Konsekvensutredning – Förslag till föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn

## Innehåll

1. Innehåll 1

2. Förordning och mall för konsekvensutredning 2

3. Sammanfattning 2

4. Beskrivning av förslaget till föreskrifter och allmänna råd 3

5. Problem och lösning 4

5.1 Problem- och målformulering 4

5.2 Alternativa lösningar och effekterna utan reglering 4

6. Rättsliga förutsättningar 6

6.1 Bemyndiganden och regeringens medgivande 6

6.2 EU-rätt och annan internationell rätt 6

6.3 Vilka berörs? 7

6.5 Samråd med berörda leverantörer 7

6.6 Ekonomiska effekter 7

6.7 Övriga konsekvenser 8

7 Remiss 8

8 Avstämningar mot förordningar m.m. 9

9 Hänsyn till tiden för ikraftträdande 9

10 Uppföljning 9

11 Kontakt 10

## Förordning och mall för konsekvensutredning

Denna konsekvensutredning är utformad efter de krav som finns i 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning och är uppbyggd efter Regelrådets mall för handledning för konsekvensutredning.

## Sammanfattning

I juli 2016 antog Europaparlamentet och rådet direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (”NIS-direktivet”). Den svenska lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, ”NIS-lagen”, trädde i kraft den 1 augusti 2018. Syftet med lagen är att införliva NIS-direktivet i svensk rätt och uppnå dess syfte att nå en hög nivå på säkerheten i nätverk och informationssystem bland annat för samhällsviktiga tjänster inom energisektorn.

Myndigheten för samhällsskydd och beredskap, MSB, har en samordnande roll för NIS-lagen i Sverige. Det innebär bland annat att de ska ta fram övergripande föreskrifter för alla sektorer som omfattas av NIS-lagen. Bland annat får MSB meddela föreskrifter om systematisk och riskbaserat informationssäkerhetsarbete enligt 11 § NIS-lagen.

Statens energimyndighet, som har utsetts till tillsynsmyndighet för sektorn energi, har bemyndigats att meddela föreskrifter om säkerhetsåtgärder enligt 12 - 14 §§ NIS-lagen för leverantörer inom energisektorn enligt 8 och 17 §§ förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, ”NIS-förordningen”.

Huvudsakliga skyldigheter för leverantörer enligt 12–14 §§ NIS-lagen:

* 12 § - Utför en riskanalys som ska ligga till grund för val av säkerhetsåtgärder.
* 13 § - Vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker.
* 14 § - Vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem.

Som anges ovan är Energimyndigheten tillsynsmyndighet för leverantörer av samhällsviktiga tjänster inom energisektorn. På motsvarande sätt har Transportstyrelsen, Finansinspektionen, Livsmedelsverket och Post- och telestyrelsen samt Socialstyrelsen utsetts till tillsynsmyndigheter inom andra sektorer.

Av 21 § NIS-lagen framgår att tillsynsmyndigheten ska utöva tillsyn över såväl lagen som de föreskrifter, inkl. NIS-förordningen, som har meddelats i anslutning till lagen. För energisektorn omfattar Energimyndighetens tillsynsansvar även följande föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster som MSB har meddelat.

* MSBFS 2018:7 – Anmälan och identifiering av leverantörer av samhällsviktiga tjänster
* MSBFS 2018:8 – Informationssäkerhet för leverantörer av samhällsviktiga tjänster
* MSBFS 2018:9 – Rapportering av incidenter för leverantörer av samhällsviktiga tjänster
* MSBFS 2018:11 – Frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet.

Det bör även noteras att MSB genom sina föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster har identifierat leverantörer av samhällsviktiga tjänster inom sektorn energi, enligt 3 kap 1 – 3 §§ MSBFS 2018:7. Nu angivna MSB-föreskrifter används i definitionen av begreppet ”leverantör” enligt Energimyndighetens förslag till föreskrifter.

I detta dokument används ordet ”föreskrifter” som beskrivning av både föreskrifterna och dess tillhörande allmänna råd.

Denna utredning dokumenterar konsekvenserna av införandet av just dessa föreskrifter, och inte den underliggande lagstiftningen eller MSB:s föreskrifter.

## Beskrivning av förslaget till föreskrifter och allmänna råd

I de inledande bestämmelserna i föreskrifternas 1 kapitel regleras föreskrifternas tillämpningsområde, definitioner som används i föreskrifterna samt vilka nätverk och informationssystem som omfattas av föreskrifterna.

