Sveriges internationella överenskommelser

ISSN 1102-3716

Utgiven av Utrikesdepartementet

SÖ 2004: 8

Nr 8
Avtal med Amerikas förenta stater om tillämpning av säkerhetsskyddsavtal för industriell verksamhet mellan Konungariket Sveriges regering, företrädd av Försvarets materielverk, och Förenta staternas försvarsdepartement
Washington den 20 maj 2004

Regeringen beslutade den 4 mars 2004 att underteckna avtalet. Avtalet trädde i kraft vid undertecknandet, den 20 maj 2004.

AVTAL OM TILLÄMPNING AV SÄKERHETSSKYDDSAVTAL FÖR INDUSTRIELL VERKSAMHET MELLAN KONUNGARIKET SVERIGES REGERING, FÖRETRÄDD AV FÖRSVARETS MATERIELVERK, OCH FÖRENTA STATERNAS FÖRSVARSDEPARTEMENT

1. SYFTE

a. Följande förfaranden har utarbetats av Konungariket Sveriges regering företrädd av Försvarets materielverk (FMV) och Förenta staternas försvarsdepartement (DOD), nedan kallade "parterna," för genomförande av bestämmelserna i den allmänna överenskommelsen med Amerikas Förenta Stater om sekretesskydd av militär information mellan Konungariket Sveriges regering och Förenta staternas regering, som trädde i kraft den 23 december 1981, och ersätter Security Procedures for Industrial Operations between the Supreme Commander of the Swedish Armed Forces and the Department of Defense of the United States (Industrial Security Annex) av den 16 februari 1982. 1981 års överenskommelse innehåller bestämmelser om skydd av sekretessbelagd militär information som utväxlas mellan regeringarna. Detta tillämpningsavtal (nedan kallat avtalet) kommer att vara tillämpligt på de fall där kontrakt, underleverantörskontrakt, avtalsförhandlingar eller andra av regeringen godkända överenskommelser som innehåller parternas sekretessbelagda information genomförs eller ingås av FMV eller på dess vägnar i Förenta staterna eller av DOD eller för dess räkning i Sverige.

b. Vardera parten skall inom ramen för sin nationella lagstiftning vidta alla nödvändiga åtgärder för att se till att sekretessbelagd information eller materiel som tillhandahållits enligt detta avtal skyddas.

c. I Sverige är den behöriga säkerhetsmyndigheten (DSA) FMV (Försvarets materielverk). DOD utser härmed Deputy Under Secretary of Defense (Technology Security Policy & Counterproliferation) som sin DSA för att utöva övergripande tillsyn avseende bestämmelserna i detta avtal.

2. DEFINITIONER

I detta avtal används följande beteckningar med de betydelser som här anges:

– *sekretessbelagt kontrakt*: ett kontrakt som innebär, eller kommer att innebära, att en leverantör eller dess anställda måste få tillgång till sekretessbelagd information vid genomförandet av ett kontrakt.

– *sekretessbelagd information*: officiell information eller materiel som i den överlåtande eller ägande regeringens nationella säkerhetsintresse och i enlighet med tillämpliga nationella lagar och bestämmelser behöver skyddas mot otillåtet röjande och som har sekretessbelagts av en behörig säkerhetsmyndighet. Den omfattar all information, oavsett form, innefattande skriftlig, muntlig eller visuell, eller i form av materiel.

– *försvarsmaterielansvarig säkerhetsmyndighet (CSO)*: den eller de statliga myndigheter som har utsetts att handha den industriella säkerheten vid en leverantörs anläggning.

– *kontrakt*: en verkställbar överenskommelse att tillhandahålla varor eller tjänster.

– *leverantör*: en fysisk eller juridisk eller annan person som samtycker till att tillhandahålla varor eller tjänster.

– *behörig regeringsföreträdare (DGR)*: en person eller en myndighet som har utsetts att företräda den avsändande eller mottagande parten vid överföring eller godkännande av överföring av sekretessbelagd information från regering till regering.

– *behörig säkerhetsmyndighet (DSA)*: den regeringsmyndighet som ansvarar för säkerheten för sekretessbelagd information som omfattas av detta avtal.

– *handling*: skrivelse, anteckning, protokoll, redogörelse, promemoria, meddelande, teckning, fotografi, film, karta, grafisk framställning, plan, anteckningsbok, stencil, karbonpapper, skrivmaskinsband, diskett, magnetband eller annan form av bevarad information.

– *försäkran om säkerhetsklarering för verksamhetsställe (FSCA)*: ett intyg som utfärdas av en DSA eller CSO för en leverantörs verksamhetsställe enligt dess territoriella behörighet där det anges att verksamhetsstället är säkerhetsklarerad på en viss nivå och att lämpligt säkerhetsskydd på en viss nivå även har införts för att skydda sekretessbelagd information. En FSCA innebär även att sekretessbelagd information med beteckningen CONFIDENTIAL eller högre kommer att skyddas av den leverantör till vilken FSCA utfärdats i enlighet med bestämmelserna i detta avtal samt att efterlevnaden skall övervakas och upprätthållas av ansvarig DSA eller CSO. En FSCA krävs inte för en leverantör som åtar sig kontrakt som innebär att sekretessbelagd information på nivån HEMLIG/RESTRICTED tas emot eller framställs.

– *överföring mellan regeringar*: principen att sekretessbelagd information och materiel med beteckningen CONFIDENTIAL och högre kommer att överföras genom officiella kanaler mellan regeringar eller genom andra kanaler som de sändande och mottagande parterna skriftligen kan komma överens om.

– *materiel*: alla handlingar, produkter eller ämnen som kan förses med eller innehålla information. Materiel omfattar allt, oberoende av fysisk art eller beskaffenhet, inbegripet men ej begränsat till, handlingar, skrifter, hårdvara, utrustning, maskiner, apparater, anordningar, modeller, fotografier, upptagningar, reproduktioner, anteckningar, skisser, planer, prototyper, ritningar, figurer, kartor och brev samt alla andra produkter, ämnen eller föremål från vilka information kan erhållas.

– *behov av information*: ett beslut som fattas av en behörig innehavare av sekretessbelagd information att en framtida mottagare behöver ta del av viss sekretessbelagd information för att genomföra eller biträda i en lagenlig och godkänd myndighetsfunktion.

– *part*: i Sverige avser part den regering som företräds av FMV (inbegripet organ och myndigheter under Sveriges försvarsdepartement). I Förenta staterna avser part försvarsdepartementet (inbegripet dess myndigheter och enheterna för armén, flottan och flygvapnet).

– *försäkran om säkerhetsklarering för personal (PSCA)*:

a. För en person som är anställd av ett regeringsorgan eller vid en leverantörs verksamhetsställe som lyder under en DSA eller CSO, skall en försäkran från denna DSA eller CSO utfärdas angående nivån på den säkerhetsklarering för personal som innehas av denna person.

b. För en person som är medborgare i en part men skall anställas av den andra parten eller av dess leverantörer, en försäkran från DSA eller CSO i det land där den personen är medborgare om att personen är berättigad till säkerhetsklarering till en nivå som den begärande parten anger.

– *mottagande part*: den part till vilken sekretessbelagd information överförs.

– *sändande part*: den part som överför sekretessbelagd information till den mottagande parten.

3. INSKRÄNKNINGAR I FRÅGA OM UTNYTTJANDE OCH RÖJANDE AV UTVÄXLAD SEKRETESSBELAGD INFORMATION

a. Om inte föregående särskilt skriftligt tillstånd lämnas om motsatsen, får den mottagande parten inte röja eller utnyttja eller tillåta röjande eller utnyttjande av sekretessbelagd information utom för de ändamål och med de begränsningar som angivits av den sändande parten.

b. Den mottagande parten får inte till en offentlig tjänsteman, leverantör, dennes anställda eller någon annan person som är medborgare i tredje land, eller till internationell organisation förmedla eller röja sekretessbelagd information med beteckningen CONFIDENTIAL eller högre som tillhandahållits enligt bestämmelserna i det allmänna avtalet eller detta avtal, eller offentligen röja sekretessbelagd information utan föregående skriftligt tillstånd från den sändande parten.

c. Ingen bestämmelse i detta avtal skall tolkas som ett bemyndigande eller vara bestämmande för att tillkännage, utnyttja, utväxla eller röja information i vilken immateriell äganderätt förekommer förrän särskilt skriftligt tillstånd har erhållits av rättsinnehavaren.

