Myndigheten för civilt försvar

Konsekvensutredning

Datum	Ärendenummer
2026-05-13	MCF 2026-04335

Konsekvensutredning rörande Myndigheten för civilt försvars föreskrifter om rapportering av it-incidenter för statliga myndigheter

Beskrivning av problemet och vilken förändring som eftersträvas

Statliga myndigheter är enligt 14 § förordningen (2022:524) om statliga myndigheters beredskap (beredskapsförordningen) skyldiga att till stöd för arbetet med samhällets informationssäkerhet skyndsamt rapportera it-incidenter som har inträffat i den rapporterande myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller som har inträffat i tjänster som myndigheten tillhandahåller åt en annan organisation. Rapportering ska idag ske till Myndigheten för civilt försvar och regleras närmare i föreskrifter.

Syftet med föreslagen uppdatering av myndighetens föreskrifter om incidentrapportering för statliga myndigheter är att få en mer heltäckande bild av inträffade incidenter på ett tidigare stadium än idag, förenkla för de statliga myndigheter som omfattas av krav på incidentrapportering enligt både beredskapsförordningen och cybersäkerhetslagen (2025:1506) samt korrigera hänvisningen till mandatet att utfärda föreskrifter respektive genomföra de justeringar som följer av att uppgiften att ta emot incidentrapporter enligt beredskapsförordningen kommer att flyttas över från Myndigheten för civilt försvar (tidigare Myndigheten för samhällsskydd och beredskap) till Försvarets radioanstalt den 1 juli 2026. För de statliga myndigheter som endast omfattas av beredskapsförordningens krav på incidentrapportering kommer förändringarna som görs i syfte att skapa en förbättrad lägesbild att innebära att rapportering sker i ytterligare ett skede.

Förbättrad lägesbild

Enligt 4 § i nu gällande föreskrifter[1] ska en statlig myndighet skyndsamt, dock senast sex timmar från det att myndigheten har identifierat att en it-incident omfattas av rapporteringsskyldighet, lämna en övergripande beskrivning av vad som har inträffat (notifiering). Därefter ska myndigheten enligt 5 § samma reglering, inom fyra veckor från det att myndigheten har identifierat att en it-incident omfattas av rapporteringsskyldighet, lämna ytterligare uppgifter om den inträffade it-incidenten (slutrapportering) till den

[1] MSBFS 2020:8 föreskrifter om rapportering av it-incidenter för statliga myndigheter

myndighet som pekas ut som mottagare av it-incidenter i beredskapsförordningen (nedan benämnd mottagande myndighet).[2]

Nuvarande utformning och tidpunkt för de olika skeden som statliga myndigheter rapporterar i innebär att mottagande myndighet får kännedom om inträffade it-incidenter på ett tidigt stadium (efter sex timmar) och ges därmed förutsättningar att agera operativt. En utmaning i arbetet att bygga upp en lägesbild är dock att inrapporterade notifieringar kan vara knapphändiga. De statliga myndigheterna är inte ålagda att komplettera informationen om inträffade incidenter förrän efter en månad från det att incidenten har rapporterats. Detta innebär att det tar lång tid innan mottagande myndighet kan bygga upp en mer fullständig bild över vad som har inträffat och dess konsekvenser för rapporterande myndighet, andra organisationer och samhället i stort. Mot bakgrund av den säkerhetspolitiska utvecklingen, och den förhöjda hotbilden på cyberområdet, bedöms inte detta längre motsvara behoven vad gäller lägesbild. Som en jämförelse kan nämnas att motsvarande incidentrapporteringsskeden i 5, 6 och 8 §§ cybersäkerhetslagen utgörs av *Upplysning* efter 24 timmar, *Incidentanmälan* efter 72 timmar och *Slutrapport* alternativt *Lägesrapport* efter en månad. Upplysning kan närmast ses motsvara nuvarande Notifiering och Incidentanmälan samt Slutrapport i stort sett innehållsmässigt motsvara statliga myndigheters slutrapportering.

Undanröja dubbelrapportering och förenkla förfarandet

I samband med att cybersäkerhetslagen trädde ikraft den 15 januari 2026 ska de statliga myndigheter som även omfattas av den regleringen rapportera *betydande incidenter* till Myndigheten för civilt försvar (efter den 1 juli 2026 ska rapporteringen gå till Försvarets radioanstalt). En incident ska enligt 2 kap. 5 § andra stycket cybersäkerhetslagen anses vara betydande om den ”har orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren”, eller ”om den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada”.

