Sveriges internationella överenskommelser

ISSN 1102-3716

Utgiven av Utrikesdepartementet

SÖ 2008: 58

Nr 58
Säkerhetsskyddsavtal med Amerikas förenta stater upprättat i enlighet med avtalet den 13 april 2007 (SÖ 2007:63) om vetenskapligt och tekniskt samarbete till skydd för den nationella säkerheten Washington den 11 april 2008

Regeringen beslutade den 28 februari 2008 att underteckna avtalet och att utse Försvarets materielverk till ansvarig myndighet för säkerhetsskyddsfrågor som rör avtalet.

Avtalet trädde i kraft vid undertecknandet den 11 april 2008.

Översättning

SÄKERHETSSKYDDSAVTAL UPPRÄTTAT I ENLIGHET MED AVTALET MELLAN KONUNGARIKET SVERIGES REGERING OCH AMERIKAS FÖRENTA STATERS REGERING OM VETENSKAPLIGT OCH TEKNISKT SAMARBETE TILL SKYDD FÖR DEN NATIONELLA SÄKERHETEN AV DEN 13 APRIL 2007

Syfte

Konungariket Sveriges regering och Amerikas förenta staters regering, nedan kallade *parterna*, har utarbetat följande förfaranden som komplettering till artikel 12 i avtalet mellan Konungariket Sveriges regering och Amerikas förenta staters regering om vetenskapligt och tekniskt samarbete till skydd för den nationella säkerheten av den 13 april 2007, nedan kallat *avtalet*. Dessa förfaranden fortsätter genomförandet av bestämmelserna i överenskommelsen mellan Sveriges regering och Amerikas förenta staters regering om sekretesskydd av militär information av den 4 och 23 december 1981.

Parterna ska inom ramen för sin nationella lagstiftning vidta alla lämpliga åtgärder för att se till att sekretessbelagd information och sekretessbelagd utrustning och materiel som tillhandahålls i enlighet med dessa säkerhetsförfaranden skyddas. I detta dokument genomförs avtalet, och alla villkor och bestämmelser i själva avtalet ska därför tillämpas på dessa förfaranden. Om innebörden skiljer sig åt, är det bestämmelserna i avtalet som gäller.

ARTIKEL 1

Definitioner

För dessa förfaranden gäller följande definitioner:

– *säkerhetsskyddsmyndighet för avtalet* (*säkerhetsskyddsmyndigheten*): den offentliga myndighet som har ansvar för att utarbeta riktlinjer och förfaranden som gäller säkerheten för sekretessbelagd information som omfattas av dessa förfaranden.

– *sekretessbelagt avtal*: ett kontrakt som innebär eller kan komma att innebära att en leverantör eller dess anställda delges sekretessbelagd information vid genomförandet av ett kontrakt.

– *utrustning och materiel*: alla handlingar, produkter eller substanser som kan förses med eller innehålla information. Materiel omfattar allt, oberoende av fysisk karaktär, bl.a. handlingar, skrifter, maskinvaror, utrustning, maskiner, apparater, anordningar, modeller, fotografier, upptagningar, reproduktioner, anteckningar, skisser, planer, prototyper, konstruktioner, konfigurationer, kartor och brev samt alla andra produkter, substanser eller materiel från vilka information kan hämtas.

– *intyg om säkerhetsklarering för anläggningar*: ett intyg som säkerhetsskyddsmyndigheten har utfärdat för en anläggning som omfattas av dess territoriella behörighet. Intyget visar att anläggningen är säkerhetsklarerad till en viss nivå och att det finns lämpligt säkerhetsskydd på en viss nivå för att skydda sekretessbelagd information. Intyget om säkerhetsklarering för

anläggningar innebär också att sekretessbelagd information kommer att skyddas av den leverantör som intyget utfärdas till i enlighet med bestämmelserna i dessa förfaranden och att säkerhetsskyddsmyndigheten för avtalet ska övervaka och se till att bestämmelserna efterlevs.

– *behov av kännedom i tjänsten*: en klassificering som gjorts av en behörig innehavare av sekretessbelagd information att en tilltänkt mottagare behöver ha tillgång till viss sekretessbelagd information för att genomföra eller biträda i en lagenlig och godkänd myndighetsfunktion.

– *intyg om säkerhetsklarering för personer*:

a) ett intyg utfärdat av säkerhetsskyddsmyndigheten om nivån på den säkerhetsklarering för personer som innehas av en person som är anställd av en offentlig myndighet eller en leverantör som lyder under säkerhetsskyddsmyndighetens jurisdiktion.

b) ett intyg utfärdat av säkerhetsskyddsmyndigheten i det land där en person är medborgare om personens rätt att få säkerhetsklarering för personer på en nivå som anges av den begärande parten för personer som är medborgare i en part men som ska anställas av den andra parten eller av dess leverantörer.

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

– *sändarpart:* den part som framställer och/eller överför sekretessbelagd information till mottagarparten.

Artikel 2

Utnämnande av myndigheter

1. Parterna ska utse varsin säkerhetsskyddsmyndighet för avtalet (*säkerhetsskyddsmyndigheten*) som ska vara statens gemensamma kontaktpunkt och den myndighet som har ansvar för att utarbeta riktlinjer och förfaranden som gäller säkerheten för sekretessbelagd information som omfattas av dessa förfaranden. Dessa personer ska ha ansvar för de riktlinjer och förfaranden som rör säkerheten för sekretessbelagd information. När det gäller Konungariket Sveriges regering är säkerhetsskyddsmyndigheten chefen för säkerhetsavdelningen vid Försvarets materielverk (FMV). När det gäller Amerikas förenta stater är säkerhetsskyddsmyndigheten chefen för direktoratet för säkerhet, vetenskap och teknik vid ministeriet för nationell säkerhet. Båda säkerhetsskyddsmyndigheterna ska utöva politisk tillsyn över bestämmelserna i avtalet. Andra säkerhetsskyddsmyndigheter får vid behov utses för enskilda projekt som ingås i enlighet med avtalet.

2. Säkerhetsskyddsmyndigheterna får utse andra offentliga myndigheter som ska utföra den egna partens säkerhetsskyldigheter. Vid en sådan utnämning ska säkerhetsskyddsmyndigheten ändå ha tillsyns- och förvaltningsansvaret för tillämpningen av bestämmelserna i detta säkerhetsskyddsavtal.

Artikel 3

Inskränkningar i fråga om utnyttjande och röjande av sekretessbelagd och kontrollerad icke-sekretessbelagd information

1. Parterna ska vidta alla tillgängliga rättsliga åtgärder för att se till att sekretessbelagd information som utbyts, framställs eller tillhandahålls på annat sätt i enlighet med avtalet skyddas från att lämnas vidare om sändarparten inte samtycker till att informationen röjs.

