Ej sekretess

REMISSVAR

Datum	Diarienummer	Ärendetyp
2024-08-09	24FMV4254-3	1.3
	Dokumentnummer	Sida
		1(6)

Försvarsdepartementet
fo.remissvar@regeringskansliet.se
carolina.hofgren@regeringskansliet.se

Er referens	Ert datum	Er beteckning
Christelle Bourquin	2024-06-20	Fö2024/00785

Svar på remissen Ett nytt Nationellt cybersäkerhetscenter – Förutsättningar för en effektiv verksamhet, Del 2 (Fö2024/00785)

Sammanfattning

- Överväg att ha en gemensam myndighetsöverenskommelse för samtliga i centret ingående myndigheter för att reglera gemensamma villkor kring personallån mm.
- Förtydliga vad som avses med begreppen *deltar i, bidrar till, inom ramen för* samt *placeras i* centret. Av särskild relevans i detta sammanhang är tydlighet kring vilken myndighet som står för arbetsledning av personal.
- Ytterligare förtydliganden behövs avseende informationsdelning mellan de ingående myndigheterna. FMV anser att det bör utredas om det ska införas en ny lag eller bestämmelse som utökar och förenklar möjligheterna till informationsdelning inom centret. Inte minst för samarbetet med privata aktörer behöver det finnas smidiga och effektiva sätt för informationsdelning.
- Frågorna rörande formerna för informationsdelning och informationssystem avseende säkerhetsskyddsklassificerade uppgifter behöver ytterligare belysas. Här ingår var ansvaret för exempelvis ackreditering av informationssystem som ska hantera säkerhetsskyddsklassificerade uppgifter ligger.
- FMV anser att deltagande i centret medför utökade personalkostnader som inte enbart täcks av befintlig verksamhet, särskilt inom samordning av myndighetens centersamverkan och effekter på förmågan att utföra de angränsande uppdrag som myndigheten har (t.ex. inom tillsyn).
- FMV menar att effekterna av Nato-medlemskapet på centrets verksamhet också behöver tas i beaktande, både verksamhetsmässigt och rörande t.ex. informationshantering och -delning.

FMV:s yttrande avseende utredningens förslag

Försvarets materielverk (FMV) har av Försvarsdepartementet delgivits delbetänkandet Ett nytt Nationellt cybersäkerhetscenter – Förutsättningar för en effektiv verksamhet, Del 2 (utredningen) och ombetts inkomma med remissvar på detta (Fö2024/00785) till den 9 augusti 2024.

Synpunkter på utredningens förslag

FMV har nedan synpunkter på olika förslag som lämnas i delbetänkandet. Nedanstående synpunkter utgår från promemorians disposition (avsnitt i utredningen inom parentes).

Personal, arbetsgivaransvar och arbetsledning (avsnitt 4)

I denna del vill FMV hänvisa till de resonemang som myndigheten framförde i svar på remissen för Del 1 av utredningen om myndigheternas medverkan och bidrag i centret (FMV diarienummer 24FMV3104-2, sid. 6) rörande otydligheten i vad begreppen *deltar*, *bidrar* respektive *inom ramen för centret* innebär konkret i hur personalresurser ska ställas till centrets förfogande. Utredningen föreslår att det i förordningen om nationellt cybersäkerhetscenter framgår att personal från de ingående myndigheterna ska placeras i centret. Här tillförs ytterligare ett begrepp i form av *placeras* i centret.

FMV delar utredningens redogörelse rörande personallån reglerade genom samarbetsöverenskommelser mellan FRA/centret och den utlånande myndigheten. Överenskommelsen mellan myndigheterna bör innehålla avsnitt om ledning, styrning, arbetsmiljö och eventuellt andra villkor som kan bli aktuella när en annan myndighet arbetsleder utan att ha arbetsgivaransvaret. Utgångspunkten bör vara reglerna om personallån.

Även andra sätt att bidra till centrets verksamhet som inte innebär direkt arbetsledning från FRA/centerchefen behöver förtydligas, till exempel deltagande av experter från de ingående samverkansmyndigheterna i olika projekt som utförs i centrets namn.

