SOFF
Säkerhets- och försvarsföretagen

YTTRANDE
Fö2021/00796

Försvarsdepartementet
fo.remissvar@gov.se

Remissvar avseende Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)

Säkerhets- och försvarsföretagen (SOFF) är en branschorganisation för företag inom säkerhets- och försvarsområdet med verksamhet i Sverige.

Föreningen uppskattar möjligheten att delta i utredningen genom en expertroll samt att yttra sig över delbetänkandet av cybersäkerhetsutredningen.

Övergripande kommentarer på utredningen och dess förslag
SOFF anser att utredningen har gjort ett väl genomarbetat jobb och att dess material är gediget. SOFF anser vidare att utredningens förslag är bra, men otillräckliga. Förslagen bör i vissa avseenden utvecklas för att få avsedd effekt och i andra avseende förtydligas för att kunna genomföras på ett ändamålsenligt sätt.

SOFF sammanfattar sina kommentarer nedan:

- SOFF bejakar utredningens förslag att FMV bör ges uppdraget att utveckla formerna kravställning på IKT-produkter, -tjänster och -processer. SOFF bedömer dock att myndighetens roll bör vara bredare och åtminstone omfatta NIS-området.
- SOFF föreslår även att det inom ramen för uppdraget till FMV också utreds hur företag kan inkluderas i samrådet kring de tänkta gemensamt framtagna hot-, sårbarhets- och riskbedömningar samt skyddsprofiler som ska tas fram till stöd för kravställning på IKT-produkter, -tjänster och -processer som ska användas i nätverks- och informationssystem.
- SOFF bedömer vidare att det är av stor vikt att staten säkerställer – till exempel genom förordning till tillsynsmyndigheten - att från företag på ett eller annat sätt inhämtad information skyddas otillbörliga aktörer såväl inom som utom staten. Detta inkluderar otillbörliga aktörer inom den myndighet som utövar tillsynen.
- SOFF föreslår därför att staten genomför en översyn avseende nuvarande sekretessregelverk syftande till att säkerställa att information som den av utredningen föreslagna tillsynsmyndigheten kan erhålla vid, eller genom, sitt tillsynsuppdrag kan skyddas till fullo.

- SOFF bedömer att införande av utredningens förslag utan sekretessregelverk och myndighetsförordningar kräver att det tydliggörs för tillsynsmyndigheten och trovärdiggörs för i sammanhanget aktuella företag att all information som tillsynsmyndigheten inhämtar från företagen skall hanteras med hög sekretess inom staten - och inom myndigheten själv. I annat fall riskerar staten att företagens vilja till samverkan begränsas betydligt.

Det bör i sammanhanget nämnas att även tillsynsmyndigheten, och därmed staten, har goda skäl att hantera samtlig från företagen erhållen information med hög sekretess. Spridande av – i statligt perspektiv till synes oförarglig eller oviktig - information kan:

- Vara börspåverkande
- Därför ligga under s.k. insiderlagstiftning vilken har omfattande sanktionsmöjligheter
- Påverka det drabbade företagets förtroende för - eller vilja att samverka med - staten/tillsynsmyndigheten/andra myndigheter.

Dessutom kan omfattande eller återkommande "läckage" av företagsspecifik information mellan eller inom myndigheter få påverkan på företaget i frågas långsiktiga strategi och syn på Sverige som verksamhetsland.

- Om en översyn enligt ovan genomförs och om denna kommer fram till att nuvarande regelverk inte till fullo skyddar företagens information från otillbörliga aktörer såväl inom som utom staten, inklusive den myndighet som utövar tillsynen, anser SOFF att utredningens förslag bör kompletteras (eller andra ändringar görs) så att sådant skydd kan säkerställas på ett för företagen trovärdigt sätt.
  Om ovan föreslagen översyn ej genomförs, eller i det fall sådan översyn genomförs men för företag trovärdig informationshantering och sekretess inte kan säkerställas, avråder SOFF från att utredningens förslag genomförs.

SOFF
Säkerhets- och försvarsföretagen

Fördjupad kommentar: Informations- och cybersäkerhet

SOFF instämmer i utredningens bedömning av att det i dag finns ett omfattande behov av personal med kompetens i informations- och cybersäkerhet på olika nivåer hos många verksamhetsutövare, såväl inom den offentliga verksamheten som i näringslivet. Tillgången på personal med kompetens inom informations- och cybersäkerhet behöver därför öka.