En jämförelse mellan rapporteringsplikten enligt beredskapsförordningen och cybersäkerhetslagen visar att alla incidenter som omfattas av rapporteringsplikt enligt beredskapsförordningen inte är rapporteringspliktiga enligt cybersäkerhetslagen. Bedömningen är dock att de incidenter som är rapporteringspliktiga enligt cybersäkerhetslagen, eventuellt med något enstaka undantag, omfattas av rapporteringsplikt enligt beredskapsförordningen. För statliga myndigheter som ska rapportera en incident som bedöms som betydande enligt cybersäkerhetslagen innebär det ett samtidigt krav på rapportering enligt beredskapsförordningen, dvs. krav på rapportering av samma incident enligt olika regelverk och delvis olika intervaller till en och samma mottagande myndighet.

[2] Det vill säga fram till den 30 juni 2026 till Myndigheten för civilt försvar och efter den 1 juli 2026 Försvarets radioanstalt.

Rapporteringsplikten kan därtill jämföras med framtida CER-rapportering. Hur CER-rapportering kommer att utformas i detalj är dock fortfarande oklart i och med att författningsförslag och proposition ännu inte är på plats. Beredskapsförordningen gäller alla statliga förvaltningsmyndigheter under regeringen, med några undantag. CER-regleringen kommer sannolikt, liksom NIS 2-regleringen, att gälla ett urval av statliga myndigheter. De incidenter som är rapporteringspliktiga enligt beredskapsförordningen kommer sannolikt vara rapporteringspliktiga även enligt kommande CER-reglering. Därför kommer det rapporteringsverktyg som ska användas i den nationella portalen att utformas för att tillgodose rapporteringskraven enligt såväl NIS 2-regleringen, beredskapsförordningen som kommande CER-reglering. För att förenkla för verksamhetsutövaren kommer frågor och struktur i formuläret vara utformade på ett sätt som undviker dubbelrapportering.

I vissa fall kan det vara befogat att rapportera en och samma incident flera gånger, exempelvis när syftet med och efterfrågad information skiljer sig åt i olika rapporteringsspår. När det gäller beredskapsförordningen och cybersäkerhetslagen bedöms skälen till varför det finns rapporteringskrav och kraven på vilken information som ska lämnas dock som snarlika. För att inte belasta berörda statliga myndigheter i onödan skulle därför formerna för rapporteringen behöva ses över i syfte att minimera konsekvenserna av överlappande krav.

Som stöd för incidentrapporteringen behöver beredskapsförordningens föreskrifter åtminstone tydligt reglera hur ofta information ska lämnas in (vilka skeden) och när detta ska ske (tidsintervall). Vad gäller vilken information som ska lämnas i respektive skede bedöms det finnas möjlighet att antingen reglera detta i mer detalj, såsom i nuvarande föreskrifter, eller på en mer övergripande nivå där kraven istället konkretiseras i vägledning och vid användning av systemstöd.

I vilka skeden och inom vilka tidsintervall som incidentrapportering enligt cybersäkerhetslagen ska ske regleras redan i nu gällande lag medan vilken information som ska lämnas i respektive skede vid rapportering enligt cybersäkerhetslagen ska förtydligas i kommande föreskrifter.

Harmonisering av beredskapsförordningens föreskrifter gentemot cybersäkerhetslagens incidentrapportering bedöms i nuläget enkelt kunna göras mot *skeden och tidsintervaller* eftersom cybersäkerhetslagen redan har trätt ikraft. Några föreskrifter som reglerar vilken *information* som ska lämnas i respektive skede vid rapportering av incidenter enligt cybersäkerhetslagen är dock ännu inte beslutade. De kan därför inte användas som förlaga för beredskapsförordningens föreskrifter när det gäller en detaljerad kravbild på vilken information som ska lämnas i respektive skede. Detta talar för att minska risken för motsägelser mellan regelverken genom att istället välja alternativet att låta beredskaps-förordningens föreskrifter endast reglera vilken information som ska lämnas i olika skeden på övergripande nivå och sedan konkretisera detta för de statliga myndigheterna i vägledning och genom systemstöd.

Hur redan genomförd rapportering enligt beredskapsförordningen närmare förhåller sig till kraven på rapportering enligt cybersäkerhetslagen bedöms lämpligast regleras i kommande föreskrifter om incidentrapportering enligt cybersäkerhetslagen.

