Lausunto

Päivämäärä: 2.3.2026

Eduskunnan talousvaliokunta

HE 2/2026 vp Hallituksen esitys eduskunnalle laiksi julkisista hankinnoista ja käyttöoikeussopimuksista annetun lain muuttamisesta ja siihen liittyviksi laeiksi

Eduskunnan talousvaliokunta on pyytänyt liikenne- ja viestintäministeriöön sijoitetulta valtion kyberturvallisuusjohtajalta kirjallista asiantuntilausuntoa hallituksen esityksestä eduskunnalle laiksi julkisista hankinnoista ja käyttöoikeussopimuksista annetun lain muuttamisesta ja siihen liittyviksi laeiksi (HE 2/2026 vp). Liikenne- ja viestintäministeriö kiittää mahdollisuudesta lausua asiassa ja toteaa lausuntonaan seuraavasti:

Hankintalain uudistuksen tavoitteita voidaan pitää yleisellä tasolla kannatettavina. Kyberturvallisuuden näkökulmasta esityksen keskeisin ongelmakohta liittyy sidosyksiköitä koskevaan 10 prosentin omistusosuusrajoitukseen, joka todennäköisesti heikentäisi julkisen sektorin ja erityisesti pienten sekä keskisuurten kuntien ICT-palveluiden kyberturvallisuutta, jatkuvuutta ja kustannustehokkuutta.

Kybertoimintaympäristön muutos ja julkisen sektorin kyvykkyys

Kybertoimintaympäristö on muuttunut pysyvästi: uhkakenttä laajenee, häiriöt realisoituvat nopeasti ja valtiollinen toiminta on entistä keskeisempi osa vaikuttamista yhteiskuntien toimintakykyyn. Tämä korostaa tarvetta riittävälle pitkäjänteiselle kehittämiselle, rakenteille ja osaamiselle, jotka tukevat tilannekuvaa, jatkuvuutta ja kyvykkyyksien yhteiskäyttöä.

Kunnissa kyberturvallisuus on erottamaton osa ICT-palveluiden järjestämistä. Pienillä ja keskisuurilla kunnilla on usein suurimmat haasteet osaamisessa ja resursoinnissa, ja toimivimmat tulokset on saavutettu vapaaehtoisen alueellisen yhteistyön kautta.

Vuosien sidosyksikköyhteistyön merkitys ja kyvykkyyksien yhteiskäytön tehokkuus on todennettu kansallisissa kyberturvallisuusharjoituksissa, joissa eri toimijoiden välistä osaamista, yhteistyötä ja prosesseja on testattu. Vaikuttavinta kuntien ja sidosyksiköiden välistä yhteistyötä ja kyvykkyyksien kasvua on syntynyt alueille, joilla on paljon pieniä kuntia, markkinatarjonta on vähäistä ja kuntien omat voimavarat ovat rajalliset. Esimerkkeinä ICT-sidosyksiköt Lapissa (LapIT Oy), Pohjois-Pohjanmaalla (Joki ICT Oy) sekä Etelä- ja Pohjois-Karjalassa (Meidän IT ja talous Oy). On myös huomioitava, että vaikuttava sidosyksikköyhteistyö ei koske pelkästään kuntia vaan myös hyvinvointialueita.

Olisikin toivottavaa, että kuntien ICT-palveluiden järjestämisessä rakennettaisiin entistä suurempia kokonaisuuksia. Se auttaisi varmistamaan riittävän korkean laadun ja kyberturvallisuuden tason.

Esitetyn sidosyksikkörajoituksen vaikutukset kyberturvallisuuteen

Palvelurakenteen sirpaloituminen: turvallisuusaukkojen riski kasvaa, kun kokonaisuus jakautuu useille toimijoille ja sopimusrajapinnoille, jotka heikentävät nykyisellään eheää kyberturvallisuuden- ja jatkuvuudenhallintaa.

Siirtymävaiheiden haavoittuvuus: toimittaja- ja järjestelmämuutokset ovat tyypillisesti vaihe, jossa hyökkääjät pyrkivät hyödyntämään epäselviä vastuita, keskeneräisiä kontrolliketjuja ja käyttöönottojen riskejä.

