Energi-, Forsynings- og Klimaministeriet

# Høringsnotat vedr. bekendtgørelse om It-beredskab i el- og naturgassektorerne

**Kontor/afdeling**
Center for Forsyning

**Dato**
17. maj 2017

**J nr.** 2017-988

JCV/MMO/SMT

Udkast til bekendtgørelse om it-beredskab i el- og naturgassektorerne har været udsendt i ekstern høring i perioden den 13. januar til 14. februar 2017. Et udkast til samme bekendtgørelse har tidligere været i høring i forbindelse med høring af udkast til L68 lovforslag om ændring af lov om elforsyning og lov om naturgasforsyning (beredskab for forsyningskritiske it-systemer i el- og naturgassektoren) fra den 22. august til den 19. september 2016. Dette høringsnotat omhandler alene den seneste høringsperiode, dog inddrages tidligere høringssvar i de tilfælde, hvor høringsparterne henviser til tidligere afgivne svar.

Høringsnotatet redegør indledningsvis for de væsentligste punkter i høringssvarene knyttet til hovedemner, og efterfølgende behandles en række bemærkninger relateret til konkrete paragraffer. Ønskes der detaljerede oplysninger om høringssvarenes indhold, henvises der til de fremsendte høringssvar.

Energistyrelsens bemærkninger til høringssvarene er angivet med kursiv efter hvert emne.

Udover de i høringsnotatet behandlede punkter indeholder høringssvarene en række mere tekniske og redaktionelle kommentarer til bekendtgørelsen. Disse kommentarer er efterfølgende indarbejdet i bekendtgørelsen i fornødent omfang.

Energistyrelsen (ENS) har modtaget i alt 11 eksterne høringssvar:
Følgende høringsparter har oplyst, at de ingen bemærkninger har til udkastet til bekendtgørelsen: Danske Erhvervsskoler og -Gymnasier, Danske Universiteter, SRF Skattefaglig Forening.

Følgende eksterne høringsparter har fremsendt bemærkninger til udkastet til bekendtgørelsen: Dansk Energi (DE), Dansk Gasdristribution (DGD), Sekretariatet for Energitilsynet (SET), FSR - danske revisorer (FSR), Radius Elnet A/S, Vestjyske Net A/S, Verdo A/S og Dansk Industri (DI).

**Energi-, Forsynings- og Klimaministeriet**

Stormgade 2-6
1470 København K

T: +45 3392 2800
E: efkm@efkm.dk

www.efkm.dk

ENS har endvidere inkluderet høringssvar fra Energinet.dk (ENDK) i dette høringsnotat, idet bemærkninger fra ENDK vurderes at være af væsentlig karakter.

**1. Tidsfrister**
DE, Radius Elnet, Verdo, DGD og Vestjyske Net har udtrykt bekymring om de i bekendtgørelsen beskrevne tidsfrister for implementering af bekendtgørelsen. Der lægges til grund for denne bekymring, at der er tale om et komplekst område (DE), samt at kvaliteten af it-beredskabsarbejdet vil være sammenhængende med den tidsramme, der afsættes (Verdo). Endvidere lægges til grund, at der vil være øgede omkostninger ved at gennemføre arbejdet med kort tidsfrist (DE og Vestjyske Net), samt at en kort tidsfrist begrænser muligheden for at udnytte mulige synergieffekt, som der er med andet beslægtet arbejde og myndighedskrav (DE og Radius Elnet). Det påpeges imidlertid, at it-beredskabsarbejdet og det almene beredskabsarbejde med fordel kan have samme frister, da der er synergi mellem opgaverne (DE). ENDK har anbefalet, at synkronisere fristerne, så fremsendelsesfristen for it-beredskabsplaner, beredskabsplaner for almen beredskab samt risiko- og sårbarhedsvurderingerne er 1. september fremadrettet. ENDK har desuden pointeret, at afleveringen bør styres af det vigtigste, som skal godkendes af tilsynsmyndigheden, hvilket er beredskabsplanerne.

*ENS' bemærkninger:*
*Høringssvarene afspejler, at implementering af bekendtgørelsen for flere virksomheder vil aflede arbejdsopgaver, hvilket inkluderer risiko- og sårbarhedsvurderinger, udarbejdelse af beredskabsplaner samt iværksættelse af tiltag og beredskabsforanstaltninger. ENS anerkender, at dette arbejde vil kunne aflede omkostninger i arbejdstid og evt. ekstern bistand. Disse omkostninger er beregnet på baggrund af et tidligere udkast til bekendtgørelsen af Ernst & Young på vegne af Erhvervsstyrelsen. Opgørelsen af disse omkostninger er opgjort i tidligere offentliggjort rapport. De gennemførte beregninger anses for at tage højde for områdets kompleksitet, ligesom beregningerne anses for at tage højde for synergi med andet beredskabsarbejde i virksomhederne.*
*Det bemærkes, at beredskabsarbejde generelt ikke kan anses for stationært, men at beredskabet kræver løbende analyse og justering i takt med forandrede vilkår af såvel beslægtede myndighedskrav og andet beredskabsarbejde samt udviklingen i de enkelte virksomhederes forhold og konkrete trusler. Det er derfor hensigtsmæssigt hurtigst muligt at få startet it-beredskabsarbejdet, velvidende at det vil kræve efterfølgende tilpasning.*

