Viss översyn av verksamhet och organisation på informationssäkerhetsområdet

Betänkande från Informationssäkerhetsutredningen

SOU 2010:25

Till statsrådet och chefen för Försvarsdepartementet

Regeringen beslutade den 19 november 2009 att tillkalla en särskild utredare med uppdrag att utreda formerna för och konsekvenserna av att flytta ansvaret för dels Sveriges IT-incidentcentrum (Sitic) från Post- och telestyrelsen (PTS) dels Sveriges certifieringsorgan för IT-säkerhet (CSEC) från Försvarets materielverk (FMV). Utredaren ska undersöka vilken myndighet av Försvarets radioanstalt (FRA) och Myndigheten för samhällsskydd och beredskap (MSB) som bedöms bäst lämpad att vara ansvarig utifrån de behov och målsättningar som regeringen angett när det gäller att bland annat samla informationssäkerhetsfrågorna. Utredaren ska också föreslå en myndighet att vara signatär för både CCRA (*Common Criteria Recognition Arrangement*) och SOGIS-MRA (*Senior Officials Group Information Systems Security – Mutual Recognition Agreement*).

Som särskild utredare förordnade chefen för Försvarsdepartementet den 11 december 2009 departementsrådet Jan Hyllander. Som sekreterare förordnades Avdelningschef Magnus Hjort, analytiker Andreas Wedner (från den 7 december 2009 till den 1 februari 2010) och analytiker Nina Wilhelmson (från den 1 februari 2010). Anders Jacobsson har varit utredningsassistent. Departementssekreterarna Ingolf Berg och Linda Ericson har varit sakkunnig respektive expert i utredningen.

Den 14 januari 2010 beslutade regeringen om tilläggsdirektiv för uppdraget. Utredningstiden förlängdes och uppdraget ska slutredovisas senast den 1 april 2010. En delrapport, Lokalisering av Sveriges IT-incidentcentrum, om formerna för och konsekvenserna av att flytta Sitic från PTS lämnades till regeringen den 1 februari 2010.

Utredningen, som har tagit namnet Informationssäkerhetsutredningen, överlämnar härmed betänkandet *Viss översyn av*

verksamhet och organisation på informationssäkerhetsområdet (SOU 2010:25).

Stockholm 31 mars 2010

Jan Hyllander

/ Magnus Hjort
Andreas Wedner
Nina Wilhelmson

Innehåll

Sammanfattning

Utredarens uppdrag är att utreda formerna för och konsekvenserna av en eventuell förflyttning av ansvaret för dels Sitic från PTS, dels CSEC från FMV, till antingen MSB eller FRA. Utredaren ska undersöka vilken av de två myndigheterna som bedöms bäst lämpad att vara ansvarig utifrån de behov och målsättningar som regeringen angett när det gäller bland annat att samla informationssäkerhetsfrågorna. Vidare ska utredaren föreslå en myndighet att vara signatär för de internationella överenskommelserna CCRA och SOGIS-MRA.

En delrapport, Lokalisering av Sveriges IT-incidentcentrum, lämnades till regeringen den 1 februari 2010. I den rapporten föreslår utredaren att personalen och verksamheten vid Sitic inordnas i MSB. Formellt torde detta kunna ske den 1 januari 2011. De lokaler som är särskilt anpassade för Sitics verksamhet, då PTS den 1 mars 2010 flyttat till Valhallavägen, kan dock behöva disponeras under en övergångsperiod under 2011. Utredaren vill betona att denna övergångsperiod bör vara så kort som möjlig då de synergieffekter som redovisats kräver en samlokalisering med relevanta verksamheter vid MSB.

Utredaren föreslår vidare att PTS nuvarande uppgifter enligt 6 § i myndighetens instruktion gällande Sitics verksamhet i sin helhet överförs till MSB. I förordningen (2008:1002) med instruktion för MSB bör därför en motsvarande bestämmelse föras in samtidigt som nuvarande 6 § i PTS instruktionsförordning ska upphävas. Ändringen bör träda i kraft den 1 januari 2011.

Utredarens bedömning är att förslaget att inordna verksamheten vid Sitic i MSB skulle få positiva konsekvenser både för arbetet med informationssäkerhet samt för arbetet med samhällets krisberedskap i stort och alltså gagna både det arbete som Sitic och MSB utför idag. Genom att placera Sitic vid MSB åstadkoms en mer samlad lösning av ansvaret för informationssäkerhet på central

myndighetsnivå. Det skapas också möjligheter att bättre integrera informationssäkerhetsarbetet i arbetet med samhällets krisberedskap, t.ex. arbetet med risk- och sårbarhetsanalyser.

Utredaren föreslår att CSEC tills vidare blir kvar som en organisatorisk enhet inom FMV. Utredarens bedömning är att det i nuvarande läge saknas goda skäl att flytta CSEC. Verksamheten vid CSEC och placeringen vid FMV fungerar väl. Vid en omlokalisering finns en risk för ett avbrott eller en betydande nedgång i verksamheten. På längre sikt bör lokaliseringen av CSEC övervägas i anslutning till det av regeringen aviserade fortsatta arbetet med anledning av Stödutredningens rapport *Ett användbart och tillgängligt försvar – Stödet till Försvarsmakten*.

Vid framtida överväganden om lokalisering av CSEC bör det säkerställas att det finns en långsiktig och hållbar lösning som tillgodoser högt ställda krav på oberoende, säkerhet och effektivitet. Den organisatoriska lösning som Sverige väljer måste inge förtroende, både nationellt och internationellt. För att en flytt av verksamheten vid CSEC ska anses rimlig att genomföra bör det finnas betydande synergieffekter att vinna.

Utredaren föreslår vidare att signatärskapet för både CCRA och SOGIS-MRA bör utövas av den myndighet som är certifieringsorgan. Tills vidare bör därför signatärskapet för CCRA överföras från MSB till FMV. Utredaren ser inga skäl till ett uppdelat signatärskap och i flertalet andra länder innehas signatärskap av samma organisation som är certifieringsorgan.

1 Inledning

1.1 Utredarens uppdrag

Regeringen beslutade den 19 november 2009 om kommittédirektiv rörande viss översyn av ansvarsfördelning och organisation när det gäller samhällets informationssäkerhet. Översynen omfattar formerna för och konsekvenserna av en eventuell förflyttning av ansvaret för Sveriges IT-incidentcentrum (Sitic) från Post- och telestyrelsen (PTS) samt Sveriges certifieringsorgan för IT-säkerhet (CSEC) från Försvarets materielverk (FMV). Myndigheten för samhällsskydd och beredskap (MSB) och Försvarets radioanstalt (FRA) har pekats ut som möjlig hemvist för de olika verksamheterna. Vidare ska utredaren föreslå en myndighet som ska vara signatär för den internationella överenskommelsen för ömsesidigt erkännande av certifiering av IT-säkerhetsprodukter kallad *Common Criteria Recognition Arrangement* (CCRA), samt ett liknande europeiskt avtal kallat *Senior Officials Group Information Systems Security – Mutual Recognition Agreement* (SOGIS-MRA).

Ansvaret för informationssäkerhet på nationell nivå är idag uppdelat på ett flertal myndigheter vilket innebär att ansvaret är splittrat. Regeringen ser ett behov av att samla verksamheten på färre aktörer samtidigt som konsekvenserna av eventuella förflyttningar behöver ses över.

Utredaren ska, utöver de verksamhetsmässiga och ekonomiska konsekvenserna även redovisa de personella konsekvenserna av sitt förslag. Utredaren ska kontinuerligt informera Regeringskansliet om arbetets bedrivande. Utredaren ska bland annat beakta det fortsatta arbetet med anledning av Stödutredningens rapport *Ett användbart och tillgängligt försvar - Stödet till Försvarsmakten* (Fö

2009:A), det arbete som Delegationen för e-förvaltning (2009:19) genomför samt InfoSäkutredningens delrapport och betänkanden (SOU 2004:32, 2005:42, 2005:71).

Ett beslut om tilläggsdirektiv fattades av regeringen den 14 januari 2010 (Fö 2009:04) om förlängd utredningstid som innebär att uppdraget ska slutredovisas senast den 1 april 2010. En delrapport Lokalisering av Sveriges IT-incidentcentrum (Fö 2009:04) om formerna för och konsekvenserna av att flytta Sitic från PTS lämnades till regeringen den 1 februari 2010.

1.2 Arbetsform

Utredaren har tagit del av tidigare utredningar och propositioner, samt underlag från myndigheter. Vidare har samtal förts med företrädare för närmast berörda myndigheter, samt med företrädare för Svenska bankföreningen, IT- & Telekomföretagen, Svenskt näringsliv och evalueringsföretag.

1.3 Tidigare utredningar

1.3.1 Sårbarhets- och säkerhetsutredningen

Sårbarhets- och säkerhetsutredningen tillsattes i juni 1999 i syfte att lämna förslag till principer för att åstadkomma en förbättrad helhetssyn avseende planeringen för civilt försvar och beredskapen mot svåra påfrestningar på samhället i fred. Enligt utredningen var ansvaret för informationssäkerhet i Sverige splittrat och det saknades ett sammanhållande system för att hantera allvarliga IT-hot. Med utgångspunkt från bland annat internationella erfarenheter föreslog utredningen i sitt betänkande *Säkerhet i en ny tid* (SOU 2001:41) från i maj 2001 att följande funktioner skulle inrättas:

- Ett tvärsektoriellt samordningsorgan för IT-säkerhet och skydd mot informationsoperationer med placering i Regeringskansliet,
- en funktion för IT-incidenthantering med PTS som chefsmyndighet,

- en funktion för teknikkompetens inom IT-säkerhet med FRA som chefsmyndighet,
- ett svenskt system för evaluering och certifiering med placering vid FMV.

Utredningen föreslog vidare att den tänkta planeringsmyndigheten (sedermera Krisberedskapsmyndigheten) borde ges ett sammanhållande ansvar för samhällets IT-säkerhet och även kunna ha kapacitet att bedriva omvärldsanalys inom områdena IT-säkerhet och informationsoperationer.

1.3.2 InfoSäkutredningen

Regeringen beslutade i juli 2002 att utreda behovet av signalskydd i samhällsviktig verksamhet. Utredningen tog namnet InfoSäkutredningen. Den 20 februari 2003 utökades uppdraget genom ett tilläggsdirektiv där utredningen bland annat fick i uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet borde utvecklas samt hur Sveriges engagemang i det internationella arbetet på informationssäkerhetsområdet skulle utformas.

En delrapport om signalskydd (SOU 2003:27) lämnades till regeringen i februari 2003. En andra delrapport, *Informationssäkerhet i Sverige och internationellt – en översikt*, lämnades i april 2004 (SOU 2004:32). Ytterligare ett delbetänkande *Säker information - Förslag till informationssäkerhetspolitik* lämnades i maj 2005 (SOU 2005:42). InfoSäkutredningens slutbetänkande överlämnades därefter till regeringen i september 2005 (SOU 2005:71) med förslag på organisatoriska förändringar inom informationssäkerhetsområdet.

InfoSäkutredningen konstaterade att rapporteringen av IT-incidenter till Sitic varit mer begränsad än vad som förväntats, bland annat beroende på att verksamheten varit relativt okänd och att sekretessfrågan varit oklar.[1] InfoSäkutredningen såg tydliga fördelar med att ge signalunderrättelsetjänsten en mer aktiv roll i bekämpandet av IT-relaterade hot genom dess unika möjlighet att kartlägga och identifiera illasinnade aktörer.

Utredningen konstaterade att PTS/Sitic genomförde tekniska analyser vars resultat publicerades brett i syfte att kunna informera

[1] SOU 2005:71, s. 104.

samhällets organisationer om nya problem som kunde störa IT-system. Rättsväsendet genomförde tekniska analyser i syfte att säkra bevis. FRA genomförde teknisk analys i syfte att kunna stödja individuella organisationers arbete med informationssäkerhet.

Beträffande ett svenskt system för certifiering och evaluering konstaterade utredningen att de motiv som framfördes i propositionen Samhällets säkerhet och beredskap (2001/02:158) alltjämt var giltiga. Etableringen av ett svenskt system för evaluering och certifiering av säkerhetsegenskaper i produkter och system (i enlighet med standarden *Common Critera)* var genomförd. Systemet återfanns som det statliga certifieringsorganet CSEC, Sveriges Certifieringsorgan för IT-säkerhet, som en oberoende funktion inom FMV.

Utredningen konstaterade samtidigt att det fanns skilda uppfattningar om vem som hade det nationella huvudansvaret för certifieringsordningen, certifieringsorganet eller signatären, vilket regeringen borde tydliggöra.[2] Utredningen föreslog även att signatärskapet för CCRA skulle övertas av KBM från Styrelsen för ackreditering och teknisk kontroll, SWEDAC.

I betänkande *Informationssäkerhetspolitik – organisatoriska konsekvenser* (SOU 2005:71) framfördes att informationssäkerhetsarbetet borde organiseras så att kraftsamling kan ske till administrativa (exempelvis omvärldsanalys och publikationer) respektive tekniska (exempelvis utveckling av teknik för aktiv IT-kontroll) frågeställningar. Av detta drog utredningen slutsatsen att gemensamma behov och tvärsektoriella frågeställningar borde samlas under en myndighet för administrativa funktioner respektive en myndighet för tekniska funktioner.