Utöver behovet av att undvika dubbelrapportering finns även anledning att tillförsäkra myndigheter som omfattas av beredskapsförordningen samma flexibilitet som ges i föreskrifterna enligt cybersäkerhetslagen gällande vem som ska rapportera in incidenter. Nuvarande föreskrifter ställer krav på att myndigheten, om den överlåter en del av sin informationshantering till en aktör som inte omfattas av rapporteringsskyldighet, ska se till att aktören åtar sig att rapportera it-incidenter till myndigheten på ett sådant sätt att myndigheten kan uppfylla kraven i dessa föreskrifter. Det är enligt nuvarande reglering myndigheten som ska fullgöra rapporteringsplikten. Motsvarande krav saknas i föreskrifterna för cybersäkerhetslagen. Därför har kraven även tagits bort i beredskapsförordningens föreskrifter i syfte att förenkla för de myndigheter som omfattas.

Korrigera hänvisning till föreskriftsmandat och myndighetsnamn

Nuvarande föreskrifter hänvisar rörande föreskriftsmandatet i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (krisberedskapsförordningen). Krisberedskapsförordningen har upphävts och ersattes 2022 med beredskapsförordningen. Eftersom föreskriftsmandatet utformades på samma sätt i den nya förordningen som i den tidigare bedömdes det inte av formella skäl finnas ett omedelbart behov av en översyn av föreskrifterna enbart av den anledningen. När föreskrifterna nu uppdateras ska dock en korrigering göras.

En korrigering behöver även göras när det gäller namnet på den myndighet som ska ta emot rapporter om incidenter. Den 1 januari 2026 bytte Myndigheten för samhällsskydd och beredskap namn till Myndigheten för civilt försvar. Till detta kommer att uppgiften att ta emot incidentrapporter enligt beredskapsförordningen per den 1 juli 2026 flyttas från Myndigheten för civilt försvar till Försvarets radioanstalt. Då dessa föreskrifter träder i kraft först den 1 juli 2026 bör därför refereras till Försvarets radioanstalt som mottagande myndighet.

Föreslagna justeringar

Följande förändringar syftar till att förbättra lägesbilden:

1. Ett ytterligare rapporteringsskede införs efter 72 timmar där statliga myndigheter åläggs att ge en fördjupad bild av en inträffad it-incident.

2. Myndigheten för civilt försvar ges möjlighet att redan i ett tidigt stadium begära in relevanta statusuppdateringar istället för att som i nuvarande föreskrifter göra det i form av en komplettering av inlämnad slutrapport.

Följande förändringar syftar till att harmonisera beredskapsförordningen och cybersäkerhetslagens krav på rapportering av incidenter och därmed minska faktisk dubbelrapportering för de myndigheter som omfattas av båda regleringarna:

1. Benämningen på de olika rapporteringsskedena harmoniseras med cybersäkerhetslagens terminologi.

2. Nuvarande mer detaljerade specifikation av vilken information som ska lämnas i respektive skede ersätts med mer generella och övergripande skrivningar för att minska risken för motsägelser mellan regelverken.

3. Tidpunkten för rapportering av Upplysning enligt beredskapsförordningen ska av operativa skäl enligt föreskriftsförslaget ske senast 6 timmar efter att myndigheten har identifierat incidenten som rapporteringspliktig.

4. Tidpunkterna för rapportering av Incidentanmälan och Slutrapport enligt beredskapsförordningen ensas med tidpunkterna för motsvarande rapportering enligt cybersäkerhetslagen.

5. Möjligheten att inkomma med en lägesrapport i de fall incidenten fortfarande är pågående en månad efter det att upplysningen har inkommit.

Följande förändring syftar till att skapa flexibilitet i hur myndigheten utformar sin rapportering vid utkontraktering:

1. Nuvarande krav på att myndigheten ska se till att leverantören informerar myndigheten så att den kan fullgöra sin rapporteringsskyldighet i 8 § tas bort.

Följande förändringar syftar till att uppdatera hänvisningar och myndighetsnamn:

1. Nuvarande hänvisning till 21 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ersätts med en hänvisning till 27 § 2 p. förordningen (2022:524) om statliga myndigheters beredskap.

2. Föreskrifterna justeras vad gäller myndighetens namn från Myndigheten för samhällsskydd och beredskap till Försvarets radioanstalt.

Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

Av 14 § beredskapsförordningen framgår att en myndighet ska, till stöd för arbetet med samhällets informationssäkerhet, till Myndigheten för civilt försvar skyndsamt rapportera it-incidenter som inträffat i den rapporterande myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller som inträffat i tjänster som myndigheten tillhandahåller åt en annan organisation.

