Energiavirasto

Lausunto

28.11.2023 3838/000100/2023

Asia: VN/18157/2023

Lausuntopyyntö: luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Liikenne- ja viestintäministeriö on 3.10.2023 pyytänyt lausuntoa luonnoksesta hallituksen esitykseksi eduskunnalle kyberturvallisuusdirektiivin (jäljempänä NIS2-direktiivi ja direktiivi) täytäntöönpanemiseksi. Energiavirasto lausuu luonnoksesta seuraavaa:

Energiavirasto kannattaa NIS2-direktiivin tavoitetta vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta kriittisiksi katsottujen sektoreiden ja toimijoiden osalta. Asetettuun tavoitteeseen pyritään velvoittamalla jäsenvaltiot asettamaan direktiivin soveltamisalaan kuuluville toimijoille velvoittavia riskienhallintatoimia kyberturvallisuushäiriöiden varalta. Näin ollen hallituksen esityksen luonnoksessa ehdotetaan NIS2-direktiivi pantavaksi täytäntöön säätämällä sen edellyttämistä velvoitteista keskitetysti uudessa kyberturvallisuuden riskienhallinnasta annettavassa laissa. Lisäksi esityksessä ehdotetaan muutettavaksi julkisen hallinnon tiedonhallinnasta annettua lakia (906/2019) ja sektorikohtaista lainsäädäntöä. Hallituksen esityksen luonnoksessa ehdotetaan kumottavaksi edeltävän verkko- ja tietoturvallisuusdirektiivin eli NIS1-direktiivin (EU) 2016/1148 täytäntöönpanosäännökset useista sektorikohtaisista laeista. Esitysluonnoksessa ehdotetaan NIS2-direktiivin täytäntöönpano tehtäväksi sen vähimmäistason mukaisesti ja kansallinen liikkumavara täysimääräisesti hyödyntäen.

NIS2-direktiivillä pyritään poistamaan sen edeltäjän NIS1-direktiivin implementoinnin jälkeen havaittuja jäsenvaltioiden välisiä suuria eroja erityisesti vahvistamalla vähimmäissäännöt koordinoidun sääntelykehyksen toiminnalle, vahvistamalla järjestelyt kunkin jäsenvaltion vastuuviranomaisten toimivaa yhteistyötä varten, ajantasaistamalla luettelo aloista ja toiminnoista, joihin sovelletaan kyberturvallisuusvelvoitteita, ja säätämällä tehokkaista oikeussuojakeinoista ja täytäntöönpanotoimenpiteistä, jotka ovat olennaisen tärkeitä velvoitteiden tehokkaan täytäntöönpanon kannalta. NIS2-direktiivin soveltamisala on NIS1-direktiiviä laajempi ja se koskee suurempaa osaa taloudesta. NIS2-direktiivin johdanto-osan 6 kohdan mukaan näin sen piiriin

saadaan kaikki toimialat ja palvelut, jotka ovat elintärkeitä sisämarkkinoiden yhteiskunnallisten ja taloudellisten avaintoimintojen kannalta.

NIS1-direktiivi implementointiin Suomessa sisällyttämällä siitä tulevat velvoitteet sektorikohtaiseen lainsäädäntöön. Energiavirasto katsoo, että velvoitteiden säätäminen keskitetysti yhdessä kansallisessa yleislaissa on perusteltua NIS2-direktiivin soveltamisalan läpi leikatessa horisontaalisesti eri toimialasektoreita. Tämä edesauttaa direktiivin tavoitteiden toteutumisessa sekä varmistaa direktiivin yhdenmukaisen täytäntöönpanon toimialojen kesken.

Soveltamisalaa koskevat huomiot

Kokoperusteinen soveltamisala

NIS2-direktiivin liitteiden mukainen soveltamisala on NIS1-direktiiviä kattavampi ja direktiivillä määritetään suoraan, minkä kokoiset toimijat kuuluvat direktiivin soveltamisalaan. Hallituksen esityksen luonnoksen mukaan kyberturvallisuuden riskienhallinta- ja raportointivelvoitteiden soveltamisala kattaisi toimijat, jotka harjoittavat lain liitteessä tarkoitettua toimintaa tai ovat liitteessä tarkoitettua toimijatyyppiä ja täyttävät tai ylittävät soveltamisalan kokokriteerin tai niitä koskee poikkeus velvoitteiden soveltamisesta koosta riippumatta. Lisäksi velvoitteita sovellettaisiin CER-direktiivin (EU 2022/2557) nojalla kriittisiksi tunnistettuihin toimijoihin koosta riippumatta. Muutoksena NIS1-direktiiviin soveltamisalaan kuuluvia toimijoita ei määriteltäisi toimialoilla implementoinnin yhteydessä, vaan kaikki liitteessä tarkoitettua toimintaa harjoittavat tai toimijatyyppiä olevat, kokokriteerin täyttävät tai kokopoikkeuksen piiriin kuuluvat toimijat kuuluisivat soveltamisalaan suoraan.

Hallituksen esityksen luonnos noudattelee NIS2-direktiivissä edellytettyjä vaatimuksia sen soveltamisalasta. Energiavirasto kannattaa hallituksen esityksen luonnoksessa esitettyä muutosta aiempaan, jonka mukaan toimijoiden velvollisuutena olisi itse tunnistaa, kuuluvatko he sääntelyn soveltamisalaan, sekä ilmoittautua valvovalle viranomaiselle toimijaluetteloon.

NIS2-direktiivin sekä ehdotetun kansallisen lain mukaan velvoitteiden soveltamisalan kokokriteerinä olisi keskisuuren yrityksen määritelmä. Määritelmä perustuu komission suositukseen 2003/361/EY. Energiavirasto korostaa, että hallituksen esityksen luonnoksessa on todettu edellä mainitun suosituksen mukaiset keskisuuren yrityksen kynnysarvot, mutta ei ole tuotu esiin, miten kynnysarvojen määrittämiseen tarvittavat tunnusluvut lasketaan. Useat soveltamisalaan kuuluvat toimijat, esimerkiksi energiatoimialalla, ovat konsernimuotoisia yrityksiä. Energiavirasto toteaa, että selkeyden lisäämiseksi ja väärinymmärrysten välttämiseksi hallituksen esityksen perusteluissa tulisi tuoda esiin suosituksen liitteen 3 artiklan mukaiset henkilöstömäärän ja rahamääräisten arvojen laskennassa huomioon otettavat yritystyypit. Tätä perustelee osaltaan myös se, että toimijoiden on itse tunnistettava itsensä lain soveltamisalaan.

Hallituksen esityksen luonnoksen 2 §:n 10 kohdassa ehdotetaan keskisuuren toimijan määritelmää. Kyseisen kohdan yksityiskohtaisissa perusteluissa todetaan määrittelyssä käytettyjen kynnysarvojen lisäksi merkittävä soveltamisalaan liittyvä päätös. Säännöksen yksityiskohtaisten perustelujen mukaan: ”Mikäli toimija toimii usealla eri toimialalla ja vain osa sen toiminnasta on liitteessä I tai II tarkoitettua toimintaa, kokorajoitusta arvioidaan toimijan kokonaistoiminnan perusteella. Näin ollen liikevaihtoa, tasetta ja henkilöstömäärää arvioidaan koko toimijan osalta eikä arviointia tule rajata vain liitteessä I tai II tarkoitetun toiminnan laajuuteen. Arviointi tehdään toimijakohtaisesti.”

Luonnoksen liitteen I mukaan ehdotetun lain soveltamisalaan kuuluvat esimerkiksi ”sähkömarkkinalain (588/2013) 3 §:n 1 momentin 15 kohdassa tarkoitetut tuottajat”. Tuottajalla tarkoitetaan sähkömarkkinalaissa sähköä tuottavaa luonnollista henkilöä tai oikeushenkilöä. Sähkömarkkinalain eikä sen taustalla olevaan sähkömarkkinadirektiivin (EU 944/2019) määritelmään kuuluminen ole riippuvaista sähköä tuottavan laitoksen koosta. Hallituksen esityksen luonnoksessa ehdotettu toimijan kokoluokan arviointi ja näin ollen lain soveltamisala tarkoittaisi siten, että pienimuotoinen sähkön tuotanto (sähkömarkkinalain 3 §:n 1 momentti 14 kohta), kuten aurinkopaneelien hyödyntäminen omassa energiantuotannossa, voisi merkitä pääasiallisesti muuta toimintaa harjoittavan yrityksen kuulumista Energiaviraston valvontatoimivaltaan jopa keskeisenä toimijana. Energiavirasto katsoo, että tämä ei ole tarkoituksenmukaista ja voi johtaa suhteettomaan lopputulokseen joidenkin toimijoiden osalta.

Energiavirasto toteaa, että sähköntuottajien osalta ehdotettu kokoluokan tarkastelu on kriittisin, mutta tämä ei poissulje vastaavaa haastetta myös muissa toimijatyypeissä. Energiaviraston näkemyksestä hallituksen esityksen luonnokseen tulisi lisäksi lisätä perustelut, mistä syystä on päädytty esittämään, että kokoluokan arviointiin sisällytetään koko yritys, vaikka se toimii vain osittain jollain liitteessä mainitulla toimialalla.

Energiavirasto katsoo, että jos kokoluokan arviointiin liittyvä ratkaisu pysyy ennallaan, ehdotetun lain liitteen 8. kohdan d alakohta muutetaan seuraavasti: ”Sähkömarkkinalain 3 §:n 1 momentin 15 kohdassa tarkoitetut tuottajat, pois lukien toimijat, jotka harjoittavat ainoastaan sähkömarkkinalain 3 §:n 1 momentin 14 kohdan mukaista pienimuotoista sähkön tuotantoa.”

Toimijat koosta riippumatta

Ehdotetun lain 3 §:n 2 momentin e kohdan mukaan toimijalla lisäksi tarkoitetaan koosta riippumatta oikeushenkilöä tai luonnollista henkilöä, joka on muun muassa CER-direktiivin nojalla määritelty kriittinen toimija. Lisäksi saman ehdotetun säännöksen 3 momentin mukaan valtioneuvoston

asetuksella säädetään tämän lain soveltamisesta sellaiseen liitteessä I tai II tarkoitettua toimintaa harjoittavaan tai toimijatyyppiä olevaan toimijaan sen koosta riippumatta, jos 1) toimija tarjoaa ainoana palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen; 2) häiriö toimijan tarjoamassa palvelussa vaikuttaisi merkittävästi yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen; 3) häiriö toimijan tarjoamassa palvelussa voisi aiheuttaa merkittävän systeemisen riskin erityisesti aloilla, joilla tällaisella häiriöllä voisi olla rajat ylittäviä vaikutuksia; tai 4) toimija on kriittinen, koska sillä on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan tai palvelutyypin tai jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta.