2. Mottagarparten får inte förmedla eller röja sekretessbelagd information till 1) personer som är medborgare i ett tredjeland, 2) internationella organisationer eller 3) allmänheten utan att sändarparten i förväg har gett sitt skriftliga tillstånd.

3. Inget i dessa förfaranden ska tolkas som rätt att lämna ut, använda, utbyta eller röja information om immateriella rättigheter förrän ett särskilt skriftligt tillstånd har erhållits från innehavaren av dessa rättigheter.

4. Kontrollerad icke-sekretessbelagd information ska hanteras i enlighet med bestämmelserna i bilaga A.

Artikel 4

Skydd av sekretessbelagd information

1. När mottagarparten tar emot sekretessbelagd information som överlämnas i enlighet med avtalet ska den se till att ge informationen minst samma grad av säkerhetsskydd som sändarparten ger.

2. Parterna ska ha ansvar för att administrera säkerhetsåtgärderna för alla kontrakt som omfattar sekretessbelagd information som lämnats till industrin för att verkställas inom deras respektive territorium i enlighet med avtalet.

3. Rätt att ta del av information. Rätten att ta del av sekretessbelagd information ska vara förbehållen personer som har behov av den i tjänsten och som har genomgått säkerhetsklarering av den lämpliga parten i enlighet med dess nationella lagar och andra författningar för minst samma nivå som sekretessgraden hos den information som det ska tas del av.

4. Inspektion/säkerhetsöversyn. Säkerhetsskyddsmyndigheten ska se till att det görs regelbundna industriella säkerhetsinspektioner/säkerhetsöversyner av alla offentliga myndigheter och leverantörer i landet som deltar i genomförandet av eller förhandlingar om alla aktiviteter inom ramen för avtalet som omfattar sekretessbelagd information.

5. Säkerhetsklareringar. Säkerhetsklareringar för anläggningar och personer som ska inneha eller ges rätt att ta del av sekretessbelagd information ska handläggas i enlighet med gällande bestämmelser för det land som har ansvar för att sköta säkerhetsåtgärderna för den sekretessbelagda informationen.

6. Säkerhetsutbildning. Parterna ska se till att de personer och anläggningar som delges sekretessbelagd information underrättas om sin skyldighet att skydda informationen i enlighet med tillämpliga nationella lagar och andra författningar som överensstämmer med bestämmelserna i dessa säkerhetsförfaranden.

Artikel 5

Överföring av sekretessbelagd information

1. Sekretessbelagd information ska normalt överföras mellan parterna via regeringarnas officiella kanaler (t.ex. diplomatisk kurir eller militärkurir). Säkerhetsskyddsmyndigheterna får också gemensamt komma överens om att upprätta andra kanaler, under förutsättning att regeringens ansvar och kontroll bibehålls från ursprungsorten till slutdestinationen. Säkerhetsskyddsmyndigheterna ska godkänna förfarandena och informera anläggningarna om vilka alternativa överföringskanaler som får användas. Materiel ska förberedas för överföring i enlighet med sändarpartens nationella lagar och andra författningar om säkerhetsskydd.

2. Sekretessbelagd information får överföras elektroniskt om det sker på ett säkert sätt som har godkänts av de båda parternas kommunikationssäkerhetsmyndigheter.

Artikel 6

Utlämnande av information till allmänheten

1. Offentliga myndigheters, leverantörers eller underleverantörers utlämnande av sekretessbelagd information till allmänheten ska i Sverige regleras av tryckfrihetsförordningen med beaktande av de tillämpliga undantagen i sekretesslagen. I Förenta staterna regleras utlämnandet av sekretessbelagd information till allmänheten av NISPOM (National Industrial Security Program Operating Manual) och DOD 5220.22-M.

2. Svenska anläggningar med ett amerikanskt sekretessbelagt kontrakt får enbart lämna ut information till allmänheten efter att ha fått ett skriftligt förhandsgodkännande från den amerikanska säkerhetsskyddsmyndigheten och i enlighet med sekretesslagen (Official Secrets Act). När det gäller amerikanska anläggningar med ett svenskt sekretessbelagt kontrakt ska förhandsinspektionen och -godkännandet regleras av NISPOM med slutgiltigt godkännande av den svenska säkerhetsskyddsmyndigheten.

Artikel 7

Märkning

Sändarparten ska se till att handlingar som innehåller sekretessbelagd information märks med lämplig sekretessbeteckning, föregången av ursprungs- eller ägarlandets namn, innan de överförs till mottagarparten. Vid mottagandet ska den sekretessbelagda informationen om så är nödvändigt märkas med motsvarande sekretessbeteckning enligt nedan. Om informationen senare ingår i andra handlingar ska handlingarna märkas så att sändarparten och den tillämpliga beteckningen kan identifieras.

Tabell över motsvarande sekretessbeteckningar

Konungariket Sverige		**Amerikas förenta stater**
Försvarsmyndigheter	**Civila myndigheter**	
HEMLIG/ TOP SECRET	HEMLIG Av synnerlig betydelse för rikets säkerhet	US TOP SECRET
HEMLIG/SECRET	HEMLIG	US SECRET
HEMLIG/CONFIDENTIAL	Hänvisn. 1	US CONFIDENTIAL
HEMLIG/RESTRICTED	Inte tillämplig	TREAT AS US CONFIDENTIAL (hänvisn. 2)

Hänvisn. 1. Amerikansk information på nivån US CONFIDENTIAL ska behandlas som HEMLIG av de civila myndigheterna i Sverige.

Hänvisn. 2. Svensk information på nivån HEMLIG/RESTRICTED ska märkas med beteckningen ”TREAT AS US CONFIDENTIAL” och behandlas som US CONFIDENTIAL.

2. Sekretessbelagd information som framställts eller återgetts av en sändarpart ska markeras med båda ländernas sekretessbeteckningar enligt ovan. Märkningarna ska göras på det sätt som föreskrivs i bestämmelserna för det land där informationen framställs eller återges.

Artikel 8

Kontrakt

1. En part som avser att göra en beställning eller en underbeställning som innefattar sekretessbelagd information hos en leverantör i den andra partens land, ska vid behov via sin säkerhetsskyddsmyndighet begära ett sådant intyg om säkerhetsklarering för anläggningar som avses i punkt 2 från den andra partens säkerhetsskyddsmyndighet. Intyget om säkerhetsklarering för anläggningar ska innehålla en försäkran om att den klarerade leverantörens sekretessbeteende ska stå i överensstämmelse med nationella lagar och andra författningar om sekretess och övervakas av den partens säkerhetsskyddsmyndighet.