Enligt 27 § p 2 beredskapsförordningen får Myndigheten för civilt försvar meddela närmare föreskrifter om it-incidentrapportering enligt 14 § efter att ha gett Polismyndigheten, Säkerhetspolisen och Försvarsmakten tillfälle att yttra sig.

Uppföljning av konsekvenser av föreskrifter och allmänna råd

Enligt 7 § 5 p. i förordningen (2024:183) om konsekvensutredningar ska en myndighet följa upp konsekvenserna av sina föreskrifter och allmänna råd. En första uppföljning kommer att ske så snart det är möjligt att utvärdera reglernas effekter, sannolikt cirka ett och ett halvt år efter det att föreskrifterna har trätt ikraft. Synpunkter kommer att hämtas in från ett representativt urval av de statliga myndigheter som är rapporteringsskyldiga.

Föreskrifter och föreskriftsmandat gällande beredskapsförordningens krav på statliga myndigheter avseende incidentrapportering kommer att flyttas över till Försvarets radioanstalt den 1 juli 2026. Med anledning av detta kommer uppföljningen av konsekvenser ske hos Försvarets radioanstalt.

Om de grundläggande förutsättningarna för regleringen har ändrats kommer reglerna att omprövas och en ny konsekvensutredning att göras.

Beskrivning av alternativa lösningar för det som ska uppnås och vilka effekterna blir om någon reglering inte kommer till stånd

Förbättrad lägesbild

En alternativ lösning för att på ett tidigt stadium få in ytterligare information om inträffade incidenter skulle kunna vara att endast införa en regel som utökar mottagande myndighets möjligheter att begära in kompletteringar av lämnade rapporter. Sådana kompletteringar skulle sannolikt behöva ske med manuella inslag och därmed vara förhållandevis resurskrävande. Det skulle sannolikt även öka belastningen på inrapporterande myndigheter eftersom det kan bli mindre förutsägbart om, när och vilken komplettering som önskas.

Nollalternativet

Om ingen reglering kommer till stånd kvarstår nuvarande förhållanden där mottagande myndighet har en mer komplett bild av vad som inträffat först efter en månad från det att incidenten har identifierats som rapporteringspliktig. Som nämnts ovan bedöms detta inte längre motsvara behoven av lägesbild utifrån den säkerhetspolitiska utvecklingen och den förhöjda hotbilden på cyberområdet.

Undanröja dubbelrapportering

Föreskrifter om incidentrapportering enligt cybersäkerhetslagens krav träder ikraft den 1 juli 2026. Kravet att rapportera betydande incidenter, såsom det är formulerat i cybersäkerhetslagen, gäller redan sedan lagens ikraftträdande den 15 januari 2026. Föreskrifterna om incidentrapportering enligt cybersäkerhetslagen tydliggör dock för verksamhetsutövarna vilka incidenter som ska anses betydande och vilken information som ska lämnas vid rapportering. Det är därför främst i samband med att dessa föreskrifter träder i kraft som konsekvenserna av att omfattas av båda regelverkens krav på incidentrapportering blir påtagliga.

Ett alternativ till nuvarande förslag är att låta rapportering enligt cybersäkerhetslagen helt ersätta rapportering enligt beredskapsförordningen. Detta kan ske på två sätt.

1. Revidera föreskrifterna enligt beredskapsförordningen så att de fullt ut speglar kraven i cybersäkerhetslagen och tillhörande föreskrifter om incidentrapportering för väsentliga och viktiga verksamhetsutövare. Detta innebär att samtliga statliga myndigheter, oavsett om de omfattas av cybersäkerhetslagens krav eller inte, rapporterar incidenter på samma sätt som verksamhetsutövare som omfattas av cybersäkerhetslagen.

2. Justera föreskrifterna enligt beredskapsförordningen så att de tydliggör att de statliga myndigheter som omfattas av cybersäkerhetslagens krav på rapportering helt uppfyller beredskapsförordningens krav på rapportering genom att rapportera enligt cybersäkerhetslagens kriterier och tidsramar.

En utmaning med båda ovanstående upplägg är skillnaderna mellan vad som är rapporteringspliktigt enligt cybersäkerhetslagen respektive beredskapsförordningen. Såsom ovan har redovisats bedöms inte alla incidenter som omfattas av rapporteringsplikt enligt beredskapsförordningen vara rapporteringspliktiga enligt cybersäkerhetslagen. Bedömningen är dock att de incidenter som är rapporteringspliktiga enligt cybersäkerhetslagen, eventuellt med något enstaka undantag, omfattas av rapporteringsplikt enligt beredskapsförordningen. Betydande incidenter enligt cybersäkerhetslagen bedöms vara allvarligare och i högre grad riskera att ge konsekvenser för andra.

