Beslutande
T.f. GD Dan Ohlsson

Föredragande
Thomas Palfelt, Juridik- och säkerhetsstaben

FMV:s yttrande över betänkandet SOU 2015:23 avseende informations- och cybersäkerhet i Sverige – strategi och åtgärder för säker information i staten

1. Ärendet

Justitiedepartementet har den 6 maj 2015 (Ju2015/2650/SSK) remitterat betänkandet SOU 2015:23 avseende informations- och cybersäkerhet i Sverige – strategi och åtgärder för säker information i staten. Synpunkter ska lämnas senast den 15 september 2015.

2. Sammanfattande kommentarer

FMV ställer sig överlag positivt till utredningens förslag avseende en strategi i syfte att stärka informations- och cybersäkerhet i staten.

Ansats och intention avseende förslag är bra och en modern terminologi genomsyrar underlaget. FMV anser att införandet av ett myndighetsråd är väsentligt liksom genomförandet av den nationella handlingsplanen som enligt FMV bör styra den prioritering som krävs. Själva införandet bör ske stegvis och konkret i närhet med aktuella myndigheter. En prioriterad åtgärd borde vara att införa en grundskyddsnivå för informationssäkerhet hos alla myndigheter.

Krav på intern revision av informationssäkerhet i myndigheterna är bra. Dock är förslagen överlag abstrakta och inte tillräckligt tydliga avseende konkreta åtgärder. Exempelvis är förslaget gällande att etablera ett myndighetsråd i sig ett bra koncept men det saknas tydlighet i hur rådet är tänkt att styras och vilka mandat det ska ha. Den kompetensförsörjning som kommer att krävas för att realisera de olika förslagen är inte tydliggjort i utredningen.

Utredningen har inte till fullo förhållit sig till den översyn som parallellt har skett gällande en ny säkerhetsskyddslag. Den förordning som föreslås avseende statliga myndigheters informationssäkerhet täcker även delar av det som egentligen omfattas av den föreslagna säkerhetsskyddslagstiftningen vilket leder till motsägelser och svåra avvägningar avseende vilket regelverk som ska tillämpas.

I den föreslagna förordningen så definieras begreppet samhällsviktig verksamhet på ett sätt som egentligen ingår i begreppet Sveriges säkerhet i förslaget till ny säkerhetsskyddslag, dvs för nationen primärt skyddsvärda verksamheter såsom svåra störningar och skadeverkningar i samhället. Detta leder till två regelverk som reglerar samma sak. Förordningen i sig innehåller därutöver vissa tveksamma regleringar som skulle kunna komma i konflikt med gällande lagstiftning avseende upphandling.

Vad avser bedömning av kostnader så bedömer utredaren att dessa, utom för MSB, kan finansieras inom befintlig budget för respektive myndighet vilket, enligt FMVs erfarenhet inte är en realistisk bedömning mot bakgrund av de förslag som presenteras i utredningen. Som exempel kan nämnas det arbete som föreslås bedrivas inom ramen för ett myndighetsråd med underliggande arbetsgrupper och rapportering och uppföljning av it-incidenter.

FMV gör följande ställningstaganden avseende de enskilda förslagen:

- FMV tillstyrker utredningens förslag i avsnitt 9.1 avseende att regeringen antar en strategi som tar sikte på att stärka informations- och cybersäkerheten i staten.

- FMV tillstyrker delar av utredningens förslag i avsnitt 9.1.5 att överväga inrättandet av en genomförandekommitté och att MSB ges i uppdrag att i samverkan med ett nybildat myndighetsråd ta fram en handlingsplan. FMV delar utredningens uppfattning att vissa av strategins åtgärder kommer att behöva tas om hand av Regeringskansliet.

- FMV tillstyrker utredningens förslag i avsnitt 9.2.1 att en nationell styrmodell för informationssäkerhet i samhället bör etableras. Detta är en av de mest centrala förutsättningarna för ett samlat arbete med informationssäkerhet på nationell nivå och är utredningens viktigaste förslag. Den föreslagna modellen bör ha en mer övergripande inriktning kopplat till utredningen om en ny säkerhetsskyddslag och FMV anser att man bör ensa kravhanteringen genom att införa en nationell styrmodell för informationssäkerhet tillsammans med förslagen från en ny säkerhetsskyddslag i ett sammanhang. FMV tror att detta skulle främja ett mer sektorsövergripande arbete vad gäller informationssäkerhet för civil respektive militär verksamhet. Den nationella styrmodellen bör utifrån skyddsvärde utgå från en för myndigheterna enhetlig och gemensam nivå avseende kondifentialitet, riktighet och tillgänglighet.