2. Klausul om säkerhetskrav: Den part eller leverantör som förhandlar om ett sekretessbelagt kontrakt eller ett underleverantörskontrakt ska införa lämpliga säkerhetsklausuler i alla handlingar. Parterna ska införa säkerhetsbestämmelserna i bilaga A i alla kontrakt som innehåller kontrollerad icke-sekretessbelagd information. En kopia av de aktuella delarna av kontraktet, anbudsinfordran eller underleverantörskontraktet ska tillsammans med klausulen om säkerhetsskydd genom lämpliga kanaler omedelbart lämnas till säkerhetsskyddsmyndigheten i den part där beställningen görs för att den ska kunna utöva säkerhetstillsyn av kontraktet.

3. Anvisningar om sekretessbeteckningarna. Säkerhetsskyddsmyndigheten i den avtalsslutande parten ska ge leverantören eller underleverantören anvisningar om sekretessbeteckningarna för varje sekretessbelagd aspekt av kontraktet. För Sveriges del ska dessa anvisningar läggas fram i en skrivelse om säkerhetsaspekten (SAL) och för Förenta staternas del genom en specifikation av sekretessbeteckningarna för kontrakt (Contract Security Classification Specification, DD-formulär 254). De amerikanska leverantörerna ska dessutom samarbeta med försvarets säkerhetstjänst (Defense Security Service) och följa NISPOM. I anvisningarna måste en lämplig sekretessbeteckning identifieras och fastställas för all sekretessbelagd information som lämnas av den avtalsslutande parten i samband med kontraktet eller som framställs i enlighet med det sekretessbelagda kontraktet. En kopia av de skriftliga anvisningarna om sekretessbeteckningarna ska lämnas till säkerhetsskyddsmyndigheten i leverantörens land.

4. Underleverantörskontrakt. Om det inte är uttryckligen förbjudet enligt det sekretessbelagda kontraktet får en leverantör ingå underleverantörskon-

trakt inom parternas respektive länder i enlighet med de säkerhetsrutiner som gäller i för sekretessbelagda underleverantörskontrakt i det landet och de förfaranden som fastställs i detta avtal för att ingå ett sekretessbelagt huvudkontrakt i det landet.

5. Utländskt ägande, kontroll eller inflytande. Företag som enligt de nationella säkerhetsskyddsmyndigheterna står under finansiell, förvaltningsmässig eller politisk kontroll eller ledningskontroll av fysiska eller juridiska personer i ett tredjeland får enbart delta som part i ett kontrakt eller ett underleverantörskontrakt som innebär rätt att ta del av sekretessbelagd information från den andra parten om det finns gällande verkställbara åtgärder som säkerställer att fysiska eller juridiska personer från tredjeländer inte får ta del av sekretessbelagd information som görs tillgänglig eller framställs genom kontraktet. Om det inte finns några verkställbara åtgärder som hindrar fysiska eller juridiska personer från tredjeländer att ta del av sådan information, ska upphovspartens tillstånd inhämtas innan sådan rätt att ta del av information tillåts.

Artikel 9

Internationella besök

1. Alla internationella besök ska godkännas i förväg av båda parterna. Framställningar om tillstånd för besök ska lämnas i enlighet med förfarandena i bilaga B. Underleverantörerna ska dessutom alltid informera sin huvudleverantör innan de besöker anläggningar som berörs av samarbete enligt avtalet.

2. Tillstånd för sådana besök får enbart beviljas personer som har genomgått säkerhetsklarering för minst den nivå som rätten att ta del av information avser. Rätten för besökare att ta del av sådan sekretessbelagd information ska begränsas till personer som har behov av den i tjänsten.

Artikel 10

Säkerhetsgarantier i samband med nationell säkerhetsklarering för anläggningar eller personer från den andra partens land

1. Varje part ska utfärda ett intyg om säkerhetsklarering för anläggningar eller för personer, om detta begärs av den andra parten för en anläggning eller person i det egna landet.

2. Den part som mottar begäran ska fastställa säkerhetsklareringsstatus för den anläggning eller person som är föremål för prövning. Om anläggningen eller personen redan är klarerad ska den översända ett intyg om säkerhetsklarering för anläggningar eller för personer. Om anläggningen eller personen saknar intyg om säkerhetsklarering eller om intyget gäller en lägre sekretessgrad än den som har begärts, ska den begärande parten underrättas om att intyget om säkerhetsklarering för anläggningar eller för personer inte kan utfärdas utan ytterligare samråd. Om så är fallet kan ytterligare åtgärder vidtas för att genomföra den prövning som är nödvändig för att uppfylla kravet. Om prövningen ger godkänt resultat ska ett intyg om säkerhetsklarering för anläggningar eller för personer lämnas till den begärande parten.

3. Om den part som mottar begäran fastställer att en anläggning som är

belägen i landet och har registrerats för att bedriva verksamhet där inte kan komma i fråga för säkerhetsklarering ska den begärande parten underrättas.

4. Om någon av parterna får kännedom om information som inverkar negativt på en anläggning eller en person för vilken den har utfärdat ett intyg om säkerhetsklarering för anläggningar eller för personer, ska den underrätta den andra parten om vilka åtgärder den har vidtagit eller avser att vidta. Parterna får när som helst begära omprövning av intyg om säkerhetsklarering för anläggningar eller för personer som utfärdats av den andra parten. Den begärande parten ska underrättas om resultatet av omprövningen och om eventuella följdåtgärder.

5. Om någon av parterna ogiltigförklarar, upphäver eller vidtar åtgärder för att dra in en säkerhetsklarering för personer eller anläggningar ska den part som begärde intyget om säkerhetsklarering för anläggningar eller för personer underrättas om åtgärden.

6. Varje part ska på begäran av den andra parten samarbeta vid omprövningar och undersökningar som avser säkerhetsklareringar.

Artikel 11

Förlust eller fara

1. I händelse av förlust av eller fara för sekretessbelagd information eller sekretessbelagd utrustning och materiel eller misstanke om att sådan sekretessbelagd information, utrustning eller materiel har förlorats eller utsatts för fara ska mottagarparten omedelbart underrätta sändarparten.

2. Mottagarparten ska omedelbart genomföra en undersökning, vid behov tillsammans med sändarparten, i enlighet med det egna landets lagar och andra författningar. Mottagarparten ska så snart som möjligt underrätta sändarparten om omständigheterna kring undersökningen, dess resultat och vilka åtgärder som har vidtagits för att förhindra att händelsen upprepas.

Artikel 12

Tvister

Tvister om tolkningen eller tillämpningen av detta avtal ska uteslutande lösas genom samråd mellan parterna; de får inte hänskjutas till nationell eller internationell domstol eller till någon annan fysisk eller juridisk person för avgörande.

Artikel 13

Ikraftträdande

Avtalet träder i kraft den dag det har undertecknats av båda parterna.

