Valiokunnan lausunto LiVL 10/2026 vp– U 17/2026 vp

Liikenne- ja viestintävaliokunta

Valtioneuvoston kirjelmä eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS 2-muutosdirektiiviksi

Suurelle valiokunnalle

JOHDANTO

Vireilletulo

Valtioneuvoston kirjelmä eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS 2-muutosdirektiiviksi (U 17/2026 vp): Asia on saapunut liikenne- ja viestintävaliokuntaan lausunnon antamista varten. Lausunto on annettava suurelle valiokunnalle.

Asiantuntijat

Valiokunta on kuullut:
- neuvotteleva virkamies Marième Korhonen-Cara, liikenne- ja viestintäministeriö
- hallitussihteeri Veikko Vauhkonen, liikenne- ja viestintäministeriö
- neuvotteleva virkamies Anna Saarela, oikeusministeriö
- neuvotteleva virkamies Antti Helin, valtiovarainministeriö
- johtava asiantuntija Tomi Kinnari, Liikenne- ja viestintävirasto
- lakiasiainjohtaja Vesa Vuoti, DNA Oy
- turvallisuusjohtaja Jaakko Wallenius, Elisa Oyj
- lakiasiainjohtaja Tuomas Latola, Huawei Technologies Finland Co. Ltd.
- senior legal counsel Mika Enäjärvi, Telia Finland Oyj
- lakimies Janne Hälinen, FiCom ry
- toimitusjohtaja Peter Sund, Finnish Information Security Cluster — Kyberala ry

Valiokunta on saanut kirjallisen lausunnon:
- Suomen Erillisverkot Oy

VALTIONEUVOSTON KIRJELMÄ

Ehdotus

Euroopan komissio antoi 20.1.2026 ehdotuksen (COM(2026) 11 final) Euroopan parlamentin ja neuvoston asetukseksi Euroopan unionin kyberturvallisuusvirasto ENISA:sta, Euroopan

kyberturvallisuuden sertifiointikehyksestä ja ICT-toimitusketjujen turvallisuudesta sekä asetuksen (EU) 2019/881 kumoamisesta (CSA2-ehdotus). CSA2-ehdotuksella kumotaan vuonna 2019 voimaan tullut Euroopan parlamentin ja neuvoston asetus (EU) 2019/881 Euroopan unionin kyberturvallisuusvirasto ENISA:sta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (kyberturvallisuusasetus, CSA).

Asetusehdotuksessa ehdotetaan EU:n kyberturvallisuusvirasto ENISA:n tehtävien selkeyttämistä ja päivittämistä kyberturvallisuuden uhkaympäristöön sopivaksi. Tulevaisuudessa ENISA:n toiminnan tavoitteena olisi vahvistaa EU:n ja jäsenmaiden kyberturvallisuutta, kyberresilienssiä ja luottamusta. Virasto toimisi koko unionin keskeisenä kyberturvallisuuden neuvonantajana ja asiantuntijakeskuksena. ENISA:n tehtävänä olisi muun muassa tukea jäsenvaltioita ja EU-toimielimiä kyberturvallisuuteen liittyvän EU-lainsäädännön ja politiikkojen kehittämisessä ja toimeenpanossa, vahvistaa kyberturvallisuusvalmiuksia ja resilienssiä koko EU:ssa, edistää operatiivista yhteistyötä ja tiedonvaihtoa, osallistua EU:n kyberturvallisuussertifiointijärjestelmän kehittämiseen ja ylläpitoon, sekä edistää kyberturvallisuusosaamista ja -koulutusta.