*Det anerkendes imidlertid, at en kort frist mellem første og anden risiko- og sårbarhedsvurdering og beredskabsplan kan være unødigt fordyrende og ikke giver mulighed for, at virksomhederne kan indsamle erfaringer med egne it-beredskabsplaner, før de revideres. Det findes endvidere relevant at præcisere i bekendtgørelsen, at det er virksomhedernes beredskabsplaner, der skal fremsendes til ENDK til godkendelse.*

*På ovennævnte baggrund har ENS fundet det relevant at udskyde fristen for den første fremsendelse af virksomhedernes ROS-konklusioner til den 1. oktober 2017 og fremsendelsen af virksomhedernes it-beredskabsplaner til den 1. januar 2018. Herefter er det hensigten at synkronisere disse frister med tilsvarende frister i bekendtgørelser om beredskab for elsektoren og naturgassektoren, således at disse frister i alle tre bekendtgørelser fremadrettet vil være 1. september, første gang 1. september 2018. Der gælder forskellig frekvens for virksomhedernes udarbejdelse af risiko- og sårbarhedsvurderinger og it-beredskabsplaner afhængig af virksomhedens kategorisering. Ved behov for opdatering af virksomhedens risiko- og sårbarhedsvurdering imellem nævnte frister skal virksomhedens beredskabsplan opdateres senest 3 måneder efter gennemførelse af en risiko- og sårbarhedsvurdering.*

**2. Gennerelle bestemmelser og den risikobaserede tilgang til it-beredskab**
ENDK, DI og Vestjyske Net har udtrykt generel støtte til, at der tages initiativ til en styrkelse af it-beredskabet. Dette afspejles ligeledes i tidligere fremsendte høringssvar fra FSR. FSR har henvist til deres tidligere fremsendte høringssvar, hvoraf der udtrykkes bekymring vedr. den risikobaserede tilgang til it-beredskabet og dermed de øgede krav til it-beredskabet.

*ENS' bemærkninger:*
*Høringssvarene indikerer, at it-beredskabet er et væsentligt område, der fortsat bør have bevågenhed. Den risikobaserede tilgang kræver en lokal forankring af it-beredskabet, hvilket medfører risiko for, at det kan være vanskeligt at omsætte myndighedskrav til krav i den lokale kontekst, som pointeret af FSR. Den valgte risikobaserede tilgang til området fastholdes, vel vidende at dette kan medføre et fokus på risiko- og sårbarhedsvurderingerne frem for specifikke tiltag.*

**3. Fortrolighed**
DE har påpeget, at it-sikkerhed i modsætning til meget andet beredskabsarbejde beror på ondsindede, menneskeskabte aktiviteter og handlinger, hvorfor der er et behov for fortrolighed. DE ønsker derfor, at planmaterialet alene stilles til rådighed ved personligt møde.

*ENS' bemærkninger:*
*ENS deler DE's opfattelse af, at der er behov for beskyttelse af følsomme oplysninger i forbindelse med it-beredskabsarbejdet. Det er imidlertid en forudsætning for ENDK's koordinerende arbejde og tilsynsarbejdet, at der kan udveksles oplysninger mellem virksomheder, ENDK og myndighederne. Såfremt nogle informationer vurderes at være følsomme, anbefales det, at dette fremgår tydeligt af materialet, ligesom forholdsregler for opbevaring og håndtering aftales ved overlevering. ENDK kan evt. på foranledning af virksomhederne udarbejde en beskrivelse af, hvordan denne type oplysninger håndteres ved ENDK. Fortrolighed*

*er i den endelige version af bekendtgørelsen nu reguleret i en separat paragraf jf. § 29, således at dette fremgår mere tydeligt.*

FSR har generelt efterlyst retningslinjer for den indledende kortlægning og klassifikation af de anvendte it-systemer som forsyningskritiske eller ej, som ifølge FSR skal dokumenteres og bør være obligatorisk.