1.3.3 Utredningen om översyn av Försvarets radioanstalt

I mars 2003 presenterade Utredningen om översyn av Försvarets radioanstalt sitt betänkande (SOU 2003:30). Utredningen betonade att den betraktade informationssäkerhetsområdet som en betydelsefull uppgift för FRA i framtiden. Enligt utredningen borde den teknik som FRA använder för att följa och inhämta information kunna användas för att skydda Sverige och svenska intressen mot attacker mot IT-system. Genom signal-

[2] Ibid., s. 106.

spaningsinsatser mot global kommunikation till och från Sverige skulle FRA kunna upptäcka attacker mot svenska informationssystem oberoende av var en aktör befann sig. Enligt utredningen borde FRA i framtiden kunna bistå myndigheter och andra aktörer med bland annat underrättelser som skulle kunna läggas till grund för skydd mot IT-relaterade hot mot system.

1.3.4 Utredningen om en myndighet för säkerhet och beredskap

Utredningen om en myndighet för säkerhet och beredskap betonade i sitt betänkande *Alltid redo* (SOU 2007:31) från maj 2007 signalunderrättelsetjänstens stora betydelse för att stärka den svenska informationssäkerheten. Utredningen föreslog därför att informationssäkerhetsansvaret vid dåvarande Krisberedskapsmyndigheten (KBM) skulle överföras till FRA. Detta skulle medföra vissa effektiviseringsvinster genom att samla både det administrativa och det tekniska informationssäkerhetsarbetet under en och samma myndighet. Genom signalunderrättelsetjänsten skulle kunskap också genereras om brister i olika informationssystem vilket skulle gagna säkerheten i svenska system. Utredningen menade även att det internationella samarbetet skulle gynnas av en sådan lösning då Sverige i och med detta endast skulle få en kontaktpunkt utåt. Utredningens förslag kom dock endast marginellt att genomföras i och med beslutet att KBM:s signalskyddsverksamhet i Sollefteå skulle föras över till FRA. I övrigt överfördes informationssäkerhetsfrågorna från KBM till den nya myndigheten MSB då denna bildades i januari 2009.

1.3.5 IT-standardiseringsutredningen

I juni 2007 presenterade IT-standardiseringsutredningen sitt betänkande *Den osynliga infrastrukturen – om förbättrad samordning av offentlig IT-standardisering* (SOU 2007:47). Uppdraget var att bedöma och föreslå förbättringar beträffande samordningsformer för utveckling av standarder inom IT-området. I ett tilläggsdirektiv betonade regeringen informationssäkerhetsfrågorna för utredningens arbete. En del av utredningens arbete var att kartlägga IT-standardiseringsområdet och ett uppdrag lades på Verket för

förvaltningsutveckling (Verva) att beskriva informationssäkerhetsområdet med avseende på standardiseringsfrågan och samtidigt föreslå en fortsättning på säkerhetsarbetet inom e-förvaltningen.[3]

I Vervas rapport kommenterades den pågående debatten inom den offentliga sektorn.[4] Områden som bland annat togs upp var att betydelsen av standardisering för evaluering och certifiering i IT-produkter och system hade betonats för utvecklingen inom IT- och informationssäkerhet, men att konkreta förslag för detta saknades. Skäl antogs delvis vara statsförvaltningens splittrade engagemang avseende standardisering inom informationssäkerhet. En annan fråga som berördes var hur den offentliga sektorns efterfrågan på säkra IT-produkter skulle kunna ökas.

Därtill nämndes den besvärande och ogynnsamma diskussionen om signatärskap och rollfördelning mellan SWEDAC och FMV. Denna bedömdes dels ha påverkat FMV:s etablering av CSEC som en självständig organisation, och dels ha påverkat svenska intressenters inställning till tillämpningen av *Common Criteria*.[5]

1.3.6 Uppdrag till Myndigheten för samhällsskydd och beredskap angående samhällets samlade förmåga att förebygga och hantera IT-incidenter

I oktober 2009 fick MSB i uppdrag av regeringen (Fö2009/2162/SSK) att lämna förslag på åtgärder för att förebygga och hantera IT-incidenter. Uppdraget slutfördes genom en skriftlig rapport i januari 2010. MSB föreslår i rapporten att ett nationellt operativt samverkanscenter för informationssäkerhet inrättas och placeras vid MSB. Uppgiften för detta samverkanscenter bör enligt MSB vara att stödja samhällets förebyggande informationssäkerhetsarbete och att samordna hanteringen av allvarliga IT-incidenter. Vid samverkanscentret ska experter från både offentlig och privat sektor vid behov kunna arbeta. Centret ska enligt MSB:s förslag vara en integrerad del av krishanteringssystemet och ha en nära

[3] E-förvaltning definieras i regeringens Handlingsplan för e-förvaltning (dnr Fi2008/491) från den 17 januari 2008 som: ”E-förvaltning är verksamhetsutveckling i offentlig förvaltning som drar nytta av informations- och kommunikationsteknik kombinerad med organisatoriska förändringar och nya kompetenser.” (Bilaga 1, s. 5.)
[4] Verva, Informationssäkerhet – standardisering för ledning och styrning samt för säkerhet i system, produkter och tekniska skyddskomponenter. PM 2007-03-30. Integrerad i kapitlet Informationssäkerhet i e-förvaltningen, SOU 2007:47.
[5] SOU 2007:47, s. 164-65.

koppling till den lägesbildsfunktion som finns vid myndigheten. Enligt MSB bör en verksamhet med uppgifter av liknande slag som Sitic integreras i samverkanscentret. MSB betonar i rapporten även vikten av en tydlig nationell struktur för privatoffentlig samverkan inom informationssäkerhetsområdet.[6]

[6] Åtgärder för att förbättra samhällets samlade förmåga att förebygga och hantera IT-incidenter. MSB 2010-01-13. (Dnr 2009-14471.)

2 Utgångspunkter

2.1 Nuvarande myndighetsstruktur

Den nuvarande ansvarsfördelningen för informationssäkerhet på nationell nivå bygger i huvudsak på en struktur som inrättades i början av 2000-talet. Som en följd av de förslag som Sårbarhets- och säkerhetsutredningen lämnade (SOU 2001:41) och regeringens proposition Samhällets säkerhet och beredskap med påföljande riksdagsbeslut (prop. 2001/02:158, bet. 2001/02:FöU 10, rskr. 261) inrättades år 2002 KBM med ett sammanhållande myndighetsansvar för samhällets informationssäkerhet. Vid PTS inrättades en funktion med ansvar för att hantera uppgifter om IT-incidenter (Sitic). FRA fick ansvar för att tillhandahålla teknikkompetens inom informationssäkerhetsområdet och FMV fick i uppgift att bygga upp ett system för evaluering och certifiering av IT-säkerhetsprodukter. Från och med 2009 är de uppgifter som hanterades av KBM överförda till MSB.

Nedan redogörs för de arbetsuppgifter inom informationssäkerhetsområdet som idag vilar på PTS/Sitic, MSB, FMV/CSEC och FRA. Ett urval av andra myndigheter (Försvarsmakten, Rikspolisstyrelsen och Datainspektionen) med ansvar inom informationssäkerhetsområdet redovisas endast kortfattat i detta sammanhang.

2.1.1 PTS/Sitic

PTS fick i maj 2002 regeringens uppdrag att inrätta en funktion för IT-incidentrapportering och sedan januari 2003 är Sitic i drift. Bakgrunden till att Sitic inrättades och placerades vid PTS finns i det förslag som år 1998 lämnades av Regeringens arbetsgrupp för

informationskrigsföring (AgIW) att en StatsCERT skulle inrättas under PTS.[7] Förslaget bearbetades vidare av PTS[8] och därefter av Sårbarhets- och säkerhetsutredningen.

Sitic är en organisatorisk enhet inom nätsäkerhetsavdelningen vid PTS med för närvarande 13 personer. Av dessa utför personal motsvarande 3 årsarbetskrafter uppgifter som stöder myndighetens generella informationssäkerhetsarbete och robusthetsstärkande insatser för elektroniska kommunikationer, utanför den direkta IT-incidenthanteringen enligt PTS instruktion. Det gäller bland annat insatser avseende Internetsäkerhet där PTS har ett särskilt regeringsuppdrag, *Internet Governance* och arbete med att höja medvetenhet och säkerhet för konsumenter och användare av elektroniska kommunikationer inom myndigheter, företag och organisationer.

Inom informationssäkerhetsområdet ansvarar PTS idag för att utveckla robustheten i de elektroniska kommunikationsnäten samt för att förhindra att system slås ut vid störningar. Myndigheten har sektorsansvar för elektroniska kommunikationer och förvaltar därigenom bland annat lagen (2003:389) om elektronisk kommunikation (LEK) som PTS även har föreskriftsrätt för enligt förordningen (2003:396) om elektronisk kommunikation.

PTS deltar i internationellt samarbete som berör informationssäkerhetsområdet, bland annat via EU och Internationella teleunionen (ITU), EU:s IT-säkerhetsmyndighet Enisa, OECD, organisationer verksamma med Internets förvaltning etc. Inom EU är Sitic medlem av *European Government CERT Group* (EGC) där liknande nationella funktioner ingår. Ett annat samarbete som Sitic deltar i är *Task Force Collaboration of Security Incident Response Teams* (TF-CSIRT) vilket betyder att Sitic är ackrediterat att ta del av organisationens hantering av incident- och sårbarhetsinformation. Sitic är även medlem i *Forum of Incident Response and Security Teams* (FIRST) som är en världsomspännande organisation som utgörs av incident-hanteringsfunktioner som gemensamt hanterar och förebygger incidenter på informationssäkerhetsområdet.

PTS budgeterade kostnader för Sitics verksamhet 2010 uppgår till totalt 18,3 mnkr.

---

[7] Statskontoret föreslog i ett parallellt uppdrag också en statlig incidenthantering. (Statskontoret 1998:18, rapport, Sammanhållen strategi för samhällets IT-säkerhet, 24 juni 1998.)

[8] Förutsättningar för att inrätta en särskild funktion för IT-incidentrapportering. PTS 28 november 2000. (Dnr 99-194489.)

Enligt instruktionen ska PTS svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Sitic ska vid inträffade IT-incidenter agera skyndsamt genom att sprida information samt vid behov medverka i samordning av åtgärder som krävs för att avhjälpa eller lindra effekter av det inträffade. Sitic ska vidare samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet, lämna råd och stöd avseende förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer i frågor om nätsäkerhet.

Sitic bedriver verksamhet dygnet runt och är Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder. Sitic bevakar endast trafikflöden i elektroniska kommunikationsnät, således inte innehållet i meddelanden och har ingen legal möjlighet att beordra nedstängning av kommunikationsnät. Motsvarande trafikövervakning utförs också av de större teleoperatörerna/*Internet Service Providers* (s.k. ISP:er) vid deras driftcentraler som en del i verksamheten. De har med andra ord egna CERT- (*Computer Emergency Response Team*-) funktioner avseende sin egen trafik.

Sitic strävar efter att öka IT-säkerhetsmedvetandet i Sverige genom att förmedla kunskap och fakta. Sitic utfärdar kontinuerligt varningar och råd om sårbarheter i IT-system. För detta bedrivs omvärldsbevakning rörande hot och säkerhetsproblem på IT-området samt ett nära samarbete och informationsutbyte med liknande nationella och internationella organisationer. Sitic sammanställer varje vecka ett veckobrev med de viktigaste nyheterna på IT-säkerhetsområdet. Sitic har även en tjänst som går ut med blixtmeddelanden vid allvarliga IT-händelser, som det går att kostnadsfritt ansluta sig till på Sitics webbplats. Sitic handhar systemen Honeynet, som detekterar och registrerar skadlig kod och intrångsförsök på Internet, och LISA som är ett system för insamling och analys av webbloggar. Sitic har även ett system som övervakar den svenska delen av Internet vilket möjliggörs genom ett samarbete med åtta svenska internetoperatörer.

2.1.2 MSB

MSB har ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning inte någon annan myndighet

har ansvaret. Ansvaret avser åtgärder före, under och efter en olycka eller en kris. MSB ska vara pådrivande i arbetet med förebyggande och sårbarhetsreducerande åtgärder, utveckla och stödja samhällets beredskap mot olyckor och kriser, arbeta med samordning mellan berörda aktörer i samhället för att förebygga och hantera olyckor och kriser. MSB ska vidare bidra till att minska konsekvenser av olyckor och kriser, följa upp och utvärdera samhällets krisberedskapsarbete samt se till att utbildning och övningar kommer till stånd inom myndighetens ansvarsområde.

MSB har vidare enligt instruktionen (6 §) till uppgift att stödja och samordna arbetet med samhällets informationssäkerhet och har föreskriftsrätt inom samma område. MSB ska dessutom inom informationssäkerhetsområdet analysera och bedöma omvärldsutvecklingen samt rapportera till regeringen om förhållanden som kan resultera i behov av åtgärder inom olika nivåer och områden i samhället.

MSB ska kunna bistå med stödresurser i samband med allvarliga olyckor och kriser samt stödja samordningen av de berörda myndigheternas åtgärder vid en kris. I detta kan ingå att stödja samordning av krishanteringsåtgärder, av information till allmänhet och media samt att samordna stödet till centrala, regionala och lokala organ i fråga om information och lägesbilder (7 §).

MSB har även till uppgift att samordna de civila myndigheternas arbete med säkra kryptografiska funktioner samt förvaltar den nationella handlingsplanen för samhällets informationssäkerhet.

CCRA

Det finns en internationell överenskommelse från år 2000 för ömsesidigt erkännande av certifieringar av IT-säkerhetsprodukter kallad *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security.* Överenskommelsen brukar vanligen benämnas *Common Criteria Recognition Arrangement* (CCRA) och grundas på den internationella standarden ISO/IEC IS 15408, Evalueringskriterier för IT-säkerhet, även kallad *Common Criteria*.