Kyberturvallisuusasetuksen uudistamisella on kaksi keskeistä tavoitetta: kyberturvallisuuden kyvykkyyksien ja resilienssin lisääminen sekä sisämarkkinoiden pirstaloitumisen ehkäiseminen. Tavoitteena on ensinnäkin vahvistaa Euroopan unionin kyberturvallisuuden hallinnointia sekä varmistaa, että asiaankuuluvilla toimielimillä, viranomaisilla ja muilla sidosryhmillä on paremmat edellytykset estää, havaita ja torjua kyberturvallisuusuhkia koordinoidulla ja tehokkaalla tavalla. Lisäksi kyberturvallisuusasetuksen uudelleentarkastelun tavoitteena on tukea unionin yhteisten kyberturvallisuusinstrumenttien kuten sertifiointijärjestelmien kehittämistä, täytäntöönpanoa ja käyttöönottoa sekä tarjota yhdenmukaistettuja keinoja rakentaa luottamusta ja yhteen toimivuutta jäsenvaltioiden välillä. Ehdotuksella pyritään kehittämään Euroopan kyberturvallisuuden sertifiointikehystä, ratkaisemaan kyberturvallisuuteen liittyviä monimutkaisia ja hajanaisia prosesseja, sekä puuttumaan lisääntyviin ICT-toimitusketjujen turvallisuusriskeihin. Tavoitteena on ICT-toimitusketjuihin, mukaan lukien viestintäverkkoihin, liittyvien ei-teknisten kyberturvallisuusriskien hallintatoimien yhdenmukaistaminen EU:ssa, joilla varmistettaisiin sisämarkkinoiden toiminta, edistettäisiin teknologista suvereniteettia ja vahvistettaisiin EU:n yhteistä kyberturvallisuuden ja resilienssin tasoa. Kyse olisi vähimmäistason velvoitteista. Jäsenvaltioiden olisi mahdollista asettaa ehdotuksen velvoitteiden tasoa korkeampia kansallisia toimenpiteitä, jotka ovat linjassa unionin oikeuden kanssa.

Valtioneuvoston kanta

Kyberturvallisuusasetus (CSA2)

Valtioneuvosto katsoo kyberturvallisuuden olevan olennainen osa EU:n sisämarkkinoiden häiriöttömän toiminnan ja yhteiskuntavakauden sekä kansalaisten yksityisyyden turvaamista. Valtioneuvosto kannattaa EU:n lainsäädännön tavoitetta vahvistaa kyberturvallisuuden hallinnointia sekä sitä, että asiaankuuluvilla toimielimillä, viranomaisilla ja muilla sidosryhmillä olisivat paremmat edellytykset estää, havaita ja torjua kyberturvallisuusuhkia koordinoidulla ja tehokkaalla tavalla. Valtioneuvosto suhtautuu myönteisesti Euroopan kyberturvallisuusvirasto ENISA:n mandaatin kokonaisvaltaiseen uudelleentarkasteluun muuttunut uhkaympäristö sekä

unionin kyberturvallisuuslainsäädäntö huomioiden. Valtioneuvosto katsoo, että ENISA:n toiminnan tulee olla tehokasta, priorisoitua ja läpinäkyvää. ENISA:n toiminnan ja tehtävien tulisi ensisijaisesti täydentää jäsenmaiden viranomaisten kyberturvallisuustehtäviä.

Valtioneuvosto suhtautuu myönteisesti ENISA:n toiminnan laajentamiseen operatiivisen yhteistyön tukeen sekä tilannekuvan tuottamiseen huomioiden kuitenkin, että ensisijainen vastuu kyberturvan tasoa varmistavissa ja yhteiskunnan toimijoita tukevissa viranomaistehtävissä on jäsenmailla ja sen viranomaisilla. Tiedonvaihtoon, jolla voisi olla negatiivisia vaikutuksia kansalliseen turvallisuuteen, suhtaudutaan varauksellisesti. Valtioneuvosto suhtautuu kuitenkin myönteisesti ENISA:n yhteistyön tiivistämiseen kumppanimaiden ja kansainvälisten organisaatioiden, kuten NATO:n kanssa.

Valtioneuvosto pitää ENISA:n tehtävien laajentamista tietojärjestelmähaavoittuvuuksien hallintaan liittyviin palveluihin erityisen tärkeänä. Unionin omien kyvykkyyksien vahvistaminen tietojärjestelmähaavoittuvuuksien hallinnassa vahvistaa unionin strategista autonomiaa.

Valtioneuvosto pitää tärkeänä, että jäsenmaat ja komissio ovat jatkossakin tasa-arvoisessa asemassa ENISA:n toimintaan liittyvässä päätöksenteossa. Jäsenmaiden tulee itse voida päättää viraston toimielimiin nimitettävistä edustajista sekä virastoon lähetettävistä asiantuntijoista.

Valtioneuvosto pitää tärkeänä, että tällä asetuksella ei ennakoida tulevan rahoituskehyksen (2028–2034) rahoitusta. Tulevan kauden rahoituksen mitoitukseen otetaan kantaa erikseen osana rahoituskehysneuvottelujen kokonaisuutta.

