Puolustusvaliokunta
PuV@eduskunta.fi

Asiantuntijalausunto puolustusvaliokunnalle valtioneuvoston kirjelmästä eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS2-muutosdirektiiviksi (U 17/2026 vp)

Puolustusvaliokunta on pyytänyt Liikenne- ja viestintävirastolta lausuntoa valtioneuvoston kirjelmästä eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS2-muutosdirektiiviksi (U 17/2026 vp). Liikenne- ja viestintävirasto kiittää mahdollisuudesta lausua asiassa ja esittää lausunnossaan seuraavaa:

Liikenne- ja viestintävirasto tukee kirjelmässä esitettyjä huomioita ja toteaa yhtyvänsä valtioneuvoston kantaan. Kyberturvallisuus on keskeinen osa Suomen kokonaisturvallisuutta, ja kyberturvallisuuden merkitys on korostunut entisestään nykyisessä turvallisuusympäristössä. Liikenne- ja viestintävirasto pitää tärkeänä, että kyberturvallisuutta koskevia kyvykkyyksiä ja resilienssiä lisätään kaikilla yhteiskunnan osa-alueilla. Muun muassa EU:n yhteisen sisämarkkinan pirstaloitumisen ehkäisemiseksi on keskeistä, että myös kyberturvallisuuden kannalta keskeisistä osa-alueista säädetään unionin tasolla. Liikenne- ja viestintävirasto pitää perusteltuna, että nyt käsillä olevassa säädösehdotuksissa on keskitytty erityisesti EU:n kyberturvallisuusvirasto (ENISA:n) tehtäviin, EU:n yhteiseen sertifiointikehykseen, ICT-toimitusketjujen turvallisuuteen sekä NIS2-direktiiviä (kyberturvallisuusdirektiivi) koskeviin muutoksiin erityisesti soveltamisalan laajentamisen näkökulmasta.

Liikenne- ja viestintävirasto haluaa muistuttaa, että sääntelyehdotukset pitävät sisällään myös lukuisia uusia osa-alueita ja tehtäviä kansallisille viranomaisille. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimii uutta asetusehdotusta sivuten jo tällä hetkellä muun muassa kansallisena kyberturvallisuuden sertifiointiviranomaisena sekä valvoo digitaalisen infrastruktuurin ja palveluiden sekä julkishallinnon osalta myös ICT-toimitusketjujen turvallisuutta. On kuitenkin selvää, että Liikenne- ja viestintävirasto ja sen Kyberturvallisuuskeskus, taikka mikään muukaan suomalainen viranomainen, ei kykene hoitamaan mahdollisia uusia ja laajennettuja kyberturvallisuutta koskevia viranomaistehtäviä nykyisellä resursoinnilla.

Liikenne- ja viestintävirasto muistuttaa, että virastossa sijaitsevalla Kyberturvallisuuskeskuksella on korvaamaton rooli suomalaisessa yhteiskunnassa. Kyberturvallisuuskeskuksen luottamukseen perustuvaa viranomaisroolia niin elinkeinoelämän kuin muiden viranomaisten kanssa tehtävässä yhteistyössä on rakennettu jo yli vuosikymmen. Kyberturvallisuuskeskuksen yhtenä keskeisimpänä ydintehtävänä on kyberturvallisuuden tilannekuvan tuottaminen ja jakaminen suomalaisessa yhteiskunnassa. Kyberturvallisuuden kehittynyttä tilannekuvaa

hyödynnetään aina suurten suomalaisten yritysten toiminnasta maanpuolustuksen tarpeisiin. Liikenne- ja viestintävirasto pitää välttämättömänä, että Kyberturvallisuuskeskuksen asemaa vahvistetaan viranomaisten välisessä yhteistyössä ja samalla vaalitaan kansainvälisestikin vertaillen Kyberturvallisuuskeskuksen poikkeuksellisen läheistä yhteistyötä suomalaisen elinkeinoelämän kanssa.

