Datum
2026-04-20

Dnr/Beteckning
TSG 2026-771

Ert datum
2026-01-26

Er beteckning
Fi2026/00065

Kopia till
fi.ofa.dis.remisser@regeringskansliet.se

Finansdepartementet
fi.remissvar@regeringskansliet.se

Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115)

Sammanfattning

Transportstyrelsen tillstyrker i huvudsak förslagen i betänkandet men har följande synpunkter:

- Ansvaret mellan den föreslagna marknadskontrollmyndigheten och berörda sektorsmyndigheter behöver förtydligas
- Samordning av incidentrapportering bör säkerställas gentemot cybersäkerhetslagens bestämmelser
- Sekretessreglering bör medge det informationsutbyte som krävs för en effektiv tillsyn och riskhantering
- Viktigt att förberedelser sker i god tid för en effektiv tillämpning av regelverket

Transportstyrelsens synpunkter

Transportstyrelsen bedömer att betänkandet utgör ett viktigt steg för att stärka cybersäkerheten i produkter med digitala element och därmed bidra till en mer robust och säker digital infrastruktur.

Transportstyrelsen delar utredningens bedömning att EU:s cyberresiliensförordning ställer långtgående krav på säkerhet i produkter med digitala element och att kompletterande nationella bestämmelser är nödvändiga för ett effektivt genomförande. Förordningens fokus på hela produktens livscykel, inklusive krav på riskhantering, sårbarhetshantering och incidentrapportering, är enligt Transportstyrelsens mening centralt för att uppnå en hög cybersäkerhetsnivå.

Transportstyrelsen vill samtidigt uppmärksamma att inom transportsektorn kan samma aktör både vara tillverkare eller leverantör av produkter med digitala element och samtidigt omfattas av cybersäkerhetslagen (2025:1506)

Transportstyrelsen
Generaldirektör
601 73 Norrköping
Besöksadress
Olai Kyrkogata 35, Norrköping

Telefon 0771-503 503
Telefax 011-185 256

transportstyrelsen.se
kontakt@transportstyrelsen.se

Daniel Jönsson
daniel.jonsson2@transportstyrelsen.se
010-495 32 96

som leverantör av samhällsviktiga tjänster. Inom dessa områden utövar Transportstyrelsen tillsyn enligt andra författningar inom cybersäkerhetsområdet. Mot denna bakgrund ser myndigheten ett behov av att det tydliggörs hur ansvarsfördelningen mellan den föreslagna marknadskontrollmyndigheten och sektorsmyndigheter ska fungera i praktiken. Utan en sådan tydlighet finns en risk för överlappande ansvar eller oklarheter i tillsynen, särskilt i situationer där brister i produkter får konsekvenser för transportsystemens informations- och nätverkssäkerhet.

När det gäller incidentrapportering och hantering av sårbarheter ser Transportstyrelsen positivt på att tillverkare, enligt EU:s cyberresiliensförordning, ska rapportera allvarliga incidenter och aktivt utnyttjade av sårbarheter till den nationella CSIRT-enheten. Samtidigt finns det i cybersäkerhetslagen parallella krav på incidentrapportering för verksamhetsutövare. Transportstyrelsen bedömer att det finns ett behov av att samordna dessa rapporteringsflöden så att de inte leder till onödig administrativ börda eller fragmenterad lägesbild. En mer integrerad hantering av incidentinformation skulle också stärka den nationella förmågan att upptäcka och hantera cyberhot.

Transportstyrelsen tillstyrker även de föreslagna bestämmelserna om sekretess till skydd för sårbarhets- och incidentrapporter. Myndigheten vill dock framhålla att sekretessregleringen behöver utformas så att den inte i onödan försvårar nödvändig informationsdelning mellan myndigheter. En väl avvägd balans mellan sekretess och informationsutbyte är avgörande för att tillsyn och riskhantering ska kunna bedrivas effektivt.

Myndigheten vill betona vikten av tidig och strukturerad samverkan mellan berörda aktörer samt behovet av gemensamma arbetssätt och riktlinjer för att säkerställa en enhetlig och effektiv tillämpning.

———

Beslut i detta ärende har fattats av ställföreträdande generaldirektör Ann-Cathrine Wikström. I den slutliga handläggningen av ärendet deltog tf. ställföreträdande säkerhetschef Björn Nord och informationssäkerhetsansvarig Daniel Jönsson, den senare föredragande.