- FMV tillstyrker utredningens förslag i avsnitt 9.2.2 att regeringen inrättar ett statligt myndighetsråd för informationssäkerhet bestående av företrädare för de relevanta myndigheterna på området, men anser att myndighetsrådets roll, medlemmar och mandat är otydligt och att det i förslag till förordning bör specificeras vilka myndigheter som här ingår och vem som leder rådet.

- FMV tillstyrker utredningens förslag i avsnitt 9.2.3 avseende en ny förordning. Specifika synpunkter i detalj ges i avsnitt 4 i detta remissvar.

- FMV tillstyrker utredningens förslag i avsnitt 9.2.4 gällande tillsyn. Det är viktigt att den sektorsvisa tillsynen ses över, inte minst ur ett ekonomiskt perspektiv. Den enhetliga styrmodell som anges i avsnitt 9.2.1 utgör i detta sammanhang en god grund för en enhetlig kravställning.

- FMV delar utredningens bedömning i avsnitt 9.2.5 att revision av informationssäkerhet bör utvecklas.

- FMV tillstyrker utredningens förslag i avsnitt 9.3.1 att staten blir en mer tydlig kravställare vid upphandling. Dock vill FMV betona att avseende hur detta regleras i förslag till en ny förordning ytterligare behöver analyseras så att det inte riskerar att komma i konflikt med angränsande lagstiftning avseende upphandling.

- FMV tillstyrker utredningens förslag i avsnitt 9.3.2 att regeringen fördjupar dialogen mellan privata och offentliga aktörer, inte minst bakgrund av den gemensamma styrmodell för informationssäkerhet som föreslås.

- FMV tillstyrker utredningens förslag i avsnitt 9.4.1 gällande statliga nätverk för säkrare kommunikation i staten. Emellertid är det inte tydligt om SGSI är den infrastruktur som garanterar detta och förslaget saknar en beskrivning på hur samtliga myndigheter ska anslutas och vilka incitament som finns i sig för att myndigheterna ska ansluta sig.

- FMV tillstyrker utredningens förslag i avsnitt 9.4.2 avseende säkra kryptografiska funktioner gällande att den av Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Försvarets materielverk och Försvarsmakten, föreslagna nationella strategin med åtgärdsplan (bilaga 4) bör ligga till grund för utvecklingen av processerna på området.

- FMV tillstyrker utredningens förslag i avsnitt 9.5 avseende incidentrapportering. Dock kommer mycket höga säkerhetskrav att ställas på ett system som omfattar att rapportera alla typer av allvarliga it-incidenter vilket förmodat leder till höga kostnaderna för att etablera och förvalta denna typ av rapporteringssystem. Detta behöver tydliggöras. Därutöver anser FMV att krav bör ställas på MSB avseende återrapportering gällande inrapporterade it-incidenter.

- FMV tillstyrker utredningens förslag i avsnitt 9.6.1 avseende It-brottskonventionen.

- FMV tillstyrker utredningens förslag i avsnitt 9.6.2 avseende informationsutbyte.

- FMV tillstyrker utredningens förslag i avsnitt 9.6.3 gällande en översyn av bestämmelserna om tvångsmedel i 27 och 28 kap. rättegångsbalken och övriga lagrum.

- FMV tillstyrker utredningens förslag i avsnitt 9.7 att regeringen säkerställer att Sverige agerar kraftfullt och konsistent i samtliga internationella och regionala fora av relevans. Dock behöver detta förslag utvecklas och förtydligas avseende hur det ska genomföras.

- FMV tillstyrker utredningens övriga förslag i avsnitt 9.8.1 att övningsverksamhet inom informations- och cybersäkerhetsområdet bör fortsätta och förstärkas.

- FMV tillstyrker utredningens övriga förslag i avsnitt 9.8.2 att regeringen fördjupar dialogen mellan privata och offentliga aktörer samt utbildnings- och forskningsinstitutioner i fråga om utbildning och forskning inom informationssäkerhetsområdet.