Osaamisen ja kyvykkyyden heikkeneminen: nykyisissä yhteistyörakenteissa kriittinen osaaminen on yhteiskäytössä ja skaalautuu omistajille; rakenteiden purkautuessa osaamisvaje korostuu ja henkilöstön saatavuus muodostuu pullonkaulaksi.

Kustannus- ja saatavuusriskit: erityisesti vaativat, jatkuvat kyberturvallisuuspalvelut, kuten ympärivuorokautinen valvonta, voivat muodostua huomattavasti kalliimmiksi, jos ne joudutaan järjestämään hajautetusti tai markkinoilta ilman riittävää hankinta- ja turvallisuusosaamista.

Vaikutukset eivät jää yksittäisiin hankintayksiköihin: Jos kyberturvallisuudessa ja niihin liittyviin häiriöihin varautumisessa syntyy vakavia puutteita, seuraukset heijastuvat palveluihin, kansalaisiin ja laajemmin yhteiskunnan toimintakykyyn, josta korjausvastuu kohdistuu viime kädessä myös valtiolle.

Seurauksena syntyisi rakenteellinen haavoittuvuus: Kokonaisuuteen jäisi väistämättä heikkoja kohtia, jos vastuu ja hallinta pirstaloituvat useille toimijoille ja poikkeamatilanteessa reagointi on hidasta sekä epäselvää.

Huomioita alueellisista ICT-sidosyksiköistä

Alueelliset ICT-sidosyksiköt ovat käytännössä mahdollistaneet pienille ja keskisuurille kunnille sellaisia ICT- ja kyberturvallisuuskyvykkyyksiä, joita ne eivät yksin kykene rakentamaan, kuten yhteishankinnat, osaamisen keskittäminen, jatkuvuudenhallinta ja pitkäjänteiset investoinnit. Useissa alueellisissa kokonaisuuksissa yhteistyön mittakaava (useita kymmeniä omistajia) on ollut nimenomaan vaikuttavuuden ja kyberturvallisuuden edellytys.

Tällaiseen rakenteeseen kohdistuva 10 prosentin omistusosuusrajoitus purkaisi optimaalisen yhteistyömallin, joka koskisi myös sidosyksiköihin jääviä suurempia toimijoita, koska skaalaedut pienenevät ja optimaalinen yhteistyörakenne purkautuisi.

Ratkaisuehdotukset kyberturvallisuuden näkökulmasta

Luovutaan ICT-sidosyksiköitä koskevasta 10 prosentin omistusosuusrajoituksesta siltä osin kuin se heikentää alueellisten ICT-sidosyksiköiden toimintaedellytyksiä ja kuntien kyberturvallisuutta.

Tehdään alueellisten ICT-sidosyksiköiden osalta yksityiskohtaisempi poikkeus, jolla turvataan erityisesti pienten kuntien asema ja säilytetään alueelliset sidosyksiköt elinkelpoisina. 10 % omistusosuusrajoitusta ei sovellettaisi maantieteellisen toiminta-alueen tai väestöpohjan perusteella.

Siirtymäaikaa pidennetään merkittävästi ja mitoitetaan se ICT- ja kyberturvallisuusriskien hallinnan ehdoin. Siirtymäajan tulee olla riittävän pitkä, jotta muutoskustannuksia, sopimuskatkoja, kyberturvallisuusriskejä ja jatkuvuudenhallinnan heikentymistä voidaan ehkäistä. Siirtymäajan tulisi olla vähintään 4 vuotta lain voimaantulosta ja lisäksi olisi mahdollistettava perustellusta syystä 2–3 vuoden lisäsiirtymäaika.

Lopuksi

Erityisesti nykyisessä geopoliittisessa tilanteessa kyberturvallisuuden kannalta keskeistä on turvata sellaiset rakenteet, joissa osaaminen, jatkuvuus ja kyberturvallisuus ovat aidosti johdettavissa kokonaisuutena ja skaalautuvat myös pienille toimijoille. HE 2/2026 vp:n käsittelyssä tulisi varmistaa, ettei sääntelyllä synnytetä kyberturvallisuuden kannalta heikompaa ja kalliimpaa palvelurakennetta tai altisteta julkista sektoria tarpeettomille siirtymävaiheen riskeille.

Rauli Paananen
Valtion kyberturvallisuusjohtaja
Valtion kyberturvallisuusjohtajan toimisto