Kompetensförsörjning är en förutsättning för ett långsiktigt och livskraftigt försvar av ett digitalt Sverige. SOFF instämmer med utredningens i kap 10.7 att tillgången till personal och kompetens inom informations- och cybersäkerhet behöver förbättras. SOFF ser att det finns ett stort behov av nytänkande och konstaterar att kunskapsförsörjning är avgörande för försvaret av det digitala Sverige. SOFF:s cyberförsvarsgrupp har därför under flera år har haft kompetensförsörjning inom cybersäkerhet som en av sina kärnfrågor. Sedan 2018 har SOFF genomfört undersökningar avseende cyberkompetens hos föreningens medlemsföretag. Under 2020 publicerades rapporten *"Hur säkrar vi kompetensen inom Cybersäkerhet?"*[1] och under 2022 avser SOFF publicera en uppföljande undersökning kring det aktuella behovet.

Fördjupad kommentar: Kapitel 12 Certifiering av nätverks- och informationssystem

SOFF bejakar utredningens förslag att ge FMV ett uppdrag att analysera och lämna förslag på formerna för framtagande av en ordning för nationell kravställning på området och att detta ska ske i samråd med övriga myndigheter som ingår i det nationella cybersäkerhetscentret samt övriga tillsynsmyndigheter inom säkerhetsskyddsområdet. Men SOFF anser att uppdraget inte endast bör omfatta säkerhetskänslig verksamhet utan även bör omfatta åtminstone hela NIS-området, det vill säga kravställning på IKT-produkter, -tjänster och -processer som ska användas i samhällskritisk verksamhet.

SOFF bejakar utredningens förslag att ge FMV i uppdrag att i samråd med övriga myndigheter som ingår i det nationella cybersäkerhetscentret och övriga tillsynsmyndigheter inom säkerhetsskyddsområdet i enlighet med vad som framgår i kapitel 12 där följande föreslås som uppdrag till FMV:

- *analysera och lämna förslag på formerna för framtagande av ordning för nationell kravställning som utgör grund för evaluering och/eller certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet,*

[1] Cyberkompetens_rapport-200602.pdf (soff.se)

- *analysera och lämna förslag på vilka resurser som behövs för att inrätta en sådan ordning, vilka myndigheter som bör ges i uppgift att bidra till kravställningsarbetet samt hur näringsliv och företag kan beredas möjlighet att delta i arbetet,*
- *analysera och lämna förslag på formerna för hur myndigheter och andra verksamhetsutövare kan få stöd vid upphandling och användning av certifierade IKT-produkter, -tjänster och -proces-ser i syfte att främja ökad användning av certifierade IKT-produkter, -tjänster och -processer i säkerhetskänslig verksamhet, och*
- *analysera behov av och formerna för framtagande av en nationell sammanställning över certifierade och rekommenderade IKT-produkter, -tjänster och -processer för användning i nätverks- och informationssystem i säkerhetskänslig verksamhet.*

SOFF anser att uppdraget till FMV inte endast bör omfatta säkerhetskänslig verksamhet utan även bör omfatta åtminstone hela NIS-området (Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Syftet med detta är att Sverige som nation ska kunna ta ett helhetsgrepp kring de kort- och långsiktiga behov som finns av certifierade IKT-produkter, -tjänster och -processer i nätverks- och informationssystem.

I utredningen står att:
"om det kan anses föreligga tillräckliga förutsättningar för att införa en nationell särskilt anpassad ordning med krav på certifiering av IKT-produkter, -tjänster och -processer enbart för att täcka det nationella behovet på området för säkerhetskänslig verksamhet. Bl.a. har ifrågasatts möjligheterna att nationellt ställa enskilda certifieringskrav för det begränsade användningsområde som det nationella området i detta sammanhang utgör. Från experthåll framhålls vidare att dessa IKT-produkter, -tjänster och -processer som eventuellt tas fram för nationella behov även måste ha en internationell räckvidd eftersom den nationella marknaden inte bedöms som tillräcklig. Det innebär att det föreligger en risk för att det kommer att saknas marknadsmässiga förutsättningar för att ta fram särlösningar för enbart nationella behov. På motsvarande sätt behöver svenska företag som tar fram olika IKT-produkter, -tjänster och -processer verka på den globala marknaden och därför även ha en internationell räckvidd."

SOFF vill understryka att denna beskrivning är något som vi som förening helt står bakom. Det är därför av största vikt att den certifieringsordning som nu införs även tar sin utgångspunkt i en kravställning som kommer ligga i linje med övriga EU och EFTA länder samt om möjligt även de länder som nu ingår i Common Criteria Recognition Arrangement (CCRA) för att på sätt underlätta för svenska företag.

Därför är det centralt att den kravställning som FMV föreslås få i uppdrag att närmare utreda inte bara tar sin utgångspunkt i säkerhetskänslig verksamhet utan även breddas till

åtminstone NIS-området för att på så sätt öka området för krav på IKT-produkter, -tjänster och -processer, det vill säga kravställning på IKT-produkter, -tjänster och -processer som ska användas i samhällskritisk verksamhet.