Artikel 14

Ändringar

Bestämmelserna i detta avtal får ändras efter skriftligt samtycke från båda parterna.

Artikel 15

Uppsägning och översyn

1. Detta avtal ska förbli i kraft till dess att den allmänna överenskommelsen om sekretesskydd av militär information av den 4 och 23 december 1981 eller avtalet sägs upp. När avtalet har upphört att gälla ska båda parterna vara ansvariga för skyddet av sekretessbelagd information som har utbytts i enlighet med avtalet och för kontrakt som har ingåtts eller framställts till följd därav i enlighet med nationella lagar och andra författningar.

2. Parterna får göra en gemensam översyn av avtalet senast tio år från dess ikraftträdande.

3. Likaså ska sekretessbelagd information, utrustning och materiel som utbytts i enlighet med detta avtal skyddas, även om överföringen har skett efter det att någon av parterna har sagt upp avtalet.

Bilagor till säkerhetsskyddsavtalet mellan Sverige och Förenta staterna:

A. Rutiner för hantering av kontrollerad icke-sekretessbelagd information

B. Besöksrutiner

Till bekräftelse härav har undertecknade, därtill vederbörligen bemyndigade av sina respektive regeringar, undertecknat detta avtal.

Upprättat i två exemplar på engelska språket.

För Konungariket Sveriges regering
Jonas Hafström
Ambassadör
April 11, 2008
Washington DC

För Amerikas Förenta Staters regering
Jay M Cohen
DHS Undersecretary S+T
April 11, 2008
Washington DC

BILAGA A

Rutiner för hantering av kontrollerad icke-sekretessbelagd information

1. DEFINITION

Kontrollerad icke-sekretessbelagd är information för vilken det har fastställts begränsningar i fråga om delgivning och spridning i enlighet med Förenta staternas nationella lagar, andra författningar och riktlinjer. Information som tillhandahålls eller framställs med stöd av avtalet ska märkas så att det framgår att det rör sig om känslig information. Kontrollerad icke-sekretessbelagd information ska i Sverige behandlas i enlighet med tryckfrihetsförordningen och sekretesslagen.

2. Rätt att ta del av information

Kontrollerad icke-sekretessbelagd information ska vid behov spridas i tjänsten. Kontrollerad icke-sekretessbelagd information får också lämnas ut till tjänstemän på andra verkställande, lagstiftande och rättsliga myndigheters ministerier och organ för ett lagligt och tillåtet offentligt ändamål.

Det slutgiltiga ansvaret för att fastställa om en person har ett giltigt skäl att få ta del av information som betecknats som kontrollerad icke-sekretessbelagd information ligger hos den person som är behörig innehavare av, har kunskap om eller kontrollerar informationen. För att få ta del av känslig information och känsliga uppgifter måste alla tilltänkta mottagare besvara vissa frågor från informationsinnehavaren om varför de behöver informationen.

2.1. Alla behöriga personer har ansvar för att säkerhetsskydda de handlingar som de själva innehar som innehåller kontrollerad icke-sekretessbelagd information.

2.2. Handlingar som innehåller kontrollerad icke-sekretessbelagd information ska förvaras på ett säkert ställe när de inte används, t.ex. i ett låst arkivskåp eller kontor.

2.3. Alla handlingar som innehåller icke-sekretessbelagd information ska säkerhetsskyddas vid dagens slut. Personer som hanterar handlingar som innehåller kontrollerad icke-sekretessbelagd information ska säkerhetsskydda dem innan de lämnar arbetsplatsen.

2.4. Behöriga användare får inte på något sätt sprida kontrollerad icke-sekretessbelagd information till obehöriga personer.

2.5. Handlingar som innehåller kontrollerad icke-sekretessbelagd information ska täckas över, vändas med texten nedåt, läggas åt sidan eller skyddas på annat sätt när obehöriga personer är närvarande.

2.6. Kontaktpersoner för program måste försöka vara diskreta när de diskuterar känslig information i offentliga lokaler eller på andra mötesplatser, t.ex. när de är på resa eller deltar i ett offentligt möte.

3. MÄRKNING AV KONTROLLERAD ICKE-SEKRETESSBELAGD INFORMATION

Information som har fastställts som kontrollerad icke-sekretessbelagd information ska märkas tydligt så att det är lätt att se att det rör sig om kon-

trollerad icke-sekretessbelagd information. Om ytterligare nationella restriktioner eller förfaranden måste tillämpas ska märkningen se ut på följande sätt: CONTROLLED UNCLASSIFIED/KONTROLLERAD ICKE-SEKRETESSBELAGD (-- namn på restriktion --). För att se till att informationen skyddas på lämpligt sätt ska märkningen göras när handlingarna utarbetas eller så snart kontrollerad icke-sekretessbelagd information inkluderas i en befintlig handling. Materiel som innehåller kontrollerad icke-sekretessbelagd information ska märkas med

PROPERTY OF (JURISDICTION NAME OR GOVERNMENT AGENCY PROGRAM)
CONTROLLED UNCLASSIFIED/TILLHÖR (NAMN PÅ JURISDIKTION ELLER MYNDIGHETSPROGRAM)
KONTROLLERAD ICKE-SEKRETESSBELAGD

längst ned på framsidan, titelsidan och alla sidor i handlingen eller akten. Annan materiel än pappershandlingar, t.ex. diabilder, datormedier och filmer, måste också märkas på samma sätt på varje sida eller diabild. Elektroniskt överförda meddelanden, t.ex. e-postmeddelanden, som innehåller kontrollerad icke-sekretessbelagd information måste märkas med förkortningen CUI innan själva texten börjar. Handlingar med kontrollerad icke-sekretessbelagd information som överförs till kontakter som inte dagligen arbetar med den här typen av information ska vara försedda med en utökad märkning på handlingens framsida så att innehavarna förstår vad för slags information det rör sig om.

4. ELEKTRONISK ÖVERFÖRING

4.1. Överföring via e-post eller Internet

4.1.1. Kontrollerad icke-sekretessbelagd information som skickas med e-post ska skyddas med hjälp av kryptering eller överföras i säkra kommunikationssystem. Om detta är opraktiskt eller omöjligt får den kontrollerade icke-sekretessbelagda informationen skickas som vanlig e-post. För att öka säkerheten när informationen skickas med vanlig e-post kan den kontrollerade icke-sekretessbelagda informationen bifogas som en lösenordsskyddad bilaga och lösenordet skickas i ett separat meddelande. Mottagarna av kontrollerad icke-sekretessbelagd information ska följa alla restriktioner från avsändaren när det gäller e-post.

4.1.2. På grund av den inneboende sårbarheten uppmanar ministeriet för nationell säkerhet myndigheterna att om möjligt inte skicka kontrollerad icke-sekretessbelagd information till personliga e-postkonton.