*ENS' bemærkninger:*
*Det vurderes ikke for hensigtsmæssigt at udstede bekendtgørelse om klassifikation af materiale, som der beskyttes af hensyn til virksomheders behov for beskyttelse. Såfremt informationer findes omfattet af justitsministeriets sikkerhedscirkulære under henvisning til den nationale sikkerhed, finder dette cirkulære anvendelse.*

**4. Indtægtsrammen for netvirksomheder**
SET har bemærket, at der bør være en præcisering af formuleringen vedr. dokumenterede meromkostninger i udkastets § 20 i forhold til reguleringen og forhøjelse af netvirksomhedernes indtægtsramme. Derudover har SET bemærket, at der bør fastsættes tidsfrist for ansøgning for forhøjelse af indtægtsrammen. Endvidere har SET bemærket behovet for en beregningsmetode for udregningen af indtægtsrammeforhøjelser ved afholdte omkostninger/udgifter til tilmeldelse af en it-sikkerhedstjeneste. Endeligt har SET bemærket, at der i bekendtgørelsen ikke tages tilstrækkelig højde for SET's administrative opgave og ressourcebehov. SET har påpeget, at der vil være tale om en væsentlig større administrativ opgave for SET med at vurdere ansøgningerne om forhøjelse af indtægtsrammen.

DE har bemærket, at det ikke kun burde være dokumenterede meromkostninger forbundet med tilmelding til it-sikkerhedstjenesten, som netvirksomhederne kan få forhøjet deres indtægtsrammer ved. DE har foreslået, at muligheden for forhøjelse af indtægtsrammen skal gælde alle omkostninger, der er forbundet med udførelsen af opgaver, som er fastsat i bekendtgørelsen.

*ENS' bemærkninger:*
*ENS anerkender SET's ønske om at få en klarere definition af, hvordan dokumenterede meromkostninger til en IT-sikkerhedstjeneste skal forstås. ENS har derfor tilføjet en ny, mere afgrænsende formulering om disse meromkostninger i bekendtgørelsen, der bestemmer, at det udelukkende er tilmeldingen til tjenesten, der kan skabe grundlag for forhøjelse af indtægtsrammen og ikke øvrige omkostninger forbundet hermed som f.eks. uddannelse af personale til at varetage denne opgave.*

*ENS anerkender behovet for at fastsætte en tidsfrist for ansøgning for forhøjelse af indtægtsrammen. Dette skrives ind i bekendtgørelsen, således at dette fremgår tydeligt.*

*ENS anser ikke bekendtgørelsen for at pålægge SET en større administrativ opgave, eftersom det udelukkende er tilmelding til it-sikkerhedstjenesten, der kan forhøje indtægtsrammen. Dette præciseres yderligere i bekendtgørelsen, og derfor mener ENS ikke, at der bliver behov for en større vurdering af, hvad dette omfatter. Derudover skal det bemærkes, at ENS godkender netvirksomhedernes tilmelding til IT-sikkerhedstjenesten forinden, at netvirksomhedernes ansøgning om forhøjelse af indtægtsrammen kommer SET i hænde. SET skal derfor blot godkende de omkostninger, som er dokumenterede i relation til den af ENS godkendte tilmelding til IT-sikkerhedstjenesten.*

*Til DE's bemærkning om muligheden for, at forhøjelse af indtægtsrammen skal gælde alle omkostninger, kan ENS oplyse, at de gennemførte undersøgelser af de økonomiske konsekvenser anser hovedparten af de meromkostninger, der pålægges netvirksomhederne som følge af lovforslaget, for at være direkte forbundet med kontrakter med en it-sikkerhedstjeneste. Denne meromkostning vurderes at være dokumenterbar og kvantificerbar. Netvirksomhedernes øvrige administrative meromkostninger anses for begrænsede (ca. 75.000 kr. årligt gennemsnitligt pr. netvirksomhed jf. AMVAB-målingen). På denne baggrund afgrænses muligheden for indtægtsrammeforøgelse til alene at omfatte omkostninger til en it-sikkerhedstjeneste.*

**5. Sammenhæng med anden lovgivning**

DI har påpeget, at denne bekendtgørelse bør tilpasses andre myndighedskrav, således at virksomhederne ikke pålægges forskellige rapporteringskrav. DE har samtidig påpeget, at ikrafttrædelse af denne bekendtgørelse kan udsættes til ikrafttrædelse af EU-regulering af persondata-området og netværks- og informationssikkerhedsområdet.

*ENS' bemærkninger:*

*Den 6. juli 2016 blev Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer (NIS-direktivet) vedtaget. Efter dette direktivs artikel 25 vedtager og offentliggør medlemsstaterne senest den 9. maj 2018 de love og administrative bestemmelser, der er nødvendige for at efterkomme dette direktiv. Denne bekendtgørelse er imidlertid udtryk for nationale regler, der har til formål at udmønte den nationale strategi for cyber- og informationssikkerhed fra december 2014 og de heri indeholdte krav om gennemførelse af it-beredskabsforanstaltninger på energiforsyningsområdet.*

*ENS anerkender behovet for at se denne bekendtgørelse i relation til andre nuværende og kommende regler. Der foregår en tværministeriel koordination af det lovforberedende arbejde med henblik på at implementere NIS-direktivet. Der arbejdes i regi af denne koordination på at begrænse antallet af forskellige formater*

*og meldepligter. Det vurderes imidlertid ikke forsvarligt at afvente implementeringen af NIS-direktivet før ikrafttrædelse af denne bekendtgørelse.*

**6. Behandling af konkrete paragraffer**
I det følgende gennemgås de konkrete paragraffer i bekendtgørelsesudkastet på baggrund af relaterede høringssvar.