Det andra kapitlet innehåller regleringar avseende riskanalys. Där anges krav på att en leverantör av samhällsviktig tjänst ska upprätta en systemföreteckning samt vad denna ska innehålla. Vidare anges krav på leverantören att genomföra omvärldsbevakning och vad som ska beaktas när denna görs. Kapitlet innehåller även regleringar avseende vilka risker som ska beaktas, vad riskanalysen ska innehålla och hur risker ska bedömas. Detta kapitel avser 12 § i NIS-lagen.

Det tredje kapitlet avser informationssäkerhetskrav som leverantör av samhällsviktig tjänst ska uppfylla. Dessa krav ska mynna ut i säkerhetsåtgärder för att förebygga och minimera verkningar av incidenter enligt 14 § i NIS-lagen.

Det fjärde kapitlet avser hur en leverantörs säkerhetsåtgärder ska hantera risker och informationssäkerhetskrav. Kapitlet beskriver även hur säkerhetsåtgärder ska prioriteras och vilken typ av information som ska finnas för varje åtgärd. Detta utgör förtydliganden av 13 § i NIS-lagen.

Det femte kapitlet ger Energimyndighetens möjlighet att medge undantag från föreskriften vid särskilda skäl.

## Problem och lösning

## 5.1 Problem- och målformulering

NIS-lagen syftar till att uppnå en hög nivå på säkerheten i nätverk och informationssystem för samhällsviktiga tjänster inom bland annat energisektorn. NIS-lagens 12 – 14 §§ anger krav på leverantörer av samhällsviktiga tjänster avseende riskanalys, åtgärder för att hantera risker samt åtgärder rörande incidenter.

De föreslagna föreskrifterna innehåller förtydliganden av hur kraven i lagen ska genomföras. Målet med föreskrifterna är således att konkretisera de krav som ställs i lagen och att föreskriften kan användas i leverantörers interna diskussioner och beslut om informationssäkerhet. Detta bedöms även medföra en underlättad tillsyn av kraven på informationssäkerhet.

I syfte att ytterligare förtydliga föreskrifternas innehåll har Energimyndigheten tagit fram allmänna råd till föreskriften, och kommer även att ta fram en vägledning som lanseras i samband med att föreskrifterna träder i kraft.

## 5.2 Alternativa lösningar och effekterna utan reglering

I förarbetena till NIS-lagen[[1]](#footnote-2) uttalas att det krävs relativt omfattande och detaljerade föreskrifter om vad leverantörer av samhällsviktiga tjänster ska göra för att fullgöra lagens krav på säkerhetsåtgärder. Lagstiftaren har därför bedömt att det utöver möjligheten att meddela verkställighetsföreskrifter krävs föreskrifter om exempelvis tekniska och organisatoriska säkerhetsåtgärder för att mer i detalj innehålla skyldigheter för dem som träffas av lagen.

I förarbetena[[2]](#footnote-3) uttalas vidare att fördelarna med ett samlat regelverk för att genomföra direktivet, d.v.s. en gemensam lag och förordning som gäller samtliga sektorer som omfattas av direktivet, är att det blir tydligt för myndigheter, enskilda och tillsynsmyndigheten vilken reglering som finns när det gäller samhällsviktiga och digitala tjänster. Bestämmelser som behöver anpassas till respektive sektor kan därmed, enligt lagstiftaren, regleras i myndighetsföreskrifter.

**Nollalternativet**

NIS-lagen anger att tillsynsmyndigheten *får* meddela föreskrifter enligt 12 - 14 §§ av lagen. Om Energimyndigheten hade valt att inte ge ut sektorspecifika föreskrifter skulle lagens krav vara alltför otydliga, och det skulle inte uppställas specifika krav på informationssäkerhet inom energisektorn. Detta skulle i sin tur således resultera i att den allmänna säkerhetsnivån i sektorn inte skulle höjas lika mycket som med en specifik föreskrift, och det skulle göra det svårare att utföra tillsyn.

Det är tveksamt om NIS-direktivet skulle kunna anses implementerat i sin helhet utan att NIS-lagen och NIS-förordningen kompletteras med mer detaljerade föreskrifter för respektive sektor.