Energiavirasto kannattaa ehdotettua ratkaisua, jossa soveltamisalaan kuuluvat koostaan riippumattomat toimijat määritellään valtioneuvoston asetuksella. Toisaalta Energiavirasto tuo esiin, että energia-alalla valtioneuvoston asetuksen merkitys voi vähentyä, kun toimijoita tunnistetaan CER-direktiivin nojalla NIS2-keskeisiksi toimijoiksi. Ehdotettu laki tulee voimaan 18. lokakuuta 2024. CER-direktiivin mukaan kriittiset toimijat kuitenkin tunnistetaan viimeistään 1.7.2026, joten on syytä ehdotetun lain ja CER-direktiiviä koskevan lain voimaantulon välissä määrittää edellytykset täyttävät koosta riippumattomat toimijat nyt ehdotetun lain soveltamisalan piiriin. Lisäksi on syytä huomioida, että NIS2- ja CER-direktiivin soveltamisala eroaa jossain määrin toisistaan niin määritelmiltään kuin toimijatyypeiltään.

Energiavirasto lisäksi katsoo, että toimijoille asetettavat velvoitteet tunnistaa itsensä soveltamisalaan kuuluvaksi toimijaksi ja ilmoittautua valvovan viranomaisen toimijaluetteloon tulee koskea myös toimijoita, jotka katsotaan koostaan riippumatta soveltamisalaan annettavan valtioneuvoston asetuksen nojalla riippuen asetuksen sisällöllisistä ratkaisuista. Jos valtioneuvoston asetuksessa määritellään esimerkiksi kriteerit koostaan riippumattomille toimijoille, on toimijoilla itsellään paras tieto kriteeristön täyttymisestä.

Kaukolämmityksen tai kaukojäähdytyksen haltijat

Hallituksen esityksen luonnoksessa ehdotetaan Energiaviraston valvottaviksi toimijoiksi muun muassa uusiutuvista lähteistä peräisin olevan energian käytön edistämisestä annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/2001 2 kohdan 19 alakohdassa määritellyn kaukolämmityksen tai kaukojäähdytyksen haltijat. Hallituksen esityksen luonnoksessa kaukolämmityksen tai kaukojäähdytyksen haltijoihin viitataan jakelijoina. Esityksen mukaan kaukolämmön tai -jäähdytyksen tuottajat, joilla ei ole ollenkaan jakelutoimintaa jäisivät soveltamisalan ulkopuolelle.

Energiavirasto on valvonut NIS1-direktiivin velvoitteita energiasektorilla ainoastaan sähköverkonhaltijoiden ja maakaasun siirtoverkonhaltijan osalta. Energiavirastolla ei ole siten lausunnon kirjoittamisen aikaan syvällisempää tietoa kaukolämmitys- ja kaukojäähdytysalan toimijoista. Energiavirasto tuo kuitenkin toimijan määritelmästä esiin seuraavia seikkoja.

Ensinnäkin ehdotetun lain valmistelussa on tärkeää varmistaa, että NIS2-direktiivin implementoinnissa tehty ratkaisu toimijoiden määritelmän osalta on yhdenmukainen CER-direktiivin nojalla annettavan kansallisen lainsäädännön kanssa. CER-kriittiset toimijat ovat NIS2-yleislain mukaisia keskeisiä toimijoita.

Toisekseen Energiavirasto tuo esiin pohdinnan siitä, että jääkö edellä mainitun määritelmän myötä lain soveltamisalan ulkopuolelle merkittäviä kaukolämmityksen ja -jäähdytyksen toimijoita ja, miten valvonta järjestetään muun muassa niiden toimijoiden osalta, jotka tuottavat niin sähköä kuin lämpöä eli niin sanotut CHP-laitokset. Ehdotettu lain määritelmä tarkoittaisi, että CHP-laitosten osalta valvottaisiin jatkossa ainoastaan mahdollisesti sähköntuotantoa, jos tällainen sähköä ja lämpöä tuottava laitos ei harjoita myös jakelutoimintaa. Sähköntuotanto voi olla valtakunnallisesti tällaisilla laitoksilla pientä, mutta lämmöntuotanto paikallisesti merkittävää. Toisaalta esitysluonnoksen pohjalta voi syntyä myös tilanne, jossa jakelutoimija tulisi valvottavaksi, mutta verkkoon syöttävät kaukolämpötuottajat eivät, jos kyseiset tahot ovat erillisiä toimijoita. Energiateollisuus ry:n ylläpitämän kaukolämpötilaston mukaan yli 100 GWh vuodessa kaukolämpöä lämmönjakelijoille toimittavia yhtiöitä on hieman alle 30 yritystä vuonna 2021.

Kolmanneksi Energiavirasto lausuu erikseen valvonnan kohdistamista koskevasta näkemyksestä kohdassa 5 ”Valvontaa koskevat huomiot”, mutta tuo esiin soveltamisalaan kuuluvan problematiikan tässäkin yhteydessä. Hallituksen esityksen luonnoksessa on tuotu esiin, että kaukolämmön tai -jäähdytyksen tuottajat, joilla ei ole ollenkaan jakelutoimintaa jäisivät soveltamisalan ulkopuolelle. Energiavirasto kuitenkin tulkitsee, että velvoitteiden valvonta kohdistuu siihen toimintaan, jonka vuoksi toimija kuuluu lain soveltamisalaan. Näin ollen maininta siitä, että jakelutoimintaa harjoittavien toimijoiden osalta myös tuotantotoiminta kuuluu lain soveltamisalaan, on tältä osin epäjohdonmukainen. Energiavirasto katsoo, että kaukolämmityksen ja kaukojäähdytyksen haltijoita koskevaa hallituksen esityksen perusteluja tulee täsmentää sekä ottaa selkeästi kantaa valvovan viranomaisen valvonnan kohdistamiseen niiden toimijoiden osalta, jotka toimivat usealla toimialalla tai toimialan osalla.

Suhde muuhun lainsäädäntöön

Ehdotetun 5 §:n mukaan, jos muussa laissa on tästä laista poikkeavia säännöksiä, joilla varmistetaan korkeampi kyberturvallisuuden taso, niitä sovelletaan tämän lain lisäksi. Lisäksi, jos Euroopan unionin asetuksessa tai NIS2-direktiivin nojalla säädetyssä komission asetuksessa edellytetään toimialakohtaisesti, että toimija ottaa käyttöön kyberturvallisuusriskien hallintatoimenpiteitä tai ilmoittaa merkittävistä poikkeamista, ja vaatimukset ovat vaikutuksiltaan vähintään tässä laissa säädettyjä vastaavia velvoitteita vastaavia, toimijaan ei sovelleta näiden velvoitteiden tai niiden valvonnan osalta tämän lain 2, 4 ja 5 lukua eikä 43 §:ää.

EU:n komissio on antamassa sähkön toimialalle niin sanottua verkkosääntöä, joka sisältää alakohtaisia säännöt rajat ylittävien sähkönsiirtojen kyberturvallisuusnäkökohdista: ”Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (NCCS)”. Kyseinen verkkosääntö on komission sähkökauppa-asetusta EU (2019/943) täydentävä delegoitu säädös, joka on suoraan jäsenvaltiossa sovellettavaa oikeutta. Verkkosäännössä annettavat alakohtaiset säännöt sisältävät yhteisiä vähimmäisvaatimuksia, suunnittelua, seurantaa, raportointia ja kriisinhallintaa koskevat säännöt.

Verkkosäännön suhdetta NIS2-direktiiviin on kuvattu verkkosäännön luonnoksen johdanto-osan 3 kohdassa seuraavasti: Regulation (EU) 2019/943 complements Directive (EU) 2022/2555 and Regulation (EU) 2019/941 by setting out specific rules for the electricity sector at Union level. Furthermore, this Delegated Regulation complements the provisions of Directive (EU) 2022/2555 regarding the electricity sector, whenever cross-border electricity flows are concerned.”

Lisäksi verkkosäännön luonnoksen johdanto-osan 14 kohdassa todetaan seuraavasti: ”In order to avoid gaps between or duplications of cybersecurity risk-management obligations imposed on high-impact and critical-impact entities, national authorities under Directive (EU) 2022/2555 and the competent authorities under this Regulation should cooperate in relation to the implementation of cybersecurity risk-management measures and the supervision of compliance with those measures at national level. The compliance of an entity with the cybersecurity risk management requirements laid down in this Regulation could be considered by the competent authorities under Directive (EU) 2022/2555 as ensuring compliance with the corresponding requirements laid down in that Directive, or vice-versa.”

Verkkosääntö on Energiaviraston lausunnon jättämisen aikaan edelleen luonnos, mutta edellä mainituin perustein verkkosääntö näyttäisi täydentävän NIS2-direktiiviin ja kyberturvallisuuden riskienhallinnasta ehdotettua lakia. Nyt ehdotetun 5 §:n 2 momentin sanamuoto kuitenkin tunnistaa EU-oikeuden lainsäädäntöinstrumentteina ainoastaan Euroopan unionin asetuksen tai NIS2-direktiivin nojalla säädetyn komission asetuksen. Energiavirasto näin ollen lausuu, että kyseisen säännöksen sanamuotoa olisi hyvä muuttaa niin, että se ottaa huomioon myös muut suoraan jäsenvaltioissa sovellettavat säännökset koskien kyberturvallisuutta niin, että myös verkkosääntöä vastaavien täydentävien säännösten soveltaminen on selkeämpää. Uusi säännösmuotoilu voisi olla esimerkiksi seuraavanlainen: ”[…] jos Euroopan unionin asetuksessa tai sen nojalla säädetyssä komission delegoidussa säädöksessä taikka NIS2-direktiivin nojalla säädetyssä komission asetuksessa edellytetään […]”.

Riskienhallintavelvoitetta koskevat huomiot

Hallituksen esityksen luonnoksen mukaan verrattuna NIS1-direktiivin aikaisiin riskienhallintavelvoitteisiin, laissa säädettäisiin yksityiskohtaisemmin osa-alueista, jotka riskienhallinnassa on huomioitava. Toimijat voisivat halutessaan ottaa käyttöön pidemmälle meneviä riskienhallintatoimia ja kansallisesti olisi jatkossakin mahdollista säätää tiukemmista riskienhallintavelvoitteista.