CCRA används även som benämning på den samarbetsorganisation som har formats av de länder som har signerat CCRA-överenskommelsen. Dessa länder har genom överenskommelsen ett gemensamt övergripande mål att höja den

nationella säkerheten genom att *Common Criteria* används för kravställning och granskning av IT-produkter och system. I praktiken innebär detta för köpare att dessa kan beskriva sina IT-säkerhetskrav genom s.k. skyddsprofiler (*Protection Profile)* och att leverantörer kan beskriva IT-säkerheten i sina produkter genom s.k. säkerhetsmål (*Security Target*). Ytterligare mål med CCRA är att verka för att öka antalet säkra IT-produkter, samt genom att effektivisera metodiken (*Common Evaluation Methodology*) minska kostnaderna som uppstår i samband med certifiering.

Överenskommelsen har för närvarande 26 nationer som medlemmar. Av dessa är 14 länder (däribland Sverige) utfärdare av certifikat inom *Common Criteria*.[9]

Vid överlämnandet av Sårbarhets- och säkerhetsutredningens rapport i maj 2001 var CCRA ännu inte undertecknat. Utredningen ansåg att Sverige skyndsamt skulle underteckna överenskommelsen och föreslog att regeringen skulle göra detta. Under 2002 undertecknade SWEDAC överenskommelsen för Sverige. Efter ett förslag i InfoSäkutredningens slutbetänkande om att signatärskapet borde föras över från SWEDAC till KBM, och efterföljande regeringsbeslut i juni 2006,[10] uppdrogs KBM att från och med den 1 januari 2007 överta det svenska signatärskapet i CCRA. Motivet för detta var InfoSäkutredningens bedömning att signatärskapet borde handhas av en myndighet med övergripande ansvar för informationssäkerhetsarbetet.

MSB förvaltar idag KBM:s signatärskap för CCRA. MSB utövar därmed det ansvar som följer av rollen som signatär i enlighet med CCRA-överenskommelsen. Det innebär bland annat att MSB avger Sveriges röst i samband med att nya länder söker medlemskap i CCRA. FMV/CSEC utövar rollen som nationellt certifieringsorgan i enlighet med samma överenskommelse och beslutar i frågor om hur Sverige i samverkan med andra länder tillämpar den tekniska standarden *Common Criteria.* Med dessa olika roller företräder MSB och certifieringsorganet FMV/CSEC Sverige i *Management Committee* och *Executive Subcommittee*.

MSB:s budgeterade kostnader under 2010 för signatärskapet inom CCRA är 160 tkr.[11]

[9] Det finns för närvarande 14 länder som utger certifikat inom ramen för 13 certifieringsordningar (s.k. scheman). Australien och Nya Zeeland delar certifieringsordning.
[10] Uppdrag om svenskt signatärskap för vissa informationssäkerhetsfrågor. Regeringsbeslut nr 10, 2006-06-29.
[11] Internpromemoria, MSB, 2010-03-10.

2.1.3 FMV/CSEC

År 2002 fick FMV uppdrag att, i enlighet med vad regeringen uttalat i propositionen Samhällets säkerhet och beredskap,[12] bygga upp ett system för evaluering och certifiering av IT-säkerhetsprodukter inom ramen för den internationella överenskommelsen *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security* (även kallad *Common Criteria Recognition Arrangement*, CCRA).[13]

Enligt myndighetens instruktion (5 §) ska det vid FMV finnas ett certifieringsorgan som ska upprätta och driva en certifieringsordning för säkerhet i IT-produkter och system. Försvarets materielverk ska verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat. Inom FMV bedrivs arbetet av CSEC (Sveriges Certifieringsorgan för IT-säkerhet) som har en oberoende ställning inom myndigheten. Kraven på certifieringsorgans opartiskhet och oberoende framgår av CCRA och svensk standard EN 45011.[14]

Den internationella överenskommelsen för erkännande av IT-säkerhetscertifikat grundas (enligt avsnittet om CCRA ovan) på *Common Criteria* vilken är en internationell standard med beteckningen ISO/IEC IS 15408 innehållandes evalueringskriterier för IT-säkerhet. Standarden används för att definiera:

- krav på IT-säkerhet i en viss kategori av IT-produkter,
- anspråk på IT-säkerhet som tillhandahålls av en viss IT-produkt,
- metodik och regler för oberoende granskning av IT-produkter gentemot ovan nämnda krav och anspråk.

Behovet av ett certifieringsorgan för IT-säkerhet grundar sig på att man med internationellt accepterade standarder kan bidra med tillit och förtroende (s.k. assurans) såväl inom som mellan organisationer, nationellt och internationellt. Ytterligare skäl som framförts för behovet av ett svenskt system för att kunna evaluera

[12] 2001/02:158, s. 110-12.
[13] Regleringsbrev för budgetåret 2003 avseende Försvarets materielverk. Regeringsbeslut nr 24, 2002-12-19.
[14] Enligt SIS, Standardiseringen i Sverige, gäller Europastandarden som svensk standard. För certifieringsorgan gäller Europastandarden EN 45011:1998. Denna innehåller Allmänna krav vid certifiering av produkter enligt ISO/IEC Guide 65:1996. På motsvarande sätt gäller EN 45001 med krav på evalueringsföretag enligt ISO Guide 25. (SIS, svensk standard SS-EN 45011 och SOU 2001:41, s. 245.)

och certifiera IT-säkerhetsprodukter och system är efterfrågan från såväl Försvarsmakten och IT-industrin, som behovet för det generella arbetet för bättre IT-säkerhet. Certifieringsfunktionen är därmed att betrakta som ett stöd för såväl försvarssektorn som för övriga delar av samhället, däribland näringslivet.

CSEC:s huvuduppgifter är att utöva tillsyn av evalueringar, granska evalueringsrapporter, skriva certifieringsrapporter, utfärda certifikat och publicera en lista på certifierade produkter. Vidare ska CSEC licensiera evalueringsföretag och utöva tillsyn av deras verksamhet, bidra med utbildning och stöd, samt vidareutveckla det nationella schemat (certifieringsordningen med regler och metoder för oberoende granskning), se till att schemats regler följs, delta i internationellt samarbete för tolkningar av *Common Criteria* och utveckling av standarder, samt marknadsföra *Common Criteria.* Certifiering enligt *Common Criteria* omfattar evaluering av IT-säkerhet i såväl produkter som system.

CSEC:s arbete bedrivs inom ramen för CCRA där samverkan sker mellan för närvarande 26 länder (varav 14 är ackrediterade för att utfärda certifikat) upp till och med evalueringsnivå EAL 4.[15] MSB är Sveriges signatär i CCRA (se vidare avsnittet om MSB) och FMV/CSEC är certifikatutgivare. Sedan september 2009 är CSEC:s verksamhetschef ordförande i CCRA *Management Committee* vilket är organisationens högsta beslutande organ där samtliga 26 signatärer finns representerade. Sverige kan under 2010 få förfrågan om ytterligare ett års ordförandeskap. Detta p.g.a. av att flera nya länder nu söker medlemskap i CCRA, samt en önskan från övriga signatärer om god kontinuitet i hanteringen av dessa frågor. CSEC deltar även i CCRA *Maintenance Board* och *Development Board* för bland annat utveckling av och regler kring *Common Criteria*.

FMV/CSEC är erkänt som certifikatutgivare inom CCRA sedan våren 2008 och är, liksom evalueringsföretagen, ackrediterat av Sveriges nationella ackrediteringsorgan, SWEDAC, sedan sommaren 2008. CSEC har licensierat två evalueringsföretag i Sverige och ett tredje har nyligen ansökt om licensiering. Sedan CSEC började sin verksamhet har åtta certifieringsuppdrag påbörjats, två certifikat och en uppdatering har publicerats och två certifieringar pågår. Övriga uppdrag har avbrutits av kunden.

[15] *Evaluation Assurance Level* (EAL) är en numerisk bedömning från 1-7 av hur ingående och rigorös en säkerhetsgranskning enligt *Common Criteria* är. EAL 1 är den mest grundläggande nivån och den billigaste att såväl implementera som utvärdera, medan EAL 7 således är den mest rigorösa och mest dyrbara.

Samtliga certifieringsuppdrag som genomförts har avsett produkter som används av Försvarsmakten.

Certifieringsprocessen går till så att utvecklaren av en produkt tillhandahåller produkt och dokumentation till ett oberoende, och av SWEDAC ackrediterat samt av certifieringsorganet CSEC licensierat, evalueringsföretag. Detta företag analyserar dokumentationen och testar produkten gentemot ställda krav. Evalueringsföretagets arbete omfattar bland annat sårbarhetsanalyser, penetrationstester, verifiering av krypto, kontroll av produktleverantörens utvecklingsmetodik, analys av design-, test och användardokumentation, egna funktionstester samt användning av automatiska analysverktyg. CSEC granskar och övervakar evalueringsföretaget och utfärdar certifikat om produkten bedöms motsvara de krav som angivits i dess säkerhetsmålsättning.

CSEC samverkar med MSB i frågor rörande *Common Criteria* såväl nationellt som internationellt. Vidare samverkar CSEC med andra organisationer och projekt i syfte att främja användningen av *Common Criteria*. Exempel på organisationer som CSEC samverkar med eller har genomfört presentationer för är: Försvarsmakten/Militära underrättelse- och säkerhetstjänsten (MUST), Försvarshögskolan, Carelink, Ringhals kärnkraftverk, SIS/Stöldskyddsföreningen, Strålskyddsmyndigheten, och JAS-projektet. MSB och CSEC sammankallar även en svensk referensgrupp bestående av MSB, FMV/CSEC, Säkerhetspolisen, FRA, PTS m.fl. för diskussioner relaterade till certifieringsorganets delaktighet i CCRA och SOGIS-MRA (se nedan).

På grund av Försvarsmaktens ansvar för kryptogodkännande och säkerhetsskydd verkar CSEC i nära samarbete med MUST. Detta har bidragit till att Försvarsmakten via FMV har gett CSEC två särskilda uppdrag. Det ena är ett uppdrag att utveckla ett evaluerings- och certifieringssystem för kryptofunktioner i kommersiella produkter och det andra är att utveckla ett evaluerings- och certifieringssystem för granskning av IT-säkerhet i Försvarsmaktens IT-system i enlighet med MUST Krav på säkerhetsfunktioner i IT-system (KSF).

Vid CSEC arbetar för närvarande 10 personer (7 fast anställda och 3 konsulter). Under 2010 hoppas CSEC kunna nyrekrytera ytterligare en person varvid antalet som arbetar inom CSEC ska

uppgå till 11 personer.[16] CSEC finansieras via anslag samt därtill intäkter från certifieringstjänster samt uppdrag från Försvarsmakten. Budgeten för 2010 uppgår till 17,2 mnkr och fördelas på 13,004 mnkr i anslag (12,635 mnkr är anslaget för 2010 och resterande 369 tkr utgör anslagssparande från föregående år), 475 tkr från certifieringstjänster och 3,75 mnkr för uppdrag från Försvarsmakten.[17]

SOGIS-MRA

Senior Officials Group Information Systems Security (SOG-IS) är en grupp av nationella IT-säkerhetsexperter som utsågs av EU:s ministerråd i början av 1990-talet. Samtidigt anmodade rådet att de medlemsstater som arbetade aktivt med evaluering och certifiering av IT-säkerhet skulle skapa ett avtal om ömsesidigt erkännande av certifieringar av IT-säkerhetsprodukter inom Europa. Med denna anmodan som grund skapade dessa medlemsstater ett sådant avtal, *Mutual Recognition Agreement of Information Technology Security Evalution Certificates*. Avtalet brukar kallas för SOGIS-MRA (*Senior Officials Group Information Systems Security – Mutual Recognition Agreement)* och liknar CCRA, men är endast öppet för EU och EEA-länder. Det har för närvarande åtta medlemmar. Av dessa är fyra (Storbritannien, Frankrike, Tyskland och Nederländerna) certifikatutgivare, övriga (inklusive Sverige) är så kallade certifikatkonsumerande medlemmar.

Inom SOGIS-MRA gäller ett ömsesidigt erkännande av IT-produkters säkerhet upp till EAL 4 (i likhet med CCRA). För granskningsnivåer däröver (s.k. högassuransgranskning på nivå EAL 5-7) är grundregeln ett ömsesidigt godkännande inom specifika teknikområden (t.ex. smarta kort), vilket regleras genom tilläggsavtal. SOGIS-MRA tillämpar således såväl *Common Criteria* som ITSEC[18] och används som verktyg då CCRA inte bedöms lämpligt.

---

[16] Beslut CSEC Verksamhetsplan 2010 (diarienr 10FMV1845-2:1).
[17] Underlag FMV/CSEC budget 2011-2013 (diarienr 10FMV1845-1:1).
[18] *Information Technology Security Evaluation Criteria* (ITSEC) från 1990, 1992, är en uppsättning kriterier för IT-säkerhetsevaluering skapade av Storbritannien, Frankrike, Tyskland och Nederländerna under åren 1988-1991. Utvecklingen skedde parallellt med etableringen av anvisningar och rekommendationer under namnet *The Orange Book* (baserad på *Trusted Computer System Evaluation Criteria* (TCSEC) från 1983) i USA och *Canadian*

FMV är signatär och FMV/CSEC svensk representant i SOGIS-MRA som tillsammans med sin *Management Committee* etablerades 1997. Detta efter ett flerårigt arbete med utvecklingen av en europeisk standard för IT-säkerhet i produkter. Den första versionen av överenskommelsen undertecknades av FMV 1998, den andra 1999 och den tredje versionen från januari 2010 undertecknades i mars i år.

CCRA och SOGIS-MRA medför bland annat inom krypto- och säkerhetsskyddsområdet endast ett begränsat ömsesidigt erkännande av certifikat. De nationella reglerna kring vilka kryptografiska funktioner som får användas, hur dessa ska kontrolleras och vem som får utföra kontrollerna kan vara mycket känsligt. De nationella reglerna har företräde framför såväl CCRA som SOGIS-MRA.