**6.1 Udkastets § 2 om generelle bestemmelser**
DE og Radius Elnet har påpeget en uhensigtsmæssig formulering i de indledende bestemmelser, der kan opfattes således, at ENS forventer 100 % forsyningssikkerhed.

*ENS' bemærkninger:*
*Den påpegede uhensigtsmæssighed ved den indledende formulering anerkendes, hvorfor formuleringen er ændret i den endelige version af bekendtgørelsen jf. § 1 og § 2, stk. 2.*

**6.2 Udkastets § 3 om definitioner**
DE har påpeget, at definitionen af balanceansvarlige virksomheder er uklar. Uklarheden består i, hvorvidt ikke styrbar produktionskapacitet, der indgår i disse virksomhederes portefølje, vil danne grundlag for kategorisering af virksomhederne efter udkastets § 7.

*ENS' bemærkninger:*
*Den påpegede uklarhed anerkendes, hvorfor der er tilføjet en præcisering i den endelige version af bekendtgørelsen jf. § 3, nr. 1.*

DE har endvidere fundet behov for en præcisering af begrebet it-sikkerhedshændelse anvendt i udkastets § 5 og § 14.

*ENS' bemærkninger:*
*Der er tilføjet en definition af it-sikkerhedshændelse til listen af definitioner.*

FSR har foreslået en udvidet definition af begrebet "cybersikkerhed", således at begrebet også rummer interne trusler mod it-systemerne.

*ENS' bemærkninger:*
*Dette forslag afvises under henvisning til, at begrebet cybersikkerhed i kontekst af forsyningskritiske it-systemer i el- og naturgassektoren primært relaterer til at begrænse adgangen til industrielle styringssystemer (SCADA) og lignende. Samtidig skal bekendtgørelsen kun indeholde definitioner, som anvendes i bekendtgørelsen.*

FSR har endvidere foreslået at uddybe begrebet "ikke kritiske it-systemer", således at det tydeliggøres, at disse systemer er fysisk adskilt fra kritiske it-systemer.

*ENS' bemærkninger:*
*Dette forslag afvises også med den begrundelse, at bekendtgørelsen kun skal indeholde definitioner, som anvendes i bekendtgørelsen.*

**6.3 Udkastets § 4 om operative forhold**
DE og Radius Elnet har fundet det uklart, hvorvidt udkastets § 4 stk. 1. skal tolkes således, at enhver virksomhed skal have en formaliseret vagtordning for it-området på alle tider af døgnet. DE har tolket et sådan krav som et pålæg. Radius Elnet har påpeget, at det er uklart, hvorvidt en it-sikkerhedstjeneste efter udkastets § 27 kan anses for en sådan vagtordning.

*ENS' bemærkninger:*
*Den påpegede uklarhed anerkendes, hvorfor § 4 er blevet omskrevet. Denne omskrivning skal tydeliggøre, at de enkelte virksomheder har ansvaret for at vurdere, hvilken form for assistance der er påkrævet. Denne vurdering bør bero på virksomhedens samlede it-beredskabsarbejde, herunder egne risiko- og sårbarhedsvurderinger samt relevante tekniske og organisatoriske forhold, således at virksomheden kan tilpasse denne assistance til lokale forhold på en omkostningseffektiv måde. Det er muligt at anvende egne medarbejdere eller eksterne til at varetage denne opgave (enten sammenhængende med eller uafhængigt af it-sikkerhedstjenesten beskrevet i § 25).*
*Denne bestemmelse er ikke et konkret pålæg, men et myndighedskrav, der skal tilsikre en hensigtsmæssig efterlevelse af § 85 c i elforsyningsloven og § 15b i naturgasforsyningsloven.*

**6.4 Udkastets § 5 om operative forhold**
DE har påpeget, at udkastets § 5 stk. 7 er overflødig, da dette gentages i udkastets § 17 stk. 1.

*ENS' bemærkninger:*
*Den påpegede gentagelse anerkendes, hvorfor udkastets § 5 stk. 7 udgår.*

**6.5 Udkastets § 6 om organisatoriske forhold**
FRS har påpeget, at udkastets § 6 stk. 3 med fordel kan uddybes, således at den pligtige koordinering 4 gange årligt tilføjes krav om koordinering efter behov baseret på en løbende vurdering. Det kunne eksempelvis være i forbindelse med implementering af nye forsyningskritiske it-systemer eller teknologier. I sådanne tilfælde bør koordinering også finde sted.