Valtioneuvosto korostaa, että EU:n toimielinten ja virastojen hallintomenojen taso sekä henkilöstömäärä on pidettävä maltillisena. Valtioneuvosto pyytää jatkovalmistelussa tarkennuksia ENISA:n keräämiin maksuihin ja toiminnan rahoittamiseen liittyen.

Valtioneuvosto suhtautuu kyberturvallisuuden osaamiseen liittyvän tarkemman sääntelyn kehittämiseen varauksellisesti. Valtioneuvosto pitää tärkeänä varmistaa, että osaamisen liittyvät toimenpiteet ovat jäsenvaltioille vapaaehtoisia ja resurssineutraaleja.

Valtioneuvosto tukee yleisesti eurooppalaisen kyberturvallisuuden sertifiointikehyksen uudistamista, tehostamista ja selkeyttämistä. Valtioneuvosto suhtautuu lähtökohtaisesti myönteisesti kybertason ja EU:n lainsäädännön vaatimustenmukaisuusolettaman sisällyttämistä sertifiointijärjestelmien soveltamisalaan. Lisäksi valtioneuvosto kannattaa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien ylläpitostrategian ja -toimien lisäämistä osaksi sertifiointikehystä. Valtioneuvosto pitää tärkeänä, että jäsenvaltioilla on mahdollisuus osallistua eurooppalaisen kyberturvallisuuden sertifiointikehyksen prosesseihin. Lisäksi valtioneuvosto katsoo, että sertifiointien tulee säilyä lähtökohtaisesti vapaaehtoisina.

Valtioneuvosto pitää kannatettavana, että EU:ssa haetaan ehdotuksen pohjalta yhteisiä ICT-toimitusketjuja koskevia ratkaisuja, jotka vahvistavat näiden turvallisuutta, edistävät sisämarkkinoiden toimintaa ja EU:n teknologista suvereniteettia. Toimenpiteiden tulee olla ennakoitavia ja hallittuja sekä perustua asianmukaiseen kuulemiseen ja vaikutusarviointiin. Valtioneuvosto katsoo, että ehdotuksessa esitettyjen toimenpiteiden tulee olla myös

oikeasuhtaisia ja riskiperustaisia. Valtioneuvosto pitää tärkeänä, että jäsenvaltiot voivat jatkossakin asettaa asetusehdotusta pidemmälle meneviä kansallisia velvoitteita ja toimenpiteitä, erityisesti viestintäverkkojen turvallisuuden varmistamiseksi. Valtioneuvosto tukee ehdotuksen tavoitetta ja pitää samalla tärkeänä, että unionin ja jäsenvaltioiden toimivallan rajat säilyvät selkeinä erityisesti kansallista turvallisuutta koskevissa asioissa. Valtioneuvosto myös korostaa jäsenvaltioiden keskeistä roolia ICT-toimitusketjujen riskien arvioinnissa.

Valtioneuvosto edellyttää, että komissiolle delegoitavat toimivaltuudet ovat tarkkarajaisia, oikeasuhtaisia, tarkoituksenmukaisia ja perusteltuja.

Suomen kantoja komission ja korkean edustajan tiedonantoon unionin taloudellisen turvallisuuden vahvistamiseksi on muodostettu selvityksessä E 3/2026 vp. Selvitys sisältää nyt kyseessä olevan ehdotuksen näkökulmasta olennaisen kirjauksen kansainvälisestä yhteistyöstä haitallisten riippuvuuksien vähentämiseksi:

Haitallisten riippuvuuksien vähentämiseksi EU:n tulee edetä nopeasti kauppaneuvotteluissa sekä kumppanuuksissa esimerkiksi kriittisten raaka-aineiden, teollisuuden, energian ja kriittisten teknologioiden toimitus- ja arvoketjuissa. EU:n tulisi kartoittaa standardipohjaisten markkinoiden luomisen edut ja mahdollisuudet ja panostaa sääntely-yhteistyöhön kolmasmaakumppaneiden kanssa. EU:n tulee hyödyntää unionin olemassa olevia välineitä laajasti myös kolmasmaayhteistyössä haitallisten riippuvuuksien purkamiseksi.