2.1.4 FRA

FRA har två verksamhetsområden: signalunderrättelsetjänst och informationssäkerhetstjänst. Det förstnämnda är att på uppdrag av regeringen och de myndigheter som regeringen bestämmer bedriva signalspaning. Syftet är att kartlägga yttre militära hot och andra utländska förhållanden som kan påverka Sveriges säkerhet, till exempel internationell terrorism.

Det andra är informationssäkerhet där FRA har ett expertuppdrag sedan 2003. FRA ska enligt instruktionen ha hög teknisk kompetens inom informationssäkerhetsområdet och får efter begäran stödja sådana statliga myndigheter och statliga bolag som hanterar information som bedöms vara känslig ur sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende.

FRA ska särskilt kunna stödja insatser vid nationella kriser med IT-inslag, medverka till identifieringen av inblandade aktörer vid IT-relaterade hot mot samhällsviktiga system, genomföra IT-säkerhetsanalyser och ge annat tekniskt stöd. FRA ska vidare samverka med andra organisationer inom informationssäkerhets-området såväl inom som utom landet. FRA har även till uppgift att

Trusted Computer Product Evaluation Criteria (CTCPEC) från 1990, 1991. ITSEC kom att rekommenderas av EU:s Ministerråd i april 1995. (SOU 2001:41, s. 240-41.)

förse civila myndigheter, kommuner och företag med säkra kryptografiska funktioner. FRA stödjer Säkerhetspolisen i tillsynen enligt säkerhetsskyddslagsstiftningen.

2.1.5 Andra myndigheter med ansvar inom informationssäkerhetsområdet

Försvarsmaktens ansvar på informationssäkerhetsområdet omfattar säkra kryptografiska funktioner, säkerhetsskydd och signalskydd. Försvarsmakten tillverkar och distribuerar kryptonycklar inom Försvarsmakten samt till FMV, Försvarshögskolan, Totalförsvarets forskningsinstitut, Pliktverket och Fortifikationsverket. Försvarsmakten och Rikspolisstyrelsen delar på tillsynsansvaret över myndigheter gällande kontroll av säkerhetsskyddet. Båda har även rätt att inom sina ansvarsområden meddela föreskrifter om utförandet av bestämmelserna i säkerhetskyddslagen (1996:627). Därtill leder och samordnar Försvarsmakten signalskyddstjänsten.

Rikspolisstyrelsen kontrollerar genom Säkerhetspolisen säkerhetsskyddet hos myndigheter som inte lyder under Försvarsdepartementet (undantag Kustbevakningen, MSB, Statens haverikommission). Därtill ska Rikspolisstyrelsen samordna polisens beredskap för åtgärder vid IT-incidenter.

Datainspektionen är bland annat tillsynsmyndighet enligt personuppgiftslagen (PUL). Därtill är den remissinstans gällande utveckling av standarder inom IT- och informationssäkerhet.

3 Analys av alternativen för lokalisering av Sitic och CSEC

3.1 Inledning

Enligt regeringens direktiv ska utredaren se över formerna för och konsekvenserna av en eventuell förflyttning av ansvaret för verksamheten vid Sitic och CSEC. Utgångspunkten ska vara de behov och målsättningar som regeringen angett när det gäller bland annat att samla informationssäkerhetsfrågorna. I detta kapitel redovisas först en genomgång av hur regeringen behandlat informationssäkerhetsfrågorna i relevanta propositioner under 2000-talet, med tonvikt på de senaste åren. Därefter analyseras för- och nackdelar med olika alternativ.

3.2 Regeringens bedömning i tidigare propositioner

I propositionen Samhällets säkerhet och beredskap (2001/02:158) presenterade regeringen år 2002 en övergripande strategi för informationssäkerhet i samhället och skydd av samhällsviktiga IT-beroende system. Regeringen gjorde här följande bedömning:

> Målet bör vara att upprätthålla en hög informationssäkerhet i hela samhället som innebär att man skall kunna förhindra eller hantera störningar i samhällsviktig verksamhet. Strategin för att uppnå detta mål bör liksom övrig krishantering i samhället utgå från ansvarsprincipen, likhetsprincipen och närhetsprincipen. Principiellt gäller att den som ansvarar för informationsbehandlingssystem även ansvarar för att systemet har den säkerhet som krävs för att

> systemet skall fungera tillfredsställande. En viktig roll för staten är därför att se till hela samhällets behov av informationssäkerhet och vidta de åtgärder som rimligen inte kan åvila den enskilda systemägaren. För att förhindra allvarliga informationsattacker mot Sverige bör underrättelse- och säkerhetstjänstens arbete förstärkas.[19]

Regeringen betonade också vikten av att delta i det internationella samarbetet på informationssäkerhetsområdet och där främja användningen av standarden *Common Criteria*. FMV, med dess erfarenhet av evaluerings- och certifieringsfrågor, bedömdes av regeringen vara den lämpligaste myndigheten att bygga upp en funktion för detta.[20]

I propositionen Från IT-politik för samhället till politik för IT-samhället (prop. 2004/05:175) återupprepade regeringen grunddragen i den ovan redovisade strategin för informationssäkerhet. Regeringen gjorde även bedömningen att den viktigaste rollen för Sitic hittills varit omvärldsbevakning och informationsspridning men att få sårbarheter upptäckts genom rapporter till Sitic. Regeringen betonade också att det internationella CERT-samarbetet borde stärkas. I propositionen beskrevs även regeringens strategi för ett säkrare Internet i Sverige med målet att kunna säkerställa kritiska funktioner i Internets infrastruktur.[21]

I mars 2006 presenterade regeringen propositionen Samverkan vid kris – för ett säkrare samhälle (prop. 2005/06:133). Regeringen framhöll här att den år 2002 fastställda strategin för informationssäkerhet borde utvecklas till att även omfatta att kunna upptäcka, ingripa mot och agera i samband med störningar i samhällsviktiga IT-system. I propositionen framhölls vikten av ett förbättrat integritetsskydd samt att en handlingsplan för informationssäkerhet borde utarbetas med utgångspunkt i en nationell strategi för informationssäkerhetsarbetet. Regeringen menade också att det var angeläget med en bred syn på informationssäkerheten i samhället. Ett allt för snävt perspektiv på teknikutveckling och hot borde undvikas och det sågs som viktigt att flera aktörer deltog i informationssäkerhetsarbetet och att formerna och ansvaret för detta klarlades.[22]

---

[19] Prop. 2001/02:158, s. 103.
[20] Ibid., s. 110-12.
[21] Prop. 2004/05:175 s. 169-85.
[22] Prop. 2005/06:133 s. 89-93.

I propositionen En anpassad försvarsunderrättelseverksamhet (prop. 2006/07:63) framhöll regeringen att det är angeläget att de unika inhämtningsmetoder och det avancerade tekniska kunnande som finns inom de myndigheter som bedriver försvarsunderrättelseverksamhet också kan utnyttjas för att möta de IT-relaterade yttre hoten mot den svenska tekniska infrastrukturen, inte minst tele- och datasystemen. Enligt regeringens bedömning ökade antalet rapporter om såväl spridning av datavirus som mycket kvalificerade attacker utförda av t.ex. transnationella kriminella grupperingar eller främmande länders underrättelsetjänster. Ett flertal studier hade också visat hur sårbart samhället är från angrepp från mer kvalificerade aktörer. Regeringen anförde vidare:

> Dessa studier förstärker argumenteringen från t.ex. Informationssäkerhetsutredningen för att staten måste påta sig ett ytterligare ansvar på detta område, framförallt för att möta de IT-relaterade hot som är så allvarliga att de kan betecknas som yttre hot mot rikets säkerhet. Det viktigaste skyddet mot de kvalificerade IT-hoten är det förebyggande arbetet, t.ex. tekniska och administrativa säkerhetsarrangemang. Underrättelseverksamheten kan bidra till dessa, men har också kompetens att tidigt möta de kvalificerade IT-hoten. Samma teknik som används för signalspaning i det globala nätet för traditionell underrättelseinhämtning kan också användas för att skydda mot kvalificerade attacker via det globala nätet mot våra IT-system. En förutsättning för detta är att såväl eter- som trådburen trafik får följas, och att signalspaningens unika metoder kan användas. Sverige riskerar annars att utnyttjas av främmande stater och andra aktörer, som vill begagna våra informationssystem.[23]

Regeringen betonade vidare att de senaste årens stora förändringar av den säkerhetspolitiska miljön och den tekniska utvecklingen medfört ett ökat behov av underrättelser. Regeringen framhöll i detta sammanhang signalspaningens allt viktigare roll i att upprätthålla informationssäkerheten i samhället och för att skydda kommunikation mot intrång från andra länder och aktörer.

[23] Prop. 2006/07:63 s. 59.

I propositionen Stärkt krisberedskap för säkerhets skull (2007/08:92) föreslog regeringen att Krisberedskapsmyndigheten, Statens räddningsverk och Styrelsen för psykologiskt försvar skulle läggas ned och att en ny myndighet (MSB) inrättades för frågor om samhällets krisberedskap och skydd mot olyckor. I anslutning till detta anförde regeringen att ”informationssäkerhetsfrågorna är sektorsövergripande varför de sammanfaller väl med det ansvar och de uppgifter i övrigt som den nya myndigheten bör få”.[24] Med anledning av detta borde den nya myndigheten ta över KBM:s verksamhet inom området och uppdraget borde också förtydligas.

I 2009 års budgetproposition betonade regeringen att god informationssäkerhet är en förutsättning för att kunna förhindra och hantera störningar i samhällsviktig verksamhet och att MSB borde hålla samman och utveckla det nationella informationssäkerhetsarbetet. Regeringen behandlade också samhällets ökade beroende av Internet och elektronisk kommunikation vilket i sin tur kunde innebära en ökad sårbarhet för samhället. Enligt regeringen hade robusthets- och krishanteringsarbetet inom sektorn för elektronisk kommunikation byggts upp under flera år och vilade på samverkan och ömsesidigt förtroende mellan privata och offentliga aktörer.[25]

Den 21 september 2009 lämnade regeringen budgetpropositionen för år 2010 (prop. 2009/10:1) till riksdagen. Regeringen anförde här bland annat följande:

> Regeringen anser att ett ändamålsenligt arbete med informationssäkerhet på nationell och internationell nivå är av central betydelse för samhällsutvecklingen. Det är också viktigt att arbeta förebyggande, ha en operativ förmåga samt att ha förmågan att snabbt kunna återgå till normalläget. Det är också viktigt att detta arbete bedrivs på EU-nivå och internationellt. Regeringen anser att det är väsentligt att integrera informationssäkerhetsfrågorna och se dem som en naturlig del i bedömningen av samhällets förmåga, i arbetet med risk- och sårbarhetsanalyser och i beroendeanalyser. Med utgångspunkt från befintliga rekommendationer och gällande föreskrifter är det viktigt att se till att det finns stöd, vägledning och information för införande av godtagbar informationssäkerhet för såväl myndigheter som andra

[24] Prop. 2007/08:92 s. 36.
[25] Prop. 2008/09:1, utgiftsområde 6, s. 79; utgiftsområde 22, s. 93.

> aktörer. Det är också viktigt att på nationell nivå verka för utbildning och medvetandehöjande åtgärder för att öka kompetensen inom området på alla nivåer i samhället, t.ex. genom att utbildning i informationssäkerhet ingår som en naturlig del i skolväsendet. Inom ramen för regeringens översyn för en effektiv myndighetsförvaltning finns anledning att även se över informationssäkerhetsfrågorna. Det finns ett behov av att samla resurserna för att skapa goda förutsättningar för att förebygga IT-incidenter liksom för att hantera dem när de inträffar. Rapporteringen av IT-incidenter som utgör hot mot eller medför allvarliga konsekvenser för samhällsviktig verksamhet och kritisk infrastruktur i samhället behöver förbättras.[26]

Regeringen framhöll vidare att uppgiften att ”hålla samman det nationella informationssäkerhetsarbetet för samhällsviktiga verksamheter och tydliggöra olika aktörers ansvar inom området” blir viktig för MSB.[27] Regeringen betonade också informationssäkerhetsfrågornas betydelse i den vardagliga IT-användningen. Fokus borde enligt regeringen ligga på det förebyggande arbetet och en höjd vardagssäkerhet för individer och små och medelstora företag som måste ha kunskap om vilka åtgärder som kan vidtas för den egna säkerheten.[28]

I budgetpropositionen för år 2010 aviserar regeringen vidare att den avser tillsätta en eller flera genomförandekommittéer med uppdrag att lämna förslag på hur stödet från bland annat FMV till Försvarsmakten ska vara närmare utformat. Utgångspunkten för kommitténs arbete ska vara Stödutredningens rapport *Ett användbart och tillgängligt försvar – Stödet till Försvarsmakten*.[29]

3.3 För- och nackdelar med att placera Sitic vid MSB

MSB har ett brett uppdrag som sträcker sig från att bidra till att förebygga att olyckor och incidenter inträffar till att förbereda samhället på att hantera olyckor och kriser, ge stöd vid inträffade

[26] Prop. 2009/10:1, utgiftsområde 6, s. 78.
[27] Ibid., s. 70.
[28] Ibid., utgiftsområde 22, s. 100.
[29] Ibid., utgiftsområde 6, s. 16.

händelser och att löpande och i efterhand utvärdera och följa upp hantering och händelseförlopp. MSB har breda kontaktytor mot kommuner, landsting, företag, myndigheter, organisationer och enskilda. Genom SAMFI[30] och Informationssäkerhetsrådet har MSB tillgång till nätverk för samverkan med både myndigheter och enskilda organisationer. Myndigheten har föreskriftsrätt när det gäller informationssäkerhetsarbetet hos statliga myndigheter.