*ENS' bemærkninger:*
*Den påpegede gentagelse anerkendes, og det anses for implicit i beredskabsarbejdet, at koordinering i lighed med andre processer finder sted i nævnte tilfælde. Da baggrunden for en koordinering som udgangspunkt må bero på en vurdering, findes det imidlertid mest hensigtsmæssigt alene at tilpasse bestemmelsen, således at det står tydeligt, at kravet til fire gange årligt at koordinere skal forstås som et minimumskrav.*

**6.6 Udkastets § 7 om kategorisering af virksomheder**
DE og Vestjyske Net har påpeget uklarhed om kategoriseringen af virksomheder, der formidler energi mellem transmissionsnettet og underliggende net.

*ENS' bemærkninger:*
*Kategoriseringen af virksomheder har til hensigt at fremme en mere rimelig og risikobasseret fordeling af krav til virksomhederne afhængig af virksomhedernes betydning for det samlede el- eller naturgassystem. Ved afvejning af betydningen af det samlede el- eller naturgassystem er det hensigten at opdele virksomhederne efter antallet af forbrugere, der berøres ved en it-beredskabshændelse. Det er derfor hensigten at kategorisere virksomhederne efter antallet af mulige berørte forbrugere. For at afklare den mulige forvirring ved anvendelsen af begrebet "aftagere" ændres begrebet i den endelige version af bekendtgørelsen til "slutforbrugere" jf. § 9.*

DE og Verdo har endvidere påpeget, at udkastets § 7 stk. 4 skaber uklarhed, da den referer til bestemmelser gældende for det almene beredskab, hvorefter virksomhedernes anlæg klassificeres efter andre regler.

*ENS' bemærkninger:*
*Det tilstræbes i videst muligt omfang at ensarte reglerne for anlæg og it-systemer. Det er dog ikke til alle tider hensigtsmæssigt, ligesom det er fundet for omfattende at klassificere alle it-anlæg efter gældende regler for kategorisering af anlæg.*

DE har foreslået at grænserne for kategorierne rykkes, da der er flere netvirksomheder, der har omkring 30.000 kunder, hvorfor disse virksomheder kan blive placeret i både kategori 3 og kategori 2 på baggrund af en relativt lille ændring i kundeantal. Ligeledes har DE påpeget, at det kan være uhensigtsmæssigt, at ENDK varetager en skønsmæssig kategorisering.

*ENS' bemærkninger:*
*Det afvises at flytte grænsen for kategori 3-virksomhederne. Dette begrundes med, at 30.000 forbrugere findes at være en hensigtsmæssig grænse, da virksomheder med flere end 30.000 forbrugere vurderes at kunne have konsekvenser for den regionale elforsyning i tyndt befolkede områder af Danmark. Det lægges til grund,*

*at strømforsyningen i disse områder ofte har færre muligheder for redundant forsyning fra andre forsyningsområder i forhold til tæt befolkede områder. Det erkendes, at der i grænsetilfælde kan være behov for en skønsmæssig vurdering, og at ENDK varetager denne vurdering. Disse vurderinger anses dog for begrænsede på baggrund af reglerne i den endelige version af bekendtgørelsen jf. § 9 stk. 3, der tilsiger et forsigtighedsprincip. Udkastets § 7 stk. 4 kan medvirke til øget brug af denne skønsmæssige vurdering som påpeget af DE. Hvorfor der er tilføjet en præcisering i den endelige version af bekendtgørelsen jf. § 9 stk. 2, således at skøn efter denne bestemmelse i videst muligt omfang begrænses.*

DE har endvidere opfordret til mulighed for dispensation fra reglerne for it-beredskab, herunder for standby-produktion grundet administrativ belastning.

*ENS' bemærkninger:*
*Der findes som udgangspunkt ikke grund til at kunne dispensere fra reglerne for produktionsanlæg, der er standby. Dette begrundes med at disse anlæg i perioder har konsekvenser for den samlede elforsyning. Der henvises i øvrigt til den generelle dispensationsbestemmelse, hvorefter ENS kan dispensere fra bestemmelser i denne bekendtgørelse, hvor sådanne bestemmelser i væsentligt omfang har mindre betydning eller reduceret effekt for it-beredskabet.*

**6.7 Udkastets § 8 om risiko- og sårbarhedsvurdering**
DE har påpeget, at der er meget kort frist til at udarbejde risiko- og sårbarhedsvurderinger.

*ENS' bemærkninger:*
*Der henvises til det indledende punkt 1. vedr. tidsfrister.*

FSR har påpeget, at begreberne "revision" og "revideret" kan misforstås.

*ENS' bemærkninger:*
*ENS anerkender den mulige begrebsforvirring, hvorfor begrebet "opdateret" anvendes i stedet for "revision".*

FSR har påpeget, at det bør præciseres, at den øverste ledelse har ansvaret for risiko- og sårbarhedsvurderingerne og derfor bør godkende disse.