4. SKYDD AV SEKRETESSBELAGD INFORMATION

När den mottagande parten mottar sekretessbelagd information som lämnats i enlighet med detta avtal, skall den förbinda sig att ge informationen minst samma grad av säkerhetsskydd som den sändande parten. Den mottagande parten skall vara ansvarig för information som mottagits på detta sätt medan den är inom dess regerings territoriella jurisdiktion och medan den innehas av eller lämnas till personer som har tillstånd att göra utlandsbesök enligt detta avtal. I Sverige är

FMV försvarsmaterielansvarig säkerhetsmyndighet (CSO) och i Förenta staterna är Defense Security Service (DSS) försvarsmaterielansvarig säkerhetsmyndighet (CSO). Dessa organisationer skall ikläda sig ansvaret för att säkerställa handhavandet av säkerhetsåtgärder för ett kontrakt som innehåller sekretessbelagd information med beteckningen CONFIDENTIAL eller högre och som tilldelas industrin för utförande i deras respektive länder. Sekretessbelagd information på den svenska nivån HEMLIG/RESTRICTED skall skyddas i USA i enlighet med bestämmelserna i tillägg A.

a. Rätt att ta del. Rätt att ta del av sekretessbelagd information med beteckningen CONFIDENTIAL eller högre skall vara förbehållen personer som har behov av den och som har genomgått säkerhetsklarering av endera av parterna i enlighet med dess nationella lagar och bestämmelser på minst samma nivå som säkerhetsgraden hos den information varav del skall tas.

b. Inspektion/säkerhetsgranskning. CSO, som definierats ovan, skall se till att industriella inspektioner/säkerhetsgranskningar görs regelbundet av varje leverantörs verksamhetsställe som är belägen och registrerad för affärsverksamhet inom deras land och som utför eller förhandlar om ett sekretessbelagt kontrakt.

c. Säkerhetskostnader. Kostnader som uppkommer för genomförandet av inspektioner/granskningar skall täckas av den part som utför tjänsten. Kostnader som uppkommer för endera parten på grund av genomförande av andra säkerhetsåtgärder, inbegripet kostnader som uppkommer på grund av nyttjande av diplomatisk kurirtjänst eller någon annan behörig officiell budtjänst kommer inte att återbetalas. Det skall finnas bestämmelser i sekretessbelagda kontrakt om säkerhetskostnader som uppkommer enligt kontraktet, till exempel särskilda kostnader för paketering, transport och liknande, som skall täckas av den part som har behov av tjänsten enligt kontraktet. Om säkerhetsbeteckningen eller säkerhetskraven enligt kontraktet ändras efter avtalsdagen, och säkerhetskostnaderna därmed ökas eller minskas, skall de bestämmelser i kontraktet som eventuellt påverkas justeras på ett skäligt sätt på grund av sådana ökade eller minskade kostnader. Sådana skäliga justeringar skall göras på grundval av de bestämmelser i kontraktet som rör ändringar.

d. Säkerhetsklareringar. Klareringar av leverantörs verksamhetsställe och av personer som kommer att inneha eller ges tillstånd att få ta del av sekretessbelagd information i samband med ett sekretessbelagt kontrakt eller ett potentiellt sekretessbelagt kontrakt skall genomföras enligt de relevanta bestämmelserna i det land som ansvarar för handhavandet av säkerhetsåtgärderna för det sekretessbelagda kontraktet.

e. Anvisningar. CSO skall se till att leverantörer eller underleverantörer som har rätt att ta del av sekretessbelagd information får instruktioner som fastställer deras ansvar att skydda informationen i enlighet med tillämpliga nationella lagar och bestämmelser som motsvarar bestämmelserna i detta avtal.

5. ÖVERFÖRING AV SEKRETESSBELAGD INFORMATION

a. Sekretessbelagd information med beteckningen CONFIDENTIAL och högre skall normalt överföras mellan parterna genom DGR med användning av kanaler mellan regeringarna. Kanaler mellan regeringarna är officiella regeringskanaler (t.ex. diplomatisk kurirtjänst). Andra kanaler som får upprättas, om parterna skriftligen kommer överens om det, skall säkerställa att

regeringens ansvar och kontroll upprätthålls från ursprungsplatsen till slutdestinationen. CSO för varje sekretessbelagt kontrakt skall godkänna förfarandena, eller underrätta leverantören om vilka kanaler för överföring som skall användas och fastställa DGR. Materiel skall förberedas för överföring i enlighet med den sändande partens nationella lagar och bestämmelser om säkerhetsskydd.

b. Sekretessbelagd information med beteckningen CONFIDENTIAL och högre som skall överföras elektroniskt skall förmedlas på säkert sätt som har godkänts av båda parternas kommunikationssäkerhetsmyndigheter.

c. Sekretessbelagd information på den svenska nivån HEMLIG/RESTRICTED kommer att förmedlas i USA i enlighet med bestämmelserna i tillägg A.

6. UTLÄMNING AV INFORMATION

En leverantörs eller underleverantörs utlämning av sekretessbelagd information med beteckningen CONFIDENTIAL eller högre som hänför sig till ett sekretessbelagt kontrakt skall i Sverige regleras genom ett säkerhetsskyddsavtal (SA) som innehåller en Industrisäkerhetsskyddsmanual (ISM) mellan leverantören eller underleverantören och den svenska parten och i USA genom National Industrial Security Program Operating Manual (NISPOM), DOD 5220.22-M. För ett svensk verksamhetsställe med ett sekretessbelagt USA-kontrakt skall förhandsinspektionen och godkännandet regleras genom svenska SA och ISM med slutligt godkännande av USA:s behöriga myndighet. För ett verksamhetsställe i USA med ett svenskt sekretessbelagt kontrakt skall förhandsinspektion och godkännande regleras genom NISPOM med slutligt godkännande av den svenska parten.

7. MÄRKNING

a. Den sändande parten skall se till att handlingar som innehåller sekretessbelagd information märks med lämplig sekretessbeteckning och med ursprungs- eller ägarlandets namn framför innan överföring sker till den mottagande parten. Vid mottagandet skall informationen, om nödvändigt, märkas med motsvarande sekretessbeteckning, enligt nedan. Om sådan information senare ingår i andra handlingar, skall dessa handlingar märkas så att den sändande parten och den tillämpliga beteckningen kan identifieras.

Tabell över motsvarande sekretessbeteckningar

Sverige	Förenta staterna
KVALIFICERAT HEMLIG	TOP SECRET
HEMLIG/SECRET	SECRET
HEMLIG/CONFIDENTIAL	CONFIDENTIAL
HEMLIG/RESTRICTED	Ingen motsvarighet (Se tillägg A)

b. På sekretessbelagd information som framställs eller återges av en mottagande part skall anges om den innehåller information från främmande makt. Märkningarna skall anbringas på det sätt som anges i bestämmelserna i det land där informationen framställs eller återges.

8. KONTRAKT

När en part avser att göra en beställning, eller bemyndigar en leverantör i sitt land att göra en beställning, som innefattar sekretessbelagd information med beteckningen CONFIDENTIAL eller högre hos en leverantör i den andra partens land, skall den part som avser att göra en beställning, eller bemyndigar leverantören att göra en sådan beställning, vid behov begära en FSCA från det andra landets CSO. I en FSCA skall ingå en förbindelse att den klarerade leverantörens handhavande av sekretess kommer att stå i överensstämmelse med nationella sekretesslagar och bestämmelser och övervakas av dess CSO.

a. Klausul om säkerhetskrav

1. Den ansvariga myndigheten i den part som förhandlar om ett sekretessbelagt kontrakt som skall utföras inom det andra landet och varje leverantör som innehar ett sekretessbelagt kontrakt eller förhandlar om ett sekretessbelagt underleverantörskontrakt som skall utföras inom det andra landet skall införliva lämpliga säkerhetsklausuler i kontraktet, anbudsinfordran eller underleverantörskontraktet. För sådan verksamhet som innehåller sekretessbelagd information på nivån CONFIDENTIAL eller högre skall de säkerhetsklausuler som återfinns i tillägg B användas.

2. En kopia av de relevanta delarna av kontraktet, anbudsinfordran eller underleverantörskontraktet, skall, tillsammans med klausulerna om säkerhetskrav, omedelbart genom lämpliga kanaler lämnas till den CSO där beställningen görs för att de skall kunna utöva tillsyn.

3. Kontrakt som ingås med leverantörer i USA och som innehåller sekretessbelagd information på den svenska nivån HEMLIG/RESTRICTED skall innehålla en klausul om krav på särskilda villkor där det anges vilka åtgärder som skall tillämpas för att skydda den svenska informationen med beteckningen HEMLIG/RESTRICTED.

b. Anvisningar om säkerhetsklassificering. Den beställande regeringens vederbörande myndighet (se 8 a 1 ovan) skall förse leverantören eller underleverantören med de anvisningar om sekretessklassificering som hänför sig till varje sekretessbelagd aspekt som rör kontraktet. För Sveriges del skall dessa anvisningar läggas fram i en säkerhetsskyddsplan eller programsäkerhetsinstruktioner (PSI) tillsammans med en handledning för säkerhetsklassificering och i USA genom en Contract Security Classification Specification (DD Form 254). I anvisningarna måste den sekretessbelagda information som lämnas av den beställande parten i samband med kontraktet, eller som framställs till följd av det sekretessbelagda kontraktet, identifieras och ges rätt sekretessbeteckning. Två exemplar av de skriftliga anvisningarna om sekretessklassificering och av de skyddade delarna av det sekretessbelagda kontraktet, eller anbudsinfordran, eller underleverantörskontrakt som innehåller klausulen om säkerhetskrav skall överlämnas till CSO i den part som ansvarar för handhavandet av säkerhetsåtgärder. Adresserna till CSO är följande:

Sverige

Försvarets materielverk – FMV
Defence Materiel Administration
Security
Banérgatan 62
SE-115 88 Stockholm
SVERIGE

Förenta staterna

Defense Security Service
Attn: Deputy Director for Industrial Security
Department of Defense
1340 Braddock Place
Alexandria, Virginia 22314-1651
AMERIKAS FÖRENTA STATER

c. Underleverantörskontrakt. Om det inte är uttryckligen förbjudet i det sekretessbelagda kontraktet får en leverantör ingå underleverantörskontrakt inom sitt eget land i enlighet med de säkerhetsföreskrifter som gäller i dess land för sekretessbelagda underleverantörskontrakt och inom den beställande partens land enligt de föreskrifter som upprättas genom detta avtal för att ingå ett sekretessbelagt huvudkontrakt i det landet, i enlighet med de klausuler som anges i tillägg B till detta avtal.