**Specifika ställningstaganden**

Föreskrifterna är utarbetade med beaktande av att energisektorn inte är en enhetlig sektor. Inom sektorn finns det leverantörer med väldigt olika typer av verksamhet, storlek och digital mognad. Föreskrifterna är således utformade i syfte att kunna tillämpas för leverantörer med vitt skilda förutsättningar. Nedan följer några av de mest väsentliga överväganden som gjorts avseende utformningen av föreskrifterna.

**Teknisk detaljnivå**

Föreskrifterna innehåller bland annat angivna informationssäkerhetskrav som respektive leverantör ska ta fram åtgärder till. Föreskrifterna innehåller dock inte någon förteckning med specifika tekniska åtgärder som ska vidtas och inte heller någon företeckning med risker. Att i föreskrifterna eller i de allmänna råden publicera en företeckning med specifika tekniska åtgärder som alla leverantörer ska efterleva har bedömts kunna leda till ett ineffektivt arbetssätt hos leverantörerna. Ett sådant arbetssätt bedöms inte leda till att energisektorn når den höga nivå på säkerhet i nätverk och informationssystem som NIS-lagen syftar till. Det skulle även ha inneburit en risk att leverantören inte gör någon självständig värdering av vilka åtgärder som behövs i den egna verksamheten, utan istället använt förteckningen som en uttömmande checklista. Med hänsyn till att leverantörerna inom energisektorn är väldigt olika har Energimyndigheten bedömt att det saknas förutsättningar att ta fram en förteckning med tekniska åtgärder som passar alla leverantörer.

Energimyndigheten har även värdesatt att leverantören ska känna ett ägande över sina åtgärder och sitt arbete inom informationssäkerhet, vilket uppnås genom att uppställa funktionella krav snarare föreskrivande av specifika tekniska åtgärder.

Att ange vilka specifika risker som samtliga leverantörer ska hantera har bedömts inte leda till en tillräcklig nivå av säkerhet i nätverk och informationssystem. Olika leverantörer har olika risker, varför det inte har bedömts ändamålsenligt att föreskriva om en och samma lista med risker för alla leverantörer inom sektorn.

Att uppställa informationssäkerhetskrav till vilka leverantören ska ta fram åtgärder innebär att leverantören har kontroll över sin åtgärdshantering. Respektive leverantör kan därmed anpassa åtgärderna till sin egen infrastruktur och sin egen organisations förutsättningar.

**Omfattning**

I föreskrifterna anges att respektive leverantör ska analysera vilka nätverk och informationssystem som omfattas av föreskrifterna.

Föreskrifterna innehåller inte några detaljerade krav på hur en leverantör ska utföra denna analys. En detaljreglering skulle inte uppnå den flexibilitet som behövdes i regleringen. Med anledning av energisektorns heterogenitet saknas förutsättningar att beskriva en detaljnivå som skulle vara tillämplig på alla leverantörer.

Respektive leverantör ska själv utföra denna analys. Leverantören ska dokumentera vilka nätverk och informationssystem som omfattas av föreskrifterna och hur man kom fram till denna slutsats.

I de allmänna råden anges vad leverantören kan och bör ta ställning till i denna analys.

**Definitioner**

Föreskriften utgår från de definitioner som finns i NIS-lagen, med några tillägg.

Definitionen av uttrycken "säkerhet i nätverk och informationssystem" och "risk" i lagen har bedömts behöva förtydligas. Ordet "risk" definieras som ett hot mot "säkerhet", och definitionen av ”säkerhet” i lagen kan tolkas som om detta endast beskriver en motståndskraft, eller en "förmåga att … motstå åtgärder". Energimyndigheten har bedömt att en riskanalys bör innefatta dels dessa säkerhetsaspekter som de är beskrivna i lagen dels de händelser som direkt påverkar ett nätverk eller informationssystems tillgänglighet, riktighet eller konfidentialitet.

Även begreppet "åtgärder" i definitionen av "säkerhet" kan enligt Energimyndigheten tolkas alltför snävt. Detta mot bakgrund av att NIS-direktivets syfte är att ha ett helhetsperspektiv på riskhantering. Begreppet "åtgärder" kan tolkas som att det endast anspelar på antagonistiska angrepp (det vill säga hackers). Föreskrifterna innehåller inte några alternativa definitioner av dessa begrepp i förhållande till NIS-lagen. I de allmänna råden framgår dock hur omfattningen av dessa begrepp kan tolkas inom energisektorn (2 kap. 4 §).

