

Ärendenummer  
TRV 2020/117405  
Motpartens ärendenummer  
Fö2020/00954

Dokumentdatum  
2021-01-13

Mottagare:  
Försvarsdepartementet

Kopia till:  
Diariet  
GD Kansli  
Webb och projektstöd (KM)

## **Trafikverkets remissyttrande avseende EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering (SOU 2020:58)**

### **Sammanfattning**

Trafikverket instämmer med utredningens förslag i alla väsentliga delar.

Det vi saknar i utredningen är resonemang kring hur man avser hantera industriella kontrollsystem, samt befintlig infrastruktur. Vi önskar också förtydligande i författningsförslagen gällande reglering av sanktioner samt ackrediterat organ för bedömning av överensstämmelse.

Vi anser att uppdraget och ansvaret som åläggs FMV tills vidare bör formuleras så snävt som möjligt med tanke på svårigheterna att bedöma konsekvenser exempelvis i form av kostnader. Vi bedömer också att det bör formuleras så att alla delar av cybersäkerheten beaktas.

Givet att de produkter, tjänster och processer som omfattas av cybersäkerhetscertifiering kan förväntas utgöra kritiska komponenter för landets försvars- och krishanteringsförmåga, ställer vi oss tveksamma till bedömningen att det inte finns tillräckliga skäl att införa straffrättsliga sanktioner.

Avsnittet om sekretess känns väl genomarbetat och skulle eventuellt kunna förbättras ytterligare genom ett tillägg om säkerhetsskyddslagstiftningen i förhållande till sekretess.

För övrigt ser vi fram emot den förmågehöjning inom cybersäkerhet som implementering av cybersäkerhetsakten tveklöst kommer att föra med sig och önskar att Trafikverket får möjligheten att delta i arbetet med att ta fram en nationell strategi för att tillvarata nationella intressen när det europeiska ramverket utvecklas, samt vid analys av behov av en fortsatt ordning för certifiering av IT-säkerhet i system och produkter.

Ärendenummer  
TRV 2020/117405  
Motpartens ärendenummer  
Fö2020/00954

Dokumentdatum  
2021-01-13

## Yttrande

### Generellt

Utredningen behandlar främst traditionella IT-system för administrativa arbeten. Vi saknar resonemang kring hantering av industriella kontrollsystem och hur man ska hantera befintlig infrastruktur. I många organisationer består denna av en stor flora system och delsystem med varierande ålder, som kommer att utgöra system av system framöver. Detta behöver finnas med i de fortsatta diskussionerna.

Utvecklingen inom detta område kommer med sannolikt att bidra till tydligare direktiv och lagstiftning inom andra säkerhetsområden. Vi ser det positivt att utredningen belyser och föreslår åtgärder för att stärka samverkan och informationsutbyte mellan offentliga och privata aktörer, då detta, liksom strukturerad samverkan med svenskt deltagande på EU-nivå, är en nyckelfaktor för framgång.

En hög nivå av cybersäkerhet tillsammans med en väl fungerande marknad är en förutsättning för att vi ska kunna klara vår uppgift och nå våra mål i Trafikverket.

Utgångspunkterna i utredningen är mycket bra, inte minst konstaterandet att väsentliga delar i nuvarande cybersäkerhetsförmåga, vilar på aktörer som har sin hemvist utanför EU. Att implementera cybersäkerhetsakten och införa en gemensam reglering för cybersäkerhetscertifiering kommer att kunna utgöra grunden för en allmän förmågeförhöjning både inom Sverige och EU.

## Avsnitt Författningsförslag

### 1.1 Förslag till lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt § 8

Det bör framgå om det finns någon begränsning av hur många gånger en organisation, vid upprepade förseelser, kan påföras sanktionsavgift.

### 1.2 Förslag till förordning med kompletterande bestämmelser till EU:s cybersäkerhetsakt § 7

För tydlighetens skull bör det framgå till vem denne skall rapportera.