FMV instämmer med utredningens slutsats att alla bidrag av bemanning från andra myndigheter ska vara efterfrågestyrd och ske efter överenskommelse mellan FRA och den bidragande myndigheten. I detta sammanhang bör det vara tydligt att det är just FRA som är den mottagande myndigheten för de personalresurser som görs tillgängliga för FRA inom ramen för myndighetens huvudmannaskap för centret. Det bör även förtydligas att huvudansvaret för att säkra bemanning av centret som uppfyller uppdraget ligger på FRA som huvudman.

FMV vill även framföra att vissa gemensamma förutsättningar för hur bemanningen ska gå till kan tas fram som en gemensam myndighetsöverenskommelse mellan samtliga i centret ingående myndigheter. För en välfungerande arbetsgrupp kan en gemensam villkorsöverenskommelse för samtliga centermyndigheter vara att föredra, såsom Nationellt centrum för terrorhotbedömning (NCT) vid Säkerhetspolisen fungerar idag. Regleringen av de som ska bemanna centret under FRA:s arbetsledning kan sedan ske utifrån dessa gemensamma villkor och den efterfrågan av kompetenser och personal som FRA har i sin roll som huvudman för centret.

FMV har tillsynsroller inom cybersäkerhetsområdet, bl.a. i sin roll som nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt. Därför är det viktigt att särskilja på utförande av sådana tillsynsuppgifter och den verksamhet som utförs inom centret. Därför kan det komma att finnas personal från de ingående myndigheterna som till viss del kommer delta i centrets verksamhet men som även arbetar med tillsyn enligt den bidragande myndighetens uppdrag.

På samma sätt kan situationen uppstå där personal arbetsleds av FRA under tjänstgöring i centret för arbete där det formella uppdraget ligger kvar hos den bidragande myndigheten och inte är överfört till FRA (t.ex. olika roller enligt EU-lagstiftning) samtidigt som viss verksamhet med koppling till dessa uppdrag kan komma att genomföras i centret under FRA:s arbetsledning. FMV betonar vikten av att sådana frågor är tydligt identifierade och reglerade i den dialogen och den myndighetsöverenskommelse som sker inför en placering hos FRA/i centret.

Informationsdelning (avsnitt 5)

En ändamålsenlig informationsdelning utgör en förutsättning för att centret ska fungera som det är tänkt. De möjligheter som finns idag till viss informationsdelning utgör inte en tillräcklig grund för ändamålsenlig informationsdelning. Centermyndigheterna kan göra olika bedömningar kring vad som kan delas eller inte och det kan också vara tidskrävande. Detta leder till otydlighet och ineffektivitet, som bara i viss mån kan åtgärdas med rutiner. FMV anser att det bör utredas om det ska införas en ny lag eller bestämmelse som utökar och förenklar möjligheterna till informationsdelning inom centret.

Det är viktigt att det sker en tydlig inventering av de olika typer av information och uppgifter som kommer att delas mellan centermyndigheterna och med övriga externa aktörer. En exemplifiering av de olika typer av uppgifter som omfattas av denna informationsdelning och vilka entiteter de ska delas med vore värdefullt. På så sätt kan en kategorisering av dessa göras för att bättre illustrera både olika tillämpliga sekretessbestämmelser och hur sådant utbyte kan ske på ett smidigt och effektivt sätt.

Det kan tänkas att relevant information för centrets verksamhet kan inkomma inom ramen för EU-samarbetet. För FMV:s del kan det t.ex. röra sådan sårbarhetsrapportering som ska lämnas inom ramen för hantering av cybersäkerhetscertifierade produkter och tjänster där de nationella myndigheterna för cybersäkerhetscertifiering (i Sverige FMV) ska dela sådana inlämnade sårbarhetsrapporter med sina motsvarigheter i andra medlemsstater. Dessa kan komma att omfattas av sekretess.

Det anges att det inom ramen för NCSC:s verksamhet kan finnas behov av ett eller flera gemensamma informationssystem där de ingående myndigheterna samverkar för att bearbeta säkerhetsskyddsklassificerad information, exempelvis via gemensamma arbetsytor och databaser. FMV saknar en analys avseende hur kravbilden ser ut för denna typ av informationsdelning. I första hand bör de informationssystem som används i centrets verksamhet ägas av tydligt utpekade myndigheter.