- FMV avstyrker föreslagen tidpunkt för när förordningen föreslås träda i kraft. Januari 2016 är ur flera aspekter orimlig, inte minst mot bakgrund av föreslagen tidpunkt för när en ny säkerhetslag ska träda i kraft (januari 2017).

3. Specifika synpunkter – överväganden och förslag

Styrning och tillsyn av informationssäkerheten i staten stärks
Förslaget gällande att etablera en nationell styrmodell för informationssäkerhet i samhället är en viktig reformering avseende att åtgärda den fragmentering av terminologi, informationsklassnings- och arbetsprocesser samt säkerhetsåtgärder som idag råder mellan olika sektorsmyndigheter. FMV anser att en nationell styrmodell för informationssäkerhet behövs från basnivå upp till skydd för Sveriges säkerhet.

Ansats och grundläggande idé är bra men det är också här som motsägelsen i förhållande till föreslagen säkerhetsskyddslagstiftning blir som mest tydlig. Vi får två parallella regelverk att förhålla oss till och NISU 2014 föreslår en mer förstärkt tillsyn vilket inte är i överensstämmelse med det som föreslås i en ny säkerhetsskyddslagstiftning. Tyvärr har utredningen inte strukturerat rapporten på ett tydligt sätt. Mycket fokus har lagts på befintliga författningar och föreskrifter och det är svårt att hålla isär vad som är framåtriktande förslag och vad som är bakgrundsmaterial.

I den föreslagna förordningen så definieras begreppet *samhällsviktig verksamhet* på ett sätt som egentligen ingår i begreppet *Sveriges säkerhet* i förslaget till ny säkerhetsskyddslag, dvs för nationen primärt skyddsvärda verksamheter såsom svåra störningar och skadeverkningar i samhället. Vi får två regelverk som reglerar samma sak. Detta anser inte FMV, som har att följa båda författningarna, vara optimalt.

Myndighetsrådets roll, medlemmar och mandat är otydligt. Det bör specificeras vilka myndigheter som här ingår och vem som leder rådet. Hur rådet ska arbeta är alldeles för vagt formulerat, exempelvis begrepp som ”förebygga, följa och åtgärda brister i statens informationssäkerhet” måste konkretiseras. Arbetet föreslås ske genom ”samråd” utan att detta förklaras närmare. Uppgifterna för myndighetsrådet som föreslås i paragraf 18 medför inte att styrning och tillsyn av informationssäkerhet i staten stärks. Rådet bör få uppgift och mandat så att en nationell styrmodell för informationssäkerhet kan etableras i syfte att skapa ett systematiskt informationssäkerhetsarbete i statlig verksamhet.

Myndighetsrådet ska enligt förslaget säkerställa verkställandet av den nationella informations- och cybersäkerhetsstrategin. Inte heller detta begrepp är tillräckligt tydligt beskrivet.

Staten ställer tydliga krav som upphandlare av tjänster som innehåller informationshantering eller av it-tjänster
Vad gäller bestämmelser i samband med upphandling avseende vilka it-produkter som ska användas i samhällsviktig verksamhet som bedrivs av staten, saknar FMV en mer fullödig analys avseende hur de föreslagna reglerna korrelerar med angränsande lagstiftning som finns avseende offentlig upphandling. Bl.a. föreslås att om säkra it-produkter finns utpekade i verkställighetsföreskrifter så ska dessa upphandlas och användas.

Det finns i förslaget ett krav på certifiering vilket FMV menar ytterligare behöver förtydligas. Det är otydligt om avsikten är att företagen som är aktuella vid upphandling ska vara certifierade samt om ISO 27000 certifiering är det som avses.