4.1.3. Kontrollerad icke-sekretessbelagd information får enbart läggas ut på en webbplats på Internet om tillträdet till webbplatsen är begränsat till en viss målgrupp och informationen är krypterad.

4.2. Överföring via fax

4.2.1. Om avsändaren inte har infört några andra begränsningar får kontrollerad icke-sekretessbelagd information skickas via en ej säkerhetsgodkänd fax. Om en ej säkerhetsgodkänd fax används ska sändarparten stämma av med mottagaren att den materiel som faxas inte lämnas utan tillsyn eller utsätts för eventuellt otillåtet röjande hos mottagarparten.

5. POST

Kontrollerad icke-sekretessbelagd information får skickas med förstaklasspost, paketpost eller – om det rör sig om bulktransporter – fjärdeklasspost. Dubbla kuvert (ett ytterkuvert och ett innerkuvert) måste användas när kontrollerad icke-sekretessbelagd information skickas med post. Ytter- och innekuverten måste vara märkta med mottagarens namn och adress och avsändarens namn. Innerkuvertet måste dessutom vara försett med en stämpel. Avsändaren måste använda *mottagningsbevis* eller skicka brevet med rekommenderad post.

6. DISKUSSION

Kontaktpersoner för program som behöver diskutera kontrollerad icke-sekretessbelagd information i telefon, särskilt i mobiltelefon på offentlig plats, måste vara medvetna om sin omgivning och behovet av att vara diskret. Kontrollerad icke-sekretessbelagd information får exempelvis inte diskuteras på platser där det finns risk att personer som inte är delaktiga i programmet kan råka höra det. Om informationen måste diskuteras måste det ske så diskret som möjligt.

7. KOPIERING

Kopiering av handlingar som innehåller kontrollerad icke-sekretessbelagd information måste begränsas till ett minimum.

8. FÖRSTÖRING

Handlingar som innehåller icke-sekretessbelagd information ska när de inte längre behövs förstöras genom strimling eller på annat sätt så att handlingen blir oläslig. Förstöringen kan göras på följande sätt:

8.1. Pappershandlingar ska förstöras genom strimling, bränning, makulering eller pulvrisering så att de inte går att känna igen och rekonstruera.

8.2. Elektroniska lagringsmedier ska tömmas på lämpligt sätt genom överskrivning eller avmagnetisering.

BILAGA B

BESÖKSRUTINER

1. I denna bilaga beskrivs rutinerna för framställningar om besök. För alla besök krävs förhandstillstånd från båda parterna. För besök i Sverige och Förenta staterna som omfattar rätten att ta del av eller utbyta sekretessbelagd information krävs ett intyg om säkerhetsklarering för personer. Detta intyg krävs emellertid inte vid övriga besök som omfattar icke-sekretessbelagd information eller kontrollerad icke-sekretessbelagd information.

2. De enskilda parterna har utsett följande myndigheter att handlägga framställningar om besök från den andra parten:

Sverige:	Förenta staterna:
Försvarets materielverk	Science and Technology Directorate
Säkerhet	Department of Homeland Security
SE-115 88 Stockholm	Washington, D.C. 20528
SVERIGE	USA

Parterna får komma överens om att låta andra myndigheter som har utsetts av säkerhetsskyddsmyndigheten för avtalet handlägga framställningar om besök.

3. Följande uppgifter krävs för att framställningar om besökstillstånd ska beviljas:

a. Begärande anläggning. Ange anläggningens fullständiga namn, postadress (inklusive postnummer, ort, land samt i USA även delstat) telefon- och faxnummer.

b. Anläggning som ska besökas. Ange fullständigt namn, postadress (inklusive postnummer, ort, land samt i USA även delstat), telefon- och faxnummer.

c. Kontaktpunkt vid den anläggning som ska besökas. Ange fullständigt namn, titel, kontor, telefonnummer och e-postadress.

d. Besöksdatum. Ange aktuellt datum eller tidsperiod (fr.o.m.–t.o.m.) för besöket. Dag/månad/år.

e. Ämne som ska diskuteras/motivering. Ge en kortfattad beskrivning av de frågor eller ämnen som ska diskuteras och anledningen till besöket. Använd inte förkortningar som inte förklaras. Om det är fråga om en framställning om återkommande besök bör denna punkt inledas med orden ”återkommande besök” (t.ex. återkommande besök för att diskutera) eller om det är fråga om en ändring (ändring av besök id-nummer).

f. Sekretessgraden för den information som ska diskuteras. Ange högsta sekretessgrad för den information som ska diskuteras. Ange också fullständigt namn på det avtal, program eller den aktivitet som föranleds av besöket.

g. Närmare upplysningar om besökaren/besökarna.

Namn
Befattning
Leverantör/offentlig myndighet
Kön
Födelsedatum
Födelseort (ort och land)

Status för säkerhetsklarering (bara om sekretessbelagd information ska diskuteras)

Säkerhetsklarering utfärdad av (bara om sekretessbelagd information ska diskuteras)

Passnummer/identitetsnummer

Passets giltighetstid

Nationalitet

h. Säkerhetstjänsteman för den begärande leverantören/offentliga myndigheten.

Ange namnet på och telefonnumret till den begärande säkerhetstjänstemannen.

i. Intyg om säkerhetsklarering. Ska fyllas i av tillämplig offentlig klareringsmyndighet.

j. Anmärkningar. Den här punkten kan användas för att ange vissa administrativa krav (t.ex. föreslagen resväg, begäran om hotellbokningar och/eller transport). Vid brådskande besök bör namnet på den insatta person med vilken villkoren för besöket har gjorts upp i förväg anges samt hans eller hennes telefon- och faxnummer.

4. Framställningar om besök bör lämnas till den part som ska ta emot besöket 20 arbetsdagar i förväg vid icke-sekretessbelagda besök och 30 arbetsdagar i förväg vid sekretessbelagda besök. Vid förlängda besök, där besökarna måste stanna på platsen under en sammanhängande tidsperiod som är längre än 30 dagar, krävs en framförhållning på 30 dagar.

5. Oförutsedda händelser som kräver att enskilda personer måste göra brådskande besök som, på grund av brådskan, inte medger sedvanlig framförhållning för besöksansökan kommer att granskas kritiskt och måste godkännas av båda parterna. Tillstånd för sådana besök kan inte garanteras och får därför inte begäras om de inte är brådskande.

6. Den anläggning som tar emot besöket ska se till att besökarna aldrig lämnas ensamma och att de inte får ta del av information eller ges tillträde till områden om de inte har ett fastställt behov av kännedom i tjänsten.