Eftersom formerna för hur sekretessbelagda uppgifter respektive säkerhetsskyddsklassificerade uppgifter ska hanteras och förmedlas skiljer sig åt behöver frågan om delning av säkerhetsskyddsklassade uppgifter belysas ytterligare då det får stor effekt i hur centret ska kunna

dela information (se ytterligare kommentarer nedan under Säkerhetsskydd). Det har i andra sammanhang konstaterats att myndigheter har olika bedömningar av huruvida en uppgift ska vara säkerhetsskyddsklassificerad och även i vilken säkerhetsskyddsklass likvärdiga uppgifter ska indelas.

Eftersom en stor del av informationsdelningen som centret har att hantera ska delges externa aktörer, i många fall privata organ, behöver effektiva former för sådan informationsdelning finnas även för sekretessbelagda och säkerhetsskyddsklassificerade uppgifter. Former för delning av sådana uppgifter till externa aktörer berör t.ex. förutsättningar för säkerhetsskyddsavtal (SUA). Utredningen nämner även möjligheten att uppställa förbehåll enligt 10 kap. 14 § offentlighets- och sekretesslagen (OSL). Båda dessa förfaranden är relativt omständliga. Här kan de sekretessbrytande bestämmelserna som redogörs för i utredningen vara av värde för att möjliggöra delgivning. Men hanteringen kräver att centermyndigheterna har en mer ensad syn på hur information klassas och även se över olika former för att t.ex. kunna ”tvätta” information för att möjliggöra en effektiv informationsdelning som samtidigt är tillräckligt konkret för att vara till nytta för mottagande organisationen.

Säkerhetsskydd (avsnitt 7)

Verksamhetsutövaransvaret för hantering av säkerhetsskyddsklassificerade uppgifter i gemensamma informationssystem i NCSC

Det har tidigare diskuterats att man i NCSC:s verksamhet har behov av gemensamma informationssystem: ett gemensamt som hanterar säkerhetsskyddsklassificerad information med säkerhetsskyddsklass *begränsat hemlig* respektive ett gemensamt informationssystem som hanterar säkerhetsskyddsklassificerad information med säkerhetsskyddsklass *hemlig*. Det är inte tydligt i ett sådant sammanhang vem som är att betrakta som verksamhetsutövare om de (flera eller alla) ingående myndigheterna i NCSC gemensamt arbetar i systemet. För ett informationssystem som hanterar säkerhetsskyddsklassificerad information med säkerhetsskyddsklass *hemlig* så åligger det verksamhetsutövaren att genomföra en särskild säkerhetsskyddsbedömning i enlighet med 3 kap. 1 § respektive samråda med tillsynsmyndigheten i enligt med 3 kap. 2 § i säkerhetsskyddsförordningen (2021:955).

Det är oklart om detta träffar en eller flera verksamhetsutövare (alla) i detta sammanhang. Det är även oklart vilken myndighet som ansvarar för ackreditering och godkännande från säkerhetssynpunkt i denna situation. Det gäller även krav på fysisk säkerhet inom ramen för ackreditering och godkännande från säkerhetssynpunkt. Om Säkerhetspolisen exempelvis i detta sammanhang är verksamhetsutövaren för informationssystemet så kan frågan ställas om det då inom ramen för ackrediteringen ska kravställas gentemot FRA avseende fysiska säkerhetskrav för informationssystemet om FRA är säkerhetsskyddsansvarig för den fysiska säkerheten (avsnitt 7.2.2 i utredningen). Vidare så kommer då Säkerhetspolisens kravmassa för it-säkerhet att gälla för uppfyllande av it-säkerhetskrav. En sådan analys behöver göras.

Verksamhetsutövaransvar avseende att teckna säkerhetsskyddsavtal med enskilda

I framtida samverkan med privata aktörer kan det under vissa förutsättningar komma att finnas behov av att delge säkerhetsskyddsklassificerade uppgifter till berörda företag. I det sammanhanget behöver säkerhetsskyddet regleras antingen genom säkerhetsskyddsavtal i enlighet med 4 kap. 1 § i förordning 2021:955 eller, om det rör säkerhetsskyddsklassificerad information som är *begränsat hemlig*, en reglering i enlighet med Säkerhetspolisens respektive Försvarsmaktens föreskrifter om

säkerhetsskydd. Återigen väcks frågan om vilken myndighet som har verksamhetsutövaransvaret i detta sammanhang. Det kan även gälla behov av drift av ovan angivna informationssystem där det utförs av en privat aktör. Detta bör analyseras vidare.