Direktiivin mukaan toimijan tulee toteuttaa riskienhallintatoimenpiteet siten, että turvallisuuden taso on oikeassa suhteessa riskeihin. Arvioinnissa on huomioitava toimijan altistuminen riskeille, toimijan koko, poikkeamien esiintymisen todennäköisyys ja vakavuus, mukaan lukien niiden yhteiskunnalliset ja taloudelliset vaikutukset. Jäsenvaltioiden on varmistettava, että toteuttaessaan riskienhallintatoimenpiteensä, toimijat huomioivat ne haavoittuvuudet, jotka ovat ominaisia toimijan harjoittamalle toiminnalle.

Kyberturvallisuuden riskienhallintavelvoitteista ehdotetaan säädettäväksi lain 2 luvussa. Yleisestä riskienhallintavelvoitteesta säädettäisiin lain 7 §:ssä, riskienhallinnan toimintamallista 8 §:ssä ja riskienhallinnan toimenpiteistä 9 §:ssä. Lisäksi lain 10 §:ssä ehdotetaan säädettäväksi johdon vastuusta. Hallituksen esityksen luonnoksen mukaan NIS2-direktiivin riskienhallintavelvoitteet ovat vähimmäistason velvoitteita ja ne on pyritty muotoilemaan mahdollisimman teknologianeutraalisti, jotta ne kestäisivät aikaa ja soveltuisivat laajalle joukolle erilaisia toimijoita. Esityksessä ei ehdoteta säädettäväksi kansallisia lisävaatimuksia eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käytölle.

Energiavirasto katsoo, että ehdotetut riskienhallintaa koskevat säännökset ovat NIS2-direktiivin mukaisia ja yksityiskohtaisesti ehdotuksessa perusteltuja. Energiavirasto pitää hyvänä, että vähimmäistason riskienhallintatoimenpiteet on lueteltu yksityiskohtaisesti ehdotetun lain säännöksessä ja ne on perusteltu tarkemmin hallituksen esityksen yksityiskohtaisissa perusteluissa.

Energiavirasto tuo esiin, että riskienhallintavelvoitteet ovat osin päällekkäisiä CER-direktiivin mukaisten toimenpiteiden osalta. Näin ollen Energiavirasto pitää hyvänä, että hallituksen esityksen luonnoksessa on todettu, että kyberturvallisuuden riskienhallinnan toimintamalli voisi olla myös osa toimijan laajempaa riskienhallintasuunnitelmaa, jossa huomioidaan myös muita toimintaan kohdistuvia riskejä tai osa muuta turvallisuusvarautumista. Tämä on tärkeää toimijoiden hallinnollisen taakan vähentämiseksi sekä valvonnan tehostamiseksi.

Hallituksen esityksessä on myös todettu, että toimijoiden tulisi varautua välttämättömien resurssien, kuten sähkönjakelun, tietoliikenneyhteyksien ja jäähdytyksen häiriöihin ja estää viestintäverkkojen ja tietojärjestelmien tuhoutuminen, vahingoittuminen tai toimijan kriittisten toimintojen keskeytyminen välttämättömien resurssien puutteen tai häiriön vuoksi. Energiavirasto pitää tärkeänä, että soveltamisalaan kuuluvat toimijat varautuvat myös itse esimerkiksi sähkönjakelun toimintahäiriöihin sen aiheuttamien vaikutusten lieventämiseksi.

Ehdotetun 9 pykälän 4 momentin nojalla valvova viranomainen voisi antaa tarkempia teknisiä määräyksiä siinä esitetyistä seikoista valvontatoimialallaan. Viranomaisen määräyksenantovaltuus koskisi 2 momentissa tarkoitettujen velvoitteiden tarkentamista ja täsmentämistä. Tarkemmat määräykset voisivat kuitenkin koskea vain teknisiä seikkoja, eli niillä ei saisi laajentaa 9 §:ssä säädettyjä velvoitteita. Määräysten olisi oltava teknologianeutraaleja. Energiavirasto kannattaa ehdotettua määräyksenantovaltuutta.

Raportointivelvoitetta koskevat huomiot

Poikkeamailmoitus

Ehdotetun lain 11 §:n mukaan toimijan on ilmoitettava viipymättä valvovalle viranomaiselle merkittävästä poikkeamasta. Merkittävällä poikkeamalla tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai asianomaiselle toimijalle taloudellisia tappioita taikka poikkeama on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.

Hallituksen esityksen luonnoksen mukaan ilmoitusvelvollisuus olisi kolmivaiheinen, eli toimijan olisi toimitettava valvovalle viranomaiselle 24 tunnin kuluessa poikkeaman havaitsemisesta ensi-ilmoitus ja 72 tunnin kuluessa poikkeaman havaitsemisesta jatkoilmoitus. Poikkeamatilanteen päätyttyä toimijan olisi toimitettava valvovalle viranomaiselle vielä 13 §:ssä tarkoitettu loppuraportti. Kolmivaiheisen ilmoitusvelvollisuuden tavoitteena on toisaalta varmistaa poikkeamien nopea ilmoittaminen ja ajantasaisen tilannekuvan muodostaminen ja toisaalta mahdollistaa toimijan resurssien suuntaaminen ensisijaisesti poikkeamien käsittelyyn liittyviin toimintoihin.

Energiavirasto katsoo ehdotettujen poikkeamailmoitusta koskevien säännösten olevan NIS2-direktiivin mukaisia. Säännökset ovat myös selkeitä ja perusteltuja. Energiavirasto pitää tärkeänä, että valvovalle viranomaiselle on annettu ehdotetun 12 §:n nojalla oikeus pyynnöstä saada

lisätietoja tai väliraportti poikkeaman tilannepäivityksistä ja käsittelyn edistymisestä. Lisäksi Energiavirasto katsoo määräyksenantovaltuuden antamisesta ehdotetuilta kohdin tarpeelliseksi. Lisäksi merkittävän poikkeaman määritelmä näyttäisi pysyneen jotakuinkin yhdenmukaisena NIS1-direktiivin kanssa. Perusteluissa on kuitenkin asianmukaisesti korostettu tilannetta, jossa toimija havaitsee merkittävän poikkeaman jonkun muun, kuten välittömän alihankkijan, toiminnassa.

Tiedonsaantioikeudet

Ehdotetun lain 16 §:n 1 momentin nojalla valvovan viranomaisen on vastattava poikkeamailmoituksen tehneelle taholle viivytyksettä. Vastauksessa on oltava alustava palaute merkittävästä poikkeamasta sekä ohjeet merkittävän poikkeaman ilmoittamisesta esitutkintaviranomaiselle, jos asiassa epäillään rikosta. Lisäksi ehdotetun lain 17 §:n 1 momentin mukaan valvovan viranomaisen on toimitettava edellä 11-13 §:ssä ja 15 §:ssä tarkoitetut ilmoitukset ja raportit CSIRT-yksikölle. CSIRT-yksikkö antaa toimijan pyynnöstä ohjeita tai operatiivisia neuvoja vaikutuksia lieventävien toimenpiteiden osalta. Ehdotetun säännöksen yksityiskohtaisten perustelujen mukaan tarvittaessa ohjeita tai neuvoja voitaisiin antaa myös valvovan viranomaisen ja CSIRT-yksikön yhteistyönä.

Ehdotetun lain 24 §:n 3 momentin mukaan siitä riippumatta, mitä viranomaisten oikeudesta saada salassa pidettäviä tietoja muualla laissa säädetään, CSIRT-yksikön tämän lain mukaista tehtävää hoitaessaan saamaa, muuta kuin pakollisen ilmoitusvelvollisuuden piiriin kuuluvaa tietoa ei saa käyttää tiedon luovuttanutta koskevassa rikostutkinnassa eikä hallinnollisessa tai muussa tiedon luovuttanutta koskevassa päätöksenteossa. Poikkeuksena on kuitenkin tilanne, jossa CSIRT-yksikön riskiarvion perusteella on tarpeen merkittävän kyberuhkan torjumiseksi ilmoittaa epäillystä vakavasta ja tahallisesta tämän lain rikkomisesta valvovalle viranomaiselle.

Lisäksi ehdotetussa 27 §:ssä koskien valvovan viranomaisen tiedonsaantioikeutta ei säädetä valvovan viranomaisen oikeudesta saada tietoa CSIRT-yksiköltä. Ehdotetun lain 46 §:n 1 momentissa säädetään valvovan viranomaisen ja CSIRT-yksikön velvollisuudesta tehdä yhteistyötä tämän lain ja NIS2-direktiivin mukaisten tehtävien toteuttamisessa, mutta yksityiskohtaisten perustelujen mukaan säännöksen nojalla tapahtuva tiedonvaihto ei itsessään perustaisi oikeutta poiketa salassapitosäännöksistä sitä toteutettaessa.

Energiavirasto nostaa esiin, että ehdotuksen mukaan ohjeita tai neuvoja voitaisiin tarvittaessa antaa valvovan viranomaisen ja CSIRT-yksikön yhteistyönä, mutta ehdotetussa laissa ei esitetä NIS-valvovalle viranomaiselle tiedonsaantioikeutta CSIRT-yksiköltä. Energiavirasto pitää tärkeänä, että ohjeita ja neuvoja voidaan antaa yhteistyössä CSIRT-yksikön kanssa sekä, että Energiavirasto saa tietoonsa ilmoitetun poikkeaman myötä CSIRT-yksikön antamista ohjeista koskien lieventäviä toimenpiteitä, joilla toimija voi minimoida aiheutuneita haitallisia vaikutuksia. Energiavirasto katsoo, että poikkeamahallintaan liittyviä tiedonsaantioikeuksia tulisi uudelleen tarkastella edellä mainituilta osin, jotta ne eivät johda lain soveltamistilanteessa epätoivottuun lopputulokseen. Energiavirasto

pitää tärkeänä, että ehdotetussa laissa turvataan ilmoitetun poikkeaman aikainen tiedonvaihto viranomaisten kesken, viranomaisten ja toimijoiden välillä sekä yhtenäinen tilannekuva.