*ENS' bemærkninger:*
*ENS anerkender dette behov og har efterfølgende tilføjet til den endelige version af bekendtgørelsens § 6, stk. 2, at virksomheden skal sikre, at virksomhedens ledelse har et samlet risikobillede, der repræsenterer kendte og mulige risici mod produktionen eller forsyningen af elektricitet eller naturgas.*

DE har efterlyst afklaring af stk. 5 vedr. inddragelse af trusselsvurderinger fra Center for Cybersikkerhed, mens FSR har efterlyst afklaring af begrebet "relevante trusler".

*ENS' bemærkninger:*
*Det er hensigten med denne bestemmelse, at virksomhederne pålægges ansvar for løbende at orientere sig om relevante trusler og sårbarheder. Det er derfor ikke hensigten at afgrænse begrebet relevante trusler, da denne afgrænsning er en del af virksomhedens beredskabsarbejde. Trusselsvurderinger fra Center for Cybersikkerhed er en kilde blandt mange til disse informationer. ENS forventer, at virksomhederne selv er i stand til at orientere sig i de til rådighed værende informationskilder og på denne baggrund udarbejde en relevant risiko- og sårbarhedsvurdering.*

DE har bemærket, at det er uklart, hvorvidt de efter udkastets § 8, stk. 6 udarbejdede risiko- og sårbarhedsvurderinger skal formidles til virksomhederne.

*ENS' bemærkninger*
*Det er ikke hensigten, at disse vurderinger direkte skal formidles til virksomhederne. Dog skal disse vurderinger danne grundlag for sektorberedskabsplanerne, og ENDK skal inddrage relevante parter i udarbejdelsen af disse. Vurderingen kan endvidere bidrage til, at ENDK udarbejder specifikke scenarier eller trusler, som virksomhederne bør behandle i deres risiko- og sårbarhedsvurderinger.*

**6.8 Udkastets § 9 om informationsstrømme**
DE og Radius Elnet har påpeget, at bestemmelserne i udkastets § 9, stk. 3 og i stk. 5, der stiller krav om, at hhv. virksomhederne og ENDK udarbejder et overblik over informationsstrømme, vil afspejle det samme billede. DE har af ressourcehensyn anbefalet, at ENDK oplyser hver enkelt virksomhed om, hvilke informationsstrømme ENDK ser som relevante, før virksomhederne selv udreder deres informationsstrømme.

*ENS' bemærkninger:*
*Det er hensigten med virksomhedernes udredning af informationsstrømme, at det overblik, der udarbejdes skal give virksomhederne indblik i egne sårbarheder og give mulighed for at kommunikere evt. delte risici og sårbarheder med andre virksomheder og ENDK. Af samme årsag skal ENDK udarbejde et planmateriale. En sammenligning af planmateriale vil afdække eventuelle uoverensstemmelser mellem opfattelsen af betydningen af og ejerskabet af informationsstrømme. Disse uoverensstemmelser forventes at aflede drøftelser, der fremmer den gensidige tillid og medvirker til at fremme sikkerheden i delte risici og sårbarheder. Det afvises på den baggrund, at lade virksomhederne afvente ENDK's optegning af informationsstrømme, før de iværksætter udarbejdelsen af eget overblik over*

*informationsstrømme. Det må forventes, at såvel ENDK's som virksomhedernes overblik vil blive forbedret over tid. Såvel virksomhederne og ENDK opfordres til at lægge vægt på den mulige læring i den løbende dialog om informationsstrømme.*

**6.9 Udkastets § 10 om beredskabsplanlægning**
DE har pointeret, at bestemmelserne i stk. 2 er i modstrid med stk. 3, da stk. 2 anbefaler, at fortrolige dele undlades i videst muligt omfang i beredskabsplanerne, mens stk. 3 stiller krav om en række oplysninger.

*ENS' bemærkninger:*
*Det er hensigten med fortrolighed at begrænse detaljerne i beredskabsplanerne, således at indholdet af følsomme oplysninger begrænses, hvorved anvendeligheden og tilgængeligheden af beredskabsplanerne øges. Det er alene de udstedende virksomheder, der kan vurdere, hvilke oplysninger der er nødvendige for en effektiv beredskabsindsats, og hvilke oplysninger der bør behandles med fortrolighed. Det er derved en anbefaling til virksomhederne, hvorfor det alene skal tilstræbes at undlade fortrolige oplysninger i beredskabsplanerne.*

DE har fundet det uklart, hvorvidt ENDK's vejledning efter stk. 4, 3. pkt. skal anses for sammenhængende med ENDK's rolle som koordinerende part eller som tilsynsmyndighed.