Att höja trösklarna för incidentrapportering för statliga myndigheters rapportering enligt beredskapsförordningen på ett sätt som motsvarar nivån i cybersäkerhetslagen i enlighet med alternativ 1 eller 2 förutsätter

- att en sådan justering inte får till följd att föreskrifterna i praktiken innebär en inskränkning i förhållande till beredskapsförordningen krav i 14 § på vilka it-incidenter som ska rapporteras, och

- att syftet med incidentrapporteringen utifrån möjligheten till operativt stöd och lägesbild även fortsättningsvis bedöms kunna uppnås.

Det bedöms i nuläget inte vara tydligt att justeringar i linje med alternativ 1 eller 2 kan göras utan att innebära en begränsning av beredskapsförordningens krav i 14 §. Till detta kommer att förutsättningarna för operativt stöd och lägesbild bedöms försämras med föreslagen höjning av rapporteringströsklarna. Alternativ 1 och 2 ses därför vid en samlad bedömning inte som aktuella vid denna föreskriftsrevidering.

Nollalternativet

Alternativet att inte göra några justeringar alls av föreskrifterna om rapportering av it-incidenter för statliga myndigheter medför att de statliga myndigheter som omfattas av cybersäkerhetslagen från och med den tidpunkt som föreskrifterna om incidentrapportering enligt cybersäkerhetslagen träder ikraft kan komma att behöva rapportera samma incident enligt två regelverk till samma myndighet. Mottagande myndighet kommer givetvis att vidta åtgärder där det är möjligt för att förenkla rapporteringen. Detta alternativ bedöms dock orsaka onödig hantering både hos rapporterande och mottagande myndighet. För de myndigheter som inte kommer att omfattas av cybersäkerhetslagen ska incidentrapportering enligt beredskapsförordningen ske som idag.

Justering av tid för initial rapportering

Ett ytterligare regleringsalternativ vore att förlänga tidsramen, även vad gäller det första rapporteringsskedet, i linje med cybersäkerhetslagens krav och tillhörande föreskrifter. Det skulle innebära att en myndighet, även enligt beredskapsförordningen, hade behövt rapportera en incident först 24 timmar efter det att den har bedömts som rapporteringspliktig. Enligt nuvarande 4 § ska den första rapporteringen ske senast sex timmar efter det att myndigheten har identifierat att incidenten omfattas av rapporteringsskyldigheten.

Samma tidsgräns för den initiala rapporteringen gällde även under tidigare NIS-reglering. En förändring av tidsfristen för det första rapporteringssteget från sex timmar till 24 timmar skulle därför vara ett avsteg från de krav och rutiner som har gällt för statliga myndigheter sedan 2020. Det skulle leda till att den mottagande myndigheten och därmed CERT-SE[3] får kännedom om incidenten betydligt senare än i nuläget och får en minskad möjlighet att ge meningsfullt stöd till den anmälande myndigheten. Givet omvärldsläget är en sådan försämring av möjligheterna till förbättrad lägesbild svår att motivera.

Den praktiska skillnaden mellan tillämpningen av kraven i föreskrifterna enligt beredskapsförordningen på rapportering efter senast sex timmar och motsvarande krav i cybersäkerhetslagen på rapportering senast efter 24 timmar bedöms vara begränsad för en statlig myndighet. Detta med anledning av att det enligt cybersäkerhetslagen åligger verksamhetsutövare att, utöver att rapportera faktiska incidenter som har fått olika allvarliga konsekvenser, även rapportera sådana incidenter som *skulle kunna* resultera i sådana allvarliga konsekvenser. Rapporteringsplikt för sådana incidenter som enligt cybersäkerhetslagen skulle kunna resultera i allvarliga konsekvenser uppstår, eventuellt

[3] Den nationella funktionen för hantering av it-incidenter.

med något undantag, tidigt i händelsekedjan. Motsvarande incidenter är inte rapporteringspliktiga enligt beredskapsförordningen. Föreskrifternas krav på rapportering efter sex timmar skapar dock förutsättningar för att, även med stöd av denna reglering, på ett tidigt stadium få kunskap om potentiellt allvarliga incidenter som har inträffat hos statliga myndigheter som inte omfattas av cybersäkerhetslagen. Sammantaget motiverar detta varför kravet på att inkomma med en upplysning inom sex timmar kvarstår.