Statliga myndigheter kommunicerar säkert
Detta är ett bra förslag ur aspekten att svenska myndigheter behöver en robust och säker infrastruktur för kommunikation och informationsutbyte och en infrastruktur som i sig tål svåra påfrestningar. Dock är det i utredningen otydligt om SGSI är den infrastruktur som uppfyller denna kravbild. Utredningen noterar att val av infrastrukturlösning bör föregås av en behovsanalys, följd av en analys av hot och risker och att utifrån denna kan designkrav och krav på tekniska lösningar, robusthet och

skyddsåtgärder utarbetas. FMV anser att en sådan analys först bör genomföras i syfte att tydliggöra om SGSI är den infrastruktur som uppfyller kravbilden. Förslaget saknar i övrigt en beskrivning på hur samtliga myndigheter ska anslutas och vilka incitament som finns för myndigheterna att ansluta sig. Därutöver saknar FMV i utredningen en estimering av kostnader som är förknippade i samband med att vara ansluten till den föreslagna infrastrukturen i form av SGSI.

Vad avser säkra kryptografiska funktioner (avsnitt 9.4.2) delar FMV utredningens uppfattning att den av Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Försvarets materielverk och Försvarsmakten föreslagna nationella strategin med åtgärdsplan (bilaga 4) bör ligga till grund för utvecklingen av processerna på området. Säker kommunikation är avgörande för informationssäkerheten och frågan är därför av stor vikt för många myndigheter och det är angeläget att processerna snabbt kan komma på plats. Försvarets materielverk har genom CSEC (Sveriges certifieringsorgan för it-säkerhet) en central roll i den föreslagna modellen och har också stor erfarenhet av utveckling av processer inom området. Mot bakgrund av det föreslår FMV att Certifieringsorganet för IT-säkerhet vid Försvarets materielverk får i uppdrag att, i samråd med de övriga nämnda myndigheterna, precisera underlaget så att det kan ligga till grund för konkreta uppgifter till respektive myndighet.

På sidan 248 noteras att SGSI är anslutet till sTESTA och att sTESTA uppfyller EU-rådets och EU-kommissionens föreskrifter för hantering av information klassificerad som EU RESTRICTED. Vad avser att sTESTA uppfyller säkerhetskrav för hantering av EU-information på nivån RESTREINT UE/EU RESTRICTED anser FMV att detta är felaktigt då sTESTA enligt FMV:s uppfattning ej är godkänt för detta ändamål – det gäller däremot för ett annat kommunikationsnät benämnt TESTA II. Vidare är hänvisningen till säkerhetskrav i Kommissionens respektive EU- rådets säkerhetsföreskrifter missvisande, dels då sTESTA är ett kommunikationsnät enbart upprättat inom Kommissionens anvarsområde, dels att respektive hänvisad säkerhetsföreskrift ej anger explicita tekniska säkerhetskrav för RESTREINT UE/EU RESTRICTED, utan enbart ställer krav på ackreditering.

Samtliga statliga myndigheter rapporterar it-incidenter
FMV stöder detta förslag men vill ändå lyfta fram att det kommer ställas mycket höga säkerhetskrav på ett system som omfattar att rapportera alla typer av allvarliga it-incidenter. Ett sådant system kräver en genomtänkt modell för att uppnå säkerhetskraven samt för kostnadsersättning och förvaltning. I utredningen föreslås rapporteringsskyldighet av it-incidenter till MSB. Dessa rapporter är att betrakta som inkommande handlingar till MSB och kan därmed bli föremål för begäran om utlämnande av allmän handling, vilket inte tas upp i utredningen. Vidare anser FMV att krav bör ställas på MSB att återkoppla till berörda myndigheter avseende de it-incidenter som inrapporteras. Detta är extra viktigt i samband med allvarliga it-incidenter som berör fler än en myndighet och där it-incidenter rör infrastruktur som tillhandahålls av företag.

Förebyggande och bekämpande av it-relaterad brottslighet stärks
FMV tillstyrker detta förslag. I förslaget saknas dock konkreta förslag hur detta ska genomföras inklusive stöd till myndigheterna hur man ska hantera och förebygga situationer där brottsmisstanke kan uppstå.

Sverige ska vara en stark internationell partner
FMV tillstyrker detta förslag men anser det otydligt hur det ska genomföras.

Övriga förslag utöver strategin
FMV tillstyrker dessa.

