

**REMISSYTTRANDE**

2026-04-16

FRA beteckning  
Dnr 2026FRA239-2

Finansdepartementet

Er handläggare  
Felisa KrzyzanskiErt datum  
2026-01-26Er beteckning  
Fi2026/00065FRA handläggare  
Miriam Christensson**Betänkandet Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115)**

Försvarets radioanstalt (FRA) har, från de utgångspunkter myndigheten har att beakta, följande synpunkter på förslagen i betänkandet.

**11.6.2 En ny sekretessbestämmelse för uppgift i sårbarhets- och incidentrapporter samt en ny sekretessbrytande bestämmelse**

FRA instämmer i att det bör införas en ny sekretessbestämmelse för uppgifter i sårbarhets- och incidentrapporter enligt artikel 14 och 15 i EU:s cyberresiliensförordning<sup>1</sup>. FRA ser emellertid en risk att utformningen av den föreslagna sekretessbestämmelsen kan komma att begränsa FRA:s möjligheter att uppfylla vissa uppgifter som ankommer eller planeras ankomma på myndigheten.

Av 3 § 2 förordning (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt följer att FRA inom ramen för det nationella cybersäkerhetscentret ska lämna råd och stöd till privata och offentliga aktörer i frågor om hot, sårbarheter och risker med koppling till cybersäkerhet. Efter den verksamhetsövergång som planeras göras från

---

<sup>1</sup> Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).

Myndigheten för civilt försvar till FRA,<sup>2</sup> kommer FRA även att få en skyldighet som CSIRT-enhet enligt artikel 11 i NIS 2-direktivet<sup>3</sup> och 33 § cybersäkerhetsförordningen (2025:1507) att tillhandahålla tidiga varningar, larm, meddelanden och sprida information om cyberhot, sårbarheter och incidenter för att skydda vissa aktörer och andra relevanta intressenter i samhället. Av skäl 66 i EU:s cyberresiliensförordning följer att tillverkare bör anmäla aktivt utnyttjade sårbarheter för att säkerställa att CSIRT-enheterna har en adekvat överblick över sådana sårbarheter och förses med den information som de behöver för att utföra sina uppgifter som anges i NIS 2-direktivet. Av EU:s cyberresiliensförordning följer också att CSIRT-enheten inte har någon uttrycklig skyldighet att lämna information om sårbarheter eller incidenter. Av 4 § första stycket förordning (2007:937) med instruktion för Försvarets radioanstalt framgår vidare att FRA efter begäran får stödja statliga myndigheter och enskilda verksamhetsutövare som hanterar information som bedöms vara känslig från sårbarhetssynpunkt. Inom ramen för ett sådant uppdrag bör FRA ha förutsättningar att lämna adekvat rådgivning avseende hur en sårbarhet kan hanteras utan att begränsas av sekretess gentemot uppdragsgivaren.

Mot bakgrund av detta bör det i det fortsatta lagstiftningsarbetet tas ett helhetsgrepp om det sekretessskydd som gäller för incident- och sårbarhetsrapportering och för förutsättningarna för informationsdelning av sådana uppgifter.

Vad gäller förslaget till sekretessbrytande bestämmelse vill FRA framhålla att förslaget välkomnas. Därutöver vill FRA uppmärksamma att det i prop. 2025/26:214 Lagändringar för ett stärkt nationellt cybersäkerhetscenter föreslås en ny sekretessbestämmelse i 40 kap. 7 i § offentlighets- och sekretesslagen (2009:400), OSL, enligt vilken sekretess gäller hos FRA i verksamhet vid det nationella cybersäkerhetscentret för uppgift om en enskilds personliga eller ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde lider skada eller men. Det skulle kunna uppstå situationer där en uppgift i en sårbarhets- eller incidentrapport omfattas av sekretess både enligt föreslagna 18 kap. 8 d § och 40 kap. 7 i § OSL, men där den nu föreslagna sekretessbrytande bestämmelsen enbart bryter sekretessen enligt 18 kap. 8 d § OSL. I det fortsatta lagstiftningsarbetet bör frågan om hur nämnda bestämmelser ska förhålla sig till varandra ses över.