SECURITY ARRANGEMENT ESTABLISHED PURSUANT TO THE AGREEMENT BETWEEN THE GOVERNMENT OF THE KINGDOM OF SWEDEN AND THE GOVERNMENT OF THE UNITED STATES OF AMERICA ON COOPERATION IN SCIENCE AND TECHNOLOGY FOR HOMELAND/DOMESTIC SECURITY MATTERS OF 13 APRIL 2007

Purpose

The following procedures have been developed by the Government of the Kingdom of Sweden and the Government of the United States of America, (hereinafter referred to as "the Parties") in amplification of Article 12 of the Agreement between the Government of the Kingdom of Sweden and the Government of the United States of America on Cooperation in Science and Technology for Homeland Security Matters dated 13 April 2007, (hereinafter "the Agreement"). These procedures further 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, dated December 4 and 23, 1981.

Within the framework of their national legislation, each Party shall take all appropriate measures to ensure the protection of Classified Information and Classified Equipment and Material provided pursuant to these security procedures. This document implements the Agreement, therefore all terms and conditions therein apply to these procedures. If there is a discrepancy as to meaning, the provisions in the Agreement take precedence.

ARTICLE 1

Definitions

The following definitions will be used for the purpose of these procedures:

Agreement Security Authority (ASA)	The government authority responsible for the development of policies and procedures governing security of Classified Information covered by these procedures.
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.

Equipment and Material	Any document, product or substance on or in which information may be recorded or embodied. Material shall encompass everything regardless of its physical character of makeup including 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 material from which information can be derived.
Facility Security Clearance Assurance (FSCA)	A certification provided by the ASA for a facility under its territorial jurisdiction which indicates that the is facility 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 will be protected by the Contractor on which the FSCA is provided in accordance with the provisions of these procedures and that compliance shall be monitored and enforced by the responsible ASA.
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.
Personnel Security Clearance Assurance	(a.) A certification provided by the ASA concerning level of personnel security clearance held by an individual who is employed by a government agency, or Contractor facility under the jurisdiction of the ASA. (b.) A statement provided by the ASA 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 for individuals who are a citizen of one Party but is to be employed by the other Party or its Contractors.
Receiving Party	The Party to which Classified Information is transferred.
Sending Party	The Party that originates and/or transfers Classified Information to the Receiving Party.

ARTICLE 2

Designation of Authorities

1. Each of the Parties shall appoint an Agreement Security Authority (ASA) as the government single point of contact and authority responsible for the development of policies and procedures governing security of Classified Information covered by these procedures. Those persons shall be responsible for the policies and procedures governing the security of Classified Information. For the Government of the Kingdom of Sweden, the Agreement Security Authority is the Director in the Office of Security of the Defense Materiel Administration (FMV). For the US, the ASA is the Director in the Office of Security, Science and Technology Directorate, Department of Homeland Security. Both ASAs shall provide policy oversight concerning the provisions of this document. As appropriate for individual Project Arrangements concluded pursuant to the Agreement, different ASAs may be named.

2. Each ASA may designate other government agencies to perform the security obligations of that Party. Notwithstanding any such designation, the ASA retains oversight and management responsibility over the implementation of the provisions of this Security Arrangement.

ARTICLE 3

Restrictions of the Use and Disclosure of Exchanged Classified and Controlled Unclassified Information

1. Each Party shall take all lawful steps available to ensure that Classified Information exchanged, generated or otherwise provided pursuant to the Agreement is protected from further disclosure, unless the Sending Party consents to such disclosure.

2. The Receiving Party shall not pass or disclose Classified Information to: (1) any person holding the citizenship of a third country, (2) any international organization, nor (3) the general public without the prior written permission of the Sending Party.

3. Nothing in these procedures shall 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 is obtained.

4. Controlled Unclassified Information shall be handled in accordance with the provisions of Appendix A.

ARTICLE 4

Protection of Classified Information

1. Upon receipt of Classified Information furnished under the Agreement, the Receiving Party shall undertake to afford the information a degree of security protection at least equivalent to the security protection provided by the Sending Party.

2. Each Party shall assume responsibility for ensuring the administration of security measures for all Contracts involving Classified Information awarded to industry for performance in their respective countries pursuant to the Agreement.

3. Access. Access to Classified Information shall be limited to those persons who have a Need-to-Know and have been security cleared by the appropriate Party in accordance with its national laws and regulations to the level at least equal to the classification of the information to be accessed.

4. Inspection/Security Review. The ASA shall ensure that periodic industrial security inspections/security reviews are made for each government and Contractor facility located within their country and engaged in the performance of, or in negotiations for any Agreement activity involving Classified Information.

5. Security Clearances. Clearances of facilities and individuals that shall possess or be authorized access to Classified Information shall be processed according to the pertinent regulations of the country having responsibility for administering security measures for the Classified Information.

6. Security Training. The Parties shall ensure that individuals and facilities 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 these security procedures.

ARTICLE 5

Transfer of Classified Information

1. Classified Information shall normally be transferred between the Parties using official government-to-government channels (e.g., diplomatic courier service or military courier). Other channels may be established if mutually agreed by the ASAs and should ensure that government accountability and control is maintained from the point of origin to the ultimate destination. The ASAs shall approve the procedures and inform the facilities of the alternative channels of transmission that may be used. Material shall be prepared for transmission in accordance with the national security laws and regulations of the Sending Party.

2. Classified Information may be transmitted electronically using security means that have been approved by each Party's communications security authorities.

ARTICLE 6

Public Release of Information

1. Public release by a government agency, Contractor, or sub-contractor of any Classified Information shall be governed in Sweden by the Freedom of the Press Act, with relevant exceptions under the Secrecy Act. In the US, public release shall be governed by the National Industrial Security Program Operating Manual (NISPOM) and DOD 5220.22-M.

2. A Swedish Facility with a US Classified Contract may publicly disclose information only after advance written approval from the US ASA and in accordance with the Official Secrets Act. In the case of a US Facility with a Swedish Classified Contract, initial prior review and approval shall be governed by the NISPOM with final approval by the Swedish ASA.

ARTICLE 7

Marking

1. The Sending Party shall ensure that documents containing Classified Information are marked with appropriate classification markings and pre-fixed with the country of origin/ownership prior to transfer to the Receiving Party. Upon receipt, the Classified 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 Markings

Kingdom of Sweden		United States of America
Defense agencies	**Civil agencies**	
HEMLIG/ TOP SECRET	HEMLIG Av synnerlig betydelse för rikets säkerhet	US TOP SECRET
HEMLIG/SECRET	HEMLIG	US SECRET
HEMLIG/CONFIDENTIAL	Ref. 1	US CONFIDENTIAL
HEMLIG/RESTRICTED	Not applicable	TREAT AS US CONFIDENTIAL (Ref. 2)

Ref. 1. US information on the level of US CONFIDENTIAL shall be treated as HEMLIG by civil agencies in Sweden.