d. Utländskt ägande, utländsk kontroll eller påverkan. Företag som enligt nationella säkerhetsmyndigheter står under finansiell, administrativ, policy- eller ledningskontroll av medborgare eller andra enheter i en tredje parts land får delta i ett kontrakt eller underleverantörskontrakt som innebär att tillgång måste ges till sekretessbelagd information som tillhandahålls av den andra parten endast när verkställbara åtgärder är i kraft för att säkerställa att medborgare eller andra enheter i tredje parts land inte får tillgång till sekretessbelagd information som tillhandahålls eller som framställs därav. Om inte verkställbara åtgärder är i kraft för att förhindra att medborgare eller andra enheter i tredje parts land får tillgång till information, skall ursprungspartens tillstånd erhållas innan sådan tillgång medges.

e. Företagsstyrning. FMV samtycker till att övervaka genomförandet av styrelsebeslut som fattas av svenska enheter i samband med DOD:s Special Security Agreements (SSAs). FMV samtycker även till att bistå DOD med att åtgärda svenska företags påstådda överträdelser av DOD:s SSA-bestämmelser. Dessa överenskommelser grundas på förutsättningen att DOD skall övervaka att styrelsebeslut/överenskommelser som fattas eller ingås av enheter i USA i samband med FMV krav avseende reglering av utländskt ägande, utländsk kontroll eller påverkan av svenska enheter som innehar svenska säkerhetsklareringar efterlevs, och att DOD skall bistå FMV med att åtgärda överträdelser av dessa bestämmelser av enheter i USA.

9. BESÖK

Framställningar om besökstillstånd skall överlämnas enligt de förfaranden som anges i tillägg C. Besökstillstånd skall lämnas endast till personer som innehar säkerhetsklarering på minst den sekretessnivå till vilken tillgång kommer att ges. Tillstånd för besökare att få ta del av sekretessbelagd information kommer att begränsas till dem som har behov av den.

10. SÄKERHETSGARANTIER SOM RÖR NATIONELLA SÄKERHETSKLARERINGAR AV VERKSAMHETSSTÄLLEN ELLER MEDBORGARE I DET ANDRA LANDET

a. Vardera parten skall på begäran av den andra parten utfärda en FSCA eller PSCA för verksamhetsställen eller personer i sitt land.

b. Den part som mottar begäran skall på begäran avgöra säkerhetsläget för det verksamhetsställe eller den person som förfrågan avser och översända en FSCA eller PSCA om verksamhetsstället eller medborgaren redan är klarerad. Om verksamhetsstället eller medborgaren inte har en säkerhetsklarering, eller om verksamhetsstället eller personen har en klarering på en lägre nivå än den som begärts, skall meddelande sändas till den begärande parten att FSCA eller PSCA inte kan utfärdas utan vidare samråd. I sådana fall får ytterligare åtgärder vidtas för att göra de undersökningar som är nödvändiga för att uppfylla kravet.

c. Om den part som mottar begäran avgör att ett verksamhetsställe som är beläget och registrerat för affärsverksamhet i dess land inte är berättigat till en säkerhetsklarering, skall den begärande parten underrättas.

d. Om endera parten får någon negativ information om ett verksamhetsställe eller person för vilken den har utfärdat en FSCA eller PSCA, skall den underrätta den andra parten om vad för slags information det gäller och om vilka åtgärder den avser att vidta, eller har vidtagit. Endera parten får begära omprövning av en FSCA eller PSCA som har utfärdats av den andra parten, under förutsättning att begäran åtföljs av en motivering. Den begärande parten skall underrättas om resultaten av omprövningen och om eventuella vidare åtgärder.

e. Om en av parterna ogiltigförklarar, upphäver eller vidtar åtgärder för att dra in en säkerhetsklarering för personal eller för ett verksamhetsställe, skall den part som begärde en PSCA eller FSCA underrättas och delges motiven för dessa åtgärder.

f. Vardera parten skall, på begäran av den andra parten, samarbeta vid omprövningar och undersökningar som rör säkerhetsklareringar.

11. FÖRLUST ELLER BEFARAD FÖRLUST

a. I händelse av förlust eller befarad förlust av sekretessbelagd information med beteckningen CONFIDENTIAL eller högre, eller misstanke om att sådan sekretessbelagd information har utsatts för fara, skall den mottagande parten omedelbart underrätta den sändande parten.

b. Den mottagande parten skall omedelbart genomföra en undersökning, med biträde av den sändande parten, om så begärs, i enlighet med gällande lagar och bestämmelser i den mottagande parten. Den mottagande parten skall så snart som möjligt underrätta den sändande parten om omständigheterna och resultatet av undersökningen samt om vilka åtgärder som vidtagits för att förhindra en upprepning av det inträffade.

12. TVISTER

Tvister om tolkningen eller tillämpningen av detta avtal skall lösas genom samråd mellan parterna och inte hänskjutas till nationell eller internationell domstol eller tredje man för lösande.

13. IKRAFTTRÄDANDE

Detta tillämpningsavtal till 1981 års allmänna överenskommelse med Amerikas Förenta Stater om sekretesskydd av militär information ersätter Security Procedures for Industrial Operations between the Supreme Commander of the Swedish Armed Forces and the Department of Defense of the United States (Industrial Security Annex) av den 16 februari 1982 och träder i kraft när båda parter undertecknar det.

14. UPPSÄGNING OCH ÖVERSYN

a. Detta avtal skall förbli i kraft tills 1981 års allmänna överenskommelse med Amerikas Förenta Stater om sekretesskydd av militär information upphört att gälla , eller tills någon av parterna sagt upp avtalet efter att ha gett den andra parten sex månaders skriftlig varsel om sin avsikt att säga upp avtalet. Detta avtal får även sägas upp när som helst efter båda parternas skriftliga samtycke. Sedan avtalet har upphört att gälla skall båda parter vara ansvariga för skyddet av all sekretessbelagd information som har utbytts enligt bestämmelserna i 1981 års överenskommelse med Amerikas Förenta Stater om sekretesskydd av militär information och detta avtal samt eventuella kontrakt som ingåtts, eller genererats av detta, i enlighet med nationella lagar och bestämmelser.

b. Parterna skall gemensamt göra en översyn av detta avtal senast fem (5) år efter dess ikraftträdande.

c. All sekretessbelagd information som utväxlats med stöd av detta avtal skall skyddas även om förmedlingen har skett efter det att någon av parterna har sagt upp avtalet.

d. I fall av uppsägning skall utestående frågor lösas genom samråd mellan de båda parterna.

15. UNDERTECKNANDE

a. Ovanstående är en överenskommelse mellan Konungariket Sveriges regering företrädd av FMV och försvarsdepartementet i Amerikas förenta stater om de frågor som avses i detta avtal.

b. Till bekräftelse härav har undertecknade, därtill vederbörligen befullmäktigade av sina regeringar, undertecknat detta avtal.

c. Upprättat i Washington, D.C. den 20 maj 2004, på engelska och svenska, vilka båda texter äger lika giltighet.

För Konungariket Sveriges regering
Försvarets materielverk

Jan-Olof Lind

T.f. Generaldirektör
Försvarets materielverk

För Amerikas förenta staters
försvarsdepartement

Lisa Bronson

Deputy Under Secretary of Defense for
Technology Security Policy and
Counterproliferation

Tillägg till tillämpningsavtalet mellan Sverige och USA:

A. Rutiner för hantering av svensk information med beteckningen HEMLIG/RESTRICTED inom Förenta staterna
B. Klausuler om säkerhetsskyddskrav
C. Besöksrutiner

TILLÄGG A

RUTINER FÖR HANTERING AV SVENSK INFORMATION MED BETECKNINGEN HEMLIG/RESTRICTED INOM FÖRENTA STATERNA

1. Svenska handlingar eller materiel med beteckningen HEMLIG/RESTRICTED skall vid mottagandet i USA hanteras som USA:s UNCLASSIFIED information som är undantagen från offentliggörande enligt en eller flera lagar i USA. Till dessa lagar hör Freedom of Information Act (FOIA) och Title 10 U.S.C. Section 130(c), "Nondisclosure of Information: Certain Sensitive Information of Foreign Governments and International Organizations." Handlingar eller materiel med denna märkning skall arkiveras i låsta skåp som ger lämpligt skydd eller i låsta utrymmen som förhindrar att obehörig personal får tillträde.

2. Svenska handlingar med beteckningen HEMLIG/RESTRICTED skall hanteras på ett sätt som förhindrar öppet offentliggörande, tillgång eller användning för annat än officiella regeringsändamål i Förenta staterna eller Sverige.

3. Innan något kommunikations- och informationssystem tillåts arkivera, behandla eller vidarebefordra svensk information med beteckningen HEMLIG/RESTRICTED, måste den erhålla säkerhetsgodkännande, så kallad ackreditering. En ackreditering är ett formellt erkännande av vederbörande myndighet att användningen av ett system uppfyller erforderliga säkerhetskrav och inte utgör någon oacceptabel risk. För system med fristående bordsdatorer och bärbara datorer som används vid DOD:s anläggningar fungerar systemets registreringsbevis tillsammans med säkra driftsmetoder som den erfordrade ackrediteringen. För leverantörer skall anvisningar om hur man använder informationstekniska system införlivas i kontraktets klausul om krav på särskilda villkor.