Ehdotus kyberturvallisuusasetukseksi (CSA2)

ENISA:n muuttuva tehtävät

ENISA:lle ehdotetut tehtävät tulevat kasvattamaan viraston tehtävämäärää merkittävästi nykyisestä. Liikenne- ja viestintävirasto korostaa, että tehtävämäärän kasvuun liittyy perusteltu huoli toiminnan resursoinnista. Liikenne- ja viestintävirasto katsoo, että ENISA:n toiminnan resursoinnin tulisi kasvaa samassa suhteessa uusien tehtävien kanssa. Liikenne- ja viestintävirasto muistuttaa, että ENISA:n tehtäväkentän tulisi tuottaa konkreettista lisäarvoa jäsenvaltioille sekä EU:n muille toimielimille ja virastoille. Tämän osalta on myös syytä välttää päällekkäistä toimintaa ENISA:n ja jäsenvaltioiden kesken sekä esimerkiksi ENISA:n ja EU:n kyberkompetenssikeskuksen (ECCC) välillä. Esimerkiksi on hyvä huomioida, että osaamisen kehittämisen teema näkyy ENISA:n lisäksi myös ECCC:n työssä, ja sillä on mm. Koordinointikeskusten (NCC) henkilöstöstä koostuva skills-työryhmä. On tärkeää varmistaa ettei näiden osalta ole päällekkäisyyksiä ENISA:n kanssa, vaan työ olisi ennemminkin täydentävää. Liikenne- ja viestintävirasto pitää tärkeänä, että ENISA:n toimintaa ja mahdollista resurssivajetta ei korjata yksinomaan lisäämällä kansallisten asiantuntijoiden (SNE) määrää, vaan ensisijaisesti ENISA:n oman budjetin lisäyksillä.

Liikenne- ja viestintävirasto pitää tärkeänä, että asetusehdotuksessa vahvistetaan entisestään EU:n laajuisten kyberturvallisuusverkostojen, CSIRT-verkosto ja CyCLONe-verkosto, toimintaa. Verkostoilla on keskeinen merkitys jäsenvaltioiden kyberturvallisuutta koskevassa tiedonvaihdossa. ENISA:n rooli korostuu nimenomaisesti verkostojen toiminnan mahdollistamisessa sekä tarvittaessa toiminnan koordinointina.

Sertifiointi

Liikenne- ja viestintävirasto pitää valtioneuvoston kannassa kuvatusti tärkeänä, että eurooppalaisen kyberturvallisuuden sertifiointikehystä uudistetaan, tehostetaan ja selkeytetään. Liikenne- ja viestintävirasto pitää valtioneuvoston tavoin tärkeänä, että jäsenvaltioilla on mahdollisuus osallistua sertifiointikehyksen prosesseihin. Liikenne- ja viestintävirasto näkee, että jäsenvaltioilla tulee olla mahdollisuus vaikuttaa toimeenpanosäädösten sisältöön ja hyväksymiseen.

Liikenne- ja viestintävirasto katsoo, että sertifiointijärjestelmien kehityksessä ja käyttöönotossa tulee mahdollisuuksien mukaan tukeutua jo olemassa oleviin eurooppalaisiin ja kansainvälisiin standardeihin. Muutoin riskinä saattaa olla se, että syntyy paljon uusia teknisiä spesifikaatioita, jotka ovat käytössä vain tietyissä sertifioinneissa, mutta ei laajemmin yhteiskunnan eri toimialoilla ja toiminnoissa.

Liikenne- ja viestintävirasto katsoo, että sääntelyn tulisi luoda selkeät vakioprosessit sertifiointijärjestelmän valmistelulle. Liikenne- ja viestintävirasto pitää ehdotettuja toimia sertifiointijärjestelmän kehittämiseksi pääasiassa positiivisena, mutta sertifiointijärjestelmien kehitykselle asetettavan määräajan osalta tulisi olla mahdollisuus tapauskohtaiseen arvioon sekä joustoon tarvittavasta ajasta kiinteän 12 kuukauden määräajan sijasta.

Asetusehdotus mahdollistaa, että arviointilaitokset voivat tarvittaessa hakea kyberturvallisuussertifiointia koskevaa valtuutusta myös toisesta jäsenvaltiosta. Liikenne- ja viestintävirasto pitää rajat ylittäviä avunanto- ja tukimahdollisuuksia tärkeänä, koska erityisesti pienimmissä jäsenvaltioissa, ml. Suomi, ei välttämättä ole kaikissa tilanteissa riittäviä resursseja tai kyseessä olevaan valtuutukseen liittyvää erityisosaamista käytettävissä. Esimerkiksi Suomessa sertifiointiviranomaisen eli Liikenne- ja viestintäviraston nykyisten resurssien suhteen on odotettavissa tilanteita, joissa rajat ylittävä avuntarve voisi tulla kyseeseen. Ottaen huomioon vallitsevan resurssitilanteen, niin Liikenne- ja viestintävirasto pitää kannatettavana mahdollisuutta pyytää ENISA:lta tukea sertifiointijärjestelmien kansallisessa täytäntöönpanossa.