Energiavirasto lisäksi toteaa, että ehdotetun lain 34 §:n 1 momentin mukaan, jos valvova viranomainen saa tässä laissa tarkoitettujen tehtävien hoitamisen yhteydessä tietoonsa, että 2 luvussa säädettyjen velvoitteiden laiminlyönti voi johtaa tai on johtanut yleisessä tietosuoja-asetuksessa tarkoitettuun henkilötietojen tietoturvaloukkaukseen, josta on yleisen tietosuoja-asetuksen 33 artiklan nojalla ilmoitettava yleisen tietosuoja-asetuksen mukaiselle valvontaviranomaiselle, valvovan viranomaisen on ilmoitettava asiasta tietosuojavaltuutetulle. Ehdotetussa laissa ei ole kuitenkaan säädetty salassa pidettävien tietojen luovuttamisesta tietosuojavaltuutetulle. Energiavirasto katsoo, että hallituksen esitystä tulee täsmentää tältä osin, mitä tietoja valvova viranomainen voi antaa ilmoituksen yhteydessä tietosuojavaltuutetulle.

Valvontaa koskevat huomiot

Energiavirasto valvovaksi viranomaiseksi

Hallituksen esityksen luonnoksessa ehdotetaan, että valvonnan järjestämisessä jatkettaisiin sektorikohtaisesti hajautettua, NIS1-direktiivin yhteydessä omaksuttua, mallia. Keskeisten ja tärkeiden toimijoiden erottelun osalta merkityksellistä on direktiivin niihin kohdistamat valvontatoimivaltuudet. Keskeisten toimijoiden osalta valvonnan tulee kattaa etukäteis- ja jälkikäteisvalvonta, mutta tärkeiden toimijoiden osalta pelkkä jälkikäteisvalvonta on direktiivin nojalla riittävä. Esityksessä ehdotetaan käytettäväksi kansallinen liikkumavara siitä, että valvova viranomainen saisi kohdentaa valvontaa riskiperusteisesti ja ensisijaisesti keskeisiin toimijoihin.

Esitysluonnoksen mukaan ”valvonnan järjestämistä sektorikohtaisesti puoltaa se, ettei kyberturvallisuus ole valvottavan toimijan muusta toiminnasta erillinen osa, vaan yhteiskunnan digitalisoituessa kyberturvallisuus hahmotetaan toiminnan kokonaisturvallisuuden osa-alueena. Toimijan näkökulmasta erilaisten riskien hallinta hahmotetaan tyypillisesti yhtenä kokonaisuutena, eikä kyberturvallisuusriskien hallintaa tai sen valvontaa ole lähtökohtaisesti perusteltua eriyttää tai tarkastella muusta riskien hallinnasta erillisenä kokonaisuutena. […] Myös valvovan viranomaisen näkökulmasta on arvioitu tarkoituksenmukaiseksi arvioida valvottavan toiminnan turvallisuutta kokonaisuutena.”

Energiavirasto kannattaa hajautettua valvontamallia esityksessä esitetyin perusteluin. Energiavirasto on sähkö- ja maakaasumarkkinoiden nimetty sääntelyviranomainen (EU-oikeudessa national regulatory authority, NRA). Energiaviraston tehtävänä on sähkö- ja maakaasumarkkinoiden valvonta ja seuranta, sähkö- ja maakaasumarkkinoiden toimivuuden, energiatehokkuuden ja uusiutuvan energian käytön edistäminen sekä energiapolitiikan, kasvihuonekaasujen päästökaupan ja energiatehokkuuden toimeenpanotehtävien hoitaminen (laki Energiavirastosta 870/2013 1 §). Sähkö- ja maakaasumarkkinoiden valvonnan ja seurannan tavoitteena on sähkön ja maakaasun hyvän toimitusvarmuuden, kilpailukykyisen hinnan ja kohtuullisten palveluperiaatteiden turvaamiseksi energian käyttäjille edistää tehokkaasti, varmasti ja ympäristön kannalta kestävästi

toimivia kansallisia ja alueellisia sähkö- ja maakaasumarkkinoita sekä Euroopan unionin sähkön ja maakaasun sisämarkkinoita (laki sähkö- ja maakaasumarkkinoiden valvonnasta 590/2013 1 §). Energiavirasto on nimitetty NIS1-direktiivin valvovaksi viranomaiseksi sekä se on valvonut sähkö- ja maakaasuverkonhaltijoiden varautumissuunnittelua. Energiavirasto myös hoitaa toimivaltaiselle viranomaiselle kuuluvat tehtävät, joista säädetään riskeihin varautumisesta sähköalalla ja direktiivin 2005/89/EY kumoamisesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2019/941.

Energiavirastolla on laaja osaaminen energia-alan markkinasta sekä sektorikohtaisista erityispiirteistä. Energiavirasto kannattaa hajautettua valvontamallia, jossa Energiavirasto valvottaviksi toimijoiksi määrätään toimijoita kyberturvallisuuden riskienhallinnasta annetun lain energiatoimialalta. Myös CER-direktiivin implementoinnin osalta on pohdittu hajautettua valvontamallia. Kuten hallituksen esityksen luonnoksessa on todettu, on tarkoituksenmukaista, että valvottavan toiminnan turvallisuutta arvioidaan kokonaisuutena. Hallituksen esityksessä on tunnistettu ja Energiavirasto arvioi, että NIS2-direktiivin hallintatoimenpiteet sekä CER-direktiivin mukaiset toimenpiteet ovat joiltain osin päällekkäisiä etenkin, jos kyseessä on verkko- ja tietojärjestelmien fyysinen turvallisuus ja suojaus. Valvovan viranomaisen resurssitarpeista Energiavirasto lausuu tarkemmin kysymyksessä 11: ”Vaikutustenarviointia koskevat huomiot”.

Vedyn siirtoa harjoittavat toimijat Energiaviraston valvontavastuulle

Ehdotetun lain 25 §:n mukaan Energiaviraston valvontavastuulle ehdotetaan seuraavia toimialoja ja toimijatyyppejä: sähkö, kaukolämmityksen tai kaukojäähdytyksen haltijat, kaasu (jakelu- ja siirtoverkonhaltijat). Edellä esitetyin perusteluin Energiavirasto katsoo, että se on oikea taho valvomaan ehdotetun lain velvoitteita Suomessa näiden toimijoiden osalta. Energiavirasto kuitenkin katsoo, että Energiaviraston valvontaan tulisi kuulua myös vedyn siirtoa harjoittavat toimijat. Nyt ehdotetussa hallituksen esityksen luonnoksessa nämä toimijat kuuluisivat Turvallisuus- ja kemikaaliviraston (Tukes) valvottaviksi.

Vetymarkkinoita koskevaa sääntelyä ei ole tällä hetkellä niin EU:n kuin kansallisellakaan tasolla. Toimiala on kuitenkin nopeasti kehittyvä ja Energiavirasto katsoo, että vetymarkkinoita koskeva EU-sääntely tai kansallinen lainsäädäntö tulee mahdollisesti rakentumaan pitkälti sähkö- ja maakaasumarkkinasääntelyn mukaisesti. Energiavirasto pitää todennäköisenä, että se tulee olemaan tuon sääntelykokonaisuuden toimivaltainen viranomainen. Vaikka vetyverkonhaltijoista ei ole tällä hetkellä voimassa olevaa sääntelyä, Energiavirasto katsoo, että on syytä jakaa viranomaisten valvontavastuuta etupainotteisesti tulevaa lainsäädäntöä silmällä pitäen. Energiavirasto näin ollen katsoo, että vedyn verkonhaltijat tulisi jo tässä vaiheessa määrittää Energiaviraston toimivaltaan kuuluviksi toimijatyypeiksi, jotta näiden valvonta on yhdenmukaista muun muassa maakaasuverkonhaltijoiden kanssa.

Valvonnan kohdistaminen ja päällekkäisyys eri viranomaisten kesken

Ehdotetun lain 25 §:n 2 momentin mukaan valvovan viranomaisen tehtävänä on valvoa tämän lain, sen nojalla annettujen määräysten ja NIS 2 -direktiivin nojalla annettujen säädösten noudattamista 1 momentissa tarkoitetun toiminnan osalta. Saman ehdotetun säännöksen 3 momentin mukaan, jos 1 momentin nojalla samaa toimijaa valvoisi useampi kuin yksi viranomainen, kukin valvova viranomainen valvoo toimijaa vain 1 momentissa tarkoitetun toiminnan osalta. Valvovien viranomaisten on tehtävä yhteistyötä valvonnan toteuttamisessa. Säännöksen yksityiskohtaisten perustelujen mukaan pykälän 3 momentissa säädettäisiin valvonnasta tilanteessa, jossa yksi toimija harjoittaisi toimintaa laaja-alaisesti usealla toimialalla siten, että toimijaan kohdistuisi 1 momentin nojalla useamman kuin yhden viranomaisen valvontatoimivalta. Tässä tilanteessa kukin valvova viranomainen valvoisi toimijaa vain sen toiminnan osalta, joka kuuluu kyseisen viranomaisen valvottavana olevaan toimialaan.

Lisäksi hallituksen esityksen luonnoksen mukaan, mikäli toimija toimii usealla eri toimialalla ja vain osa sen toiminnasta on liitteessä I tai II tarkoitettua toimintaa, kokorajoitusta arvioidaan toimijan kokonaistoiminnan perusteella. Näin ollen liikevaihtoa, tasetta ja henkilöstömäärää arvioidaan koko toimijan osalta eikä arviointia tule rajata vain liitteessä I tai II tarkoitetun toiminnan laajuuteen. Arviointi tehdään toimijakohtaisesti. Hallituksen esityksen luonnoksessa myös todetaan, että jos julkinen toimija toimii jollain NIS2-direktiivin muista toimialoista, se voi kuulua NIS2-sääntelyn piiriin myös tai vain kyberturvallisuuden riskienhallinnasta annetun lain nojalla.

Energiavirasto katsoo, että hallituksen esityksen luonnosta on hyvä täsmentää valvonnan kohdentamisen osalta, koska esitysluonnoksen perusteluissa on keskenään ristiriitaisia kannanottoja. Edellä esitetyt hallituksen esityksen luonnoksessa tuodut kohdan käsittelevät lähinnä tilannetta, jossa toimija toimii useammalla kuin yhdellä soveltamisalaan kuuluvalla toimialalla. Kuitenkin Energiavirasto katsoo, että hallituksen esityksen luonnoksesta jää täsmentämättä tilanne, jossa toimija toimii useammalla kuin yhdellä toimialalla tai toimialan osalla, mutta ainoastaan yksi toimialan osa kuuluu ehdotetun lain soveltamisalaan piiriin. Tällaisessa tilanteessa Energiavirasto katsoo ehdotetun lain 25 §:n ja 26 §:n perusteella, että se valvoisi ainoastaan soveltamisalaan kuuluvaa toimintaa, mutta kuten Energiavirasto on edellä tuonut esiin kysymyksessä 2, lain soveltamisala esimerkiksi kaukolämmön ja kaukojäähdytystoimintaa harjoittavien osalta on ehdotetun luonnoksen perusteluissa epäjohdonmukaisesti esitetty.