Uppgifter om vilka som berörs av regleringen

Kraven på incidentrapportering enligt 14 § beredskapsförordningen gäller alla statliga myndigheter under regeringen med undantag för Regeringskansliet, kommittéväsendet, Försvarsmakten, Säkerhetspolisen, Fortifikationsverket, Försvarets materielverk, Försvarets radioanstalt, Försvarshögskolan, Försvarsunderrättelsedomstolen, Statens inspektion för försvarsunderrättelseverksamheten, Totalförsvarets forskningsinstitut, Totalförsvarets plikt- och prövningsverk samt utlandsmyndigheterna.[4]

I mitten av april 2026 hade runt 90 statliga myndigheter anmält till Myndigheten för civilt försvar att de omfattades av cybersäkerhetslagen.

Uppgifter om vilka kostnadsmässiga och andra konsekvenser regleringen medför och en jämförelse av konsekvenserna för de övervägda regleringsalternativen

För de statliga myndigheter som omfattas av cybersäkerhetslagen bedöms förslaget till revidering av föreskrifterna förenkla den praktiska hanteringen när betydande incidenter enligt cybersäkerhetslagen även ska rapporteras enligt beredskapsförordningen. Bedömningen är att kostnaderna för rapportering troligen kommer att vara desamma som idag.

Revidering eller justering av föreskrifterna i enlighet med alternativ 1 och 2 ovan skulle underlätta ytterligare för de statliga myndigheter som även omfattas av cybersäkerhetslagens krav på incidentrapportering. Dessa alternativ bedöms dock få negativa konsekvenser för möjligheterna att ge operativt stöd och upprätthålla lägesbild, det finns även rättsliga aspekter som kan utgöra hinder, exempelvis om den information som behöver hämtas in för att uppfylla cybersäkerhetslagens syfte går utöver vad som ska hämtas in för att uppfylla beredskapsförordningens syfte.

För de statliga myndigheter som inte omfattas av båda regelverken innebär dock justeringarna att den rapportering som nu görs i två skeden framöver kommer att göras i tre skeden, vilket bedöms innebära att incidentrapporteringen blir något mer resurskrävande än idag. Detta begränsas dock genom ett användarvänligt rapporterings-

[4] För utlandsmyndigheterna tillämpas denna förordning endast i den utsträckning som bestäms i föreskrifter som meddelas av Regeringskansliet (Utrikesdepartementet).

verktyg och systemstöd. Rapporteringen kommer att ske i den nationella portal där även incidenter enligt cybersäkerhetslagen och kommande CER-reglering kommer att rapporteras. Trots effektiva rapporteringsverktyg kan däremot rapporteringen i två skeden innebära en administrativ börda för de statliga myndigheterna. Fördelarna med att snabbare få en lägesbild över vilka incidenter som drabbar statliga myndigheter bedöms dock överväga.

Ett ändamålsenligt systemstöd för incidentrapportering enligt både beredskapsförordningen och cybersäkerhetslagen bedöms hålla ned kostnaderna oavsett hur föreskrifterna utformas.

Bedömning av om regleringen överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen

Myndigheten bedömer inte att regleringen går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen.

Bedömning av om särskilda hänsyn behöver tas när det gäller tidpunkten för ikraftträdande och om det finns behov av speciella informationsinsatser

Det är viktigt att föreskrifterna träder ikraft samtidigt som föreskrifterna om incidentrapportering enligt cybersäkerhetslagen den 1 juli 2026, eftersom det är i samband med detta som dubbelrapporteringen aktualiseras fullt ut för de statliga myndigheter som omfattas av cybersäkerhetslagen.

För att inte orsaka avbrott i redan påbörjad rapportering bedöms föreskrifterna behöva innehålla övergångsbestämmelser som tydliggör att de föreskrifter som upphävs vid ikraftträdandet av de reviderade föreskrifterna fortfarande ska gälla för sådana it-incidenter som har identifierats och bedömts som rapporteringspliktiga före ikraftträdandet.

Det bedöms behövas både riktade informationsinsatser, vägledning och systemstöd för att ge stöd till berörda statliga myndigheter.

Konsekvenser för företag eller kommuner och regioner

Eftersom regleringen endast rör statliga myndigheter bedömer myndigheten inte att den medför några konsekvenser för företag, kommuner eller regioner.

Kontaktpersoner

Ida Sahlin, Helena Andersson eller Carl Josefson