På flera sätt liknar MSB:s uppdrag att samverka, samordna och ge stöd före, under och efter en kris det uppdrag PTS har att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. MSB:s uppdrag om samordning och stöd vid olyckor och kriser kan sägas ha en parallell i PTS uppdrag att agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt vid behov medverka i samordning av åtgärder som krävs för att avhjälpa eller lindra effekter av det inträffade. Omvärldsbevakning inom informationssäkerhetsområdet är en uppgift för båda myndigheterna.

Även om de två myndigheternas uppdrag kan beskrivas i liknande termer (stöd, förebyggande, information, omvärldsbevakning etc.) så framstår dock Sitics arbete som mer tekniskt inriktat med t.ex. analys av och information om sårbarheter i programvara medan MSB mer arbetar på policynivå. Verksamheterna framstår därför som kompletterande, snarare än överlappande.

Enligt utredarens bedömning skulle en överföring av Sitic till MSB därför ge synergieffekter som torde bidra till att utveckla och öka det stöd som centrala myndigheter idag kan ge till samhället. En placering av Sitic vid MSB skulle sannolikt också bidra till att stärka informationssäkerhetsfrågorna vid MSB som därmed kunde ges en tydligare roll av kärnverksamhet. Därtill skulle en inordning av Sitic i MSB kunna bidra till att ytterligare integrera informationssäkerhetsfrågorna dels i den samlade analys av samhällets krisberedskap som sker vid myndigheten, dels i de risk- och sårbarhetsanalyser som statliga myndigheter ska göra enligt den så kallade krisberedskapsförordningen. Tidigare har bland annat Riksrevisionen lyft fram att det finns ett utvecklingsbehov inom detta område.[31] Utredaren delar den bedömningen. Sitics

[30] Samverkansgruppen för informationssäkerhet (SAMFI) består av MSB, Försvarsmakten, FMV, FRA, PTS, Rikskriminalpolisen/Säkerhetspolisen och träffas 4-6 gånger per år. Syftet är att stödja varandra och utbyta information.

[31] Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen. RiR 2007:10. Riksrevisionen.

verksamhet skulle dessutom kunna dra nytta av det breda kontaktnät bland kommuner, landsting, företag, myndigheter, organisationer och enskilda som MSB, tidigare KBM, har byggt upp under lång tid.

Verksamhetsmässigt finns således fördelar med att inordna den verksamhet som idag bedrivs vid Sitic med den verksamhet som bedrivs vid MSB. För att synergieffekter ska kunna uppnås krävs dock att MSB förmår knyta ihop dels de olika delarna av myndighetens informationssäkerhetsarbete (förebyggande, operativt, strategiskt och lärande) inklusive Sitic-delen, dels denna verksamhet med andra relevanta verksamheter vid myndigheten såsom risk- och sårbarhetsanalyser, lägesbildsfunktion och krisinformation. I detta ligger också att skapa förutsättningar för tekniska lösningar som möjliggör informationsutbyte med högt ställda krav både på säkerhet och på funktionalitet.

En grundförutsättning för att uppnå synergieffekter är att Sitic inom rimlig tid kan samlokaliseras med relevanta delar av MSB (bland annat informationssäkerhetsenheten, lägesbildsfunktionen och krisinformation.se), vilka idag är lokaliserade i Stockholm.

Den utredning som MSB lämnade till regeringen i mitten av januari 2010 innehåller många intressanta förslag för en mer sammanhållen struktur för att förebygga och hantera IT-incidenter. Utredaren finner det dock oklart huruvida MSB har förutsättningar att inom rimlig tid lösa frågan om samlokalisering.

3.4 För- och nackdelar med att placera Sitic vid FRA

FRA besitter hög teknisk kompetens och det informationssäkerhetsarbete som myndigheten idag utför som stöd till statliga myndigheter och bolag skulle mycket väl kunna förenas med den verksamhet som idag bedrivs vid Sitic. De tekniska analyser som idag genomförs dels vid Sitic, dels vid FRA kräver i viss utsträckning likartad kompetens. En överföring av verksamheten vid Sitic till FRA skulle kunna skapa en större kritisk massa av tekniker och analytiker vilket skulle stärka Sveriges förmåga att hantera framför allt mer kvalificerade IT-hot.

I samtal med utredaren har företrädare för FRA betonat sambandet och synergierna mellan signalunderrättelsetjänst och informationssäkerhetsarbete. Detta har även noterats av tidigare utredningar (se avsnitt 1.3.2 - 1.3.4) liksom av regeringen i

propositionen En anpassad försvarsunderrättelseverksamhet (se avsnitt 3.2).

En placering vid FRA skulle också kunna kombineras med att ge myndigheten mandat att stödja aktörer som idag önskar stöd men inte kan få det med gällande regelverk, t.ex. kommuner, landsting och privata företag.

FRA har redovisat en förhållandevis klar idé om hur verksamheten vid Sitic skulle kunna integreras både organisatoriskt och fysiskt med nuvarande verksamhet vid FRA.

Ett problem vid en placering av Sitic vid FRA skulle kunna vara att förena den relativa öppenhet som kännetecknat arbetet vid Sitic i förhållande till den slutenhet som normalt kännetecknar en underrättelsemyndighet som FRA med dess krav på sekretess och källskydd. Det har också framförts både i den offentliga debatten och i samtal som utredaren haft med vissa företrädare för näringslivet att en placering vid FRA skulle kunna göra det svårare för Sitic att åstadkomma ett förtroendefullt samarbete med t.ex. privata aktörer. Med en placering av Sitic vid FRA kan det uppstå motsättningar vid inrapportering av incidenter då det ska värderas om det är skyddsintresset eller underrättelseintresset som bör väga tyngst. Det krävs en tydlig process för att hantera denna problematik.

Mot detta kan anföras att en förstärkning av informationssäkerhetsverksamheten vid FRA skulle kunna leda till ett mer öppet verkande FRA samt att det är svårt att bedöma huruvida en placering av Sitics verksamhet vid FRA verkligen skulle leda till minskad vilja till samverkan från det omgivande samhället. I utredarens samtal med näringslivet har också framkommit att det bland vissa privata aktörer kan ses som en fördel med en placering vid FRA på grund av myndighetens höga tekniska kompetens och rykte om att tidigt kunna identifiera och analysera tänkbara IT-hot.

3.5 För- och nackdelar med att placera CSEC vid MSB

Som framhållits ovan har MSB ett brett uppdrag som omfattar arbete med allt från mindre vardagsolyckor till stora katastrofer. Det är därför sannolikt att även en verksamhet som CSEC skulle kunna bedrivas inom MSB. En fördel med en placering av certifieringsverksamheten vid MSB skulle kunna vara att det

därigenom möjligen skulle bli lättare att öka intresset bland civila myndigheter och näringslivet för evaluering och certifiering av IT-produkter och IT-system. Ytterligare en tänkbar fördel är att Sverige då skulle samla CCRA-arbetet (signatär och certifieringsorgan) inom samma myndighet. Det är däremot tveksamt om några tydliga synergieffekter skulle uppstå om CSEC flyttades från FMV till MSB.

I utredarens analys av verksamheten och rollfördelning framträder en risk för intressekonflikter mellan MSB:s roll som myndighet med föreskriftsrätt och rollen som värdmyndighet för certifieringsorganet. Likaså skulle det kunna uppfattas som en intressekonflikt att som MSB vara beställare och kravställare genom s.k. skyddsprofiler (*Protection Profiles*) om myndigheten också skulle vara den myndighet som ansvarade för att produkterna blev certifierade. Ytterligare en komplikation är att MSB inte står under Försvarsmaktens tillsyn vad gäller säkerhetsskydd vilket skulle kunna påverka Försvarsmaktens förutsättningar att samverka med och att ge uppdrag åt certifieringsorganet om detta skulle placeras vid MSB. Detta torde dock gå att hantera genom författningsändringar.

3.6 För- och nackdelar med att placera CSEC vid FRA

FRA är som nämnts tidigare en myndighet med mycket hög teknisk kompetens, både på informationssäkerhetsområdet och på signalunderrättelseområdet. Vid FRA finns en god förmåga att analysera tänkbara hotbilder mot IT-system och vilken förmåga en eventuell angripare kan ha. En placering av verksamheten vid CSEC vid FRA skulle innebära en ökad kritisk massa av kompetent teknisk personal vilket skulle kunna ge synergieffekter. Det framstår också som troligt att FRA utan större problem skulle kunna erbjuda säkra lokaler och annan nödvändig infrastruktur för att kunna vara värdmyndighet för verksamheten vid CSEC.

I likhet med vad som anförts i avsnitt 3.4. skulle dock FRA:s uppgift att bedriva signalunderrättelsetjänst kunna medföra att vissa aktörer känner tveksamhet till att samverka med myndigheten. Detta argument är dock svårt att värdera.

FRA ska enligt myndighetens instruktion bedriva teknikutveckling (2 §) och inom informationssäkerhetsområdet kunna

stödja statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende (4 §). Detta skulle kunna innebära en intressekonflikt i förhållande till certifieringsorganets verksamhet i den utsträckning FRA:s uppdrag skulle innebära utveckling av produkter som också ska certifieras. Enligt utredarens bedömning skulle detta dock sannolikt kunna gå att hantera genom en tydlig ansvarsfördelning och bodelning inom myndigheten som säkerställde certifieringsorganets oberoende ställning.

3.7 För- och nackdelar med att CSEC är kvar vid FMV

Enligt utredarens bedömning finns det även skäl att överväga för- och nackdelar med att tills vidare låta CSEC vara kvar vid FMV. Verksamheten vid CSEC har byggts upp under ett antal år och fungerar nu väl, såvitt utredaren kan bedöma. Om verksamheten nu ska flyttas måste av allt att döma ackrediteringen vid både SWEDAC och CCRA göras om. Detta skulle också kunna påverka det internationella förtroendet för verksamheten. Vidare finns en risk att nyckelpersoner vid en flytt väljer att inte följa med. Sammantaget kan det därmed uppstå ett avbrott eller en betydande nedgång i verksamheten. Att bygga upp verksamheten igen i en ny myndighet med ny personal skulle sannolikt innebära att verksamheten under en period måste bedrivas med en lägre ambitionsnivå. Mot bakgrund av regeringens aviserade kommittéer som inkluderar översyn av berörda myndigheters verksamheter och roller vore det en fördel att avvakta i frågan om CSEC:s framtida hemvist. Därmed skulle kontinuitet behållas i certifieringsverksamheten.

4 Analys av signatärskapet för CCRA och SOGIS-MRA

4.1 Inledning

Enligt regeringens direktiv ska utredaren även föreslå en myndighet att vara signatär för såväl CCRA som SOGIS-MRA. Detta mot bakgrund av att signatärskapet för de båda överenskommelserna bör utövas av samma myndighet. Likt föregående kapitel redovisas inledningsvis en genomgång av hur regeringen behandlat frågan under 2000-talet. Därefter analyseras det svenska signatärskapet för CCRA och SOGIS-MRA utifrån nuvarande representation samt ges en internationell utblick av hur det ser ut i andra länder.

4.2 Regeringens bedömning

Regeringens tidigare bedömningar av Sveriges representantskap i de två överenskommelserna *Common Criteria Recognition Arrangement* (CCRA) och Senior *Officials Group Information Systems Security – Mutual Recognition Agreement* (SOGIS-MRA) är begränsade. Det nämndes övergripande i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158). Under skäl till regeringens bedömning om att FMV bör få i uppgift att bygga upp ett system för evaluering och certifiering av IT-säkerhetsprodukter beskrivs att SWEDAC är medlem i CCRA-gruppen. Vidare nämns att ”även andra organisationer skall ha möjlighet att skapa evaluerings- och certifieringssystem och dessa skall verka i konkurrens. CCRA-gruppens regler medger flera evaluerings- och certifieringsorganisationer per land. Detta i linje med lagen

(1992:1119) om teknisk kontroll".[32] Av beskrivningen följer vidare att SWEDAC som nationellt ackrediteringsorgan kan godkänna det uppbyggda systemet i Sverige. Det är därefter upp till medlemmarna inom CCRA att godkänna FMV:s organisation. "Om och när SWEDAC godkänner ytterligare någon evaluerings- och certifieringsorganisation i Sverige kommer även den att få delta tillsammans med SWEDAC i CCRA-gruppen på samma villkor som FMV."[33]

I övrigt nämns CCRA i ett regeringsbeslut från juni 2006.[34] Med detta beslut uppdrogs åt KBM att från och med januari 2007 överta det svenska signatärskapet från SWEDAC. Motivet var InfoSäkutredningens bedömning att signatärskapet borde handhas av en myndighet med övergripande ansvar för informationssäkerhetsarbetet. I regeringens beslut uppdrogs även åt KBM även att samråda med och informera berörda myndigheter, företag och organisationer inför ställningstaganden i CCRA-gruppen.

4.3 Signatärskapet för CCRA och SOGIS-MRA

Möjligheten att säkerhetscertifiera IT-produkter och system enligt *Common Criteria* och den europeiska IT-säkerhetsstandarden ITSEC är viktig för Sverige. Det ger trovärdighet till Sverige som avancerad IT-nation. Certifieringsverksamheten bygger på de internationella överenskommelserna CCRA och SOGIS-MRA angående ömsesidigt erkännande av IT-certifikat. Dessa handlar i sin tur ytterst om förtroende för hög kvalitet på utfört arbete. Därtill är skälen för certifiering att öka antalet tillgängliga evaluerade produkter och s.k. skyddsprofiler, att eliminera behovet av att duplicera redan genomförda evalueringar, samt att förbättra och kostnadseffektivisera evaluerings- och certifieringsprocessen som sådan. Verksamheten bygger i sig på kunskap om svagheter på säkerhetsteknisk nivå och om hur evaluering i praktiken går till. Vidare är utveckling och granskning av säkerhetsprodukter förknippad med sekretess. En fördel med ett svenskt certifieringssystem är att svenska leverantörer och köpare av produkter har

[32] Prop. 2001/02:158, s. 112.
[33] Ibid.
[34] Uppdrag om svenskt signatärskap för vissa informationssäkerhetsfrågor. Regeringsbeslut nr 10, 2006-06-29.

möjlighet att få en produkt eller ett system granskad och certifierad i Sverige.