4. Svenska handlingar med beteckningen HEMLIG/RESTRICTED skall befordras med första klass post inom Förenta staterna i ett säkert omslag/kuvert. Befordran utanför Förenta staterna skall ske i två säkra omslag/kuvert, varvid det inre omslaget/kuvertet märks "Swedish HEMLIG/RESTRICTED". Sådan befordran skall ske med befordringssätt som kan spåras, till exempel kommersiella kurirer eller andra befordringssätt som Sverige skriftligen har godkänt.

5. Andra oklassificerade handlingar från USA som härrör från ett regeringsorgan i USA och som innehåller information som Sverige har klassificerat HEMLIG/RESTRICTED skall på omslaget och på första sidan vara märkta "Swedish HEMLIG/RESTRICTED – Exempt from Public Disclosure under Title 10 U.S.C., Section 130(c)." Den del av handlingen som innehåller svensk information med beteckningen HEMLIG/RESTRICTED skall också anges i handlingarna.

6. Svensk information med beteckningen HEMLIG/RESTRICTED får befordras eller göras tillgänglig i elektronisk form via ett sådant allmänt nät som Internet, med användning av statliga eller kommersiella krypteringsanordningar som parternas statliga säkerhetsmyndigheter ömsesidigt kommit överens om. Telefonsamtal, videokonferenser eller fax som innehåller svensk information med beteckningen HEMLIG/RESTRICTED får vara i klartext, om det inte finns något tillgängligt godkänt krypteringssystem.

TILLÄGG B

KLAUSUL OM SÄKERHETSSKYDDSKRAV SOM SKALL INGÅ I SEKRETESSBELAGDA KONTRAKT SOM INNEHÅLLER SEKRETESSBELAGD INFORMATION MED BETECKNINGEN CONFIDENTIAL ELLER HÖGRE

Bestämmelserna i denna klausul grundas på den allmänna överenskommelsen med Amerikas Förenta Stater om sekretesskydd av militär information mellan Konungariket Sveriges regering och Förenta staternas regering och skall tillämpas i den mån detta kontrakt medför tillgång till eller innehav av information eller materiel som har försetts med sekretessbeteckningen CONFIDENTIAL och högre av den regering där informationen har sitt ursprung (nedan kallad ursprungsregeringen).

1. All sekretessbelagd information och materiel som tillhandahålls eller genereras enligt detta kontrakt skall skyddas på följande sätt:

a. Mottagaren får inte lämna ut informationen eller materielen till en regering, person eller företag i tredje land utan föregående godkännande från ursprungsregeringen.

b. Mottagaren skall ge informationen och materielen minst samma sekretessgrad som ursprungsregeringen har givit den enligt nedanstående tabell. Mottagen information skall märkas med den sekretessgrad som den part som informationen härrör ifrån har givit den och med uppgift om ursprungslandet.

c. Mottagaren får inte använda informationen och materielen för annat ändamål än det för vilket den tillhandahölls utan föregående skriftligt medgivande från den part från vilken den härrör.

2. Sekretessbelagd information och materiel som lämnas eller genereras enligt detta kontrakt skall överföras genom kanaler mellan regeringar eller andra kanaler som Förenta staternas och Konungariket Sveriges regeringar ömsesidigt skriftligen godkänt. Rätt att ta del av sekretessbelagd information och materiel skall endast beviljas personer som har en säkerhetsklarering som minst motsvarar informationens sekretessgrad och som i sin tjänst har behov av att få ta del av informationen för att fullgöra kontraktet.

3. Mottagaren skall märka om sekretessbelagd information och materiel som tillhandahållits enligt detta kontrakt med sin regerings motsvarande sekretessbeteckning.

4. Sekretessbelagd information och materiel som genereras enligt detta kontrakt skall ges en sekretessbeteckning enligt kontraktets förteckning över sekretessbeteckningar.

5. Leverantören skall omedelbart och utförligt till sin regerings säkerhetsmyndigheter rapportera alla fall där det är känt eller finns anledning att tro att sekretessbelagd information eller materiel som tillhandahållits eller genererats enligt detta kontrakt har utsatts för säkerhetsbrott eller fara, förkommit eller röjts för obehöriga.

6. Sekretessbelagd information och materiel som tillhandahållits eller genererats enligt detta kontrakt får inte lämnas vidare till en annan eventuell leverantör eller underleverantör om inte

a. en eventuell leverantör eller underleverantör som är belägen i USA eller Sverige har godkänts för rätt att ta del av sekretessbelagd information och materiel på erforderlig nivå av USA:s eller Sveriges säkerhetsmyndigheter, eller,

b. om den är belägen i tredje land, har erhållit föregående skriftligt medgivande från USA:s eller Sveriges regering, beroende på vilken regering informationen härrör från.

7. Den mottagande leverantören skall i alla underleverantörskontrakt enligt detta kontrakt som medför tillgång till sekretessbelagd information som tillhandahållits eller genererats enligt detta kontrakt införa villkor som i allt väsentligt överensstämmer med lydelsen i dessa klausuler, inbegripet denna klausul.

8. När kontraktet har fullgjorts skall all sekretessbelagd information eller materiel som tillhandahållits eller genererats enligt kontraktet antingen förstöras av leverantören i enlighet med nationella lagar och bestämmelser eller, om så begärs, återlämnas till den regering som tillhandahöll informationen.

Tabell över motsvarande sekretessbeteckningar

Sverige	Förenta staterna
KVALIFICERAT HEMLIG	TOP SECRET
HEMLIG/SECRET	SECRET
HEMLIG/CONFIDENTIAL	CONFIDENTIAL
HEMLIG/RESTRICTED	Ingen motsvarighet (Se tillägg A)

TILLÄGG C

BESÖK

1. I detta tillägg beskrivs de rutiner som skall användas vid handläggning av framställningar om besök. Besök skall godkännas i förväg av båda parter enligt förfarandena i detta tillägg.

2. Nedan angivna myndigheter har av vardera parten utsetts att handlägga framställningar om besök som mottas från den andra parten. De förtecknade myndigheterna kallas nedan centrala besökskontor (CVO).

Sverige

Försvarets materielverk – FMV
Swedish Defence Materiel Administration
Security
Banérgatan 62
SE-115 88 Stockholm
SVERIGE

Totalförsvarets Forskningsinstitut – FOI
Swedish Defence Research agency
Ranhammarsvägen 14
SE-172 90 Stockholm
SVERIGE

Försvarsmakten – Högkvarteret
Swedish Armed Forces Headquarters
Protocol
Lidingövägen 24
SE-107 85 Stockholm
SVERIGE

Förenta staterna:

Department of the Army
Office of the Deputy Chief of Staff for Intelligence
Attn: Foreign Liaison Directorate (DAMI-FL)
Washington, D.C. 20310-1040
Amerikas förenta stater

Department of the Navy
Navy International Programs Office
Foreign Disclosure Policy Control Division (Navy IPO-10)
Washington, D.C. 20350-5000
Amerikas förenta stater

Department of the Air Force
Office of the Deputy Under Secretary of the Air Force
(International Affairs)
Foreign Disclosure & Technology Transfer Division (SAF/IAPD)
1010 Air Force Pentagon
Washington, D.C. 20330-1010
Amerikas förenta stater

Defense Intelligence Agency
Foreign Liaison Staff
(DIA/PO-FL)
Washington, D.C. 20301-6111
Amerikas förenta stater

(Defense Intelligence Agency handlägger besök till Office of the Secretary of Defense (OSD), OSD:s personal, Department of Defense Agencies och "Joint Staff" samt deras leverantörer.)

3. Framställningar om beviljande av besökstillstånd skall innehålla följande information:

a. Begärande regeringsorgan/leverantör . Ange fullständigt namn och postadress (inklusive stad, land och postnummer, samt i Amerikas Förenta Stater, inkluderande stat) och telefon- och faxnummer.

b. Regeringsorgan eller industriell anläggning som skall besökas. Ange fullständigt namn, titel och besöksadress (gata, stad, land och postnummer, samt i Amerikas Förenta Stater, inkluderande stat) samt telefon- och faxnummer, e-postadress och namn på den person med vilken mötet skall hållas (kontaktperson).

c. Tid för besöket. Ange tidpunkt eller period (från datum till datum) för besöket (dag-månad-år).

d. Typ av besök. Ange om besöket är ett regeringsinitiativ eller kommersiellt initiativ och om besöket sker på initiativ av begärande regeringsorgan/leverantör eller av regeringsorgan/leverantör som skall besökas. Regeringsinitiativ skall bara anges om besöket sker med anledning av ett godkänt statligt program, vilket måste beskrivas fullständigt i punkt g nedan.

e. Ämne som skall diskuteras/motivering. Ge en kortfattad beskrivning av de frågor eller ämnen som skall diskuteras och anledningen till besöket. Använd inte oförklarade förkortningar. Vid en framställning om återkommande besök skall återkommande besök anges som de första orden i dataelementet (t.ex. Återkommande besök för att diskutera ...) eller vid en ändring (Ändring av besök ID-nummer...).

f. Förväntad nivå på den sekretessbelagda information som kommer att beröras. Ange tillämplig nivå, TOP SECRET, SECRET, CONFIDENTIAL, och det land som informationen härrör från.

g. Besökets relevans. Ange fullständigt namn på det statliga programmet, avtalet eller försäljningskontraktet (t.ex. "Foreign Military Sales case") eller anbudsinfordran och använd bara vanligt förekommande eller förklarade förkortningar.

h. Uppgifter om besökaren

Namn - efternamn, följt av förnamnet utskrivet och initial(er) på mellannamn
Födelsetid (dag-månad-år)
Födelseort (stad och land, samt i Amerikas Förenta Stater inkluderande stat)
Nivå av säkerhetsklarering (t.ex. TS, S, C)
Passnummer/identitetsnummer
Nationalitet
Ställning – Ange besökarens officiella titel eller ställning i organisationen (t.ex. direktör, produktchef, osv.)
Leverantör/regeringsorgan – Ange namnet på den industrianläggning eller det regeringsorgan som besökaren företräder.

i. Begärande leverantörens/regeringsorganets säkerhetsansvarige tjänsteman. Ange namn, telefonnummer, faxnummer och e-postadress till den begärande säkerhetsansvarige tjänstemannen.

j. Försäkran om säkerhetsklarering. Ifylls av tillämplig regerings klareringsmyndighet.

k. Anmärkningar. Denna punkt kan användas för vissa administrativa behov (t.ex. föreslagen resplan, begäran om hotellreservationer och/eller transport). Om besöket har arrangerats i förväg bör namn, telefon- och faxnummer till den insatta person med vilken arrangemangen har gjorts upp i förväg anges.