Hallituksen esityksen luonnoksen mukaan sen soveltamisalaan kuuluu kaukolämmitystä ja kaukojäähdytyksen jakelijat. Esitysluonnoksessa on kuitenkin tuotu esiin, että kaukolämmön tai -jäähdytyksen tuottajat, joilla ei ole ollenkaan jakelutoimintaa, jäisivät soveltamisalan ulkopuolelle. Näin ollen esitysluonnos antaa ymmärtää, että jakelutoimintaa harjoittavien toimijoiden osalta myös näiden harjoittama kaukolämmityksen tuotanto kuuluu lain soveltamisalaan, vaikka se ei ole ehdotetun lain perusteluissa katsottu soveltamisalaan kuuluvaksi toiminnaksi.

Valvonnan kohdentamista koskeva täsmennysvaatimus on kriittinen lisäksi edellä Energiaviraston kysymyksessä 2 esiin tuomien sähköntuottajien osalta. Tuottajalla tarkoitetaan sähkömarkkinalaissa

sähköä tuottavaa luonnollista henkilöä tai oikeushenkilöä. Sähkömarkkinalaissa eikä sen pohjautuvassa sähkömarkkinadirektiivin (EU 944/2019) määritelmään kuuluminen ei ole riippuvaista sähköä tuottavan laitoksen koosta. Hallituksen esityksen luonnoksessa ehdotettu toimijan kokoluokan arviointi ja soveltamisala tarkoittaisi näin ollen, että pienimuotoinen sähkön tuotanto (sähkömarkkinalain 3 §:n 1 momentti 14 kohta), kuten aurinkopaneelien hyödyntäminen omassa energiantuotannossa, voisi merkitä pääasiallisesti muuta toimintaa harjoittavan yrityksen kuulumista Energiaviraston valvontatoimivaltaan, jopa keskeisenä toimijana. Energiavirasto katsoo, että tämä ei ole tarkoituksenmukaista ja voi johtaa suhteettomaan lopputulokseen joidenkin toimijoiden osalta.

Lisäksi komission 13.9.2023 antamassa ohjeessa (NIS2-direktiivin 4 artiklan 1 ja 2 kohdan soveltamisesta) on todettu seuraavasti 7 kohdassa: "Direktiivin (EU) 2022/2555 21 artiklan 1 kohdassa säädetty velvoite, jonka mukaan keskeisten ja tärkeiden toimijoiden on toteutettava asianmukaisia ja oikeasuhteisia kyberturvallisuusriskien hallintatoimenpiteitä, koskee kyseisen toimijan kaikkia toimintoja ja palveluja eikä vain sen tarjoamia tiettyjä tietoteknisiä toimintoja tai kriittisiä palveluja." Koska kyseessä on komission ohje eikä sitova tulkinta direktiivin säännöksestä, Energiavirasto katsoo, että valvonnan kohdentamista on syytä selkeyttää kansallisella tasolla.

Energiavirasto pitää ehdotettua 25 §:n 3 momenttia tärkeänä toimijaan kohdistuvien päällekkäisten valvontatoimenpiteiden ehkäisemiseksi ja siten ehdotetusta lainsäädännöstä toimijoille aiheutuvan hallinnollisen taakan minimoimiseksi. Energiavirasto kuitenkin nostaa esiin, että ehdotettu säännös edellyttää yhteistyötä ainoastaan NIS-valvovien viranomaisten välillä. Energiavirastolla voi kuitenkin tulla päällekkäisiä tehtäviä liittyen esimerkiksi ydinvoimaloiden valvontaan, joka kuuluu NIS2-direktiivin soveltamisalaan sähkön tuottajina. Ydinturvallisuutta Suomessa valvoo Säteilyturvakeskus (STUK).

Velvoitteiden valvonta

Ehdotetun lain 25 §:n 2 momentin mukaan valvovan viranomaisen tehtävänä olisi valvoa toimialallaan tämän lain, sen nojalla annettujen määräysten sekä NIS2-direktiivin nojalla annettujen säädösten noudattamista 1 momentissa tarkoitetun toiminnan osalta. Lisäksi ehdotetun lain 26 §:n 4 momentin mukaan valvova viranomainen voi asettaa tässä laissa säädetyt tehtävät tärkeysjärjestykseen riskiperusteisesti. Valvovan viranomaisen on otettava valvonnan kohdistamisessa ja 29-34 §:ssä tarkoitettujen toimien käyttämisestä päätettäessä huomioon: a) liitteessä I tai II tarkoitetun toiminnan laatu ja laajuus; b) tietojärjestelmän tai viestintäverkon merkitys liitteessä I tai II tarkoitetulle toiminnalle; ja c) NIS 2-direktiivin 32 artiklan 7 kohdassa säädetyt seikat;

Viimeksi mainitun säännöksen yksityiskohtaisten perustelujen mukaan ”valvottavien toimijoiden määrä vaihtelee sektoreittain ja toimijoiden merkitys yhteiskunnan kriittisille toiminnoille sekä niihin kohdistuvien kyberturvallisuusriskien määrä vaihtelee. Näistä syistä olisi tarpeen, että valvova viranomainen voisi tarvittaessa asettaa tämän lain mukaiset valvontatehtävänsä

tärkeysjärjestykseen riskiperusteisesti. Valvonnan, eli toimijoihin kohdistettavien valvontatoimenpiteiden laadun ja määrän tulisi olla suhteellista ja perustua kyberturvallisuusriskien arviointiin. Kyberturvallisuusriskien arvioinnissa olisi otettava huomioon toimijoihin kohdistuvien kyberturvallisuusriskien laatu ja määrä, mahdollisesta poikkeamasta aiheutuvat vaikutukset yhteiskunnalle, toimijoiden yleisen kyberturvallisuusmaturiteetin laatu, valvontaviranomaisten käytettävissä olevat resurssit sekä yhteistyö muiden viranomaisten kanssa. Viranomainen voisi toteuttaa riskiperusteisuutta esimerkiksi laatimalla valvontasuunnitelman, jossa se luokittelisi valvonnan kohteet erilaisiin riskiluokkiin ja määrittelisi niiden perusteella toimijoihin kohdistettavat valvontatoimenpiteet ja niiden tiheyden tai toimijoilta säännöllisesti pyydettävät tiedot ja niiden yksityiskohtaisuudelle asetettavat vaatimukset. Valvovilla viranomaisilla ei kuitenkaan olisi velvollisuutta laatia valvontasuunnitelmaa ja tehtävien asettamista tärkeysjärjestykseen voisi tehdä myös muilla tavoin. Valvonta ja tehtävien asettaminen tärkeysjärjestykseen toteutettaisiin NIS2-direktiivin 31 artiklan 1 ja 2 kohdan mukaisesti.”

Energiavirasto katsoo, että valvovalle viranomaiselle annetaan esitysluonnoksen 4 luvussa pääasiassa riittävät toimivaltuudet ehdotetun lain ja sen nojalla annettujen määräysten valvontaan. Energiavirasto pitää ehdotettuja säännöksiä perusteltuina ja kannattaa tehtävien asettamista tärkeysjärjestykseen riskiperusteisesti.

Energiavirasto nostaa kuitenkin erikseen esiin ehdotetun lain 26 §:n 4 momentin. Sen mukaan valvova viranomainen voi jättää asian tutkimatta, jos kyse on ilmeisen perusteettomasta pyynnöstä. Päätös tutkimatta jättämisestä on tehtävä viivytyksettä. Kyseisen momentin yksityiskohtaisten perustelujen mukaan momentti olisi tarpeen esimerkiksi tilanteessa, jossa valvovan viranomaisen toimintaa pyrittäisiin haittaamaan tekemällä sille resursseja kuormittavia perusteettomia ilmoituksia käsiteltäväksi. Momentti olisi kansallinen lisäys täytäntöönpanolle. Energiavirasto ei ymmärrä ehdotetun säännöksen tarkoitusta eikä esitysluonnoksesta käy ilmi, keneltä pyyntöjä tulee ja kenelle tällainen pyyntöä koskeva päätös annetaan. Energiavirasto katsoo, että ehdotettu säännös vaatii ehdottomasti täsmennystä.

CER-direktiivin valvonta

NIS2-direktiivin johdanto-osan 79 kohdan mukaan toimijoiden olisi käsiteltävä kyberturvallisuusriskien hallintatoimenpiteissään myös henkilöstöturvallisuutta ja otettava käyttöön asianmukaiset pääsynhallintaperiaatteet. Näiden toimenpiteiden olisi oltava direktiivin (EU) 2022/2557 mukaisia. Direktiivin 2022/2557 (CER-direktiivi) 13 artiklan 1 kohdan e alakohdan mukaan kriittisten toimijoiden tulee ottaa käyttöön toimenpiteitä, jotka ovat tarpeen asianmukaisen henkilöstöturvallisuuden hallinnan varmistamiseksi, ottaen asianmukaisesti huomioon sellaiset toimenpiteet kuin kriittisiä tehtäviä hoitavien henkilöstöryhmien määrittäminen, pääsyoikeuksien vahvistaminen tiloihin, kriittiseen infrastruktuuriin ja arkaluonteisiin tietoihin pääsemiseksi, taustatarkastuksia koskevien menettelyjen käyttöönottaminen 14 artiklan mukaisesti ja sellaisten henkilöryhmien määrittäminen, joilta tällaisia taustatarkastuksia vaaditaan, sekä asianmukaisten koulutusvaatimusten ja pätevyyksien vahvistaminen.

Ehdotuksen 46 §:n mukaan valvovien viranomaisten ja CER-direktiivin mukaisen toimivaltaisen viranomaisen on vaihdettava keskenään säännöllisesti tietoja kriittisten toimijoiden määrittämisestä sekä riskeistä, kyberuhkista ja poikkeamista ja muista kuin kyberturvallisuuteen liittyvistä riskeistä, uhkista ja poikkeamista, jotka vaikuttavat CER-direktiivin nojalla kriittisiksi toimijoiksi määriteltyihin toimijoihin, sekä näiden riskien, uhkien ja poikkeamien hallintatoimenpiteistä. Valvovien viranomaisten on ilmoitettava CER-direktiivin mukaiselle toimivaltaiselle viranomaiselle, kun se käyttää 4 luvussa säädettyjä toimivaltuuksia CER-direktiivin nojalla kriittiseksi tunnistettuun toimijaan. Valvova viranomainen voi CER-direktiivin mukaisen toimivaltaisen viranomaisen perustellusta pyynnöstä kohdistaa 4 luvussa säädettyjä toimivaltuuksia CER-direktiivin nojalla kriittiseksi tunnistettuun toimijaan. Energiavirasto pitää tärkeänä, että hallituksen esityksen luonnoksessa on otettu huomioon NIS2- ja CER-direktiivin väliset liityntäkohdat.