Mot bakgrund av detta är en kommersialisering av verksamheten inte önskvärd och tillåts därför inte vare sig inom CCRA eller SOGIS-MRA. Inom CCRA *Management Committee* togs i september 2006 ett beslut om att samarbetsorganisationen inte tillåter flera eller icke-statliga (kommersiella) certifieringsorgan inom ett land.[35] I förordet om syftet med SOGIS-MRA finns ett likalydande avsnitt.[36]

Grunden till uppbyggnaden av en svensk certifieringsordning för evaluering och certifiering av säkerhet i IT-produkter och system lades i och med det arbete som FMV påbörjat redan under slutet av 1980-talet.[37] Drygt tio år senare var Sverige medlem av de internationella överenskommelserna CCRA och SOGIS-MRA.

Det svenska representantskapet i CCRA har sedan överenskommelsen skapades år 2000 förvaltats av två signatärer, SWEDAC och KBM/MSB. Detta medan FMV varit ensam signatär sedan avtalet SOGIS-MRA etablerades 1997.

För arbetet inom ramen för *Common Criteria* samt representationen av Sverige inom CCRA har riktlinjer etablerats mellan KBM (överförda till MSB) och FMV/CSEC. Dessa omfattar bland annat ett nära samarbete med regelbundna planerings- och avstämningsmöten, samt att CSEC:s oberoende säkerställs genom en rådgivande kommitté, *Scheme Advisory Committee* (SAC). Kommittén har även till uppgift att möjliggöra att relevanta intressenter deltar i utvecklingen av principer och policy för den nationella certifieringsordningen.

För samarbetet relaterat till CCRA är FMV/CSEC enligt den internationella överenskommelsen att betrakta som en *Associated CB (Certification/Validation Body*) och Sverige genom KBM/MSB och FMV/CSEC är en *Qualified Participant*. Enligt CCRA-

[35] Beslutet lyder: "*The MC has decided to exclude purely commercial CBs or multiple CBs within one country from being authorised within the CCRA.*" (Multiple CBs within one country/Commercial CBs, Common Criteria Recognition Arrangement, Management Committee, Policy Procedure, 18 September 2006.)

[36] "*The operation of multiple CBs by a Participant or of purely commercial CBs does not comply with the intent of the Agreement, which requires mutual trust and understanding between governmental organisations in addition to compliance with certain standards. Therefore, the operation of the Agreement cannot accommodate multiple or purely commercial CBs.*" (Mutual Recognition Agreement of Information Technology Security Evalution Certificates, Version 3, Management Committee, January 2010.)

[37] FMV har sedan 1989 utfört evalueringar inom den egna organisationen och har sedan 1990 varit en aktiv deltagare i det internationella standardiseringsarbetet inom ramen för standardiseringsgruppen ISO/IEC JTC 1/SC 27/WG3.

överenskommelsen är signatären MSB även sponsor för de certifikat som CSEC utfärdar och ska därför auktorisera dessa. Det är sedan upp till CSEC att anmäla desamma till CCRA. MSB deltar (enligt beskrivningen i kapitel 2) i CCRA:s ledningskommitté (*Management Committee*) och verkställande underkommitté (*Executive Subcommittee*) med CSEC som bisittare. Dessa kommittéer handhar frågor rörande CCRA-avtalet. MSB:s uppgift är att i dessa organ framföra Sveriges ståndpunkter efter samråd med Försvarsdepartementet och CSEC. CSEC deltar därutöver i ytterligare två styrelser för förvaltning och utveckling, CCRA *Maintenance Board* och *Development Board*. I dessa behandlas frågor om certifieringsordningen och andra av teknisk karaktär kring *Common Criteria* som standard. CSEC:s uppgift är att där framföra Sveriges ståndpunkter efter samråd med MSB. Avslutningsvis ska FMV/CSEC även medverka vid granskning av certifieringsorgan i andra länder enligt s.k. *Shadow Certification* och *Voluntary Periodic Assessment*.[38]

Enligt CCRA-överenskommelsen är det signatären som ska representera och tillvarata certifieringsorganets intressen inom gruppen av CCRA-medlemmar. Därtill ska signatären utse tekniskt kunniga representanter vid den ömsesidiga granskningen av andra länders certifieringsorgan.[39]

Beträffande representantskapet i SOGIS-MRA har detta, sedan överenskommelsen ingicks, förvaltats av FMV. Efter etableringen av CSEC har representationen även skett i samarbete med certifieringsorganet. Sverige, genom FMV/CSEC, är inom ramen för SOGIS-MRA ett certifikatkonsumerande medlemsland. Detta innebär att Sverige har möjlighet att ta del av evaluerade produkter och skyddsprofiler som certifierats i ett annat medlemsland på samma assuransnivå som överenskommits inom CCRA (d.v.s. EAL 1-4). För produkter som evaluerats på högre assuransnivå regleras ömsesidiga erkännanden genom tilläggsavtal. FMV/CSEC överväger att ansöka om ett svenskt medlemskap som certifikatproducent på assuransnivå EAL 1-4 inom SOGIS-MRA. Genom konsumentmedlemskap är FMV/CSEC representerat inom SOGIS-MRA *Management Committee* samt dess administrativa

[38] Arrangement on the Recognition of Common Criteria Certificates In the field Information Technology Security. May 2000; IT-säkerhetsstandarden Common Criteria (CC) – en introduktion. KBM/Informationssäkerhetsenheten och FMV/CSEC, september 2007.

[39] Riktlinjer för samarbetet mellan KBM och FMV avseende arbete med CC och representation inom CCRA. KBM 2006-12-08. (Dnr 1220/2006.)

arbetsgrupp. Genom ett producentmedlemskap underlättas FMV/CSEC:s möjlighet att även bli representerad i organisationens tekniska arbetsgrupp där diskussioner bland annat förs med övriga europeiska certifieringsorgan som deltar i SOGIS-MRA om hur standarden ska tillämpas.

Vid en internationell utblick kan det konstateras att bland de certifikatproducerande ländernas representation i CCRA är det endast Sverige som representeras av två självständiga myndigheter. I övriga länder representeras signatärskapet och certifieringsorganet av en och samma person från samma myndighet, av två olika personer från samma organisation/myndighet, eller av en person från ett departement och en annan för certifieringsorganet från en underordnad myndighet.[40] Vad gäller representationen i SOGIS-MRA representerar samtliga länder med certifieringsorgan sitt signatärskap samt certifieringsorganet med en eller två personer från samma myndighet.

Mot bakgrund av den tekniska kompetens som krävs för verksamheten och av signatären i såväl CCRA som SOGIS-MRA torde synergier finnas i att samla signatärskapet för de båda överenskommelserna inom en myndighet. Redan idag förlitar sig MSB på CSEC:s kompetens för att kunna fullgöra sina uppgifter som svensk representant inom CCRA. Det förefaller därför naturligt att samla signatärskapet och CSEC:s certifiering vid en myndighet.

MSB torde oberoende av en flytt av signatärskapet kunna fortsätta sitt arbete med förvaltningen av den nationella handlingsplanen (och dess åtgärdsförslag med målsättningar inom området för evaluering och certifiering av IT-säkerhetsprodukter) för samhällets informationssäkerhet.[41]

[40] Record of Decision, Meetings with CCRA Management Committee, Executive Subcommittee respektive Development Board, Tromsö, Norge, 2009.

[41] I planen berör åtgärdsförslagen 45 och 46 ökad tillämpning av *Common Criteria* som metodstöd vid kravställande (för att bidra till säkrare IT-produkter och system), samt åtgärder för att offentlig förvaltning ska vara tydlig kravställare gällande sin IT-verksamhet.

5 Utredarens överväganden och förslag

5.1 Lokalisering av Sitic

5.1.1 Utredarens förslag

Utredarens förslag: Sitics personal och verksamheten vid Sitic inordnas i MSB. Formellt torde detta kunna ske den 1 januari 2011. De lokaler som är särskilt anpassade för Sitics verksamhet, då PTS den 1 mars 2010 flyttat till Valhallavägen, kan dock behöva disponeras under en övergångsperiod under 2011. Utredaren vill dock betona att denna övergångsperiod bör vara så kort som möjlig då de synergieffekter som redovisats kräver en samlokalisering med relevanta verksamheter vid MSB i Stockholm.

Utredaren föreslår att 6 §, förordningen (2007:951) med instruktion för PTS som avser Sitics verksamhet upphävs och istället införs i förordningen (2008:1002) med instruktion för MSB. Ändringen bör träda i kraft den 1 januari 2011.

PTS budgeterade kostnader för Sitics verksamhet 2010 uppgår till totalt 18,3 mnkr. Sitic bör finansieras via MSB:s ordinarie anslag ur utgiftsområde 6, anslaget 2:7 för Myndigheten för samhällsskydd och beredskap. Utredaren föreslår därför att medel motsvarande Sitics nuvarande kostnader som för 2010 uppgår till 18,3 mnkr förs över från utgiftsområde 22, anslaget 2:1 Post- och telestyrelsens myndighetsanslag till MSB:s myndighetsanslag.

FRA har vid möte med utredaren framfört att det är en nackdel att myndigheten idag saknar mandat att ge stöd till icke-statliga aktörer t.ex. kommuner och landsting. Utredaren vill med anledning av detta framhålla att det kan finnas skäl för regeringen att, alldeles oavsett var Sitic placeras, överväga en ändring av FRA:s instruktion som skulle ge myndigheten möjlighet att stödja även andra organ än statliga myndigheter och bolag.

5.1.2 Skälen för utredarens förslag

Som framgått av analysen i kapitel 3 kan goda argument anföras för båda alternativen – FRA och MSB. Synergier skulle sannolikt uppstå oavsett om FRA eller MSB blev ny hemvist för verksamheten vid Sitic. Utredarens bedömning är att Sitic behöver placeras vid en myndighet med en stark och trovärdig ställning såväl bland myndigheter och andra offentliga aktörer som bland privata aktörer. Förtroendet för verksamheten är därmed en viktig aspekt då det gäller att väga de två alternativen mot varandra. Förtroendefrågan rymmer inom sig flera olika dimensioner såsom tekniskt kunnande, intern säkerhetskultur, förmåga att förmedla relevant information i rätt tid samt integritetsaspekter. Det är av största vikt att samarbetspartners både inom och utom landet, både offentliga och privata känner att en förtroendefull samverkan är möjlig.

Den mottagande myndigheten måste också ha tekniska och fysiska förutsättningar att ta emot verksamheten vid Sitic och dess idag 13 medarbetare. Under en kortare övergångsperiod kan det dock vara försvarbart att Sitic sitter kvar i de lokaler som verksamheten flyttat till våren 2010.

Det har i flera sammanhang framförts att incident-rapporteringen till Sitic varit av mindre omfattning än vad som hade förväntats när verksamheten inleddes år 2003. Tänkbara orsaker till detta kan ha varit osäkerhet om Sitics möjlighet att sekretessbelägga rapporter som kommer in, att verksamheten

inte varit tillräckligt känd och att det bland vissa aktörer kan ha upplevts som oklart vad nyttan skulle vara med att rapportera en IT-incident till Sitic. Det tillägg till sekretesslagen (1980:100) som trädde i kraft den 1 juli 2004 bedöms visserligen ha givit ökade förutsättningar att skydda känslig information som rapporteras in. Det framstår dock som rimligt att i framtiden kunna öka andelen inrapporterade incidenter till Sitic. När det gäller att bedöma de två alternativen till ny hemvist för Sitic måste därför övervägas vilken av de två myndigheterna, FRA respektive MSB, som kan antas ha bäst förutsättningar att åstadkomma detta.

Som framgått av analysen i kapitel 3 betonade regeringen i budgetpropositionen för år 2010 informationssäkerhetsfrågornas betydelse i den vardagliga IT-användningen och att fokus borde ligga på det förebyggande arbetet och en höjd vardagssäkerhet. Regeringen framhöll också betydelsen av att integrera informationssäkerhetsfrågorna och se dem som en naturlig del i bedömningen av samhällets förmåga, i arbetet med risk- och sårbarhetsanalyser och i beroendeanalyser. Enligt utredarens bedömning blir det därför en nyckelfråga för den framtida Sitic-verksamhetens placering att den mottagande myndigheten har förmåga att arbeta både förebyggande och som ett stöd vid incidenthantering. Myndigheten måste kunna agera öppet och skapa ett förtroende genom att förmedla snabb och korrekt information till ett brett spektrum av målgrupper.

Av betydelse för utredarens bedömning är att den framtida placeringen av Sitic ses som en del i ett större sammanhang och att det gäller att bedöma vilket av de två alternativen som kan antas leda till de starkaste synergieffekterna och utvecklingsmöjligheterna för samhällets informationssäkerhet.

Utredarens bedömning är att både FRA och MSB i huvudsak åtnjuter ett högt förtroende bland flertalet tänkbara samarbetspartners. MSB:s styrka torde ligga i förtroendet för myndighetens öppna och breda samverkansmandat, medan FRA i högre grad åtnjuter förtroende för myndighetens tekniska kunnande och möjlighet att ligga i den absoluta frontlinjen när det gäller att

identifiera IT-relaterade hot. Utredarens bedömning är att det synes enklare för MSB, med dess breda samverkansplattform och vana att agera öppet att hantera förtroendeproblematiken än för FRA. Med MSB:s öppna och breda samverkansplattform som bas skulle Sitic också sannolikt ha lättare att nå ut till det privata näringslivet.