## Avsnitt 8 Nationell myndighet för cybersäkerhetscertifiering

### 8.3 Nationell myndighet för cybersäkerhetscertifiering

FMV kommer att behöva öka kompetensen avsevärt för den roll som utredningen föreslår. I den stödjande rollen behöver arbetet vara utåtriktat och vägledande och samtidigt vasst i tillsynsrollen. Inför uppstarten föreslås FMV ta intryck av FRA, FM/Must och Säpo, vilka har utarbetade förmågor inom området. Det torde finnas synergier med den pågående förmågeförhöjning inom FMV gällande det utökade uppdraget som industrisäkerhetsmyndighet för försvarsföretagen.

EU cybersäkerhetsstrategi innehåller tre delar, varav en är "försvar". Då FMVs verksamhet har en tydlig försvarsinriktning är det viktigt att alla delar inom cybersäkerhet beaktas då uppdraget formuleras och ansvaret beslutas.

Ärendenummer  
TRV 2020/117405  
Motpartens ärendenummer  
Fö2020/00954

Dokumentdatum  
2021-01-13

Med anledning av svårigheterna att förutse konsekvenserna, bland annat i form av kostnader, bör ansvaret tills vidare formuleras så snävt som möjligt i avvaktan på tydliggöranden från EU i genomförandedelen.

## Avsnitt 9 Tillsynsbefogenheter och sanktioner

### 9.5.3 Finns behov av straffrättsliga sanktioner?

När det gäller sanktioner finns det en bra poäng med att ta rygg på NIS-utredningen. Inte minst när det gäller den principiella utgångspunkten kring straffrättsliga sanktioner/kriminalisering.

Den typ av produkter, tjänster och processer som kommer att omfattas av cybersäkerhetscertifiering utgör ofta kritiska komponenter för landets försvars- och krishanteringsförmåga. Det rör vår förmåga att skapa förebyggande strukturer och att integrera robusthet inom IKT-domänen. Givet detta bör man diskutera om den förväntade effekten av cybersäkerhetscertifiering riskerar att minska om inte straffrättsliga sanktioner finns att tillgå vid överträdelser.

## Avsnitt 12 Sekretess

Det bör övervägas om säkerhetsskyddslagstiftningen i relation till förslagen bör ges utrymme i egen underpunkt i detta kapitel varvid eventuella begränsningar och möjligheter belyses.

## Avsnitt 13 Övriga frågor

### 13.2.2 Behovet av nationell strategi och medverkan i Europeiska gruppen för cybersäkerhetscertifiering (ECCG)

Trafikverket bör få möjligheten att delta i arbetet med att ta fram en nationell strategi för att tillvarata nationella intressen när det europeiska ramverket utvecklas.

### 13.3.2 Nationella ordningen för certifiering av IT-säkerhet i system och produkter

Givet Trafikverkets stora IT-infrastruktur bör vi få möjligheten att medverka då FMV ska analysera behov av en fortsatt ordning för certifiering av IT-säkerhet i system och produkter.

**Ärendenummer**  
TRV 2020/117405  
**Motpartens ärendenummer**  
Fö2020/00954

**Dokumentdatum**  
2021-01-13

## Föredragande, samråd och sakgranskning

Ärendet har internremitterats och synpunkter har inhämtats ifrån flera utav Trafikverkets verksamheter. Yttrandet har sammanställts och föredragits av Jenny Axelson-Fisk, verksamhetsutvecklare verksamhetsområde Informations- och kommunikationsteknik. Yttrandet har granskats av Mathias Persson chef verksamhetsområde Informations- och kommunikationsteknik och Erica Willborg, chef avdelning Säkerhet, verksamhetsområde Informations- och kommunikationsteknik och fastställts av generaldirektör, Lena Erixon.

Borlänge 14 januari 2021

Lena Erixon  
Generaldirektör