Säkerhetsprövning av centermyndigheternas personal och inplacering i säkerhetsklass
Av utredningen framgår (avsnitt 7.2.3) att det ”huvudsakliga ansvaret för säkerhetsprövningen ligger på den verksamhet där den kontrollerade anställs, anlitas eller deltar genom annat deltagande”. Utredningen framhåller dock att FRA bör ha möjlighet att ställa krav på bl.a. viss säkerhetsklass. Detta resonemang blir motsägelsefullt även om det rent konkret är möjligt för FRA att formellt ha mandat med stöd av 3 kap. 10 § i säkerhetsskyddslagen (2018:585) att ställa sådana krav gentemot de andra centermyndigheterna.

Det är valda delar av respektive myndighets ordinarie verksamhet som kommer att bedrivas i centret med berörd personal. Den personalen är säkerhetsprövad och inplacerad i säkerhetsklass baserat på den befattningsanalys som tjänsten i sig grundar sig på för respektive centermyndighets del. Om exempelvis FMV:s befattningsanalys för en viss befattning medför inplacering i säkerhetsklass 3 för den aktuella tjänsten inom ramen för FMV:s verksamhet, men med placering för samverkan i centret, och FRA oaktat det ställer krav på inplacering i säkerhetsklass 2 blir det otydligt vilken bedömning som har företräde. Centret i sig bedriver ingen ”egen” säkerhetskänslig verksamhet eftersom det inte är en entitet som träffas av säkerhetsskyddslagstiftningen (myndighet, kommun osv) utan gör respektive ingående centermyndighets säkerhetskänsliga verksamhet, inklusive vad som utförs av FRA som huvudman för centret.

Konsekvenser och finansiering (avsnitt 8)

Utredningen bedömer att de deltagande myndigheternas nuvarande medverkan i centret kan finansieras inom befintliga anslag. FMV menar att bara samordningen av medverkan i centret i sig medfört en resursåtgång som går utöver uppgifter som myndigheten redan bedriver.

En annan aspekt är att för viss verksamhet kan det uppstå konsekvenser i förmågan att genomföra viss verksamhet genom att personal tjänstgör i eller överförs till centret samtidigt som myndigheten har kvar sitt ursprungliga uppdrag på området. Det innebär att det kan bli resursmässigt påfrestande för verksamhet som måste genomföras av myndigheten i ett utpekat uppdrag från regeringen. Detta kan särskilt komma att gälla personal som delvis deltar med expertis i myndighetens tillsynsarbete och som även kommer att ingå i centrets verksamhet.

Det är även ett styrningsmässigt asymmetriskt upplägg att anse att den bidragande myndigheten genomför sina ordinarie uppdrag genom att verksamheten bedrivs av utlånad eller genom arbetsledningsåtgärd till FRA överförd personal. Uppdraget för vissa myndighetsuppgifter ligger kvar på respektive myndighet såvida inte även uppdraget i förordning, instruktion, regleringsbrev eller på annat sätt ges till FRA. Det kommer även påverka vilka typer av resurser som en bidragande myndighet de facto kommer att bidra med till FRA/centrets verksamhet.

Av övriga konsekvenser framgår att ”utredningen bedömer inte att förslagen påverkar Sveriges åtaganden i förhållande till EU”. Dock har inte utredningen bedömt Sveriges åtaganden i förhållande till Nato. Som medlem i försvarsalliansen Nato har Sverige att bl.a. uppfylla Natos säkerhetsskyddskrav. Om NCSC, vilket i ett framtida perspektiv nog är sannolikt, behöver hantera Nato säkerhetsskyddsklassificerad information så är detta ej omhändertaget i utredningen och

behöver analyseras förslagsvis i samverkan med den nationella säkerhetsmyndigheten (NSA) i Regeringskansliet/Utrikesdepartementet.

– – –

I den slutliga handläggningen har avdelningschef John Billow, informationssäkerhetschef Thomas Palfelt, rådgivare Dag Ströman, HR-strateg Denise Björk och jurist Ewamaria Eriksson deltagit. John Billow har varit föredragande.

Försvarets materielverk

Ann Pietikäinen
Tjänsteförrättande chef Juridik- och säkerhetsstaben

Sändlista
Försvarsdepartementet

Kopia till
Arkiv
FMV Lednings- och ekonomistaben
FMV Juridik- och säkerhetsstaben