Oikaisuvaatimusmenettely

Ehdotetun lain 36 §:n mukaan valvovan viranomaisen 30-33 §:n nojalla tekemään päätökseen saa vaatia oikaisua. Oikaisuvaatimuksesta säädetään hallintolaissa. Valvova viranomainen voi päätöksessään määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei muutoksenhakuviranomainen toisin määrää.

Päätökset, joihin ehdotuksen mukaan voi vaatia oikaisua, koskevat turvallisuusauditointia, valvontapäätöstä, luvanvaraisen tai sertifioidun toiminnan rajoittamista ja luvan tai sertifioinnin peruuttamista tai johdon toiminnan rajoittamista. Energiavirasto katsoo, että oikaisuvaatimuksen mielekkyyttä olisi syytä tarkastella uudelleen. Edellä mainituissa päätöksistä ei ole kyse massapäätöksistä vaan yksittäisistä tarkasti harkituista ja perustelluista päätöksistä. Oikaisuvaatimusmenettelyn edellyttäminen voi vain viivästyttää muutoksenhakua ja asian lopullista ratkaisemista.

Toiminnan rajoittaminen osittain

Ehdotetun lain 32 §:n mukaan valvova viranomainen voi väliaikaisesti rajoittaa keskeiselle toimijalle myönnetyn luvan tai sertifioinnin mukaista toimintaa tai peruuttaa luvan tai sertifioinnin […]. Sähkömarkkinalain 4 §:n mukaan sähköverkkotoimintaa saa harjoittaa Suomessa sijaitsevassa sähköverkossa vain Energiaviraston myöntämällä luvalla (sähköverkkolupa). Vastaava säännös on maakaasumarkkinalain (587/2017) 4 §:ssä koskien maakaasuverkkotoimintaa. Sähkö- ja maakaasumarkkinoiden valvonnasta (590/2013, jäljempänä valvontalaki) annetun lain 5 luvussa säädetään Energiaviraston toimilupa- ja markkinalupavalvonnasta. Luvun 23-24 §:ssä säädetään sähkö- ja maakaasuverkkoluvan peruuttamisesta sekä toimenpiteistä tällaisen luvan peruuttamisen johdosta. Jos sähköverkkolupa tai maakaasuverkkolupa peruutetaan, Energiaviraston on tarvittaessa päätettävä niistä toimenpiteistä, joihin on ryhdyttävä kyseisen verkkotoiminnan ylläpitämiseksi.

Jollei sähköverkon tai maakaasuverkon siirtämisestä toiselle verkonhaltijalle sovita, Energiavirasto voi päättää verkkoluvan siirtämisestä ja verkon lunastamisesta täyttä korvausta vastaan.

Ehdotetussa lain säännöksessä ehdotetaan säädettäväksi, että luvan peruuttaminen määrätään olemaan voimassa toiminnassa esiintyneiden puutteiden tai laiminlyöntien vakavuuteen suhteutetun määräajan kuitenkin enintään, kunnes tarvittavat toimet puutteen tai laiminlyönnin korjaamiseksi on toteutettu. Jos puutteita tai laiminlyöntejä ei ole korjattu määräajassa, valvova viranomainen voi määräajan päättymisen jälkeen päättää tai esittää päätettäväksi luvan ehtojen muuttamista toiminnan rajoittamiseksi tai luvan peruuttamista pysyvästi.

Energiavirasto ensinnäkin katsoo, että sähkö- ja maakaasuverkkoluvan peruuttaminen määräaikaisesti on käytännössä mahdotonta toteuttaa monopolitoimintaa harjoittavien toimijoiden osalta. Tällaiset toimijat eivät voi vain lopettaa toimintaansa, vaan toiminnot on siirrettävä toisen toimijan suoritettavaksi. Tämä edellyttää laajoja toimenpiteitä, joita ei lyhyen ajanjakson vuoksi ole tarkoituksenmukaista tehdä. Määräaikaisuuteen liittyy myös kysymys siitä, kuka esimerkiksi vastaa tilapäisesti toimintaa harjoittavan toimijan tekemistä tappioista. Energiavirasto katsoo, että ehdotetussa lainsäädännössä on huomioitava edellä mainitut toimijat ja tehtävä muutokset niin, että viranomainen voi ääritapauksessa päättää kokonaan luvan peruuttamisesta, jos NIS2-direktiivin implementointi tätä edellyttää. Kun sähkö- tai maakaasuverkkolupaa ei voida peruuttaa määräajaksi, tulisi sen ilmetä lain sanamuodosta ja sen perusteluista.

Toisekseen Energiavirasto tuo esiin, että edellä mainitussa valvontalaissa on säädetty edellytykset, milloin sähkö- tai maakaasuverkkolupa voidaan peruuttaa. Hallituksen esityksen luonnoksessa ei ehdoteta muutosta tai viittausta valvontalaissa säädettyihin luvan peruuttamista koskeviin säännöksiin. Energiavirasto katsoo, että perustelluinta olisi tehdä viittaukset molempiin säännöksiin (valvontalaki ja NIS2-yleislaki) ja väliaikaisuuteen liittyvät poikkeukset tulisi näkyä säännösmuutoksena.

Määräyksenantovaltuus toimitettavista tiedoista

Valvovalle viranomaiselle esitetään hallituksen esityksen luonnoksessa kolmea määräyksenantovaltuutta. Nämä koskevat 9 §:n mukaisten riskienhallinnan toimenpiteiden, 11 §:n mukaisten poikkeamailmoituksien ja 43 §:n toimijaluetteloon tietojen ilmoittamisen tarkempia teknisiä määräyksiä.

Energiavirasto ehdottaa, että ehdotettuun lakiin lisäksi esitetään viranomaiselle määräyksenantovaltuutta 27 §:n mukaisten tiedonsaantioikeuksien osalta. Kyseisen säännöksen mukaan valvovalla viranomaisella on tämän lain mukaisia tehtäviä suorittaessaan oikeus saada salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä tehtäviensä suorittamiseksi välttämättömät tiedot tässä laissa tarkoitetuilta toimijoilta. Valvovan viranomaisen

on tietopyynnössä ilmoitettava pyynnön tarkoitus sekä täsmennettävä pyydetyt tiedot. Tiedot on luovutettava viipymättä, viranomaisen pyytämässä muodossa ja maksutta.

Energiavirasto valvoo tällä hetkellä verkonhaltijoiden varautumissuunnittelua ja NIS-direktiivin mukaisia velvoitteita varautumissuunnitelmien toimittamisen kautta. Tällä hetkellä verkonhaltijat toimittamat suunnitelmat lain mukaan 3-5 vuoden välein. Energiaviraston tavoitteena on toteuttaa NIS2-velvoitteiden valvontaan samaan tapaan, jossa toimijat tietävät vuosivälin, kun tietoja tulee velvoitteiden täyttämisestä toimittaa valvovalle viranomaiselle. Tämä on valvonnan ennakoitavuuden ja toimijan oman vuosikellon sovittamiseksi tarpeen. Ehdotetussa hallituksen esityksessä ei ehdoteta määräajoin toimitettavista tiedoista. Energiavirasto näin ollen ehdottaa, että lain 27 §:ää täydennetään niin, että valvova viranomainen voisi antaa määräyksen määräajoin toimitettavista tiedoista, joilla toimija osoittaa NIS2-velvoitteiden noudattamisen.

Edellä mainittu edesauttaisi lisäksi sitä, että CER-direktiivin ja ehdotetun NIS2-direktiivin mukaisia velvoitteita voidaan jatkossa valvoa yhdessä, jos NIS2-velvoitteiden ja CER-velvoitteiden valvova viranomainen on sama taho. Hallituksen esityksen luonnoksessa on myös todettu, että kyberturvallisuusriskit eivät varsinaisesti erotu toimijoiden muusta riskienhallinnasta, mikä osaltaan perustelee velvoitteiden valvonnan yhdistämistä.

Toimijaluettelo

Energiavirasto kannattaa ehdotetun 47 §:n 2 momentin mukaista siirtymäsäännöstä, jonka mukaan lain 43 § toimijaluettelosta tulee voimaan 1. päivänä tammikuuta 2025. Energiavirasto katsoo, että toimijoille asetetut velvoitteet tunnistaa itsensä soveltamisalaan kuuluvaksi toimijaksi ja ilmoittautua valvovan viranomaisen toimijaluetteloon tulee koskea myös toimijoita, jotka katsotaan koostaan riippumatta soveltamisalaan annettavan valtioneuvoston asetuksen nojalla riippuen asetuksen sisällöllisistä ratkaisuista. Jos valtioneuvoston asetuksessa määritellään esimerkiksi kriteerit koostaan riippumattomille toimijoille, on toimijoilla itsellään paras tieto kriteeristön täyttymisestä.

Seuraamusmaksua koskevat huomiot

Hallituksen esityksen luonnoksessa ehdotetaan, että seuraamusmaksun NIS2-direktiivin velvoitteiden vastaisesta toiminnasta määräisi Liikenne- ja viestintäviraston yhteydessä toimiva seuraamuslautakunta, joka koostuisi valvovien viranomaisten nimeämistä jäsenistä. Hallinnollisen seuraamusmaksun enimmäismäärä 26 §:ssä tarkoitetulle keskeiselle toimijalle on 10 000 000 euroa tai 2 prosenttia toimijan edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. Hallinnollisen seuraamusmaksun enimmäismäärä muulle kuin keskeiselle toimijalle on 7 000 000 euroa tai 1,4 prosenttia toimijan edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

Esitysluonnoksessa seuraamusmaksujen määräämistä koskevan toimivallan osoittaminen seuraamusmaksulautakunnalle on arvioitu olevan esillä olleista vaihtoehdoista perustelluin, kun valvonta on järjestetty toimialakohtaisesti ja lautakunnassa on edustettuna jokainen valvova viranomainen. Esitysluonnoksen mukaan seuraamusmaksujen määräämiselle ennakoidaan olevan tarvetta harvoin, sillä valvovalla viranomaisella olisi käytössään useita toimivaltuuksia toimijoiden ohjaamiseksi ja velvoittamiseksi lain vastaisen toiminnan oikaisemisesta.

