YTTRANDE
SOU 2025:115

Via e-post:
fi.remissvar@regeringskansliet.se
Kopia:
fi.ofa.dis.remisser@regeringskansliet.se
dnr: Fi2026/00065

Remissyttrande SOU 2025:115 Kompletterande bestämmelser till EU:s cyberresiliens-förordning

Säkerhets- och försvarsföretagen (SOFF) tackar för möjligheten att yttra sig över utredningen SOU 2025:115.

SOFF är en branschförening för företag inom säkerhets- och försvarsområdet med verksamhet i Sverige. SOFF har idag över 400 medlemsföretag verksamma inom bland annat försvar, samhällssäkerhet och cybersäkerhet.

Inledning

Föreningen är positiv till initiativ som stärker cybersäkerheten. Mot bakgrund av medlemsföretagens centrala roll för Sveriges säkerhet och försvar är det viktigt att genomförandet av cyberresiliensförordningen (CRA) blir förutsägbart, samordnat och proportionerligt. Nedan lyfter SOFF några centrala synpunkter.

Vikten av harmonisering med cybersäkerhetslagen

För att skapa förutsägbarhet och undvika onödigt betungande administration hos företag och myndigheter är det viktigt att nationella bestämmelser som införs för att komplettera CRA blir enhetliga och harmoniserade.

I denna del bör lagstiftaren särskilt se över hur den nationella implementeringen av CRA förhåller sig till cybersäkerhetslagen.

Ett konkret harmoniseringsproblem uppstår för företag som samtidigt omfattas av CRA och cybersäkerhetslagen. Utan tydliga samordnings- eller hänvisningsbestämmelser riskerar dessa företag att möta parallella krav på rapportering, dokumentation och tillsyn av närliggande händelser och likartade säkerhetsåtgärder.

Detta kan leda till dubbel efterlevnad, ökade administrativa kostnader och oklar ansvarsfördelning mellan myndigheter. Lagstiftaren bör därför säkerställa att överlappande krav och dubbel tillsyn undviks.

Sekretess och känslig information

Flera av SOFF:s medlemsföretag hanterar information som omfattas av sekretess, säkerhetsskyddsavtal eller kommersiellt känsliga villkor. Det är därför avgörande att incident- och sårbarhetsrapportering enligt CRA kan genomföras utan risk för att skyddsvärd information röjs.

Föreningen ser därför positivt på föreslagna sekretessbestämmelser i OSL.

SOFF bedömer i huvudsak att de föreslagna sekretesslösningarna är ändamålsenliga. Det kvarstår dock en viktig oklarhet kring hur uppgifter som lämnas inom ramen för CRA-rapportering kan användas i andra nationella tillsyns- eller sanktionsförfaranden, exempelvis enligt cybersäkerhetslagen. För företag som omfattas av båda regelverken är detta centralt för rapporteringsviljan.

Samtidigt vill föreningen uppmärksamma lagstiftaren om några utmaningar som finns eller kan uppkomma i relation till sekretess och andra känsliga uppgifter.

När incidenter eller sårbarheter rapporteras till en myndighet som också utövar tillsyn kan företag hamna i en svår situation. Det finns då en risk att information som lämnas för att möjliggöra snabb hantering senare används i tillsynsärenden. SOFF anser att regelverket bör utformas så att tidig och ansvarstagande informationsdelning uppmuntras. Regeringen bör därför överväga om frivillig rapportering och avhjälpande åtgärder bör beaktas vid sanktionsbedömningen.

Företag kan inte påverka vilka uppgifter en myndighet maskar vid en sekretessbedömning. Det ställer höga krav på myndigheternas kompetens, resurser och förståelse för vilka uppgifter som kan vara känsliga för det enskilda företaget.

Sekretessbrytande bestämmelser mellan myndigheter kan dessutom innebära att känslig och skyddsvärd information sprids utan att företaget kan påverka informationsdelningen.

Samordning av inrapportering

Utredningen föreslår att företagens rapportering enligt CRA ska ske till MCF, medan PTS hanterar marknadskontroll.

Utöver rapporteringskanalerna enligt CRA finns redan flera rapporteringsvägar inom cybersäkerhetsområdet. För att undvika dubbelrapportering, ökade administrativa kostnader och bristande lägesbilder bör staten eftersträva en samordnad struktur för inrapportering, gärna genom en gemensam nationell rapporteringskanal.

Utredningen konstaterar att det finns flera initiativ på EU-nivå för att förenkla och samordna rapportering. Trots detta kvarstår risker i svensk rätt för de företag som omfattas av både CRA och cybersäkerhetslagen, eftersom överlappande händelser annars kan behöva rapporteras genom separata regimer utan tydlig vägledning om hur överlappningen ska hanteras.

För vissa verksamheter inom försvars- och säkerhetsområdet kan en särskilt anpassad rapporteringsväg till relevant myndighet, vara nödvändig för att tidskritisk incidentrapportering ska kunna ske utan att skyddsvärd information eller operativ förmåga röjs.

Behov av stöd, vägledning och regulatoriska sandlådor
SOFF ser positivt på att marknadskontrollmyndigheten ska kunna inrätta regulatoriska sandlådor och att MCF ska ge stöd till små och medelstora företag. För många mindre aktörer är sådana åtgärder viktiga för att kunna uppfylla CRA-kraven utan oproportionerliga administrativa bördor eller rättslig osäkerhet.

För att stödet ska få avsedd effekt bör vägledning, rådgivning och sandlådor vara samordnade, lättillgängliga och praktiskt användbara. Det bör också tydliggöras hur sekretess, tystnadsplikt och hantering av företagskänsliga uppgifter ska fungera i dessa processer.

Yttrandet har beretts av föreningens medlemsgrupp för Cyberförsvar.

Stockholm den 22 april 2026.

För föreningen,

Robert Limmergård
Generalsekreterare