SOFF kan vidare konstatera att företag som exporterar till olika länder inom EU redan idag möter olika landspecifika kravställningar vid t.ex. upphandlingar och ansökningsprocesserna och lokala certifieringar är i förekommande fall en kostsam och resurskrävande insats. I kombination med avsaknaden av enhetliga regelverk medför detta att företag kan komma att avstå från att ens försöka genomföra svensk eller annat lands certifiering.

Detta kan i sin tur påverka såväl i Sverige verksamma företags konkurrenskraft på den internationella marknaden som den svenska statens/samhällets möjlighet att motverka cyberhot genom samverkan med kvalificerade, villiga och resursstarka företag.

Förslag
SOFF bejakar att uppdraget, att analysera och lämna förslag på formerna för framtagande av en ordning för nationell kravställning, som utredningen föreslår ges till FMV och att detta genomförs inom angiven tidsram, till 1 januari 2023. Men att uppdraget breddas till att omfatta åtminstone hela NIS-området. I och med detta bör det även övervägas att alla tillsynsmyndigheter inom NIS-området också beredes plats att delta i arbetet.

Fördjupad kommentar: Kapitel 14 Tillgång till informationssystem vid tillsyn och Kapitel 16 Offentlighet och sekretess

Tillsynsmyndighetens tillsyn innebär icke obetydlig tillgång till företagens information.

Sekretesskraven vid tillsynsmyndighetens hantering av företagens information vid tillsyn bör tydliggöras för att undvika tveksamheter och för att skapa nödvändig trovärdighet hos relevanta företag. Utan sådan reglering löper staten flera allvarliga risker.

Utredningen föreslår FMV, en upphandlande myndighet, som tillsynsmyndighet. För att trovärdiggöra FMV som tillsynsmyndighet bör staten måste tydliggöra behovet av myndighetens sekretess avseende vid tillsyn inhämtad företagsinformation – Inte minst internt, dvs mellan FMV tillsynsverksamhet och samtliga övriga delar av FMV.

Utredaren föreslår att en statlig tillsynsmyndighet får utökade undersökningsbefogenheter. I praktiken föreslår utredaren att tillsynsmyndigheten ges rätt till *direkt insyn* i företagens system. Det måste antas att myndigheten i fråga därmed ges *full tillgång* till den information som företaget i fråga hanterar i dessa system.

Det måste också antas vara sannolikt att tillsynsmyndigheten genom dessa befogenheter får tillgång till information som för företaget i fråga är mycket skyddsvärd. Informationen kan handla om företagets produkter, konkurrenskraft, genomförda, existerande eller planerade samarbeten med annan part än den svenska staten (dvs svenska och utländska företag samt utländska stater), samverkan med andra svenska myndigheter än tillsynsmyndigheten i fråga, samverkan med andra delar av den svenska tillsynsmyndigheten, företagets kompetensförsörjning, planerade uppköp, kostnadsstruktur, strategiska planläggning, marknadsplaner, rekryteringsbehov, patent och immaterialrätt, underleverantörsavtal, investeringsplaner, konkurrenter med mera.

Sådan information omfattas i alla företag av strikt företagssekretess och omfattas i förekommande fall s.k. insiderlagstiftning och/eller sekretessavtal med utländsk stat och/eller med svenska eller utländska företag.

SOFF anser att en *förutsättning* för att en statlig myndighet, i detta fall FMV, ska kunna tilldelas uppdraget som tillsynsmyndighet i enlighet med utredningens förslag är att staten, som uppdragsgivare, tydliggör för FMV att:

- Samtlig från företag genom tillsynsverksamhet inhämtad information skall användas till, och bara till, säkerhetsskyddshöjande verksamhet. Myndigheten är således förbjuden att använda informationen för några andra ändamål eller syften än det angivna – hur gott syftet än kan vara och hur oskyldig/ofarlig informationen än bedöms vara.
- Som en konsekvens av detta skall FMV tillsynsverksamhet därför *omgärdas av hög sekretess, även internt i staten, gentemot annan offentlig förvaltning samt gentemot övriga samhället.*
- Denna höga sekretess *även gäller intern i myndigheten*, dvs även mellan FMV tillsynsverksamhet och övriga delar av FMV.

