, la date d'expiration de l'habilitation de sécurité individuelle, la/les date(s) de la/des visite(s) et le/les nom(s) de la/des personnes(s) visitée(s). Ces registres doivent être conservés pendant au moins deux (2) ans.

8.7 L'ANS/ASD de la Partie d'accueil est en droit d'exiger de ses établissements d'accueil d'être préalablement informée des visites de plus de 21 jours. Cette autorité de sécurité compétente peut ensuite donner son accord, étant entendu qu'en cas de probléme de sécurité, elle consulte l'autorité de sécurité compétente du visiteur.

ARTICLE 9

Contrats

9.1 Une Partie concluant, ou autorisant un Contractant installé dans son Etat à conclure, un Contrat impliquant des Informations classifiées avec un Contractant installé dans l'autre Etat, doit obtenir l'assurance préalable, donnée par l'ANS/ASD de l'autre Etat, que le Contractant proposé dispose d'une habilitation de sécurité du niveau approprié ainsi que de mesures de sécurité appropriées pour garantir une protection adéquate des Informations classifiées. Cette assurance implique une responsabilité quant à une conduite en matière de sécurité du Contractant conforme aux lois et réglementations nationales relatives à la sécurité et contrôlée par son ANS/ASD.

9.2 L'ANS/ASD de la Partie d'origine communique toutes les informations nécessaire sur le Contrat classé à l'ANS/ASD de la Partie destinataire, pour permettre un contrôle appropné de la sécurité.

9.3 Chaque Contrat classé comprend un supplément/une annexe avec des indications sur les exigences en matière de sécurité et sur la classification de chaque aspect/élément du Contrat. Les indications doivent identifier chaque aspect classifié du Contrat ou aspect classifié susceptible d'être généré par le contrat, et lui attribuer une classification de sécurité spécifique. Les modifications apportées aux exigences ou aux aspects/éléments sont notifiées de la manière et au moment opportuns et la Partie d'origine informe la Partie destinataire de la déclassification de la totalité ou d'une partie des Informations.

ARTICLE 10

Accords réciproques relatifs a la sécurité industrielle

10.1 Sur demande de l'autre Partie, chaque ANS/ASD notifie l'état de sécurité du site d'une société / d'un établissement installé dans son Etat. Sur demande de l'autre Partie, chaque ANS/ASD notifie également l'état d'habilitation de sécurité d'une personne physique. Ces notifications sont portées à la connaissance de la Partie requérante par le biais d'une attestation d'habilitation de sécurité d'établissement ou d'une attestation l'habilitation de sécurité individuelle.

10.2 Si la personne morale/physique est déjà habilitée par une Partie, l'ANS/ASD de cette Partie transmet à l'autre un certificat d'habilitation de sécurité si cette dernière en fait la demande. Si la personne morale/physique ne dispose pas d'une habilitation de sécurité, ou si l'habilitation est établie à un niveau de sécurité inférieur au niveau demandé, une notification est envoyée pour indiquer que le certificat d'habilitation de sécurité ne peut être immédiatement délivré, mais que si l'ANS/ASD de l'autre Partie le souhaite, le processus d'habilitation de sécurité est engagé. A la fin du processus, la notification de la décision prise est transmise à l'Autorité ayant formulé la demande.

10.3 Si 1'ANS/ASD d'une Partie suspend ou prend des mesures pour abroger une habilitation de sécurité individuelle, ou suspend ou prend des mesures pour annuler l'accès accordé à un ressortissant de l'autre Partie, cette demière en est informée, ainsi que des raisons justifiant une telle mesure.

10.4 Si 1'ANS/ASD d'une Partie a connaissance d'informations défavorables concernant une personne physique pour laquelle une attestation d'habilitation de sécurité individuelle a été délivrée, lesdites informations sont communiquées à l'autre Partie de méme que les mesures envisagées ou adoptées.

10.5 Si 1'ANS/ASD d'une Partie a connaissance d'informations suscitant des doutes quant au maintien de l'habilitation de sécurité d'une société / d'un établissement, ces informations sont communiquées dans les meilleurs délais à l'autre Partie aux fins de permettre l'ouverture d'une enquête.