4. Engångsbesök: Engångsbesök kan vara ett enstaka besök med kort varaktighet (får inte överstiga 30 dagar för USA och 21 dagar för Sverige). Framställningar om godkännande av engångsbesök skall inges genom kanaler mellan regeringarna. Oförutsedda händelser kan inträffa som innebär att enskilda måste göra brådskande besök som, på grund av brådskan, inte medger sedvanlig framförhållning för besöksansökan. Under sådana omständigheter skall ansökningar om besök granskas kritiskt och de måste vara fullständigt dokumenterade och motiverade av den sändande parten. Sådana brådskande besök får bara anordnas i undantagsfall när

a. det avsedda besöket rör en officiell regeringsinfordran av anbud (t.ex. ingivande av eller ändring i ett anbud, närvaro vid förhandlingar före ingående av kontrakt eller samling av anbudsgivare) eller,

b. besöket skall göras som svar på en inbjudan av en värdregerings tjänsteman eller värdleverantörs tjänsteman och i samband med ett officiellt statligt projekt, program eller kontrakt och

c. en möjlighet till ett program, projekt eller kontrakt kommer att äventyras om framställningen om besök inte godkänns.

5. Periodiskt återkommande besök. Program som kommer att innebära periodiskt återkommande besök i samband med sekretessbelagda kontrakt som ingåtts enligt bilaterala program som genomförs enligt ett avtal eller avtalsmemorandum mellan regeringar eller mellan myndigheter, och sådana besök som rör affärskontrakt som har godkänts av regeringarna, skall handläggas enligt punkt a eller b nedan, beroende på vilket som är tillämpligt:

a. Bilaterala program. Varje deltagande leverantörs verksamhetsställe skall upprätta en förteckning över de personer som medverkar i programmet. Förteckningen skall ingå i en framställning om besökstillstånd som innehåller den information som anges i detta tillägg. Framställningarna skall sändas genom regeringskanaler till värdpartens centrala besökskontor, som anges i punkt 2 ovan. Besökstillstånd som handläggs på detta sätt skall vara giltiga under programmets varaktighet och det skall inte finnas någon gräns för antalet tillåtna besökare. Förteckningen skall varje år kontrolleras av begärande CVO för att säkerställa att alla besökare fortfarande behöver ingå i förteckningen. Det skall inte finnas någon gräns för hur många ändringar som får göras i förteckningen, men de skall begränsas till tillägg och strykningar av namn. När besöken har godkänts får besök till de medverkande leverantörsanläggningarna och statliga organisationerna anordnas direkt.

b. Andra än bilaterala program. Leverantörs verksamhetsställen skall upprätta en förteckning över de personer som berörs av ett visst kontrakt eller underleverantörskontrakt som har godkänts av de ansvariga statliga myndigheterna. Förteckningen skall ingå i en framställning om besökstillstånd som innehåller den information som anges i punkt 3 ovan. Framställningen skall sändas till det CVO som anges i punkt 2 ovan för besök till svenska och amerikanska leverantörs verksamhetsställen och statliga organisationer. Besök av personer på de godkända listorna får anordnas direkt med säkerhetsavdelningarna vid den leverantörs verksamhetsställe eller statliga organisation som skall besökas. Besökstillstånd som handläggs på detta sätt skall gälla i ett år, men får vid behov förnyas för perioder på upp till ett år för att utföra kontraktet eller underleverantörskontraktet.

6. Förlängda besök. En framställning om förlängt besök bör användas när det krävs att en besökare stannar på en anläggning (industri eller statlig) under en sammanhängande period av mer än 21 dagar i Sverige, eller 30 dagar i USA. Ledtiden för en framställning om förlängt besökstillstånd till Sverige är tjugoen (21) dagar och för USA trettio (30) dagar. Ett förlängt besökstillstånd kan gälla i upp till tre (3) år i Sverige och under programmets varaktighet i USA. Det finns begränsningar av vilket slags arbete som får utföras av en person på ett förlängt besökstillstånd.

7. Besök till leverantörs verksamhetsställen som endast rör oklassificerad eller svensk information med beteckningen HEMLIG/RESTRICTED skall anordnas direkt mellan de sändande och mottagande verksamhetsställen och besökaren behöver inte ha intyg om säkerhetsklarering.

8. I tillstånd att besöka huvudleverantörens verksamhetsställe skall, när det behövs för kommersiella enheter, ingå tillstånd att få tillgång till eller röja sekretessbelagd information vid en underleverantörs verksamhetsställe som utför arbete i samband med samma huvudkontrakt, om underleverantören finns med i den ursprungliga besöksframställningen.

9. Det är verksamhetsstället som besöks som ansvarar för att se till att besökare inte får tillgång till information eller områden som de inte har behov av.

10. För ändringar i godkända framställningar om besök krävs förhandsgodkännande från den mottagande parten. Brådskande besök får inte ändras efter godkännande.

SECURITY IMPLEMENTING AGREEMENT FOR INDUSTRIAL OPERATIONS BETWEEN THE GOVERNMENT OF THE KINGDOM OF SWEDEN REPRESENTED BY FÖRSVARETS MATERIELVERK AND THE DEPARTMENT OF DEFENSE OF THE UNITED STATES

1. PURPOSE.

a. The following procedures have been developed by the Government of the Kingdom of Sweden represented by Försvarets materielverk (FMV) and the Department of Defense of the United States (DoD), hereinafter referred to as "the Parties," to implement the provisions of the General Security of Military Information Agreement between the Government of the Kingdom of Sweden and the Government of the United States, which entered into force on December 23, 1981. These procedures replace the Security Procedures for Industrial Operations between the Supreme Commander of the Swedish Armed Forces and the Department of Defense of the United States (Industrial Security Annex), dated 16 February 1982. The Agreement of 1981 provides for the safeguarding of Classified Military Information exchanged between the governments. This Implementing Agreement (hereafter referred to as Agreement) will apply to those cases in which Contracts, subcontracts, pre-Contract negotiations or other government-approved arrangements involving Classified Information of the Parties are placed or entered into by or on behalf of FMV in the United States or by or on behalf of the DoD in Sweden.

b. Within the framework of their national legislation, each Party shall take all appropriate measures to ensure the protection of Classified Information or Materiel provided pursuant to this Agreement.

c. In Sweden the Designated Security Authority (DSA) is FMV (the Defence Materiel Administration). The DoD hereby designates the Deputy Under Secretary of Defense (Technology Security Policy & Counterproliferation) as its DSA to provide policy oversight concerning the provisions of this Agreement.

2. DEFINITIONS.

The following definitions will be used for the purpose of this Agreement:

Classified Contract: A Contract that requires, or will require, access to Classified Information by a Contractor or by its employees in the performance of a Contract.

Classified Information: Official information or Materiel which in the interest of national security of the releasing or owning government, and in accordance with applicable national laws and regulations, requires protection against unauthorized disclosure and which has been designated as classified by an appropriate security authority. This includes any information, in any form, including written, oral or visual, or in the form of Materiel.

Cognizant Security Office (CSO): The government office or offices designated to administer industrial security in a Contractor's facility.

Contract: A legally enforceable agreement to provide goods or services.

Contractor: An individual or a commercial or other entity that agrees to provide goods or services.

Designated Government Representative (DGR): A person or an authority appointed to represent the sending or receiving Party in making or authorizing a government-to-government transfer of Classified Information.

Designated Security Authority (DSA): The government authority responsible for the security of Classified Information covered by this Agreement.

Document: Any letter, note, minute, report, memorandum, message, sketch, photograph, film, map, chart, plan, notebook, stencil, carbon, typewriter ribbon, diskette, magnetic tape, or any other form of recorded information.

Facility Security Clearance Assurance (FSCA): A certification provided by a DSA or CSO for a Contractor facility under its territorial jurisdiction which indicates that the facility is security cleared to a specified level and also has suitable security safeguards in place at a specified level to safeguard Classified Information. The FSCA also signifies that Classified Information CONFIDENTIAL or above will be protected by the Contractor on which the FSCA is provided in accordance with the provisions of this Agreement and that compliance shall be monitored and enforced by the responsible DSA or CSO. An FSCA is not required for a Contractor to undertake Contracts that require the receipt or production of Classified Information at the HEMLIG/RESTRICTED level.

Government-to-Government Transfer: The principle that Classified Information and Materiel CONFIDENTIAL and above will be transferred through official government-to-government channels or through other channels as may be mutually agreed, in writing, by the Sending and Receiving Parties.