*ENS' bemærkninger:*
*ENDK's vejledning efter stk. 4, 3. pkt. har til formål at skabe sammenhæng mellem virksomhedernes beredskabsplaner og sektorberedskabsplanerne. Det er derfor alene ENDK som koordinerende part, der skal varetage denne opgave. Det er imidlertid klart, at ENDK som tilsynsmyndighed vil kunne forlange, at beredskabsplanerne er i overensstemmelse med sektorberedskabsplanen.*

DE har anbefalet, at ENS overvejer nødvendigheden af at fremsende potentielt følsomme oplysninger afledt af udkastets § 10 stk. 6 til tilsynsmyndigheden

*ENS' bemærkninger:*
*Der henvises til punkt 3 vedr. fortrolighed.*

**6.10 Udkastets § 14 øvelsesrapportering**
DE har påpeget, at kravet om, at virksomhederne omgående skal melde hændelser, der kan have indflydelse på andre virksomheders eller myndigheders it-beredskab efter stk. 3, kan tolkes således, at alle hændelse skal meldes.

*ENS' bemærkninger:*

*Det anerkendes, at det i nogle tilfælde kan være vanskeligt for virksomhederne at vurdere, hvorvidt en hændelse kan have indflydelse på andre virksomheders eller myndighedes it-beredskab. Denne bestemmelse skal fungere således, at ENDK som koordinerende part får mulighed for at viderebringe væsentlige oplysninger proaktivt på baggrund af meldinger for virksomhederne. Det er hensigten, at den øgede forståelse for andre virksomheders it-beredskab og det samarbejde i branchen om it-beredskab, som ENDK skal sikre, samt den gradvist øgede modenhed af virksomhedernes it-beredskab skal medvirke til at øge denne bestemmelses funktionalitet. Det bør løbende vurderes, om denne bestemmelse fungerer efter hensigten.*

**6.11 Udkastets § 15 om hændelser**
DE har påpeget, at det er uklart, hvem der skal vurdere, om virksomhederne skal udarbejde hændelsesevaluering ved hændelser, der vurderes at kunne give anledning til læring ved andre virksomheder, efter udkastets § 15 stk. 1.

*ENS' bemærkninger:*
*Det anerkendes, at det i nogle tilfælde kan være vanskeligt for virksomhederne at vurdere, hvorvidt en hændelse kan have indflydelse på andre virksomheders eller myndigheders it-beredskab. Denne bestemmelse skal fungere således, at virksomhederne kan lære af andres erfaringer på baggrund af hændelsesevalueringer. Det påhviler den enkelte virksomhed at foretage denne vurdering. ENDK kan ligeledes pålægge virksomheder at foretage hændelsesevaluering. Virksomhederne opfordres til at inddrage ENDK i overvejelser om, hvorvidt en hændelsesevaluering kan medvirke til læring ved andre virksomheder.*

**6.12 Udkastets § 16 om sikring**
DE har fundet kravene til fysisk sikring uklare.

*ENS' bemærkninger:*
*Det påregnes snarest at revidere de almene regler for beredskabet jf. bekendtgørelser om beredskab for elsektoren og naturgassektoren, hvori kravene til fysisk sikring præciseres.*

**6.13 Udkastets § 17 om leverandørstyring**
DE har påpeget, at bestemmelsen ikke lader til at tage højde for den mulige sårbarhed forbundet med vindmøllefabrikanters serviceadgang til vindmøller og mindre vindmølleparker.

*ENS' bemærkninger:*
*Den nævnte sårbarhed anses for omfattet i det omfang, at balanceansvarlige virksomheder har disse vindmøller i deres portefølje. I sådanne tilfælde finder § 24 i den endelige version af bekendtgørelsen anvendelse, således at virksomheden*

*skal betragte vindmølleproducenter som omfattet af begrebet ekstern leverandør. Heraf afledes, at den produktionsbalanceansvarlige virksomhed, der indplaceres i kategori efter § 9 i den endelige version af bekendtgørelsen anvendelse, bærer ansvaret for risikovurdering og beredskabsplanlægning for den samlede produktionskapacitet i egen portefølje, herunder elektricitet produceret ved mindre vindmøller under serviceaftale med producenten.*

**6.14 Udkastets §§ 18 og 19 om tilsyn**

DE har opfordret til, at adskillelsen mellem ENDK's opgaver som koordinerende part og som tilsynsmyndighed præciseres. Ligeledes ønskes en præcisering af formålet og indholdet af ENS' tilsyn med ENDK efter udkastets § 19 stk. 5.