10.6 Chaque ANS/ASD est en droit de demander à l'ANS/ASD de l'autre Partie de réexaminer une habilitation de sécurité d'une société / d'un établissement à condition que cette demande soit accompagnée des raisons la motivant. Suite à l'examen, 1'ANS/ASD ayant formulé la demande est infonnée des résultats.

10.7 Sur demande de 1'ANS/ASD de l'une des Parties, 1'ANS/ASD de l'autre Partie participe aux examens et enquêtes concernant les habilitations de sécurité.

ARTICLE 11

Perte ou compromission

11.1 En cas de perte d'informations classiflées ou s'i1 est possible que de telles Informations aient été compromises, l'ANS/ASD de la Partie ayant découvert ou suspectant les faits est tenue d'en informer immédiatement l'ANS/ASD de l'autre Partie.

11.2 La Partie ayant découvert ou suspectant les faits mène immédiatement une enquête (avec, si nécessaire, l'aide de l'autre Partie) conformément aux lois et réglementations nationales en vigueur dans l'Etat concerné. La Partie menant l'enquête informe aussi rapidement que possible l'ANS/ASD de l'autre Partie des circonstances, du résultat de l'enquête, des mesures adoptées et des mesures correctrices engagées.

ARTICLE 12

Divers

12.1 L'exécation du présent AGS n'entraîne en principe aucun frais spécifique.

12.2 En cas de frais éventuels, chaque Partie en supporte la charge dans le cadre et dans la limite de ses disponibilités budgétaires.

12.3 Chaque Partie et les Autorités de l'Etat concemé assistent le personnel foumissant des services et/ou exerçant des droits dans l'Etat de l'autre Partie conformément aux dispositions du présent AGS.

12.4 En tant que de besoin, les ANS/ASD des Parties se consultent au sujet des aspects techniques spécifiques concernant l'application du present AGS, et peuvent conclure, au cas par cas, de protocoles de sécurité spécifiques visant à compléter le présent AGS.

ARTICLE 13

Dispositions finales

13.1 Le present AGS remplace l'Accord de sécurité entre le Gouvernement du Royaume de Suède et le Gouvernement de la République française, relatif à certains échanges d'informations à caractère secret, signé à Stockholm le 22 octobre 1973.

13.2 Le présent AGS est conclu pour une durée indéterminée. Chacune des Parties notifie à l'autre l'accomplissement des procédures internes requises en ce qui la concerne pour l'entrée en vigueur du présent AGS qui prend effet le premier jour du second mois suivant la réception de la dernière des notifications.

13.3 Le présent AGS peut être dénoncé d'un commun accord ou unilatéralement, la dénonciation prenant effet six (6) mois après réception de la notification écrite. Après la dénonciation, les Parties restent responsables de la protection de l'ensemble des Informations classifiées échangées en vertu des dispositions du présent AGS.

13.4 Chaque Partie communique rapidement à l'autre toute modification de ses lois et réglementations nationales susceptible d'avoir un effet sur la protection d'informations classifiées en vertu du présent AGS. Dans ce cas, les Parties se concertent afin d'examiner d'éventuelles modifications au présent AGS. Dans l'intervalle, les Informations classifiées restent protégées conformément aux présentes dispositions.

13.5 Les dispositions du présent AGS peuvent être modifiées d'un commun accord par écrit entre les Parties. Ces modifications prennent effet selon les modalités prévues au paragraphe 13.2.

13.6 Tout litige quant à l'interprétation ou l'application du présent AGS est exclusivement résolu dans le cadre d'une consultation entre les Parties, sans faire appel à aucune tierce partie ou tribunal international.

EN FOI DE QUOl, les soussignés, dûment autorisés à cet effet par leur Gouvernement respectif, ont signé le présent. AGS.

Fait à Stockholm le 16 mars 2006 en double exemplaire, en langues suédoise et française, les deux textes faisant egalement foi.

Pour le Gouvernement du Royaume de Suède
Helena Lindberg

Pour le Gouvernement de la République française
Denis Delbourg

Edita Stockholm 2007