Liikenne- ja viestintävirasto korostaa, että sertifiointien käyttöä selkeyttää asetusehdotuksen kohdat, jotka koskevat sertifiointien hyödyntämistä eri EU-säädösten vaatimusten osoittamiseksi. Lisäksi on syytä muistuttaa, että virasto suhtautuu positiivisesti sertifioinnin vapaaehtoisuuteen myös tulevaisuudessa.

Toimitusketjujen turvallisuus

Liikenne- ja viestintävirasto pitää tärkeänä, että asetusehdotuksessa kiinnitetään erityistä huomiota ICT-toimitusketjujen turvallisuuteen sekä ICT-infrastruktuurin keskeisten sekä kriittisten osien tunnistamiseen. Toimitusketjujen turvallisuuteen on kiinnitetty EU:n tasolla huomiota jo vuonna 2020 annetussa 5G-keinovalikoimassa sekä alkuvuodesta 2026 annetussa ICT-toimitusketjujen turvallisuutta koskevassa keinovalikoimassa. Liikenne- ja viestintävirasto muistuttaa, että asetusehdotuksessa vahvistetaan monelta osin aikaisempien keinovalikoimien sisältö niin strategisten kuin teknisten riskien hallitsemiseksi ICT-toimitusketjussa. Toimitusketjujen turvallisuus nousee esille myös keväällä 2025 voimaan tulleessa kyberturvallisuuslaissa, jonka tarkoituksena on vahvistaa kriittisen infrastruktuurin toimijoiden kyberturvallisuutta.

Liikenne- ja viestintävirasto katsoo, että niin Suomessa kuin EU:n tasolla on pitkät perinteet teknisten riskien hallitsemisesta. Tämän vuoksi on ensiarvoisen tärkeää, että asetusehdotuksen mukaisessa erityisesti ei-teknisiin riskeihin kohdistuvassa riskienhallinnassa painotetaan myös strategisten riskien hallintaa ja muun muassa sen varmistamista, että ICT-toimitusketjuissa ei käytettäisi korkean riskin laitevalmistajien tuotteita tai laitteita. Liikenne- ja viestintävirasto muistuttaa, että strategisten riskien kuvaamisessa sekä korkean riskin laitevalmistajien tunnistamissa tulee taata jäsenvaltioille tehokkaat osallistumismahdollisuudet. Liikenne- ja viestintävirasto kiinnittää huomiota myös siihen, että unionin koordinoitu riskiarvio tulisi laatia kuudessa kuukaudessa tai niin sovittaessa tätä lyhyemmässä ajassa. Aikataulu voi osoittautua haastavaksi huomioiden riskiarvion sisällölle esitetyt vaatimukset. Lopuksi tulisi varmistaa, että asetusehdotuksen vaatimus valvovien viranomaisten itsenäisyydestä ja kiellosta saada

ohjeistusta muilta viranomaisilta ei saisi estää eri viranomaisten välistä yhteistyötä ja tiedonvaihtoa ICT-toimitusketjujen turvallisuuteen liittyen.

NIS2-muutosdirektiivi

Liikenne- ja viestintävirasto toteaa, että U-kirjelmässä esitetty valtioneuvoston kanta on NIS2-muutosdirektiivin osalta perusteltu ja kannatettava.

Yksityiskohtaisempana huomiona virasto toteaa ENISA:n uuteen tehtävään liittyen, että ENISA:n ylläpitämän toimijarekisterin ennakoiva laajentaminen vain päätoimipaikan perusteella valvottavista toimijoista kaikkiin NIS2-direktiivin soveltamisalassa oleviin toimijoihin olisi kuitenkin hyvin merkittävä muutos. Esitys näyttäisi johtavan käytännössä siihen, että ENISA:n laajennettu rekisteri sisältäisi tiedon kaikkien jäsenmaiden kaikista keskeisistä ja tärkeistä NIS2:n piiriin kuuluvista toimijoista. Se kattaisi siis myös kaikki sellaiset toimijat, jotka eivät tarjoa palveluja rajat ylittävästi, joten muutos ei olisi kaikilta osin oikeasuhtainen eikä perusteltu suhteessa esitettyihin tavoitteisiin rajat ylittävien kyberturvallisuusriskien osalta.

Liikenne- ja viestintävirasto Traficom