## Rättsliga förutsättningar

## 6.1 **Bemyndiganden och regeringens medgivande**

Det bemyndigande som Energimyndighetens föreskriftsrätt grundar sig på är 8 § NIS-förordningen:

"Statens energimyndighet får meddela föreskrifter om säkerhetsåtgärder enligt 12 - 14 §§ NIS-lagen för sitt tillsynsområde."

## 6.2 EU-rätt och annan internationell rätt

För att NIS-direktivet skulle implementeras i svensk rätt behövde det införlivas i den svenska rättsordningen. Därför beslutades en ny lag och förordning som trädde i kraft 1 augusti 2018. Nu aktuellt utkast till föreskrifter grundas således på den svenska implementeringen av NIS-direktivet.

## 6.3 Vilka berörs?

Föreskriften berör leverantörer av samhällsviktiga tjänster inom energisektorn som omfattas av NIS-lagen enligt MSBFS 2018:7 föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster.

Vi uppskattar att ungefär 250 leverantörer i Sverige faller under denna lag. Leverantörerna är aktiva i delsektorerna el, olja/drivmedel och gas. Leverantörerna är av varierande i storlek och ägandestruktur.

## 6.5 Samråd med berörda leverantörer

I framtagandet av detta förslag till föreskrifter har Energimyndigheten haft ett antal avstämningar med andra tillsynsmyndigheter, branschorganisationer och leverantörer.

I detta ingår bland annat:

* MSB
* Transportstyrelsen
* Livsmedelsverket
* PTS
* Finansinspektionen
* Energiföretagen
* SPBI
* Energigas Sverige
* Energidataföreningen
* Vattenkraft
* Norges vassdrags- og energidirektoriat (NO)
* Energistyrelsen (DK)
* Transport- och kommunikationsverket Traficom (FI)
* Nationella Energimyndigheten (IS)

## 6.6 Ekonomiska effekter

Dessa föreskrifter har ingen direkt ekonomisk påverkan på hushåll, konsumenter eller privatpersoner; utan de påverkar endast företag inom energisektorn.

Vissa av leverantörerna som omfattas av dessa föreskrifter arbetar redan på ett sådant sätt som föreskrivs i förslaget till föreskrifter, och för dem innebär föreskrifterna oftast inte några nämnvärda konsekvenser.

För vissa leverantörer kommer dock arbetet som beskrivs i föreskrifterna att mynna ut i en åtgärdsplan som kommer att innebära viss ökad administration och ökade ekonomiska kostnader. För leverantörer som inte redan utför riskanalys kan även själva riskanalysarbetet att ta tid och innebära ekonomiska kostnader. Åtgärderna kan även vara i form av nya tekniska lösningar som kräver licenser, hårdvara och driftpersonal.

Åtgärderna kan vidare påverka hur en leverantörs verksamhet bedrivs, till exempel om leverantören identifierar risker för informationssäkerheten som inte går att åtgärda. Leverantören kan till exempel välja att lägga ner en del av sin verksamhet om de IT-system som krävs har risker som är dyra eller svåra att åtgärda.

På grund av leverantörernas vitt varierande förutsättningar och storlek bedöms det inte vara möjligt att uppskatta vad den ekonomiska kostnaden kommer att bli för de leverantörer som inte redan utför informationssäkerhet enligt föreskrifterna.

Leverantörer som omfattas av föreskrifterna åläggs även att genomföra riskanalys och säkerhetsåtgärder. Detta kan komma att innebära ökade kostnader som leverantörer som inte omfattas av NIS-regleringen inte påförs.

EU har varit tydliga i sina vägledningar om NIS-direktivet att vissa leverantörer inte försöker få konkurrensfördelar genom att man sparar på kostnader för informationssäkerhetåtgärder. Ett av syftena med direktivet är att samtliga leverantörer som faller under lagen ska ha liknande förutsättningar. Leverantörer som inte faller under NIS utan som faller under andra lagstiftningar kan i vissa fall ha lägre kostnader för informationssäker, men i vissa fall kommer de att ha högre kostnader än en konkurrent som faller under NIS.

I NIS-lagen 8 §regleras att lagen inte gäller för de delar av en verksamhet som omfattas av krav på säkerhetsskydd enligt säkerhetsskyddslagen.

Föreskrifternas konsekvenser för små företag kan bli både positiva och negativa jämfört med konsekvenser för större företag. Ett mindre företag har ofta färre resurser som arbetar med informationssäkerhet, men samtidigt kan det vara betydligt enklare att genomföra en säkerhetsåtgärd i mer begränsad skala.