*ENS' bemærkninger:*

*Det påregnes, som det fremgår af betænkning til lovforslag L 68, at der inden udgangen af 2018 foretages en evaluering af den nuværende ordning, der pålægger ENDK at varetage både opgaven som tilsynsmyndighed og som koordinerende part i el- og naturgassektoren. Det er ikke hensigten, at ENS årligt skal foretage denne evaluering i forbindelse med tilsynet med ENDK. ENS' årlige rapport efter § 27 stk. 2 i den endelige version af bekendtgørelsen har til formål at redegøre for det af ENS gennemførte tilsyn, samt evt. bemærkninger, som ENS måtte have til ENDK's tilsynsførelse over for virksomhederne eller ENDK's beredskabsarbejde som virksomhed og som koordinerende part.*

DE har anbefalet, at udkastets § 19 stk. 4 udgår, således at ENS' tilsyn med ENDK ikke delvist kan baseres på interne audits foretaget af ENDK.

*ENS' bemærkninger:*

*Af hensyn til det omfattende tilsynsmateriale samt kompleksiteten af ENDK's beredskabsopgaver findes det hensigtsmæssigt at bibeholde muligheden for at lægge interne audits til grund for tilsynet med ENDK. På denne baggrund afvises Danske Energis anbefaling.*

**6.15 Udkastets § 20 om andre bestemmelser**

Der er modtaget en række bemærkninger vedrørende indtægtsrammen fra DE, Radius Elnet, FSR, Dansk Industri og Vestjyske Net.

*ENS' bemærkninger:*

*Der henvises til det indledende afsnit om indtægtsrammen.*

**6.16 Udkastets § 22 om indstationering af en ENDK-medarbejder ved Center for Cybersikkerhed**

ENDK har påpeget, at det er uklart under hvilke rammer ENDK skal indstationere en medarbejder, samt at dette generelt findes uhensigtsmæssigt.

*ENS' bemærkninger:*
*Den påpegede uklarhed er korrigeret ved en præcisering af den endelige version af bekendtgørelsens § 30. Det er ikke muligt at frafalde kravet om, at ENDK skal stille en medarbejder til rådighed for udarbejdelse af sektorspecifikke trusselsvurderinger i regi af Center for Cybersikkerhed. ENDK har vurderet, at være den institution med de bedste forudsætninger for at stille en sådan medarbejder til rådighed og derved tilsikre en løbende og relevant kontakt til sektoren. Det bemærkes, at de økonomiske omkostninger ved ENDK forbundet med denne opgave er indeholdt i opgørelsen af de økonomiske konsekvenser indeholdt i det vedtagne lovforslag L68, hvilket fremgår af bemærkningerne til lovforslaget.*

**6.17 Udkastets § 24 om sanktioner**
DE og Radius Elnet har udtrykt bekymring ved, at ENDK på baggrund af udkastets § 24 stk. 1 kan påbyde virksomhederne at foretage en it-revision. Der findes begrænset hjemmel til at delegere denne bemyndigelse fra ministeren til ENDK.

*ENS' bemærkninger:*
*Den påpegede uklarhed om ENDK's beføjelser præciseres, således at det fremgår, at ENDK kan indstille, at ENS påbyder virksomheden af foretage en it-revision.*

**6.18 Udkastets § 27 om it-sikkerhedstjeneste**
Radius Elnet har anbefalet, at det tydeliggøres i udkastets § 27, at virksomhederne selv kan varetage denne it-sikkerhedstjeneste internt, såfremt efterlevelse af kravene til denne tjeneste kan dokumenteres.

*ENS' bemærkninger:*
*Bekendtgørelsens definition af en it-sikkerhedstjeneste udelukker ikke, at it-sikkerhedstjenesten kan leveres af virksomheder, der er koncernforbundet med virksomheder i bekendtgørelsens § 2.*

DE har udbedt snarlig afklaring af konkrete krav til denne it-sikkerhedstjeneste og har samtidig påpeget, at den afsatte tid til udarbejdelse af kontrakter med it-sikkerhedstjenester er relativt kort. Vestjyske Net har påpeget, at der kan forventes variation af it-sikkerhedstjenesten ved ikrafttræden af bekendtgørelsen.

*ENS' bemærkninger:*
*Der pågår et arbejde med at udarbejde retningslinjer for godkendelse af kontrakter til it-sikkerhedstjenester. Det forventes at vejledning for indgåelse af kontrakter med it-sikkerhedstjenester vil blive udsendt samtidig med offentliggørelsen af bekendtgørelsen. ENS anerkender imidlertid DE's pointe, og fristen for indgåelse og fremsendelse af en kontrakt med en it-sikkerhedstjeneste til ENS vil derfor være den 1. oktober 2017.*

**Øvrige bemærkninger**

ENDK har pointeret, at der i bekendtgørelsesudkastet mangler en bestemmelse, som giver ENDK og ENS mulighed for at indhente oplysninger af relevans for beredskabsarbejdet i virksomhederne, som det er tilfældet med § 31 i bekendtgørelserne om beredskab for elsektoren og naturgassektoren.

*ENS' bemærkninger:*
*ENS har imødekommet denne pointe og tilføjet en lignende bestemmelse i it-beredskabsbekendtgørelsen. Der henvises til § 31 i den endelige bekendtgørelse.*