Enligt utredarens bedömning torde FRA ha lättare att fysiskt integrera och samlokalisera Sitic med nuvarande verksamhet vid myndigheten. Detta gör att samhällets kostnader för att flytta verksamheten vid Sitic sannolikt blir något högre om alternativet MSB skulle väljas.

En placering vid MSB ger dock fördelen att Sitic placeras i en myndighet som arbetar med hela kedjan, från det förebyggande och förberedande, till det hanterande och lärande. Att placera Sitic vid MSB skulle även sannolikt bidra till att stärka informationssäkerhetsarbetets ställning inom MSB. Enligt utredarens bedömning är det vidare en fördel att kopplingen mellan informationssäkerhet och övriga delar av samhällets krisberedskap, bland annat arbetet med risk- och sårbarhetsanalyser, stärks vilket skulle vara fallet om verksamheten vid Sitic inordnades i MSB.

Samtidigt kan argumenteras för att en placering vid FRA skulle bidra till att stärka informationssäkerhetsarbetet inom den myndigheten och därigenom stärka Sveriges skydd mot mer kvalificerade IT-attacker.

Frågan om vilken av de två myndigheterna som kan antas bäst lämpad att öka andelen inrapporterade incidenter till Sitic är svår att besvara med säkerhet. FRA kännetecknas av mycket hög teknisk kompetens och en stark säkerhetskultur vilket skulle kunna tala för att vissa aktörer skulle vara mer benägna att rapportera in incidenter om Sitic var placerat vid FRA. För MSB talar att myndighetens många kanaler till det omgivande samhället kan skapa ett förtroende för myndigheten bland många små och medelstora företag, liksom bland kommuner och andra

offentliga aktörer vilket skulle kunna leda till ökad vilja att rapportera incidenter.

Sammantaget är utredarens bedömning att argumenten i huvudsak talar för att verksamheten vid Sitic bör inordnas i MSB. Ett tungt vägande skäl är enligt utredaren möjligheten att skapa synergieffekter genom att tydligare knyta informationssäkerhetsfrågorna till MSB:s generella och sektorsövergripande arbete med samhällets krisberedskap. Vid MSB skulle verksamheten vid Sitic kunna knytas nära både den förebyggande informationssäkerhetsverksamheten och den lägesbildsfunktion som finns vid myndigheten och därmed bidra till att stärka både vardagssäkerhet och samhällets förmåga att förebygga och hantera mer allvarliga IT-hot. En överföring av verksamheten vid Sitic till MSB synes också ligga i linje med vad regeringen anfört som inriktning för informationssäkerhetsarbetet i ett flertal propositioner, inte minst 2010 års budgetproposition.

5.2 Lokalisering av CSEC

5.2.1 Utredarens förslag

Utredarens förslag: Verksamheten vid CSEC bör för närvarande inte flyttas från FMV. CSEC:s fortsatta hemvist bör i stället prövas inom ramen för arbetet i den genomförandekommitté som regeringen avser att tillsätta med utgångspunkt från Stödutredningens förslag. Inom ramen för detta uppdrag bör det prövas huruvida CSEC ska föras över till en annan myndighet. Utredaren föreslår därför att CSEC tills vidare är kvar som en organisatorisk enhet inom FMV.

5.2.2 Skälen för utredarens förslag

Vid överväganden om lokalisering av CSEC bör det säkerställas att det finns en långsiktig och hållbar lösning som tillgodoser högt ställda krav på oberoende, säkerhet och effektivitet. Den organisatoriska lösning som Sverige väljer måste inge förtroende, både nationellt och internationellt. Eventuella intressekonflikter inom värdmyndigheten måste kunna hanteras på ett trovärdigt sätt. Det organisatoriska oberoende som verksamheten vid certifieringsorganet kräver måste säkerställas. För att en flytt av verksamheten vid CSEC ska anses rimlig att genomföra, bör det också finnas synergieffekter utöver det faktum att det vid en flytt av verksamheten blir färre myndigheter med ansvar för informationssäkerhet på nationell nivå.

Enligt utredarens bedömning skulle det vara fullt möjligt att flytta CSEC till både MSB och FRA. Det är dock svårt att se några egentliga fördelar och synergieffekter med alternativet MSB. Som framgått av kapitel 3 ser utredaren att vissa synergieffekter skulle kunna uppstå om CSEC inordnades i FRA. FRA:s starka tekniska kompetens och höga säkerhetskultur gör att alternativet FRA framstår som bättre. Frågan om verksamhetens oberoende och eventuella intressekonflikter bör enligt utredarens bedömning kunna hanteras genom organisatoriska lösningar av liknande slag som nu finns för CSEC inom FMV.

Samtidigt kan utredaren konstatera att verksamheten vid CSEC och placeringen vid FMV fungerar väl. En flytt till FRA skulle kräva ny ackreditering vid både SWEDAC och CCRA. Vid en omlokalisering finns alltid en risk för att personalen inte följer med vilket ökar risken för ett avbrott eller en betydande nedgång i verksamheten. Utredarens bedömning är att de eventuella fördelar som skulle finnas genom en flytt av CSEC till FRA inte uppvägar de nackdelar som finns med att omlokalisera verksamheten.

Utredarens bedömning är därför att det i nuvarande läge saknas goda skäl till att flytta CSEC till något av de två nämnda

alternativen. På längre sikt bör dock lokaliseringen av CSEC övervägas i anslutning till att regeringen går vidare med de förslag som Stödutredningen lämnade i maj 2009 i rapporten *Ett användbart och tillgängligt försvar – Stödet till Försvarsmakten*. I budgetpropositionen för år 2010 aviserar regeringen att den avser tillsätta en eller flera genomförandekommittéer med uppdrag att lämna förslag på hur det stöd till Försvarsmakten som idag ges från bland annat FMV ska vara närmare utformat. Utredarens bedömning är att det inom ramen för detta uppdrag bör prövas huruvida CSEC ska föras över till en annan myndighet. Utredaren föreslår därför att CSEC tills vidare är kvar som en organisatorisk enhet inom FMV.

5.3 Signatärskapet för CCRA och SOGIS-MRA

5.3.1 Utredarens förslag

Utredarens förslag: Signatärskapet för både CCRA och SOGIS-MRA bör utövas av den myndighet som är certifieringsorgan. I avvaktan på att lokaliseringen av CSEC slutgiltigt avgörs bör signatärskapet för CCRA överföras från MSB till FMV. MSB:s budgeterade kostnader för arbetet med signatärskapet för CCRA uppgår till 160 tkr för år 2010. Utredaren föreslår att medel motsvarande dessa kostnader förs över från MSB:s ordinarie anslag ur utgiftsområde 6, anslaget 2:7 för Myndigheten för samhällsskydd och beredskap till utgiftsområde 6, anslaget 1:11 Internationella materielsamarbeten, industrifrågor och exportstöd m.m., ap.2 Evaluering och certifiering av IT-säkerhetsprodukter som används av FMV för verksamheten vid CSEC.

5.3.2 Skälen för utredarens förslag

I flertalet andra länder innehas signatärskap av samma organisation som är certifieringsorgan. Genom att föra samman dessa roller skapas ett sammanhållet system även i Sverige. De skäl som föranledde att signatärskapet för CCRA tilldelades KBM och inte FMV saknar idag enligt utredarens bedömning relevans. Som framgår ovan föreslår utredaren att frågan om certifieringsorganets hemvist slutgiltigt prövas i samband med uppföljningen av Stödutredningens förslag. I avvaktan på detta arbete bör dock signatärskapet för CCRA överföras från MSB till FMV.

6 Konsekvenser

6.1 Generella konsekvenser

6.1.1 Sitic

Utredarens bedömning är att förslaget att inordna verksamheten vid Sitic i MSB skulle få positiva konsekvenser både för arbetet med informationssäkerhet samt för arbetet med samhällets krisberedskap i stort och alltså gagna både det arbete som Sitic och MSB utför idag. Genom att placera Sitic vid MSB åstadkoms en mer samlad lösning av ansvaret för informationssäkerhet på central myndighetsnivå. Det skapas också möjligheter att bättre integrera informationssäkerhetsarbetet i arbetet med samhällets krisberedskap, t.ex. arbetet med risk- och sårbarhetsanalyser.

Några negativa konsekvenser för verksamheten vid Sitic ser utredaren idag inte under förutsättning att frågan om samlokalisering kan lösas inom rimlig tid. Utredaren förutsätter att nuvarande goda samarbete mellan de centrala myndigheter som har uppgifter och ansvar inom området informationssäkerhet fortsätter och utvecklas.

6.1.2 CSEC

Utredarens bedömning är att verksamheten vid CSEC och placeringen inom FMV fungerar väl. I avsaknad av betydande fördelar och synergieffekter av en överföring till något av de två alternativen i nuvarande läge, bedöms den bästa lösningen vara att CSEC fortsätter sin verksamhet vid FMV.

Utan en lösning som inger förtroende, såväl nationellt som internationellt, och som är hållbar i ett längre perspektiv riskerar CSEC:s verksamhet att skadas av avbrott eller en betydande nedgång. En överföring av CSEC till en annan värdmyndighet bör i stället avvakta regeringens kommande uppdrag om en uppföljning av Stödutredningens förslag. Inom detta bör det prövas huruvida CSEC ska överföras till en annan myndighet.

6.1.3 Signatärskapet

Utredarens bedömning är att signatärskapet bör utövas av den myndighet som är certifieringsorgan. I avvaktan på att CSEC:s lokalisering slutgiltigt avgörs bör signatärskapet för CCRA därför överföras från MSB till FMV. I flertalet andra länder innehas signatärskap och certifieringsorgan av samma myndighet. En liknande lösning i Sverige skapar ett mer sammanhållet system vilket är i enlighet med regeringens avsikt att samla ansvaret för informationssäkerhetsfrågor.

Några negativa konsekvenser med att samla signatärskapet för CCRA och SOGIS-MRA inom FMV ser utredaren inte idag.

6.2 Personella konsekvenser

Bestämmelser om verksamhetsövergång finns i 6 b § lagen (1982:80) om anställningsskydd (LAS) och 28 § lagen om medbestämmande i arbetslivet (MBL). Enligt LAS (6 b §) övergår de enskilda anställningsavtalen vid verksamhetsövergång automatiskt till förvärvaren, som alltså blir ny arbetsgivare. För de anställda övergår också de rättigheter och skyldigheter på grund av anställningsavtal och de anställningsförhållanden som gäller vid tidpunkten för övergången på den nya arbetsgivaren. Anställda med tidsbegränsning överförs med tidsbegränsningen, den deltidsanställde går över i oförändrad omfattning etc.

6.2.1 Sitic

Utredarens bedömning är att reglerna om verksamhetsövergång bör tillämpas för de 13 personer som arbetar vid PTS/Sitic som alltså bör erbjudas anställning vid MSB. Arbetstagare har dock

möjlighet att välja att avstå från verksamhetsövergång och vara kvar vid PTS. Han eller hon riskerar då att bli uppsagd på grund av arbetsbrist. Arbetstagare som blir uppsagd på grund av arbetsbrist kan – om de uppfyller villkoren - omfattas av trygghetsavtalet. Den som tackat nej till verksamhetsövergång till anställning på samma verksamhetsort omfattas dock inte av trygghetsavtalet. Utredarens förslag avseende Sitic innebär att verksamheten överförs till MSB med placering i Stockholm. Personal vid Sitic som tackar nej till verksamhetsövergång till MSB (Stockholm) omfattas därmed inte av trygghetsavtalet.

6.2.2 CSEC

Beträffande CSEC är utredarens bedömning att de 10 personer (7 fast anställda och 3 konsulter) som arbetar inom verksamheten vid FMV idag, fortsätter sitt arbete som tidigare.

6.2.3 Signatärskapet

Utredarens bedömning är att ett samlat signatärskap för CCRA och SOGIS-MRA inom FMV inte föranleder några personella förändringar.

Särskilt yttrande

Särskilt yttrande av sakkunnig Ingolf Berg

Arbetet med delbetänkandet har bedrivits under kort tid utan formella sammanträden i kommittén. Vid möten med PTS, FRA, MSB och RPS/SÄPO, med syfte att inhämta information och synpunkter i sakfrågan, har jag varit inbjuden. Därutöver har jag tagit del av ett utkast och lämnat synpunkter på detta, men ej slutprodukten.

Uppdraget är i denna del begränsat till att lämna förslag avseende nytt huvudmannaskap för Sitic och konsekvenser vid val mellan två alternativ, MSB eller FRA. Jag instämmer i utredarens förslag, som det redovisats i utkastet, av ny huvudman för Sitic (MSB), men inte avseende överföringen av personella och finansiella resurser från PTS (13 personer resp. 18,3 miljoner kronor).

I uppdraget ingår att utreda konsekvenser vid en överföring av Sitics verksamhet[42], redovisa kostnader och intäkter för den verksamhet som ska flyttas och att föreslå lämplig finansiering, Det ingår också att redovisa eventuella rationaliseringar som kan uppstå i samband med samordningen. Engångskostnader som t ex kan uppstå i samband med flyttning, anpassning av nya eller avveckling av befintliga lokaler ska anges särskilt. I det utkast till delbetänkande som jag tagit del av har detta inte redovisats. Uppgifterna nedan har tidigare tillställts utredaren och redovisas även i detta yttrande.