Utkastet till föreskrifter gäller för alla leverantörer som omfattas av MSB:s föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster inom energisektorn, och således även på mindre företag.

Föreskriften förväntas inte påverka varken kommuner eller landsting, så vida de inte själva levererar en samhällsviktig tjänst inom energisektorn eller äger bolag som omfattas av föreskrifterna. Regleringarna i föreskrifterna är desamma oavsett om leverantören är offentligt ägd eller inte, och konsekvenserna bedöms således vara desamma oavsett ägande.

Föreskriften förväntas inte påverka andra myndigheter utöver Energimyndigheten. Konsekvensen av föreskriften för Energimyndigheten är att den möjliggör utförandet av myndighetens tillsynsansvar. Uppdateringar av föreskriften torde framöver ske vid behov, till exempel utifrån erfarenheter från tillsyn och vid förändringar i närliggande författning.

## 6.7 Övriga konsekvenser

Föreskrifterna bedöms inte innebära några miljömässiga-, sociala- eller hälsomässiga konsekvenser.

## 7 Remiss

Förslaget till föreskrifter skickas på remiss till ett antal branschorganisationer och leverantörer inom energisektorn. Även MSB och de övriga tillsynsmyndigheterna enligt NIS-lagen får del av remissen, samt regelrådet. Förslaget kommer också att skickas till andra myndigheter som arbetar med informationssäkerhet. På så sätt omhändertas kravet i 8 § i NIS-förordningen att MSB ska ges tillfälle att yttra sig innan föreskrifterna meddelas. Remisstiden beräknas till ungefär 10 veckor efter utskick, från slutet av juni till mitten på september år 2020.

## 8 Avstämningar mot förordningar och ramverk

Förslaget till föreskrifter är avstämt mot

* EU:s NIS-direktiv (EU 2016/1148)
* lagen om informationssäkerhet för leverantörer av samhällsviktiga och digitala tjänster, och dess förordning (2018:1174, 2018:1175)
* MSB:s föreskrifter om anmälan, informationssäkerhet, incidentrapportering (MSBFS 2018:7 - 9, 11)

Även följande ramverk har beaktats:

* EU:s referensdokument om cybersäkerhet
* Internationella standarder, inklusive ISO och NIST
* MSB:s vägledningar och metodstöd inom informationssäkerhet.

Konsekvensutredningen är utformad utifrån de krav som anges i 6 och 7 §§ förordning (2007:1244) om konsekvensutredning vid regelgivning.

## 9 Hänsyn till tiden för ikraftträdande

De föreslagna föreskrifterna preciserar den reglering som införts i lag och förordning. Eftersom NIS-lagen trädde i kraft den 1 augusti 2018 bör nu aktuella föreskrifter träda ikraft så snart som möjligt för att underlätta efterlevnaden av lagen för de leverantörer som berörs.

Föreskrifterna ålägger leverantörerna att göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder. Föreskrifterna i sig ålägger dock inte leverantörerna att genomföra investeringar eller liknande som skulle kunna motivera ett senare ikraftträdandedatum.

Enligt Energimyndighetens tillsynsplan för NIS ska tillsyn av riskanalyser och säkerhetsåtgärder påbörjas under år 2021. Det vore att föredra att föreskrifterna är beslutade och i kraft innan detta arbete påbörjas.

## 10 Uppföljning

Dessa föreskrifter kommer att utvärderas och eventuellt ändras

* vid förändring av EU:s NIS-direktiv,
* förändring av svensk lagstiftning, eller
* behov baserat på utförd tillsyn.

I och med framtida uppdateringar kommer Energimyndigheten att ta ställning till om det finns behov av att föreskriva mer tekniska åtgärder som är specifika för energisektorn.

## 11 Kontakt

För eventuella frågor angående denna konsekvensutredning eller förslaget på föreskrifter kontakta:

* Stefan Jansson
* E-post: [stefan.jansson@energimyndigheten.se](mailto:stefan.jansson@energimyndigheten.se) och [nistillsyn@energimyndigheten.se](mailto:nistillsyn@energimyndigheten.se)
* Tel: 016-544 20 94

1. Prop 2017/18:205 Informationssäkerhet för samhällsviktiga och digitala tjänster s.42 [↑](#footnote-ref-2)
2. Prop 2017/18:205 Informationssäkerhet för samhällsviktiga och digitala tjänster s.17 [↑](#footnote-ref-3)