Ref. 2. Swedish information on the level of HEMLIG/RESTRICTED shall be marked as "TREAT AS US CONFIDENTIAL" and shall be treated as US CONFIDENTIAL.

2. Classified Information produced or reproduced by a Receiving Party shall be marked with the assigned classification markings of both countries as provided above. The markings shall be applied in the manner prescribed by the regulations of the country in which the information is produced or reproduced.

ARTICLE 8

Contracts

1. A Party who proposes to place a Contract or sub-contract involving Classified Information with a Contractor in the other Party's country, shall request, via their ASA, a FSCA as defined in paragraph 2, where appropriate, from the ASA of the other Party. The FSCA will carry a responsibility that the security conduct of the cleared Contractor shall be in accordance with national security laws or regulations and be monitored by that Party's ASA.

2. Security Requirements Clause. The Party or Contractor negotiating a Classified Contract or sub-contract shall incorporate appropriate security clauses in all documents. For contracts involving Controlled Unclassified Information, the Parties shall incorporate the security provisions in Appendix A into all such contracts. A copy of the relevant portions of the Contract, request for proposal, or sub-contract, including the security requirements clause, shall be furnished promptly through appropriate channels to the ASA of the Party where the Contract is placed in order to enable them to furnish security supervision over the Contract.

3. Security Classification Guidance. The ASA of the contracting Party shall furnish the Contractor or sub-contractor with the security classification guidance pertaining to each classified aspect related to the Contract. For Sweden, this guidance shall be set forth in a Security Aspect Letter (SAL) and in the US, by way of a Contract Security Classification Specification (DD Form 254). In addition, US Contractors shall coordinate with Defense Security Service and reference the NISPOM. The guidance must identify and assign a proper security classification to any Classified Information which is furnished by the contracting Party in connection with the Contract, or generated pursuant to the Classified Contract. A copy of the written security classification guidance will be submitted to the ASA of the Contractor's country.

4. Sub-Contracts. Unless specifically prohibited in the Classified Contract, a Contractor may sub-contract within the country of either Party in accordance with: the security procedures prescribed in that country for classified sub-contracts, the procedures established by this document for placing a classified prime Contract in that country.

5. 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 sub-contract 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 shall not have access to Classified Information that is provided to 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 shall be obtained prior to permitting such access.

ARTICLE 9

International Visits

1. All international visits require the prior approval of both Parties. Requests for approval of visits shall be submitted using the procedures in Appendix B. In addition, sub-contractors must always inform their prime Contractor before making a visit request to any facility related to a cooperative activity under the Agreement.

2. Approval for such visits shall be granted only to persons possessing security clearances at least at the level of the information to which access shall be given. Authorization for visitors to have access to such Classified Information shall be limited to those who have a Need-to-Know.

ARTICLE 10

Security Assurances Related to National Security Clearances of Facilities or Individuals of the Others Country

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

2. When requested, the Party receiving the request shall determine the security clearance status of the facility or individual that is the subject of the enquiry and forward a FSCA or PSCA if the facility or individual is already cleared. If the facility or individual does not have a security clearance, or the facility or individual has a clearance that is at a lower security level that that requested, notification shall 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 enquiries that are necessary to meet the requirement. Following successful enquiries, a FSCA or PSCA shall be provided to the requesting Party.

3. 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 shall be notified.

4. If either Party learns of any derogatory information about a facility or an individual for whom it has furnished a FSCA or PSCA, it shall notify the other Party of the action it intends to take, or has taken. Either Party may request, at any time, a review of any FSCA or PSCA that has been furnished by the other Party. The requesting Party shall be notified of the results of the review and any subsequent action.

5. If either Party invalidates, suspends or takes action to revoke a personnel or facility security clearance, the Party that requested the FSCA or PSCA shall be notified of the action.

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

ARTICLE 11

Loss or Compromise

1. In the event of the loss or compromise of Classified Information or Classified Equipment and Material or suspicion that such Classified Information or Classified Equipment and Material may have been lost or compromised, the Receiving Party shall immediately inform the Sending Party.

2. The Receiving Party shall carry out an immediate investigation 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 shall 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.

ARTICLE 12

Disputes

Any dispute regarding the interpretation or application of this Arrangement shall be resolved only by consultation between the Parties and shall not be referred to a national or international tribunal or to any other person or entity for resolution.

ARTICLE 13

Effective Date

This Arrangement is effective upon the date of the last signature.

ARTICLE 14

Amendment

The provisions of this document may be amended with the mutual advance, written consent of both Parties.

ARTICLE 15

Termination/Review

1. This Arrangement will remain in effect until termination of the December 4 and 23, 1981 General Security of Military Information Agreement or the Agreement. Both Parties shall remain responsible after termination for the safeguarding of all Classified Information exchanged pursuant to the Agreement and any Contracts entered into, or generated there from, in accordance with national laws and regulations.

2. This Arrangement may be reviewed jointly by the Parties no later than ten years after its effective date.

3. Similarly, any Classified Information or Classified Equipment and Material exchanged under this Arrangement shall also be safeguarded, even though its transfer may occur following notice by either of the parties to terminate.

Appendices to the Sweden-US Security Arrangement

A. Procedures for Handling Controlled Unclassified Information
B. Visit Procedures

IN WITNESS WHEREOF, the undersigned, duly authorized by their respective governments, have signed this Arrangement.

DONE, in duplicate, in the English language.

FOR THE GOVERNMENT OF THE KINGDOM OF SWEDEN

Signature

JONAS HAFSTRÖM
Name

Title

April 11, 2008
Date

Washington DC
Location

FOR THE GOVERNMENT OF THE UNITED STATES OF AMERICA

Signature

JAY M COHEN
Name

DHS Under Sec S&T
Title

April 11, 2008
Date

Washington, DC
Location

APPENDIX A

Procedures for Handling Controlled Unclassified Information

1. **DEFINITION**

Controlled Unclassified Information is information to which access or distribution limitations have been applied in accordance with the national laws, regulations or policies of the US. Whether the information is provided or generated under the Agreement, it will be marked to identify its sensitive character. Controlled Unclassified Information will be handled in Sweden in accordance with the Freedom of the Press Act and the Secrecy Act.

2. **ACCESS**

Controlled Unclassified Information should be disseminated as necessary in the conduct of official business. Controlled Unclassified Information may also be released to officials in other departments and agencies of the executive, legislative, and judicial branches, as needed for a lawful and authorized government purpose.

The final responsibility for determining whether an individual has a valid need for access to information designated Controlled Unclassified Information rests with the individual who has authorized possession, knowledge, or control of the information. In pursuing access to sensitive information and data, any prospective recipient must respond to questions from the information holder about why they need this information.