### **12.5.1 Stödåtgärder enligt artikel 33.1**

FRA välkomnar utredningens förslag att Myndigheten för civilt försvar ska tillhandahålla och samordna stöd till små och medelstora företag enligt artikel 33.1 EU:s

---

<sup>2</sup> Se regeringsuppdragen Fö2025/01703 och Fö2025/01704 från den 20 november 2025.

<sup>3</sup> Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148.

cyberresiliensförordning och rollen som NCC-SE föreslås få i det arbetet. FRA delar utredningens bedömning att uppgiften efter verksamhetsövergången från Myndigheten för civilt försvar till FRA bör utföras av FRA genom det nationella cybersäkerhetscentret (NCSC) där NCC-SE kommer inordnas<sup>4</sup>.

### **Övriga synpunkter**

FRA noterar att det redan förekommer en 8 d § i 18 kap. OSL. I det remitterade betänkandet föreslagna 18 kap. 8 d och e §§ om sekretess för sårbarhets- och incidentrapporter samt sekretessbrytande bestämmelse behöver därför justeras.

I 31 § cybersäkerhetsförordningen (2025:1507) anges att Myndigheten för civilt försvar ska vara enhet för hantering av it-incidenter (CSIRT-enhet) i enlighet med artikel 10 i NIS 2-direktivet. Hänvisningen till cybersäkerhetsförordningen i föreslagna 3 § förordningen med kompletterande bestämmelser till EU:s cyberresiliensförordning behöver därför justeras. Detsamma gäller 3 § i förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641).

---

### **Allmänt om FRA**

FRA är en civil myndighet under Förvarsdepartementet. FRA är en del av svensk underrättelsetjänst med uppgift att bedriva signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet och till lagen anslutande förordning.

FRA bedriver signalspaning i syfte att kartlägga bl.a. yttre militära hot, hot mot svensk personal under internationella insatser, internationell terrorism, främmande underrättelseverksamhet mot svenska intressen och övriga internationella företeelser som har betydelse för svensk utrikes-, säkerhets- och försvarspolitik. All signalspaning är riktad mot utländska förhållanden och sker på uppdrag av regeringen, Regeringskansliet, Försvarmakten, Säkerhetspolisen och Nationella operativa avdelningen inom Polismyndigheten. Uppdragsgivarna är fortlöpande i behov av underrättelserapportering och signalspaningsverksamheten bidrar kontinuerligt till att skydda Sverige och svenska intressen. All inhämtning genom signalspaning kräver tillstånd från Försvarsunderrättelsesdomstolen.

FRA bedriver även cybersäkerhetsverksamhet. FRA ska ha hög teknisk kompetens inom informationssäkerhetsområdet och får efter begäran stödja sådana statliga myndigheter

---

<sup>4</sup> Se regeringsuppdragen Fö2025/01703 och Fö2025/01704 från den 20 november 2025.

och enskilda verksamhetsutövare som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende.

Sedan november 2024 ansvarar FRA också för NCSC som har i uppgift att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och it-incidenter. Viss verksamhet från Myndigheten för civilt försvar planeras att överföras till FRA den 1 juli 2026.<sup>5</sup> Den verksamhet som förs över avses inordnas i NCSC vid FRA.

Uppgifter rörande FRA:s verksamhet omfattas i stora delar av sekretess bl.a. enligt 15 kap. 2 § och 18 kap. 8 § OSL.

---

I detta ärende har generaldirektören Björn Lyrvall beslutat. I den slutliga handläggningen har också deltagit överdirektören Maria Diamant, chefsjuristen Michaela Dráb, C GD:s stab Marika Dagenbrink, avdelningscheferna Gunnar Hellenius och John Billow, enhetschefen Jessica Öhlund Andersson (C JUR:s kansli/Rätts 2) samt juristen Miriam Christensson (C JUR:s kansli/Rätts 2), tillika föredragande.

Försvarets radioanstalt

Björn Lyrvall

Miriam Christensson

---

<sup>5</sup> Se regeringsuppdragen Fö2025/01703 och Fö2025/01704 från den 20 november 2025.

**FRA**

Dnr 2026FRA239-2

SändlistaExternt

Försvarsdepartementet/EFU

Försvarsdepartementet/Rättssekretariatet

Försvarsdepartementet/ECH

Internt FRA

GD

ÖD

C JUR

Bitr. C JUR

C GD:s stab

C KOM

C PS

AC

C JUR:s kansli/C Rätts 1