Energiavirasto kannattaa, että ehdotettua mallia seuraamusmaksulautakunnasta ja sen perustamisesta Liikenne- ja viestintäviraston yhteyteen.

CSIRT-yksikön tehtäviä koskevat huomiot

Energiavirasto toistaa aiemmin kohdassa 4 ”Raportointivelvoitetta koskevat huomiot” tarkemmin esitetyn näkemyksen CSIRT-yksikön ja valvovan viranomaisen välisistä tiedonsaantioikeuksista. Hallituksen esityksen luonnoksen mukaan poikkeamailmoituksen johdosta ohjeita tai neuvoja tarvittaessa voitaisiin antaa myös valvovan viranomaisen ja CSIRT-yksikön yhteistyönä. Ehdotetussa laissa ei kuitenkaan esitetä NIS-valvovalle viranomaiselle tiedonsaantioikeutta CSIRT-yksiköltä. Energiavirasto pitää tärkeänä, että ohjeita ja neuvoja voidaan antaa yhteistyössä CSIRT-yksikön kanssa sekä, että Energiavirasto saa tietoonsa ilmoitetun poikkeaman myötä CSIRT-yksikön antamista ohjeista lieventäviksi toimenpiteiksi, joilla toimija voi minimoida aiheutuneita haitallisia vaikutuksia. Energiavirasto katsoo, että poikkeamahallintaan liittyviä tiedonsaantioikeuksia tulisi uudelleen tarkastella edellä mainituilta osin, jotta ne eivät johda lain soveltamistilanteessa epätoivottuun lopputulokseen. Energiavirasto pitää tärkeänä, että ehdotetussa laissa turvataan ilmoitetun poikkeaman aikainen tiedonvaihto viranomaisten kesken, viranomaisten ja toimijoiden välillä sekä yhtenäinen tilannekuva.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Energiavirasto tunnistaa, että se kuuluu myös itse hallituksen esityksen luonnoksen soveltamisalaan julkishallinnon toimijana. Energiavirastolla ei tältä osin ole kommentoitavaa.

Verkkotunnusvälittäjiä koskevat huomiot

Energiavirastolla ei ole tähän aiheeseen kommentoitavaa.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Hallituksen esityksen luonnoksella ehdotetaan kumottavaksi sektorikohtaisesta sääntelystä NIS1-direktiivin täytäntöönpanemiseksi annettuja säännöksiä, koska säännökset olisivat jatkossa päällekkäisiä suhteessa uuteen NIS2-direktiivin täytäntöönpanemiseksi annettavaan lakiin ja NIS1-direktiivi on muutoinkin kumottu NIS2-direktiivillä. Energiavirasto kannattaa ehdotusta lainsäädännöllisten ristiriitojen välttämiseksi.

Vaikutustenarviointia koskevat huomiot

Vaikutukset energiatoimialaan

Hallituksen esityksen luonnoksessa todetaan, että energia- ja terveydenhuolto toimialat ylittivät keskiarvomaturiteetiksi määritetyn perustason Suomen Huoltovarmuuskeskuksen toimialojen kybermaturiteettiselvityksessä. Selvityksessä kuitenkin katsottiin, että alojen osalta uhka- ja riskitason vaikutus on arvioitu merkittäväksi eli aloilla on paljon toimintoja, jotka voidaan arvioida riskilähtöisesti merkittäviksi. Esitysluonnoksessa myös todetaan, että energia-alalla uhkatason merkitys toimialalle arvioidaan nousevaksi. Kypsyystaso arvioidaan yleisesti hyväksi ja erilaisiin uhkiin on varauduttu. Ala jakautuu kuitenkin korkean ja matalan kypsyystason toimijoihin ja tietoturvakulttuuri on vaihtelevaa toimijoiden välillä. Lisäksi on tunnistettu, että suuremmalla maantieteellisellä alueella toimivat organisaatiot ovat investoineet kyberturvallisuuteen paikkakuntakohtaisia toimijoita enemmän. NIS2-direktiivin velvoitteiden täyttäminen voi täten johtaa joillekin toimijoille suurempiin kustannusvaikutuksiin erityisesti sääntelyn piiriin tulevilla uusilla toimijoilla.

Energiavirasto jakaa hallituksen esityksessä edellä esiin nostetut seikat kustannusvaikutuksista. Energiavirasto myös katsoo, että alan kyberturvallisuuteen liittyvä riskienhallinta ja kyberresilienssi ovat keskeisessä asemassa yhteiskunnan toiminnan kannalta kriittisten toimintojen jatkuvuuden turvaamisessa energiasektorin ollessa läheisesti kytköksissä muihin toimialoihin. Tätä vasten, vaikka energiatoimialalla NIS2-direktiivin soveltamisalan piiriin tulee paljon uusia toimijoita, Energiavirasto katsoo ehdotetut riskienhallinta- ja raportointivelvoitteet perustelluiksi ehdotetuin laajuuksin.

Valvovan viranomaisen resurssit

Hallituksen esityksen luonnoksessa on tunnistettu, että velvoitteiden valvonnasta aiheutuu lisäresurssitarpeita valvoville viranomaisille. Valvontatehtävä edellyttäisi lisäresursseja jokaisessa valvovassa viranomaisessa, koska valvottavien toimijoiden määrä kasvaa kunkin valvovan viranomaisen valvontatoimialalla ja viranomaiselta edellytetään NIS1-direktiivin valvontaa pidemmälle menevää kyvykkyyttä valvontatoimintaan. Verrattuna NIS1-direktiivin aikaisiin riskienhallintavelvoitteisiin, ehdotetussa laissa säädettäisiin yksityiskohtaisemmin osa-alueista, jotka riskienhallinnassa on huomioitava. Lisäksi riskienhallinta- ja raportointivelvoitteita sovellettaisiin NIS1-direktiiviä laajempaan joukkoon toimijoita. NIS2-direktiivissä esitettyjen muutosten myötä energiasektorilla soveltamisalaan kuuluvien toimijoiden määrä kasvaa merkittävästi siitä, mitä toimijoita Suomessa on NIS1-direktiivin nojalla tunnistettu keskeisiksi.

Ehdotetun lain 25 §:n mukaan Energiaviraston valvontavastuulle ehdotetaan seuraavia toimialoja ja toimijatyyppejä: sähkö, kaukolämmityksen tai kaukojäähdytyksen haltijat, kaasu (jakelu- ja siirtoverkonhaltijat). Energiavirasto lisäksi on katsonut, että viraston valvontaan tulisi kuulua myös vedyn siirtoa harjoittavat toimijat. Toimijat jaetaan kahteen kategoriaan: keskeiset ja tärkeät toimijat.

Tilastokeskuksen tietokannasta voi tehdä toimialaluokituksen perusteella haun, jonka tuloksena saa yritysten määrän henkilöstön ja liikevaihdon mukaisesti suuruusluokittain. Taseen loppusummasta ei

ole saatavilla vastaavaa tilastotietoa, ja tulokset perustuvat yhden tilikauden tietoihin. Siten saadut tulokset ovat ainoastaan viitteellisiä. Tulos edellyttää, että yritys on ilmoittanut päätoimialakseen hakua vastaavan toimialan. Vuoden 2022 tietojen perusteella tulos päätoimialalta ”sähkö-, kaasu- ja lämpöhuolto, jäähdytysliiketoiminta” on seuraava: yrityksiä on yhteensä noin 1450 kappaletta. Näistä suurimmalla osalla eli 1204 yrityksellä on palveluksessaan 0-4 henkeä. Yrityksiä, joiden henkilöstön koko on 50-249, on yhteensä 38 ja yrityksiä, joiden henkilöstön koko on 250 tai yli, on 7 yritystä. Liikevaihtotietojen osalta yrityksiä, joiden liikevaihto oli 10 miljoonaa euroa tai yli oli 217 yritystä. Vastaava määrä 40 miljoonan euron osalta oli 88 yritystä, joista ainakin 26 yrityksellä oli 200 miljoonan euron liikevaihto tai yli.

Energiavirasto on alustavasti tunnistanut, että sen valvonnan alaan esitetyissä toimijoissa on mukana toimijoita, jotka voisivat täyttää koosta riippumattomien toimijoiden edellytykset (ehdotetun lain 3 §:n 3 momentti) ja näin ollen kuulua ehdotetun lain soveltamisalaan koostaan riippumatta. Lisäksi CER-direktiivin myötä kriittisiksi tunnistetut toimijat kuuluvat ehdotetun lain soveltamisalaan keskeisinä toimijoina. Näin ollen Energiaviraston lopullinen valvottavien toimijoiden määrä on riippuvainen myöhemmin tehtävistä kansallisista ratkaisuista. Energiavirasto on kuitenkin kokonaisuutena arvioinut, että sen soveltamisalaan kuuluisi jatkossa uuden kansallisen NIS2-yleislain myötä määrällisesti aikaisempaa enemmän toimijoita, mahdollisesti keskeisiä toimijoita yli kaksinkertainen määrä aikaisempaan NIS1-valvottavien määrään verrattuna.

Lisäksi Energiavirasto tuo esiin, että se on tähän mennessä valvonut NIS1-direktiivin mukaisia velvoitteita ainoastaan sähkönverkonhaltijoiden ja maakaasun siirtoverkonhaltijan osalta. Hallituksen esityksen luonnoksessa Energiaviraston valvontaan ehdotetaan merkittävästi uudenlaisia toimijatyyppejä, joiden varautumisen ja kyberturvallisuuden valvonta ei ole aikaisemmin kuulunut Energiaviraston toimivaltaan. Näitä ovat esimerkiksi kaukolämmitys- ja kaukojäähdytystoimijat, muut sähkötoimialan toimijat kuin verkonhaltijat sekä maakaasun jakeluverkonhaltijat.

Energiavirasto katsoo, että NIS2-direktiivin myötä kyberturvallisuusvelvoitteiden valvonta muuttuu aiempaa yksityiskohtaisemmaksi ja viranomaisen valvontatoimivaltuudet laajenevat. NIS2-direktiivin myötä tulevat uudet - syvällisempää alan tuntemusta edellyttävät - tehtävät tarvitsevat valvovilta viranomaisilta sekä lisäresursseja, että koulutusta ja osaamisen kehittämistä. Lisäksi hallituksen esityksen luonnoksessa ehdotetaan valvoville viranomaisille uusia tehtäviä liittyen kriisinhallintaviranomaisena toimimiseen sekä seuraamusmaksulautakuntaan.