SOFF bedömer att FMV tillsyn endast genom en sådan instruktion kan trovärdiggöras *för de företag vars verksamhet som omfattas av den.*

SOFF
Säkerhets- och försvarsföretagen

Förslag

SOFF föreslår en översyn som *åtminstone* avser skydd för företagsinformation inhämtad av tillsynsmyndighet enligt nuvarande regelverk samt framtida tillsynsstruktur ur följande perspektiv:

- Hur information som ej kan antas skyddas av statlig utrikes- och underrättelsesekretess *till fullo* kan skyddas – Detta torde bl.a. inkludera hur svensk offentlighetsprincip skall hanteras.
- Hur information som omfattas av, eller kan omfattas av, s.k. insiderlagstiftning skall hanteras av staten, inklusive hur eventuell skada mot tredje part, t.ex. visst företags utländska ägare, skall hanteras av staten om tillsynsmyndigheten kan beslås med att – medvetet eller omedvetet – sprida sådan information.
- Hur det kan säkerställas att information som erhållits eller inhämtats av myndighetens tillsynsverksamhet inte delges annan myndighet eller delges annan del av tillsynsmyndigheten – oavsett skäl och oavsett informationens bedömda skyddsvärde.
- Huruvida av utredaren förslagen insyn i företags system är förenlig med i Sverige verksamma företags sekretessavtal/sekretessåtaganden mot utländsk stat avseende information som delgivits företagen av staten i fråga inom t.ex. ramen för leveransavtal av försvarsmateriel och telekomutrustning.
- Vilken påverkan av utredaren förslagen insyn i företags system därmed, direkt eller indirekt, kan få på svenska statens och/eller i Sverige verksamma företags relation med utländsk stat och/eller utländsk industri.
- Tillämpliga lagrum och regelverk.
- Tydliga och trovärdighetsskapande myndighetsinstruktion(er)

Staten bör genomföra en översyn avseende huruvida nuvarande regelverk till fullo skyddar företagens information från otillbörliga aktörer såväl inom som utom staten, inklusive den myndighet som utövar tillsynen.

Översynen bör ha som mål att föreslagen tillsynsverksamhet kan genomföras på ett sätt som är trovärdigt för samtliga de företag vars verksamhet är aktuell för tillsyn.

SOFF bedömer att en utökad tillsynsverksamhet måste vara trovärdig ur ett företagsperspektiv för att nära och långsiktig samverkan mellan stat och företag skall kunna komma till stånd – *Och nära samverkan mellan stat och företag är nödvändig för att på ett effektivt sätt förbättra Sveriges cybersäkerhet.*

Om översynen kommer fram till att nuvarande regelverk inte kan garanteras till fullo skydda företagens information från otillbörligt spridande, till såväl aktörer inom som utom staten och inklusive inom den myndighet som utövar tillsynen, bör utredningens förslag kompletteras eller andra ändringar göras så att sådant skydd kan säkerställas på ett för företagen trovärdigt sätt.

SOFF bedömer att utredningens förslag bara kan genomföras under förutsättning att FMV:s roll, ansvar och begränsningar är tydliga och ges med stora förbehåll (enligt ovan). Endast då kan utredningens förslag genomföras *på ett för företagen trovärdigt sätt.*

SOFF bedömer att en utökad tillsyn i enlighet med utredarens förslag som införs *utan* ett regelverk som på ett tydligt sätt reglerar hur under tillsyn inhämtad företagsinformation skall hanteras inte bara torde påverka SOFF:s medlemmar, utan också många andra företag i andra branscher.

Övergripande kommentarer
SOFF instämmer i utredarens lägesbild i kap 10.3 - Hotbilden är komplex, ökar och förändras kontinuerligt.

SOFF instämmer i också med utredarens slutsatser avseende det ökade behovet av informations- och cybersäkerhet och det ökade behovet av styrning och samordning som återfinns i kap 10.5 och 10.6. SOFF delar utredningens bedömning avseende det stora behovet av att genom ett ständigt utvecklat samarbete öka det svenska samhällets skydd och motståndskraft mot exemplifierade utmaningar och hot.

Vidare instämmer SOFF till fullo med utredningens bedömning att avsevärt mer behöver ske för att möta behoven av ökad informations- och cybersäkerhet samt styrning och samordning i Sverige.

Fortsatt beredning
Föreningen har uppskattat möjligheten att fått medverka i utredningen genom en expertroll samt att tidigare fått yttra sig över delbetänkandet av cybersäkerhetsutredningen.

SOFF är öppet för att föra en fortsatt dialog med utredningen eller annan av staten utsedd part avseende hur en tydlig instruktion till FMV som tillsynsmyndighet bör utformas i syfte att skapa trovärdighet hos SOFF's medlemmar och andra företag.

SOFF
Säkerhets- och försvarsföretagen

Detta remissvar har beretts av medlemsgrupperna för Cyberförsvar, Samhällssäkerhet och Säkerhetsskydd.

Stockholm 2021-12-22.

För föreningen,

Robert Limmergård