Materiel: Any Document, product or substance on or in which information may be recorded or embodied. Materiel shall encompass everything regardless of its physical character or makeup including, but not limited to, Documents, writing, hardware, equipment, machinery, apparatus, devices, models, photographs, recordings, reproductions, notes, sketches, plans, prototypes, designs, configurations, maps and letters, as well as all other products, substances or items from which information can be derived.

Need-to-know: A determination made by an authorized holder of Classified Information that a prospective recipient requires access to specific Classified Information in order to perform or assist in a lawful and authorized governmental function.

Party: In Sweden, Party refers to the Government represented by FMV (including the agencies and authorities under the Swedish Ministry of Defence). In the United States, Party refers to the Department of Defense (including its agencies and the Departments of the Army, Navy, and Air Force).

Personnel Security Clearance Assurance (PSCA):

a. In the case of an individual who is employed by a government agency or Contractor facility under the jurisdiction of a DSA or CSO, a certification provided by that DSA or CSO concerning the level of personnel security clearance held by the individual.

b. In the case of an individual who is a citizen of one Party but is to be employed by the other Party or its Contractors, a statement provided by the DSA or CSO of the individual's country of citizenship concerning the individual's eligibility for a personnel security clearance at a level specified by the requesting Party.

Receiving Party: The Party to which Classified Information is transferred.

Sending Party: The Party that transfers Classified Information to the Receiving Party.

3. RESTRICTIONS ON USE AND DISCLOSURE OF EXCHANGED CLASSIFIED INFORMATION.

a. Unless express prior written consent is given to the contrary, the Receiving Party will not disclose or use, or permit the disclosure or use of, any Classified Information except for the purposes and within any limitations stated by the Sending Party.

b. The Receiving Party will not pass or disclose to a Government official, Contractor, Contractor's employee or to any other person holding the citizenship of any third country, or to any international organization, any Classified Information CONFIDENTIAL or above, supplied under the provisions of the General Security Agreement or this Agreement, nor will publicly disclose any Classified Information without prior written consent of the Sending Party.

c. Nothing in this Agreement 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 authorization of the owner of these rights has first been obtained.

4. PROTECTION OF CLASSIFIED INFORMATION.

Upon receipt of Classified Information furnished under this Agreement, the Receiving Party shall undertake to afford the information a degree of security protection at least equivalent to that afforded to the information by the Sending Party. The Receiving Party shall be responsible for information so received while it is within the territorial jurisdiction of its government and while it is possessed by or furnished to persons authorized to visit abroad pursuant to this Agreement. In Sweden FMV is the Cognizant Security Office (CSO) and in the United States the Defense Security Service (DSS) is the Cognizant Security Office (CSO). These organizations will assume responsibility for ensuring the administration of security measures for a Contract involving Classified Information CONFIDENTIAL or above awarded to industry for performance in their respective countries. Classified Information at the Swedish HEMLIG/RESTRICTED level will be protected in the U.S. in accordance with the provisions of Appendix A.

a. Access. Access to Classified Information CONFIDENTIAL or above will be limited to those persons who have a need-to-know and have been security cleared by either of the Parties in accordance with its national laws and regulations to the level at least equal to the classification of the information to be accessed.

b. Inspection/Security Review. The CSOs, as identified above, shall ensure that periodic industrial security inspections/security reviews are made of each Contractor facility that is located and incorporated to do business within their country engaged in the performance of, or in negotiations for, a Classified Contract.

c. Security Costs. Costs incurred in conducting security inspections/reviews shall be borne by the Party rendering the service. Costs incurred by either of the Parties through implementation of other security measures, including costs incurred through the use of the diplomatic courier service or any other authorized official courier service, will not be reimbursed. There shall be provisions in Classified Contracts for security costs to be incurred under the Contract, such as special costs for packing, transport and the like, which shall be borne by the Party for whom the service is required under the Contract. If, subsequent to the date of the Contract, the security classification or security requirements under the Contract are changed, and the security costs are thereby increased or decreased, the provisions of the Contract that may be affected shall be subject to an equitable adjustment by reason of such increased or decreased costs. Such equitable adjustments shall be accomplished under the appropriate provisions in the Contract governing changes.

d. Security Clearances. Clearances of Contractor facilities and individuals that will possess or be authorized access to Classified Information in connection with a Classified Contract or a potential Classified Contract shall be processed according to the pertinent regulations of the country having responsibility for administering security measures for the Classified Contract.

e. Orientation. The CSOs shall ensure that Contractors or subcontractors having access to Classified Information are furnished instructions setting forth their responsibility to protect the information in accordance with applicable national laws and regulations commensurate with the provisions of this Agreement.

5. TRANSFERS OF CLASSIFIED INFORMATION.

a. Classified Information CONFIDENTIAL and above shall normally be transferred between the Parties through DGRs using Government-to-Government channels. Government-to-Government channels are official government channels (e.g., diplomatic courier service). Other channels that may be established, if mutually agreed in writing by the Parties, shall ensure that government accountability and control is maintained from the point of origin to the ultimate destination. The CSO for each Classified Contract shall approve the procedures, or inform the Contractor of the channels of transmission to be used, and identify the DGR. Materiel shall be prepared for transmission in accordance with the national security laws and regulations of the Sending Party.

b. Classified Information CONFIDENTIAL and above that is to be transferred electronically shall be transmitted using secure means that have been approved by both Party's communications security authorities.

c. Classified Information at the Swedish HEMLIG/RESTRICTED level will be transmitted in the U.S. in accordance with the provisions of Appendix A.

6. RELEASE OF INFORMATION.

Release by a Contractor or subcontractor of any Classified Information CONFIDENTIAL or above pertaining to a Classified Contract shall in Sweden be governed by a Security Agreement (SA) including an Industrial Security Manual (ISM) between the Contractor or subcontractor and the Swedish Party and in the U.S. by the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M. In the case of a Swedish facility with a U.S. Classified Contract, initial prior review and approval shall be governed by the Swedish SA and ISM with final approval by the appropriate U.S. authority. In the case of a U.S. facility with a Swedish Classified Contract, initial prior review and approval shall be governed by the NISPOM with final approval by the Swedish Party.

7. MARKING.

a. The Sending Party shall ensure that Documents containing Classified Information are marked with the appropriate classification markings and prefixed with the country of origin/ownership prior to transfer to the Receiving Party. Upon receipt, the information shall, if required, be marked with the equivalent security classification, as detailed below. If such information subsequently is included in other Documents, those Documents shall be marked to identify the Sending Party and the applicable classification.

Table of Equivalent Security Classification Categories

Sweden	United States
KVALIFICERAT HEMLIG	TOP SECRET
HEMLIG/SECRET	SECRET
HEMLIG/CONFIDENTIAL	CONFIDENTIAL
HEMLIG/RESTRICTED	No equivalent (See Appendix A)

b. Classified Information produced or reproduced by a Receiving Party shall indicate when foreign government information is contained therein. The markings shall be applied in the manner prescribed in the regulations of the country in which the information is produced or reproduced.

8. CONTRACTS.

When a Party proposes to place, or authorizes a Contractor in its country to place, a Contract involving Classified Information CONFIDENTIAL or above with a Contractor in the country of the other Party, the Party that is to place or authorize the Contractor to place such Contract will request an FSCA, where appropriate, from the CSO of the other country. The FSCA will carry a responsibility that the security conduct by the cleared Contractor will be in accordance with national security laws or regulations and be monitored by its CSO.

a. Security Requirements Clause.

(1) The responsible authority of the Party in the process of negotiating a Classified Contract to be performed within the other country, and every Contractor in receipt of a Classified Contract or in the process of negotiating a Classified subcontract to be performed within the other country, shall incorporate appropriate security clauses in the Contract, request for proposal or subcontract Document. For such activity involving Classified Information at the CONFIDENTIAL or above levels, the security clauses attached at Appendix B shall be used.

(2) A copy of the relevant portions of the Contract, request for proposal or subcontract, including the security requirements clauses, shall be furnished promptly through appropriate channels to the CSO where the Contract is placed to enable them to furnish security supervision.

(3) Contracts placed with U.S. Contractors involving Classified Information at the Swedish HEMLIG/RESTRICTED level will contain a Restricted Conditions Requirement Clause identifying the measures to be applied for the protection of the Swedish HEMLIG/RESTRICTED information.

b. Security Classification Guidance. The appropriate authority (see 8.a.(1), above) of the contracting government shall furnish the Contractor or subcontractor with the security classification guidance pertaining to each classified aspect related to the Contract. In the case of Sweden this guidance shall be set forth in a Security Plan or Program Security Instruction (PSI) together with a Security Classification Guide and in the U.S. by way of a Contract Security Classification Specification (DD Form 254). The guidance must identify that Classified Information which is furnished by the contracting Party in connection with the Contract, or which is generated pursuant to the Classified Contract, and assign to such information a proper security classification. Two copies of the written security classification guidance, and of the security portions of the Classified Contract, or request for proposal, or subcontract containing the security requirements clauses will be submitted to the CSO of the Party which is responsible for administering security measures. The addresses of the CSOs are:

Sweden

Försvarets materielverk – FMV
Defence Materiel Administration
Security
Banérgatan 62
SE-115 88 Stockholm
SWEDEN

United States

Defense Security Service
Attn: Deputy Director for Industrial Security
Department of Defense
1340 Braddock Place
Alexandria, Virginia 22314-1651
UNITED STATES OF AMERICA

c. Subcontracts. Unless specifically prohibited in the Classified Contract, a Contractor may subcontract within its own country in accordance with the security procedures prescribed in its country for classified subcontracts, and within the country of the contracting Party under the procedures established by this Agreement for placing a classified prime Contract in that country, in accordance with the clauses set out in Appendix B to this Agreement.

d. Foreign Ownership, Control, or Influence. Firms that are determined by national security authorities to be under financial, administrative, policy or management control of nationals or other entities of a third party country may participate in a Contract or subcontract requiring access to Classified Information provided by the other Party only when enforceable measures are in effect to ensure that nationals or other entities of third party countries will not have access to Classified Information that is provided or that is generated there from. If enforceable measures are not in effect to preclude access by nationals or other entities of third party countries, the permission of the originating Party will be obtained prior to permitting such access.

e. Corporate Governance. FMV agrees to oversee implementation of board resolutions entered into by Swedish entities in connection with DoD Special Security Agreements (SSAs). FMV also agrees to assist the DoD in addressing alleged violations of the provisions of a DoD SSA by a Swedish company. These agreements are predicated on the understanding that the DoD will oversee compliance with board resolutions/arrangements entered into by U.S. entities in connection with FMV requirements governing foreign ownership, control or influence of Swedish entities holding Swedish security clearances, and that DoD will assist the FMV in addressing violations of these provisions by U.S. entities.