Lisäksi Suomen kantoja komission tiedonantoon osaamisunionista on muodostettu selvityksessä E 56/2025 vp, jonka osalta huomioidaan nyt kyseessä olevan ehdotuksen osalta seuraava kirjaus:

Suomi pitää tärkeänä, että komission ehdotukset perustuvat riittävän kattaviin vaikutusarviointeihin. Suomi korostaa, että EU-tason toimenpiteet on tärkeää suunnitella siten, että ne ovat kustannustehokkaita, eivät lisää hallinnollista taakkaa, huomioivat jäsenmaiden erilaiset koulutusjärjestelmät sekä työvoimapoliittiset painotukset ja hyödyntävät mahdollisimman paljon olemassa olevia rakenteita.

NIS 2 -muutosdirektiivi

Valtioneuvosto kannattaa muutosehdotuksien tavoitteita sääntelyn yksinkertaistamiseksi, sujuvoittamiseksi ja sääntelystä aiheutuvien hallinnollisten kustannuksien alentamiseksi. Valtioneuvosto suhtautuu myönteisesti muutosehdotuksiin, jotka edistävät näitä tavoitteita ja turvaavat samalla kyberturvallisuuden korkeaa tasoa.

Valtioneuvosto pitää tarpeellisena, että osana neuvotteluita arvioidaan tarkemmin ehdotuksen vaikutuksia sääntelystä toimijoille aiheutuviin kustannuksiin ja ehdotuksen tavoitteisiin.

Valtioneuvosto suhtautuu myönteisesti direktiivin soveltamisalaa koskeviin muutosehdotuksiin sekä ehdotukseen keskeisen toimijan kokorajan korottamisesta. Valtioneuvosto pitää tarpeellisena soveltamisalan tarkentamista erityisesti tuotantomäärältään vähäisten sähköntuottajien sekä kemianteollisuuden osalta. Valtioneuvosto pitää tarpeellisena, että neuvotteluissa arvioidaan yksityiskohtaisemmin komission ehdotusta strategisen

kaksikäyttöinfrastruktuurin omistajien ja operaattoreiden sisällyttämisestä direktiivin soveltamisalaan erityisesti maanpuolustuksen ja kansallisen turvallisuuden kannalta.

Valtioneuvosto pitää tärkeänä, että NIS 2 -direktiivin vaatimukset ovat oikeasuhtaisia ja riskiperusteisia. Valtioneuvosto suhtautuu alustavan varauksellisesti ehdotukseen komission toimivallasta täysharmonisoida riskienhallintatoimenpiteitä täytäntöönpanosäädöksillä. Valtioneuvosto pitää tarkoituksenmukaisena, että jäsenvaltioilla on riittävä kansallinen liikkumavara riskienhallintaa koskevien vaatimuksien asettamisessa.

Valtioneuvosto pitää lähtökohtaisesti hyvänä, että eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisia sertifiointeja voitaisiin hyödyntää NIS 2 -direktiivin vaatimustenmukaisuuden osoittamisessa.

Valtioneuvosto suhtautuu myönteisesti ehdotukseen ENISA:n tehtävästä laatia rajat ylittäviä kyberturvallisuusriskien arviointeja. Valtioneuvosto pitää kuitenkin tärkeänä, että ENISA:n toimivaltuus valvovien viranomaisten tukemisessa ja sitä koskevien tietojen saamisessa perustuu jäsenvaltion viranomaisen suostumukseen.

Valtioneuvosto suhtautuu alustavan varauksellisesti ehdotukseen kiristyshaittaohjelmatietojen ilmoittamiseen liittyviin uusiin velvollisuuksiin sekä ehdotukseen komissiolle siirretyn säädösvallan laajennuksesta kiristyshaittaohjelmatietojen ilmoittamista koskien. Valtioneuvosto pitää tältä osin tarpeellisena, että neuvotteluissa arvioidaan tarkemmin, miten ehdotus vaikuttaa sääntelystä toimijoille aiheutuviin kustannuksiin ja hallinnolliseen taakkaan.

VALIOKUNNAN PERUSTELUT

(1) Valiokunta pitää ehdotuksen sisämarkkinoiden toimivuutta ja kyberturvallisuuden edistämistä koskevia yleisiä tavoitteita hyvinä ja kannatettavina.