Ehdotetun lain mukaan poikkeamailmoittaminen on NIS2-direktiivin mukaisesti kolmivaiheinen. Ehdotetun lain mukaan valvovan viranomaisen on vastattava poikkeamailmoituksen tehneelle taholle viivytyksettä. Vastauksessa on oltava alustava palaute merkittävästä poikkeamasta sekä ohjeet merkittävän poikkeaman ilmoittamisesta esitutkintaviranomaiselle, jos asiassa epäillään rikosta. NIS2-direktiviin mukaisesti ehdotetun lain mukaan valvovan viranomaisen on otettava vastaan toimialallaan vapaaehtoisia poikkeamailmoituksia merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti-tilanteista myös muilta kuin ehdotetussa laissa tarkoitetuilta toimijoilta. Tilastokeskuksen vuoden 2022 tietojen perusteella päätoimialalla ”sähkö-, kaasu- ja lämpöhuolto, jäähdytysliiketoiminta” yrityksiä on yhteensä noin 1450 kappaletta. Vapaaehtoisen ilmoituskanavan

hyödyntämisasteesta riippuen Energiavirasto katsoo kanavan voivan merkitä lisäresursointitarvetta tavanomaisten valvontatehtävien lisäksi.

Energiavirasto nostaa esiin, että hallituksen esityksen luonnoksessa on todettu, että ”NIS1-direktiivissä omaksutusta kriittisten toimijoiden identifiointiprosessista luovuttaisiin ja velvoitteiden soveltamisala määriteltäisiin jatkossa toimijoiden toimialan ja koon perusteella. Toimijaluettelon keräämisessä hyödynnettäisiin toimijoiden omia ilmoituksia sekä olemassa olevia rekisteritietoja. Näiden tekijöiden arvioidaan vähentävän viranomaisille aiheutuvaa hallinnollista taakkaa verrattuna NIS1-direktiivin nojalla tapahtuvaan valvontaan. Valvovalla viranomaisella olisi lisäksi mahdollisuus kohdentaa valvontaa riskiperusteisesti sekä asettaa tehtäviään tärkeysjärjestykseen, mikä vaikuttaisi valvonnasta aiheutuviin kustannuksiin viranomaisessa. Toisaalta yleisesti sovellettaviin sektorisäännöksiin verrattuna NIS2-sääntelyn keskittäminen uuteen yleislakiin voi lisätä velvoitteiden soveltamisalaa koskevan neuvonnan tarvetta.”

Yllä mainittu NIS1-direktiivin aikainen identifiointiprosessi ei pidä paikkaansa energiasektorilla. NIS1-direktiivin soveltamisalaan kuuluvia toimijoita koskevaan sektorilainsäädäntöön tehtiin muutokset, jotka määrittivät suoraan ja yksiselitteisesti velvoitteiden soveltamisalan. Energiavirastossa toimijoiden tunnistaminen NIS2-direktiviin mukaisesti ei ole resursseja vähentävä seikka vaan ennemmin lisäävä seikka, kun toimijoiden kuuluminen soveltamisalaan ei ole yhtä yksiselitteinen. Energiavirasto myös arvioi, että toimijat tulevat tarvitsemaan neuvontaa kuulumisestaan soveltamisalaan, mikä osaltaan tulee tuottamaan lisäresursoinnin tarvetta. Energiavirasto pitää tärkeänä, että se voi kohdentaa valvontaa riskiperusteisesti sekä asettaa tehtäviään tärkeysjärjestykseen. Energiavirasto kuitenkin katsoo, että valvonta muuttuu esitysluonnoksen myötä aiempaa yksityiskohtaisemmaksi ja valvottavien toimijoiden määrän kasvaessa jo ennestään niukkien viranomaisresurssien vuoksi lisäresursointi on ehdottoman tarpeen valvontatehtävien ja muiden valvovalle viranomaisille esitettyjen tehtävien hoitamiseksi.

Energiavirasto arvioi, että NIS2-direktiivin asianmukainen tehtävien hoitaminen edellyttää 2 lisä-htv:tä. Resurssiarviossa on huomioitu valvottavien toimijoiden lukumäärän kasvu, valvonnan laajeneminen sekä yksityiskohtaistuminen sekä nykytila, jossa Energiavirastolle resursoitu kyberturvallisuusosaaminen ei ole riittävällä tasolla NIS2-direktiivin mukaisten tehtävien asianmukaiseen hoitamiseen. Energiavirasto katsoo, että arvioidut pysyvät lisäresurssit vuodesta 2024 ovat ehdottoman tarpeen. Lisäksi mainittakoon, että Energiavirasto on myös arvioinut CER-direktiivistä aiheutuvia resurssitarpeita ja esittänyt erikseen arvion NCCS:n täytäntöönpanoon vaadittavista resursseista. NIS2- ja CER-direktiivien sekä NCCS:n täytäntöönpanosta Energiavirastolle tulevat tehtävät tukevat toisiaan ja nämä synergiahyödyt on jo huomioitu Energiaviraston resurssiarvioissa.

Lisäksi Energiavirasto toteaa, että uusien tehtävien toimeenpano sekä uusien toimijoiden valvonta voi edellyttää henkilöresurssien lisäksi virastolta myös ulkopuolisen asiantuntijaselvitysten teettämistä esimerkiksi kyberturvallisuuden alkukartoituksen muodossa.

Energiavirasto katsoo, että ehdotetun lain täytäntöönpanon myötä Energiaviraston on otettava käyttöön erillinen asiankäsittelyjärjestelmä, jossa voidaan käsitellä ja arkistoida sähköisesti TL III-luokiteltua materiaalia. Energiavirasto arvioi käsittelyjärjestelmän kertaluontoisen kustannusarvion olevan noin 0,4 M€ vuodelle 2024 sekä järjestelmän vuosittaiset ylläpitokustannukset 0,06 M€ vuodesta 2025 eteenpäin. Energiavirasto toteaa, että edellä mainitulle kustannustehokkaampi vaihtoehto olisi rakentaa viranomaisten yhteinen sähköinen järjestelmä, johon valvovat viranomaiset saavat käyttöoikeudet ja, jossa voi käsitellä TL III-luokiteltua materiaalia.

Lisäksi Energiavirasto arvioi, että toimijaluettelon vaatiman järjestelmän kehittäminen edellyttää kertaluontoista 20 000 € kustannusta vuonna 2024 ja vuodesta 2025 eteenpäin järjestelmän ylläpitokustannuksia 2500 € per vuosi olettaen, ettei toimijaluettelon ylläpito vaadi koodaustöitä.

Muut huomiot ja avoin palaute esityksestä

Velvoitteisen sisällyttäminen lain säännökseen

Hallituksen esityksen luonnoksen 6 §:n 4 momentin mukaisten yksityiskohtaisten perustelujen mukaan ”NIS2-direktiivin 37 artiklan 1 kohdan toisen kappaleen nojalla valvova viranomainen ei saisi kieltäytyä pyynnöstä, paitsi jos sillä ei ole lain nojalla toimivaltaa antaa pyydettyä apua, pyydetty apu ei ole oikeassa suhteessa valvovan viranomaisen valvontatehtäviin tai pyyntö koskee sellaisia tietoja tai käsittää sellaisia toimintoja, joiden paljastaminen tai toteuttaminen olisi vastoin Suomen kansalliseen turvallisuuteen, yleiseen turvallisuuteen tai puolustukseen liittyviä etuja. Ennen pyynnöstä kieltäytymistä valvovan viranomaisen olisi kuultava muita asianomaisia toimivaltaisia viranomaisia sekä, jos jokin jäsenvaltioista sitä pyytää, Euroopan unionin komissiota ja ENISAa.” Energiavirasto katsoo, että jälkimmäinen kuulemista koskeva edellytys ei käy ilmi lain säännöksestä ja tulisi lisätä säännöstekstiin. Velvoitteiden ja edellytysten tulisi käydä ilmi säännöksen sanamuodosta.

Samoin hallituksen esityksen luonnoksen 9 §:n 2 momentin 4 kohdan mukaisten yksityiskohtaisten perustelujen mukaan ”NIS yhteistyöryhmä, Euroopan komissio ja ENISA laativat NIS2-direktiivin 22 artiklan mukaisesti yhteistyössä riskiarviointeja tietyistä toimitusketjuista. Siltä osin, kuin tällaisia riskiarviointeja on laadittu, toimijoiden olisi hyödynnettävä riskiarvioita soveltuvin osin.” Tämä velvoite ei kuitenkaan käy ilmi lain sanamuodosta ja se tulisi Energiaviraston näkemyksestä lisätä esimerkiksi saman säännöksen 5 momenttiin.

Lopuksi

Energiavirasto kiittää mahdollisuudesta lausua luonnoksesta hallituksen esitykseksi eduskunnalle kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. Energiavirasto katsoo, että esityksellä parannetaan yhteiskunnan toiminnan kannalta kriittisten toimijoiden ja keskeisten palveluiden kyberturvallisuutta sekä kyberhäiriöiden sietokykyä ja kykyä palautua

kyberhyökkäyksistä tai muista tietojärjestelmiin ja viestintäverkkoihin haitallisesti vaikuttavista häiriöistä.

Energiavirasto kannattaa useita kansallisessa säädösvalmistelussa tehtyjä ratkaisuja ja Energiavirasto katsoo esityksen olevan päälinjoiltaan perusteltu ja yhdenmukainen NIS2-direktiivin kanssa. Energiavirasto on tuonut lausunnossaan kuitenkin esiin joitain epäkohtia ja täydennystä vaativia seikkoja, jotka vaativat vielä osaltaan työstämistä. Näistä suurimpina huomioina mainittakoon soveltamisalaan ja valvonnan kohdentamiseen liittyvät huomiot sekä viranomaisten väliseen tiedonvaihtoon liittyvät seikat.

Energiavirasto lisäksi korostaa, että valvovan viranomaisen lisäresurssitarpeet ovat ehdottoman kriittisiä ehdotetun lain täytäntöönpanolle. Energiavirastolle nykytilassa resursoitu kyberturvallisuusosaaminen ja henkilöstömäärä eivät ole riittävällä tasolla NIS2-direktiivin mukaisten tehtävien asianmukaiseen hoitamiseen ja valvonnan järjestämiseen.

Nurmi Simo
Energiavirasto

Koivula Minna
Energiavirasto