9. VISITS.

Requests for approval of visits shall be submitted using the procedures in Appendix C. Approval for visits shall be granted only to persons possessing security clearances at least at the level of the information to which access will be given. Authorization for visitors to have access to Classified Information will be limited to those who have a Need-to-Know.

10. SECURITY ASSURANCES RELATED TO NATIONAL SECURITY CLEARANCES OF FACILITIES OR NATIONALS OF THE OTHER COUNTRY.

a. Each Party will provide a FSCA or PSCA for facilities or individuals in its country when requested by the other Party.

b. When requested, the Party receiving the request shall determine the security clearance status of the facility or individual that is the subject of the inquiry and forward a FSCA or PSCA if the facility or national is already cleared. If the facility or national does not have a security clearance, or the facility or individual has a clearance that is at a lower security level than that requested, notification will be sent to the requesting Party that the FSCA or PSCA cannot be issued without further consultation. In such cases, further steps may be initiated to conduct inquiries that are necessary to meet the requirement.

c. If the Party receiving the request determines that a facility located and incorporated to do business in its country is ineligible for a security clearance, the requesting Party will be notified.

d. If either Party learns of any adverse information about a facility or an individual for whom it has furnished a FSCA or PSCA, it will notify the other Party of the nature of the information and the action it intends to take, or has taken. Either Party may request a review of any FSCA or PSCA that has been furnished by the other Party, provided that the request is accompanied by a rationale. The requesting Party will be notified of the results of the review and any subsequent action.

e. If either Party invalidates, suspends or takes action to revoke a personnel or facility security clearance, the Party that requested the PSCA or FSCA will be notified and given the reasons for such an action.

f. If requested by the other Party, each Party will cooperate in reviews and investigations concerning security clearances.

11. LOSS OR COMPROMISE.

a. In the event of the loss or possible loss of Classified Information CONFIDENTIAL or above, or suspicion that such Classified Information has been compromised, the Receiving Party will immediately inform the Sending Party.

b. An investigation will be carried out immediately by the Receiving Party, with assistance from the Sending Party, if required, in accordance with the laws and regulations in the country of the Receiving Party. The Receiving Party will inform the Sending Party about the circumstances and outcome of the investigation as soon as possible and the measures adopted to preclude recurrence of the incident.

12. DISPUTES.

Any dispute regarding the interpretation or application of this Agreement will be resolved by consultation between the Parties and will not be referred to any national or international tribunal or third Party for settlement.

13. EFFECTIVE DATE.

This Implementing Agreement to the 1981 General Security of Military Information Agreement supersedes the Security Procedures for Industrial Operations between the Supreme Commander of the Swedish Armed Forces of the Kingdom of Sweden and the Department of Defense of the United States (Industrial Security Annex) dated 16 February 1982 and becomes effective upon signature by both parties.

14. TERMINATION/REVIEW.

a. This Agreement will remain in effect until termination of the 1981 General Security of Military Information Agreement, or until this Agreement is terminated by either Party giving the other Party six months written notification of its intent to terminate the Agreement. This Agreement may also be terminated at any time upon written consent of both Parties. Both Parties will remain responsible after termination for the safeguarding of all Classified Information exchanged under the provisions of the 1981 General Security of Military Information Agreement and this Agreement and any Contracts entered into, or generated therefrom, in accordance with national laws and regulations.

b. This Agreement will be reviewed jointly by the Parties no later than five (5) years after its effective date.

c. Any Classified Information that is exchanged under the cover of this Agreement will be safeguarded even though its transfer may occur following notice by either of the Parties to terminate.

d. In the event of termination, resolution of any outstanding problems will be achieved by consultation between the two Parties.

15. SIGNATURES.

a. The foregoing represents the understanding between the Government of the Kingdom of Sweden represented by FMV and the Department of Defense of the United States of America upon the matters referred to therein.

b. IN WITNESS WHEREOF, the undersigned, being duly authorized by their Governments, have signed this Agreement.

c. DONE, at Washington, D.C. this 20th day of May, 2004, in English and Swedish, each text being equally authentic.

For the Department of Defense
of the United States of America

Lisa Bronson

Deputy Under Secretary of Defense for
Technology Security Policy and
Counterproliferation

For the Government
of the Kingdom of Sweden
Försvarets materielverk

Jan-Olof Lind

Acting Director General
Försvarets materielverk

Appendices to the U.S.-Sweden Implementing Agreement:

A. Procedures for Handling Swedish HEMLIG/RESTRICTED Information within the United States
B. Security Requirements Clauses
C. Visit Procedures

APPENDIX A

PROCEDURES FOR HANDLING SWEDISH HEMLIG/RESTRICTED INFORMATION WITHIN THE UNITED STATES

1. Upon receipt, Swedish Documents or Materiel bearing the classification "HEMLIG/RESTRICTED" shall be handled in the U.S. as U.S. UNCLASSIFIED information that is exempt from public release under one or more U.S. laws. These laws include the Freedom of Information Act (FOIA) and Title 10 U.S.C. Section 130(c), "Nondisclosure of Information: Certain Sensitive Information of Foreign Governments and International Organizations." Documents or Materiel so marked shall be stored in locked containers affording the appropriate protection or closed spaces or areas that will prevent access by unauthorized personnel.

2. Swedish HEMLIG/RESTRICTED Documents shall be handled in a manner that will preclude open publication, access or use for other than official government purposes of the United States or Sweden.

3. Before any Communications and Information System is allowed to store, process or forward Swedish HEMLIG/RESTRICTED information, it must be given security approval, known as Accreditation. An Accreditation is defined as a formal statement by the appropriate authority confirming that the use of a system meets the appropriate security requirement and does not present an unacceptable risk. For stand-alone desktop PCs and laptop systems utilized in DoD establishments the system registration Document together with the Security Operating Procedures fulfils the role of the required Accreditation. For Contractors, guidance on the use of Information Technology systems will be incorporated within the Restricted Conditions Requirements Clause in the Contract.

4. Swedish HEMLIG/RESTRICTED Documents shall be transmitted by first class mail within the United States in one secure envelope/cover. Transmission outside the United States shall be in two secure envelopes/covers, the inner cover marked "Swedish HEMLIG/RESTRICTED". Such transmissions shall be by traceable means such as Commercial Courier or other means agreed upon by Sweden in writing.

5. Otherwise unclassified U.S. Documents originated by a U.S. Government agency which contain information that Sweden has classified HEMLIG/RESTRICTED shall bear on the cover and the first page the marking "Swedish HEMLIG/RESTRICTED - Exempt from Public Disclosure under Title 10 U.S.C., Section 130(c)." The portion of the Document containing Swedish HEMLIG/RESTRICTED information also shall be identified in the Documents.

6. Swedish HEMLIG/RESTRICTED information shall be transmitted or accessed electronically via a public network like the Internet, using government or commercial encryption devices mutually accepted by the Parties' government security authorities. Telephone conversations, video conferencing or facsimile transmissions containing Swedish HEMLIG/RESTRICTED information may be in clear text, if an approved encryption system is not available.

APPENDIX B

SECURITY REQUIREMENTS CLAUSE FOR INCLUSION IN CLASSIFIED CONTRACTS INVOLVING CLASSIFIED INFORMATION CONFIDENTIAL OR ABOVE

The provisions of this clause are based upon the General Security of Military Information Agreement between the Government of the Kingdom of Sweden and the Government of the United States and shall apply to the extent that this Contract involves access to or the possession of information or Materiel to which a security classification CONFIDENTIAL and above has been assigned by the Government that originated the information (hereafter called Originating Government).

1. All Classified Information and Materiel furnished or generated pursuant to this Contract shall be protected as follows:

a. The recipient shall not release the information or Materiel to a third country government, person, or firm without the prior approval of the Originating Government.

b. The recipient shall afford the information and Materiel a degree of protection at least equivalent to that afforded it by the Originating Government as indicated in the table below. Information received shall be marked with the originator's level of classification and denote the country of origin.

c. The recipient shall not use the information and Materiel for other than the purpose for which it was furnished without the prior written consent of the originating Party.

2. Classified Information and Materiel furnished or generated pursuant to this Contract shall be transferred through government-to-government channels or other channels mutually approved, in writing, by the Governments of the United States and the Kingdom of Sweden. Access to Classified Information and Materiel shall be granted only to persons who have a security clearance at least equal to the classification level of the information and an official need for access to the information in order to perform on the Contract.