Kyberturvallisuusasetus (CSA2)

Kyberturvallisuusvirasto ENISA:n tehtävät. (2) Valiokunta yhtyy valtioneuvoston kantaan siitä, että ENISA:n toiminnan ja tehtävien tulisi ensisijaisesti täydentää jäsenmaiden viranomaisten kyberturvallisuustehtäviä. Valiokunta pitää tärkeänä, ettei ENISA:lle säädetä päällekkäisiä tehtäviä kansallisten viranomaisten kanssa. Valiokunta yhtyy myös valtioneuvoston kantaan, jonka mukaan ENISA:n toiminnan tulee olla tehokasta, priorisoitua ja läpinäkyvää. Lisäksi valiokunta pitää keskeisenä, että ENISA:n hallintomenojen taso ja henkilöstömäärä säilyvät maltillisina.

ICT-toimitusketjut. (3) Valiokunta pitää valtioneuvoston tavoin lähtökohtaisesti hyvänä, että EU:ssa haetaan sellaisia yhteisiä ICT-toimitusketjuja koskevia ratkaisuja, jotka vahvistavat turvallisuutta sekä edistävät sisämarkkinoiden toimintaa ja EU:n teknologista suvereniteettia. Valiokunta pitää sääntelyn taustalla olevia turvallisuushuolia perusteltuina ja pitää siten hyvänä, että EU:ssa pyritään kehittämään ICT-toimitusketjujen turvallisuuden hallintaan mekanismeja.

(4) Toimittajariskin huomioiminen lainsäädännössä ja konkreettiset toimenpiteet tämän riskin ehkäisemiseksi ovat saadun selvityksen mukaan edenneet vaihtelevasti eri jäsenvaltioissa. Valiokunta toteaa, että Suomessa on toteutettu tarvittavia lainsäädännöllisiä ja muita toimenpiteitä viestintäverkkojen turvallisuuden varmistamiseksi ja katsoo, että ehdotuksista ei tule koitua oman roolinsa hoitaneille jäsenvaltioille tarpeettomia kustannuksia. Valiokunta painottaa, että sääntelystä ei myöskään saa aiheutua koko Euroopan kilpailukykyä ja -asemaa heikentäviä vaikutuksia.

(5) Asiantuntijakuulemisessa ehdotettuja ICT-toimitusketjuja koskevia keinoja on pidetty ongelmallisina ja on katsottu, että ne voivat toteutuessaan heikentää innovaatioita ja viestintäverkkojen kehittämistä Euroopassa. Valiokunta pitää erittäin tärkeänä, että ehdotuksessa vaadittavista toimenpiteistä ei aiheudu viivästystä erityisesti 6G-verkkojen kehittämiseen ja käyttöönottoon Euroopassa.

(6) Valiokunnan saaman selvityksen mukaan ehdotuksen vaikutusarvioinnit ovat puutteellisia ja erityisesti kustannusvaikutukset on arvioitu huomattavasti todellisia kustannuksia alhaisemmiksi. Valiokunta pitää tärkeänä, että sääntelyn osalta arvioidaan perusteellisesti ehdotusten kilpailukyky-, investointi- ja kustannusvaikutukset.

(7) Matkaviestinverkkojen osalta asetusehdotus määrittelee nimenomaisesti 36 kuukauden siirtymäajan kiellettyjen ICT-komponenttien vaihtamiseksi. Valiokunta pitää saamansa selvityksen perusteella ehdotettua määräaikaa erittäin lyhyenä, ottaen huomioon laitteiden määrän ja viestintäverkkojen mittakaavan. Asiantuntijakuulemisessa ehdotusta on tältä osin pidetty epärealistisena ottaen huomioon myös sen, että kaikkien toimijoiden tulisi ryhtyä laitteiden vaihtamista koskeviin toimiin samassa aikataulussa.

(8) Valiokunta pitää riskiarviointia keskeisenä sekä sääntelyn toimivuuden että toimenpiteistä aiheutuvien kustannusten hallinnan kannalta. Toimenpiteiden ei tulisi lähtökohtaisesti kohdistua sellaisiin verkon osiin tai laitteisiin, joista ei todellisuudessa aiheudu sääntelyn perustana olevaa riskiä. Asiantuntijakuulemisessa on painotettu, että velvoitteiden tulee olla riskiperusteisia, suhteellisia, ennakoitavia ja käytännössä toimeenpantavissa.