2.1. All authorized persons are responsible for securing any Controlled Unclassified Information documents in their personal possession.

2.2. When not in use, Controlled Unclassified Information documents must be stored in a secured area, such as a locked file cabinet or office.

2.3. All Controlled Unclassified Information documents must be secured at the end of the day. Persons handling Controlled Unclassified Information documents must secure them before leaving their work area.

2.4. Authorized users must not in any manner disclose Controlled Unclassified Information to an unauthorized person.

2.5. When unauthorized persons are present, Controlled Unclassified Information documents must be covered, turned face-down, removed from the area, or otherwise protected.

2.6. Program contacts must attempt to be discreet when discussing sensitive information in public venues or meeting spaces—for example, while on travel or attending a public meeting.

3. **MARKING CONTROLLED UNCLASSIFIED INFORMATION**

Information that has been designated Controlled Unclassified Information must be plainly marked so that it is easy to recognize as being Controlled Unclassified. In the event that additional domestic restrictions or procedures must be applied, the marking will appear as CONTROLLED UNCLASSIFIED (--name of restriction--). To promote proper protection of information, markings must be applied at the time documents are drafted or as soon as

Controlled Unclassified Information is added to an existing document. Materials containing Controlled Unclassified Information will be marked

PROPERTY OF (JURISDICTION NAME OR GOVERNMENT AGENCY PROGRAM)
CONTROLLED UNCLASSIFIED

at the bottom of the front cover, title page, and all pages contained within the document or file. Material other than paper documents, such as slides, computer media, or films, must also bear these markings on each page or slide. Electronically transmitted messages (for example, e-mails) containing Controlled Unclassified Information must bear the abbreviation CUI before the beginning of the text. Controlled Unclassified Information transmitted to contacts who do not work with this information on a daily basis must bear an expanded marking on the face of the document so that holders understand the status of the information.

4. ELECTRONIC TRANSMISSION

4.1. Transmittal via E-mail or the Internet

4.1.1. Controlled Unclassified Information transmitted via e-mail must be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, Controlled Unclassified Information may be transmitted over regular e-mail channels. For added security, when transmitting Controlled Unclassified Information over a regular e-mail channel, the information can be included as a password-protected attachment, with the password provided in a separate message. Recipients of Controlled Unclassified Information must comply with any e-mail restrictions imposed by the originator.

4.1.2. Due to inherent vulnerabilities, DHS recommends that agencies avoid sending Controlled Unclassified Information to personal e-mail accounts, where possible.

4.1.3. Controlled Unclassified Information may be put on an Internet Web site only if access to the site is limited to a specific target audience and the information is encrypted.

4.2. Transmittal via Fax

4.2.1. Unless otherwise restricted by the originator, Controlled Unclassified Information may be sent via nonsecure fax. Where a nonsecure fax is used, the sender must coordinate with the recipient to ensure that the materials faxed must not be left unattended or subjected to possible unauthorized disclosure on the receiving end.

5. MAILING

Controlled Unclassified Information may be transmitted via first class mail, parcel post, or—for bulk shipments—fourth-class mail. When mailing Controlled Unclassified Information, two envelopes (an outer and inner) must be used. The outer and inner envelopes must bear the recipient's name and address and the sender's name. Additionally, the inner envelope must be stamped. The sender must use an "*acknowledgement of receipt*" or registered mail service.

6. **DISCUSSION**

Program contacts that need to discuss Controlled Unclassified Information over the telephone, particularly over cell phones in public places, must be aware of their surroundings and the need to be discreet. For example, Controlled Unclassified Information must not be discussed where one can be overheard by people who have no involvement in the program. If a discussion must take place, it must be as discreet as possible.

7. **COPYING**

Reproduction of documents containing Controlled Unclassified Information must be kept to a minimum.

8. **DESTRUCTION**

When no longer needed, Controlled Unclassified Information must be destroyed by shredding or other destructive technique that renders the document unreadable. Destruction may be accomplished by either of the following methods:

8.1. Destroy paper copies by shredding, burning, pulping, or pulverizing, so as to assure destruction beyond recognition and reconstruction.

8.2. Electronic storage media must be sanitized appropriately by overwriting or degaussing.

APPENDIX B

VISIT PROCEDURES

1. This appendix describes the visit request procedures. Prior approval of both Parties is required for all visits. Visits to Sweden and the United States that involve access to, or the exchange of, Classified Information require the passing of a Personnel Security Clearance Assurance (PSCA). All other visits relating to unclassified information or Controlled Unclassified Information do not require PSCAs.

2. The offices listed below have been designated by each Party to process visit requests that are received from the other Party.

Sweden:	United States:
Defense Materiel Administration	Science and Technology Directorate
Security	Department of Homeland Security
SE 115 88 Stockholm	Washington, D.C. 20528
SWEDEN	USA

The Parties may agree to process visit requests through other agencies, as so designated by the ASA.

3. Requests for approval of visits require the following information:

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

   b. Hosting Facility. Provide the full name, postal address (include city, state, country, and postal zone), telephone and fax numbers.

   c. Point of Contact at Hosting Facility. Provide the full name, title, office, telephone and email address.

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

   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. Classification of Information to be Discussed. Indicate the highest level of Classified Information to be discussed. Specify the full name of the Agreement, program or activity that is being supported by this visit.

g. Particulars of Visitor(s).

Name
Position
Contractor/Government Agency
Gender
Date of Birth
Place of Birth (city and country)
Security Clearance status (only if discussing Classified Information)
Security Clearance granted by (only if discussing Classified Information)
Passport Number/Identification Number
Passport Expiration Date
Nationality

h. Security Officer of the Requesting Contractor/Government Agency.
Provide the name and telephone number of the requesting security officer.

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

j. Remarks. This item can be used for certain administrative requirements (e.g., proposed itinerary, requests of hotel reservations, and/or transportation. In the case of an emergency visit, the name, telephone and telefax numbers of the knowledgeable person with whom advance arrangements have been made should be stated.

4. Visit requests should be submitted to the hosting Party 20 working days in advance of Unclassified visits and 30 working days in advance of Classified visits. Extended visits, when visitors are required to remain on-site for a continuous period of greater than 30 days, require a lead-time of 30 days.

5. Unforeseen circumstances requiring individuals to undertake urgent visits which, due to the urgency, do not permit the usual visit notification lead times to be processed will be critically reviewed and must be agreed to by both Parties. Approval for such visits cannot be guaranteed and must not therefore be requested unless the urgency exists.

6. It is the responsibility of the host site to ensure that the visitor is escorted at all times and is not allowed access to information or areas for which a Need-to-Know has not been established.

Edita Stockholm 2009