3. Classified Information and Materiel furnished under this Contract will be remarked by the recipient with its government's equivalent security classification markings.

4. Classified Information and Materiel generated under this Contract shall be assigned a security classification as specified by the Contract security classification specifications.

5. All cases in which it is known or there is reason to believe that Classified Information or Materiel furnished or generated pursuant to this Contract has been subject to a security breach, compromised, lost, or disclosed to unauthorized persons shall be reported promptly and fully by the Contractor to its government's security authorities.

6. Classified Information and Materiel furnished or generated pursuant to this Contract shall not be further provided to another potential Contractor or subcontractor unless:

a. A potential Contractor or subcontractor which is located in the U.S. or Sweden has been approved for access to Classified Information and Materiel at the requisite level by U.S. or Swedish security authorities; or,

b. If located in a third country, prior written consent is obtained from the U.S. or Swedish Government, whichever is the Originating Government.

7. The recipient Contractor shall insert terms that substantially conform to the language of these clauses, including this clause, in all subcontracts under this Contract that involve access to Classified Information furnished or generated under this Contract.

8. Upon completion of the Contract, all Classified Information or Materiel furnished or generated pursuant to the Contract shall either be destroyed by the contractor in accordance with national rules and regulations or, if requested, returned to the Government that furnished the information.

Table of Equivalent Security Classification Categories

Sweden	United States
KVALIFICERAT HEMLIG	TOP SECRET
HEMLIG/SECRET	SECRET
HEMLIG/CONFIDENTIAL	CONFIDENTIAL
HEMLIG/RESTRICTED	No equivalent (See Appendix A)

APPENDIX C

VISITS

1. This Appendix describes procedures to be used in the visit request process. Visits require the prior approval of both Parties using the procedures in this Appendix.

2. The offices listed below have been designated by each Party to process visit requests that are received from the other Party. The listed offices are hereafter referred to as Central Visit Offices or CVOs.

Sweden

Försvarets materielverk – FMV
Swedish Defence Materiel Administration
Security
Banérgatan 62
SE-115 88 Stockholm
SWEDEN

Totalförsvarets Forskningsinstitut – FOI
Swedish Defence Research agency
Ranhammarsvägen 14
SE-172 90 Stockholm
SWEDEN

Försvarsmakten – Högkvarteret
Swedish Armed Forces Headquarters
Protocol
Lidingövägen 24
SE-107 85 Stockholm
SWEDEN

United States:

Department of the Army
Office of the Deputy Chief of Staff for Intelligence
Attn: Foreign Liaison Directorate (DAMI-FL)
Washington, D.C. 20310-1040
United States of America

Department of the Navy
Navy International Programs Office
Foreign Disclosure Policy Control Division (Navy IPO-10)
Washington, D.C. 20350-5000
United States of America

Department of the Air Force
Office of the Deputy Under Secretary of the Air Force
(International Affairs)
Foreign Disclosure & Technology Transfer Division (SAF/IAPD)
1010 Air Force Pentagon
Washington, D.C. 20330-1010
United States of America

Defense Intelligence Agency
Foreign Liaison Staff (DIA/PO-FL)
Washington, D.C. 20301-6111
United States of America

(The Defense Intelligence Agency processes visits to the Office of the Secretary of Defense (OSD), the OSD Staff, Department of Defense Agencies, and the Joint Staff, and their contractors.)

3. Requests for approval of visits shall include the following information:

a. Requesting Facility. Provide the full name and postal address (include city, country, and postal zone, and in the U.S. include the state) and the telephone and telefax numbers of the facility.

b. Government Agency or Industrial Facility to be Visited. Provide the full name, title, and visit (street) address (include city, country, and postal zone, and in the U.S. include the state) including telephone and telefax number, E-mail address and name of the person with whom the meeting will take place (point of contact).

c. Dates of Visit. Provide the actual date or period (date-to-date) of the visit by day-month-year.

d. Type of Visit. Specify whether the visit is a government initiative or commercial initiative and whether the visit is being initiated by the requesting facility or the facility to be visited. Government initiative will be specified only if the visit is in support of an authorized government program, which must be fully described in subparagraph g, below.

e. Subject to be Discussed/Justification. Give a concise description of the issues or subjects to be discussed and the reason for the visit. Do not use unexplained abbreviations. In the case of a request for recurring visits, this item should state Recurring Visits as the first words in the data element (e.g., Recurring Visits to discuss ...) or in the case of an amendment (Amendment to Visit ID number...).

f. Anticipated Level of Classified Information to be involved. Indicate TOP SECRET, SECRET, CONFIDENTIAL, as applicable, and country of origin of the information.

g. Pertinence of Visit. Specify the full name of the government program, agreement, or sales Contract (e.g., Foreign Military Sales case), or request for proposal or tender, using commonly used or explained abbreviations only.

h. Particulars of Visitor.

Name - Family Name, followed by forename in full and middle initial(s).
Date of Birth (day-month-year)
Place of Birth (city, and country, and in the U.S. include the state)
Security Clearance status (e.g. TS, S, C)
Passport Number/Identification Number
Nationality
Position - Indicate the official title or position the visitor holds in the organization (e.g., director, product manager, etc.).
Contractor/Government Agency – Provide the name of the industrial facility or government agency that the visitor represents.

i. Security Officer of the Requesting Contractor/Government Agency. Provide the name, telephone number, fax number and E-mail address of the requesting Security Officer.

j. Certification of Security Clearance. To be completed by the applicable government clearance agency.

k. Remarks. This item can be used for certain administrative requirements (e.g., proposed itinerary, request of hotel reservations, and/or transportation). If the visit has been pre-coordinated, the name, telephone and telefax numbers of the knowledgeable person with whom advance arrangements have been made should be stated.

4. One-time Visits: One-time visits may be for a single visit of a short duration (not to exceed 30 days for the U.S. and 21 days for Sweden). Requests for approval of one-time visits will be submitted via government to government channels. Unforeseen circumstances may occur that require individuals to undertake urgent visits which, due to the urgency, do not permit the usual lead time for the visit. In such circumstances visit applications will be critically reviewed and must be fully documented and justified by the Sending Party. Such emergency visits shall be arranged only in exceptional circumstances when:

a. The proposed visit is related to an official government request for proposal/request for tender offer (e.g.; submission of, or amendment to, a bid or proposal; attendance at pre-Contract negotiations or bidder's conference); or,

b. The visit is to be made in response to the invitation of a host government official or host contractor official and is in connection with an official government project, programme or Contract, and,

c. A programme, project or Contract opportunity will be placed in jeopardy if the visit request is not approved.

5. Intermittent Recurring Visits. Programs that will involve intermittent, recurring visits related to Classified Contracts that are awarded pursuant to bilateral programs conducted under a government-to-government or agency-to-agency agreement or memorandum of understanding, and such visits related to commercial Contracts that have been approved by the governments, shall be processed as prescribed in subparagraphs (a) or (b) below, as applicable:

a. Bilateral programs. A list shall be developed by each participating contractor facility of those individuals who are participating in the program. The list shall be included with a request for visit authorization containing the information described in this Appendix. The requests shall be sent through government channels to the Central Visit Offices of the host Party, as identified in paragraph 2, above. Visit authorizations under this procedure shall be valid for the duration of the program and there will be no limit on the number of visitors authorized. The list shall be checked annually by the requesting CVO to ensure that there is still a requirement for all visitors to continue to be included. There shall be no limit to the number of amendments which may be submitted to the list but they shall be confined to the addition and deletion of names. Upon approval, direct arrangements may be made for visits to the participating contractor facilities and government organizations.

b. Other than Bilateral Programs. A list shall be developed by contractor facilities of those individuals that are involved in a specific Contract or subcontract that has been approved by the responsible government authorities. The list shall be included with a request for visit authorization containing the information described in paragraph 3., above. The request shall be submitted to the CVO identified in paragraph 2, above, for visits to Swedish and to U.S. Contractor facilities and government organizations. Visits by individuals on the approved lists may be arranged directly with the security offices of the Contractor facility or government organization to be visited. Visit authorizations under this procedure shall be valid for one year, but may be renewed for periods of up to one year as necessary for performance on the Contract or subcontract.

6. Extended Visits. An Extended Visit Request should be used when a visitor will be required to remain on a site (industrial or government) for a continuous period of greater than 21 days in Sweden, or 30 days in the U.S. The lead-time for a request for an Extended Visit Authorization to Sweden is twenty-one (21) days, and for the U.S. is thirty (30) days. An Extended Visit Authorization can be valid for a period of up to three (3) years in Sweden, and for the duration of the program in the U.S. There are limitations on the type of work that can be carried out by an individual on an Extended Visit Authorization.

7. Visits to Contractor facilities relating only to Unclassified or Swedish HEMLIG/RESTRICTED information shall be arranged directly between the sending and receiving facilities, and the visitor does not require a security clearance.

8. When requested in regard to commercial entities, the authority to visit the facility of the prime Contractor shall include authorization to have access to or to disclose Classified Information at the facility of a subcontractor engaged in performance of work in connection with the same prime Contract provided the subcontractor is included on the original Visit Request.

9. It is the responsibility of the host site to ensure that the visitor is not allowed access to information or areas for which they do not have a need-to-know.

10. Modifications to approved Visit Requests require the prior concurrence of the receiving Party. Emergency visit requests may not be modified after approval.

Edita Norstedts Tryckeri, Stockholm 2004