(9) Asiantuntijakuulemisessa on arvioitu, että ehdotetut laitteiden korvaamista koskevat menettelyt ilman kustannusten korvausmekanismeja johtaisivat todennäköisesti myös huomattaviin korvausvaatimuksiin jäsenvaltioille.

(10) Valiokunta painottaa yleisesti kansallisen toimivallan ja päätösvallan tarvetta kansallista turvallisuutta koskevissa asioissa. Lisäksi valiokunta pitää tärkeänä, että sääntelyssä otetaan asianmukaisesti huomioon omaisuuden suoja ja muut perusoikeudet.

(11) Valiokunta katsoo, että komissiolle delegoitavia uusia toimivaltuuksia tulee arvioida kriittisesti ja varmistaa, että ne ovat tarkkarajaisia ja perusteltuja.

NIS 2 -muutosdirektiivi

(12) Valiokunta pitää hyvänä, että ehdotuksilla pyritään sääntelyn yksinkertaistamiseen ja toimijoiden hallinnollisen taakan sekä kustannusten vähentämiseen. Valiokunta pitää kuitenkin tärkeänä, että korkea turvallisuuden taso säilytetään sääntelyn osittaisesta keventämisestä huolimatta.

(13) Valiokunnan saaman selvityksen mukaan komission riskienhallintatoimia koskevat täytäntöönpanoasetukset olisivat jatkossa täysharmonisoivia. Valiokunta katsoo, että jäsenvaltioilla voi jatkossakin olla selkeä tarve asettaa tarvittaessa pidemmälle meneviä kansallisia velvoitteita ja toimenpiteitä, erityisesti viestintäverkkojen turvallisuuden varmistamiseksi. Asiantuntijakuulemisessa on tuotu esille, että myös julkishallinnossa voi olla perusteltuja tarpeita säätää pidemmälle menevistä riskienhallinnan toimenpiteistä.

Viranomaisten resurssit

(14) Asiantuntijakuulemisessa on kiinnitetty huomiota siihen, että sääntelyehdotukset pitävät sisällään myös huomattavan määrän uusia tehtäviä kansallisille viranomaisille. Liikenne- ja viestintävirasto on arvioinut, että virasto ja sen Kyberturvallisuuskeskus eivät kykene hoitamaan mahdollisia uusia ja laajennettuja viranomaistehtäviä nykyisillä resursseilla.

VALIOKUNNAN LAUSUNTO

Liikenne- ja viestintävaliokunta ilmoittaa,

> *että se korostaa tarvetta huolehtia siitä, että ICT-toimitusketjuja koskeva sääntely ei saa heikentää Euroopan kilpailukykyä ja verkkojen kehittämistä sekä erityisesti 6G-verkkojen käyttöönottoa Euroopassa, sääntelystä ei tule koitua oman roolinsa viestintäverkkojen turvallisuuden varmistamisessa hoitaneille jäsenvaltioille tarpeettomia kustannuksia, ICT-toimitusketjuja koskevien toimenpiteiden ei tulisi lähtökohtaisesti kohdistua sellaisiin verkon osiin tai laitteisiin, joista ei todellisuudessa aiheudu sääntelyn perustana olevaa riskiä, ja että se yhtyy asiassa muilta osin valtioneuvoston kantaan korostaen edellä esitettyjä näkökohtia.*

Valiokunnan lausunto LiVL 10/2026 vp

Helsingissä 9.4.2026

Asian ratkaisevaan käsittelyyn valiokunnassa ovat ottaneet osaa

puheenjohtaja Jouni Ovaska kesk
jäsen Pekka Aittakumpu ps
jäsen Marko Asell sd
jäsen Seppo Eskelinen sd
jäsen Atte Harjanne vihr
jäsen Aleksi Jäntti kok
jäsen Marko Kilpi kok
jäsen Mauri Kontu kesk
jäsen Sheikki Laakso ps
jäsen Mats Löfström r
jäsen Anna-Kristiina Mikkonen sd
jäsen Jani Mäkelä ps
jäsen Pinja Perholehto sd

Valiokunnan sihteerinä on toiminut

valiokuntaneuvos Juha Perttula