4. Förslaget till förordning för statliga myndigheters informationssäkerhet

FMV har följande synpunkter på förslaget till förordning:

§ 3
Bestämmelserna i 11, 19 och 20 §§ gäller ej för Försvarsmakten. Enligt FMV:s bedömning föreligger samma bevekelsegrunder för FMV som för Försvarsmakten, dvs undantagen borde även gälla för FMV. Som följd av Försvarstrukturutredningens betänkande *Forskning och utveckling samt försvarslogistik – i det reformerade försvaret* (SOU 2011:36) har regeringen fattat beslut om ändrad ansvarsfördelning mellan Försvarsmakten och Försvarets materielverk när det gäller inköpsverksamhet, logistikverksamhet och beställningsverksamhet. I beslutet gavs uppdrag till myndigheterna att föra över viss verksamhet från Försvarsmakten till Försvarets materielverk för att därigenom effektivisera försvarets stödverksamhet i syfte att rationalisera materiel- och logistikförsörjningen. Denna överföring har skett i flera omgångar under perioden 2013 – 2015 och omfattar även överförande av ett flertal administrativa stödsystem till FMV samt att Försvarsmakten och Försvarets materielverk i övrigt arbetar i vissa gemensamma stödsystem.

§ 4
Här kommer man i konflikt med föreslagen säkerhetsskyddslagstiftning; dels genom att definitionen av informationssäkerhet skiljer sig från förslagen i säkerhetsskyddsutredningen, dels genom att samhällsviktig verksamhet, som den här är definierad, egentligen är en del av Sveriges säkerhet som ska omfattas av ett säkerhetsskydd.

§ 7
Begreppet ”klassificera” menar FMV bör tas bort helt och om en definition anses nödvändig bör istället begreppet ”värdera” utnyttjas. Avsnittet om it-incidenter menar FMV inte hör hemma i denna paragraf.

§ 8
Det finns risk för att man kommer i konflikt med annan lagstiftning i form av LOU och LUFS.

§ 9
Risk att detta överlappar det som ingår i en ny föreslagen säkerhetsskyddslag.

§ 11
MSB ger här ett mycket omfattande mandat vilket kommer att kräva tillförsel av personalresurser för detta. FMV menar också att det bör regleras vilken myndighet som ska analysera sensortrafik för andra myndigheter. Detta saknas i förslaget.

§ 12
I detta mandat till MSB ingår att det är MSB som beslutar vilka företag som ska ha säkra kryptografiska funktioner. Om exempelvis FMV har säkerhetsskyddsavtal i nivå 1 med ett visst företag och behöver etablera signalskydd för att kommunicera kommersiell sekretess eller försvarssekretess, vilket ju är fallet idag med ett flertal företag, så är det enligt denna paragraf i föreslagen förordning MSB som beslutar om detta efter överenskommelse med FMV. Detta är enligt FMVs uppfattning inte ett effektivt och rättsäkert förfarande.

§ 15
Denna paragraf riskerar att komma i konflikt med gällande lagstiftning för upphandling.

§ 16
Se svaret under § 15.

§ 17
Här uppstår problemet med ett parallellt system med säkerhetsskyddslagstiftningen. I övrigt bör man förtydliga vad som avses med allvarlig it-incident. Som paragrafen är formulerad ska alla allvarliga it-incidenter – oaktat lagrum – rapporteras dvs även det som rör rikets/Sveriges säkerhet. FMV anser i övrigt att denna paragraf bör ställa krav på att MSB har ett återrapporteringsansvar till de myndigheter som rapporterar allvarliga it-incidenter.

§18
Ett tydligt och skarpt mandat saknas för myndighetsrådet. Regleringen om arbetsgrupper hör inte hemma i en förordningstext och bör strykas.

§19
Förslaget på förstärkt tillsyn kommer här i konflikt med den förslagna säkerhetsskyddslagstiftningen.

Föreslagen tidpunkt när förordningen träder i kraft bör anpassas till föreslagen tidpunkt för en ny säkerhetsskyddslag.

Detta yttrande har beslutats av tillförordnade generaldirektören Dan Ohlsson. I den slutliga handläggningen har också chefsjuristen Anders Sjöborg, chefen Jurstab Jur Maria Gutensparr, säkerhetsskyddschefen Erik Welleman, chefen CSEC Dag Ströman, juristen Patrik Havermann och informationssäkerhetschefen Thomas Palfelt, föredragande, deltagit.

Dan Ohlsson

Thomas Palfelt

Sändlista
Regeringskansliet, Justitiedepartementet

För kännedom
Regeringskansliet, Försvarsdepartementet
Försvarsmakten