Sitic verksamhet finansieras idag inom ramen för PTS förvaltningsanslag, ingår i en avdelning för nätsäkerhet och styrs via § 6 i myndighetens instruktion (förordning 2007:951). Det

[42] Därmed avses den verksamhet som anges i PTS myndighetsinstruktionen, § 6.

ankommer på PTS ledning och styrelse att organisera verksamheten, fördela och prioritera resurser enligt sitt förvaltningsansvar. Detta har medfört att uppgifter som stöder PTS myndighetsuppgifter, utöver de som anges i nämnda § 6, också utförs inom ramen för Sitic:s organisatoriska uppbyggnad. Dessa resurser bör enligt min mening inte överföras.

Organisatoriskt har Sitic idag 12-13 årsarbetare, varav 3 årsarbeten enligt PTS utför uppgifter som stöder myndighetens generella informationssäkerhetsarbete och robusthetsstärkande insatser för elektroniska kommunikationer, utanför den direkta IT-incidenthanteringen enligt PTS instruktion. Det gäller bl.a. insatser avseende Internet-säkerhet där PTS har ett särskilt regeringsuppdrag, Internets förvaltning och arbete med att höja medvetenhet och säkerhet för konsumenter och användare av elektroniska kommunikationer inom myndigheter, företag och organisationer.

Kostnadsfördelning enligt 2010 års budget

Sitic:s totala organisatoriska kostnader	18,3 mnkr	(föregående år 18,7 enl. budget)
- därav driftskostnader	11,8	
- därav OH-kostnader	6,5	

Fördelning av de organisatoriska driftskostnaderna

Sitic:s funktionella driftskostnader för att upprätthålla IT-incidenthanteringen enligt PTS instruktion	9,3 mnkr
Driftskostnader för PTS-verksamhet inom Sitics organisation som även fortsättningsvis måste bedrivas	2,5
TOTALT	11,8

PTS budgeterade kostnader för den verksamhet som organisatoriskt ligger inom Sitic uppgår till totalt 18,3 mnkr, varav 11,8 utgör driftskostnader (löner, avskrivningar, resor, utbildning

m.m.) och 6,5 mnkr overheadkostnader (OH) för att täcka lokalkostnader, gemensam administration och ledning m.m.

De direkta kostnaderna för Sitics funktionella IT-incidenthanteringsverksamhet som den uttrycks i instruktionen uppgår enligt myndigheten till 9.3 mnkr för verksamhetsåret 2010. Driftskostnader för PTS-relaterad verksamhet som organisatoriskt utförs inom Sitic organisation motsvarande tre årsarbetskrafter uppgår till 2,5 mnkr.

De framtida OH-kostnaderna är till viss del beroende av vem som blir ny huvudman och möjligheter till rationalisering. MSB och särskilt FRA har redan idag betydande personella resurser inom informationssäkerhetsområdet vilket torde medför rationaliseringsmöjligheter. De totala kostnaderna hos en ny huvudman är slutligen också beroende på ambition och orientering av verksamheten.

Direkta finansiella konsekvenser vid ändrat huvudmannaskap

För verksamhetsåret 2011 tillkommer kostnader för direkt-avskrivning av PTS investeringar i särskild anpassning (bl.a. skalskydd) av den nya lokalen på Vallhallavägen, Stockholm som uppgår till 3,8 mnkr, kostnader för återställande av lokalen beräknas till 1 mnkr samt kontraktsenlig hyra under uppsägningstiden om lokalen inte övertas av den nya huvudmannen. Om lokalerna övertas behöver särskild anpassning ske avseende tillträde då dessa är lokaliserade på översta våningsplanet.

Sitics nya lokaler är på 357 kvm och deras andel av den gemensamma lokalytan uppgår till 105 kvm, dvs. totalt 462 kvm. Detta motsvarar 8,4 % av den totala lokalytan som är på 5 500 kvm. Kallhyran uppgår andelsmässigt till ca 1,1 och varmhyra till ca 1,5 mnkr/år.

Det bokförda värdet av främst datautrustning och system som ska överföras uppgår till ca 1 mnkr. Därtill kommer eventuella kostnader för personal som väljer att inte följa med i övergången (t.ex. kostnader för förlängd uppsägningstid, maximalt 12 månader enligt trygghetsavtalet). Det går inte att beräkna denna kostnad idag som i genomsnitt uppgår till 750 kkr/person för 12 månader enligt PTS uppskattning.

Sammanfattning

Det belopp som kan överföras från PTS torde uppgå till 9,3 miljoner kronor plus andel av gemensamma kostnaderna. Därutöver behöver PTS kompenseras för kostnader av engångskaraktär i samband med flyttningen. Finansieringsaspekterna måste hanteras i ett sammanhang, där preliminär avräkning sker initialt från det belopp som överförs och därefter slutavräkning när flytten är genomförd.

Kommittédirektiv

Viss översyn av ansvarsfördelning och organisation när det gäller samhällets informationssäkerhet

Dir. 2009:110

Beslut vid regeringssammanträde den 19 november 2009

Sammanfattning av uppdraget

En särskild utredare ska utreda formerna och konsekvenserna av att flytta ansvaret för dels Sveriges IT-incidentcentrum (Sitic) från Post- och telestyrelsen, dels Sveriges certifieringsorgan för IT-säkerhet (CSEC) från Försvarets materielverk. Verksamheterna ska inordnas i antingen Myndigheten för samhällskydd och beredskap (MSB) eller Försvarets radioanstalt (FRA). Utredaren ska undersöka vilken av dessa två myndigheter som bedöms bäst lämpad att vara ansvarig utifrån de behov och målsättningar som regeringen angett när det gäller bl.a. att samla informationssäkerhetsfrågorna. Utredaren ska slutligen föreslå en myndighet som ska vara signatär för de internationella organen CCRA och SOGIS-MRA vilket bl.a. innebär att underteckna fördrag.

Uppdraget ska redovisas senast den 22 januari 2010.

Behovet av en utredning

Det finns ett behov av att samla resurserna för att skapa bättre förutsättningar att förebygga respektive hantera IT-incidenter. Rapporteringen av IT-incidenter som utgör hot mot eller medför allvarliga konsekvenser för samhällsviktig verksamhet och kritisk

infrastruktur i samhället behöver förbättras och anpassas till de olika behov som finns bland relevanta parter i samhället.

Ansvaret för informationssäkerhet på nationell nivå är uppdelat på ett flertal myndigheter, bl.a. MSB, PTS inkl. Sitic och FRA vilket innebär att ansvaret är splittrat. Detta betyder att styrningen och samordningen av arbetet försvåras och att resurser riskerar att inte nyttjas på ett optimalt sätt. Regeringen anser att ansvaret för informationssäkerhet bör samlas. I budgetpropositionen för 2010 (prop 2009/10:1, utgiftsområde 6 Försvar och samhällets krisberedskap sidan 79) har regeringen redovisat att det finns anledning att se över informationssäkerhetsfrågorna och att formerna och konsekvenserna av en överföring av Sitic ska utredas.

Enligt regeringens bedömning i budgetpropositionen (utgiftsområde 22 Kommunikationer) är informationssäkerhetsfrågor viktiga i den vardagliga IT-användningen och fokus bör ligga på förebyggande arbete och en höjd vardagssäkerhet för individer och företag. Konsumenter och små- och medelstora företag måste ha kunskap om vilka åtgärder de kan vidta för att öka sin säkerhet.

I den av riksdagen antagna propositionen Stärkt krisberedskap för säkerhets skull (prop. 2007/08:92, bet. 2007/08:FöU12, rskr. 2007/08:193) angav regeringen att den informationssäkerhetsverksamhet som funnits vid Krisberedskapsmyndigheten (KBM) skulle överföras till MSB och stärkas. Regeringen framförde även att informationssäkerhetsfrågorna är sektorsövergripande.

Det tvärsektoriella informationssäkerhetsarbetet bör bli mer renodlat. Ett färre antal inblandade aktörer ger bättre förutsättningar för ett mer sammanhållet informationssäkerhetsarbete. Detta innebär att verksamheterna hos Sitic och CSEC bör överföras till MSB eller FRA. Varje myndighet har enligt ansvarsprincipen att i första hand tillförsäkra den egna verksamheten en tillräcklig informationssäkerhet. Detta innebär dock inte att förtroendeskapande åtgärder som skapar tillit för informationssamhället hos medborgarna ska koncentreras till färre aktörer. Att arbeta med vardagssäkerheten i informationssamhället för att skapa förtroende är viktigt för att utnyttja den tekniska utvecklingens möjligheter på bästa sätt inom alla samhällsområden. Användningen av informationstekniken bidrar till bl.a. innovation och utveckling av nya tjänster vilket bidrar till tillväxt och konkurrenskraft. Därför behöver många aktörer inom olika

samhällssektorer arbeta för att förtroendet fortsatt vidareutvecklas och situationsanpassas på bästa sätt.

Sitics uppgift är att stödja samhället med att hantera och förebygga IT-incidenter. Arbetet omfattar bl.a. att bevaka trafikflöden i elektroniska kommunikationsnät, IT-incidentrapportering, rapportering om sårbarheter i system, att tillhandahålla olika testverktyg via nätet, seminarier m.m.. I uppgifterna ingår att agera skyndsamt vid inträffade IT-incidenter exempelvis genom att sprida information samt vid behov medverka i samordning av åtgärder som krävs för att avhjälpa eller lindra effekter av det inträffade, att samverka med relevanta nationella och internationella aktörer inom nätsäkerhetsområdet, att lämna råd och stöd avseende förebyggande arbete samt att vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder.

CSEC ansvarar för uppbyggnad, drift och förvaltning av ett system för evaluering och certifiering av IT-säkerhet i produkter och system i enlighet med standarden ISO/IEC IS 15408 (Common Criteria). CSEC som i dag bedriver sin verksamhet vid FMV stödjer såväl Försvarsmakten som det civila samhället på informationssäkerhetsområdet. CSEC är en autonom funktion inom FMV.

Krisberedskapsmyndigheten var Sveriges signatär inom CCRA[43] vilket bl.a. innebär att underteckna fördrag. CCRA är en internationell samarbetsorganisation som erkänner ömsesidigt utfärdade certifikat. Inom CCRA utvecklas såväl *Common Criteria* som metoder och regelverk för att stödja CCRA avtalet. För närvarande är 26 nationer medlemmar inom avtalet. I samband med inrättandet av MSB är signatärskapet en utestående fråga men MSB hanterar för närvarande de ärenden som ligger inom ramen för signatärskapet. En motsvarighet till CCRA är SOGIS-MRA[44] som också bygger på standarden *Common Criteria* där bara EU-länder kan ingå och där FMV är signatär. Signatärskapet för SOGIS-MRA och CCRA bör utövas av samma myndighet.

[43] CCRA (Common Criteria Recognition Arrangement)
[44] SOGIS-MRA Senior Officials Group for Information Security – Mutual Recognition Agreement

Uppdraget

En särskild utredare ska i nära samverkan med MSB, FRA, PTS, Försvarsmakten, Polisen/Säkerhetspolisen, FMV, Swedac och övriga relevanta aktörer

- utreda och redovisa formerna för och konsekvenserna av en överföring av Sitics verksamhet till MSB eller FRA,
- utreda och redovisa formerna för och konsekvenserna av en överföring av CSEC:s verksamhet till MSB eller FRA med beaktande av gällande regler kring teknisk kontroll och principen om kontrollordningar i öppna system,
- utreda och ange vilken av myndigheterna MSB eller FRA som är bäst lämpad att vara ansvarig för CSEC och Sitic,
- föreslå en myndighet att vara signatär för både CCRA och SOGIS-MRA,
- redovisa kostnader och intäkter för de resp. verksamheter som ska flyttas och föreslå lämplig finansiering,
- redovisa eventuella rationaliseringar som kan uppstå i samband med samordningen, varvid engångskostnader som t. ex. kan uppstå i samband med flyttning, anpassning av nya eller avveckling av befintliga lokaler ska anges särskilt,
- lämna förslag till författningsändringar till följd av utredningens förslag, samt
- redovisa en tidsplan för ändrade ansvarsförhållanden och gemensam signatär.

Utredaren ska, utöver de verksamhetsmässiga och ekonomiska konsekvenserna även redovisa de personella konsekvenserna av sitt förslag.

Redovisning av uppdraget och andra utredningar

Utredaren ska fortlöpande hålla Regeringskansliet (Försvarsdepartementet) informerat om arbetets bedrivande. Utredaren ska beakta bl.a. det fortsatta arbetet med anledning av Stödutredningens rapport Ett användbart och tillgängligt försvar - Stödet till Försvarsmakten (Fö 2009:A), det arbete som Delegationen för e-förvaltning (2009:19) genomför samt

Infosäkutredningens delrapport och betänkanden (SOU 2004:32, 2005:42, 2005:71).

Uppdraget ska redovisas senast den 22 januari 2010.

(Försvarsdepartementet)

Kommittédirektiv

Tilläggsdirektiv till Viss översyn av ansvarsfördelning och organisation när det gäller samhällets informationssäkerhet (Fö 2009:04) — Dir. 2010:5

Beslut vid regeringssammanträde den 14 januari 2010

Förlängd tid för uppdraget

Med stöd av regeringens bemyndigande den 19 november 2009 gav chefen för Försvarsdepartementet en särskild utredare i uppdrag att bl.a. utreda formerna för och konsekvenserna av att flytta ansvaret för dels Sveriges IT-incidentcentrum (Sitic) från Post- och telestyrelsen, dels Sveriges certifieringsorgan för IT-säkerhet (CSEC) från Försvarets materielverk (dir: 2009:110). Uppdraget ska redovisas senast den 22 januari 2010.

Utredningstiden förlängs. Uppdraget ska i stället slutredovisas senast den 1 april 2010. Uppdraget att utreda formerna för och konsekvenserna av att flytta Sitic från Post- och telestyrelsen ska dock delredovisas senast 1 februari 2010.

(Försvarsdepartementet)