Traficom

Lausunto

21.01.2026

TRAFICOM/870203/03.03.00/2025

Asia: VN/36127/2023

Lausuntopyyntö ehdotuksesta viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointia koskevan lainsäädännön muuttamisesta

Huomiot ehdotetusta soveltamisalan laajenemisesta varautumisen arviointiin sekä muutoksen mahdollisista vaikutuksista/ Kommentarer om föreslaget att utvidga tillämpningsområdet så att det omfattar bedömningen av beredskapen och om ändringarnas konsekvenser:

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Valtionhallinnon viranomaisena ja tiedonhallintayksikkönä Traficom on tieto- ja kyberturvallisuusviranomainen ja useita ihmisten ja yritysten välttämättömiä liikenteen ja viestinnän lupa-, valvonta- ja ohjauspalveluita tarjoava virasto. Siten Traficom tekee ja tekisi varautumisen suunnittelua ja arviointia ilman lain velvoitettakin ja pitää lain laajentamista varautumisen arviointiin sinänsä perusteltuna. Traficom korostaa, että kun varautumisen arviointivelvollisuus koskee kategorisesti kaikkia valtionhallinnon viranomaisen tietojärjestelmiä ja tietoliikennejärjestelyjä, on välttämätöntä voida tehdä arvioinnin tekijän ja arvioinnin kohteiden valinta riskiperusteisesti. Traficom katsoo, että monelta osin virastolla itsellään on parhaat edellytykset tosiasiallisesti arvioida eri toimintojensa kriittisyyttä ja toiminnoissa tarvittavien tietojärjestelmien ja tietoliikennejärjestelyjen varautumistarpeita.

Arviointiviranomaisena Traficomin käsitys vastaa HE-luonnoksen kirjauksia, joiden mukaan "tietojärjestelmien ja tietoliikennejärjestelyjen varautumisen arviointi on sisällöltään uusi osa-alue, eikä arviointiin ole käytössä vakiintuneita yleispäteviä perusteita". Traficom näkee, että uuden osa-alueen johdonmukaisten ja tarkoituksenmukaisten arviointiperusteiden kehittäminen edellyttää arviointiviranomaisten ja muiden viranomaisten yhteistyötä.

Myös arviointilaitoslain soveltamisalaan ehdotetaan lisättäväksi varautumisen arviointi. Varautumisen arviointiperusteiden kehittäminen on edellytys sille, että myös tietoturvallisuuden arviointilaitosten pätevyydet varautumisen arviointien tekemiseksi tulevat mahdollisiksi.

Varautumisen määritelmän perustelujen valossa arviointi voisi ulottua valmiuslain velvoitteisiin asti, mutta arviointiperusteita voitaneen lain toimeenpanossa laatia eriasteisiin häiriötilanteisiin. Traficomin käsityksen mukaan varautuminen voisi arvioinnin kohteena käsittää monenlaisia toimenpiteitä kuten tärkeiden toimintojen jatietojärjestelmien tunnistamista, riskien arviointia ja niiden hallintaa esimerkiksi teknisiä komponentteja kahdentamalla sekä resurssien ja toimintojen ja toimitusketjujen tarkastelua ja hallintaa ja toiminnan varajärjestelyjä.

Vaikutusarvioinnissa katsotaan nyt (s. 23), että arviointiviranomaisen tehtävällä arvioida varautumista ei olisi välittömiä resurssivaikutuksia Traficomin ja Pääesikunnan määrätyn turvallisuusviranomaisen resurssitarpeisiin. Tämä ei vastaa Traficomin käsitystä, vaan Traficom katsoo, että vaikutusarvioinnissa varautumisen osalta HE-luonnoksen seuraava toteamus kuvaa vaikutuksia siinä määrin kuin niitä on mahdollista arvioida: "Arviointiviranomaisten voimavarat vaikuttavat siihen, missä määrin varautumisen osaamista ja johdonmukaisia kriteerien valinnan ja tulkinnan sekä todentamisen käytäntöjä on mahdollista kehittää."

Huomiot ehdotetuista arviointimenettelyjä koskevista muutoksista sekä uusista viranomaisia koskevista arviointivelvollisuuksista ja niiden vaikutuksista organisaatiosi toimintaan (3–3 c §)/ Kommentarer om de föreslagna ändringarna i bedömningsförfarandena och om de nya bedömningsskyldigheterna för myndigheterna samt konsekvenserna av dessa för din organisation (3–3 c §):

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Valtionhallinnon viranomaisena ja tiedonhallintayksikkönä Traficom pitää itsearvioinnin nimenomaista mainitsemista laissa selkeyttävänä ja sinänsä itsestään selvänä menettelynä, koska vastuu tietoturvallisuuden riskien hallinnasta kuuluu tiedonhallintayksikön vastuulle. Riippumaton arviointi Tl I -TL III -järjestelmissä on tarkoituksenmukainen. Tieto- ja kyberturvallisuusviranomaisena Traficom katsoo, että arviointien tekeminen on tarpeellinen osa kansallisesta turvallisuudesta huolehtimista.

Arviointivelvollisuuksista Traficom toteaa, että tietoturvallisuuden johdonmukainen huomioiminen on muutoinkin kiinteä osa Traficomin tietojärjestelmien suunnittelun, hankinnan, käyttöönoton ja ylläpidon prosesseja. Varautumisen arviointi näyttäisi edellyttävän viranomaiselta omaa määrittelyä arvioinnin perusteista, koska yhteinen ja hyväksytty varautumisen kriteeristö toistaiseksi puuttuu. Arviointien vaikutus Traficomin toiminnan tietoturvallisuuteen riippuu myös yhteisten palveluiden arvioinnista.

Arviointiviranomaisena Traficom arvioi, että se pystyy huolehtimaan TL I ja TL II tietoa käsittelevien järjestelmien arviointivelvollisuudesta, kun otetaan huomioon siirtymäaika ja se, että ehdotuksen mukaan Pääesikunnan määrätty turvallisuusviranomainen vastaisi arviointiviranomaisena Puolustusvoimien kansallista TL I ja TL II tietoa käsittelevien järjestelmien arvioinnista.

TL III järjestelmien arviointia Traficom pitää jatkossakin ja myös tehtäviensä 4 §:n 3 momentissa tarkennettujen priorisointiperusteiden valossa ensisijaisesti hyväksyttyjen tietoturvallisuuden arviointilaitosten tehtävänä. Sama koskee TL IV järjestelmien arviointeja siltä osin, kun viranomainen pitää oman riskiarvionsa perusteella riippumatonta arviointia tarpeellisena tai kansallisen turvallisuuden näkökohdat puoltavat valvotun arviointitoimijan käyttämistä.

Huomiot ehdotetuista arviointiviranomaistehtävien ja tiedonsaanti- ja tarkastusoikeuksien muutoksista (3 d–6 §)/ Kommentarer om de föreslagna ändringarna i bedömningsmyndigheternas uppgifter och rätt att få information och utföra inspektioner (3 d–6 §):

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Arviointiviranomaisena Traficom pitää 3 d §:ssä ehdotettua arviointiviranomaisten tehtävien jakautumista tarkoituksenmukaisena. Traficomin yleistoimivalta ja Pääesikunnan määrätyn turvallisuusviranomaisen viranomaiskohtainen Puolustusvoimien omia järjestelmiä koskeva arviointiviranomaisen tehtävä on hyvin yhteensovitettavissa myös kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaisten toimivaltuuksien kanssa, jossa Traficom vastaa järjestelmien ja turvallisuuskriittisten ratkaisujen arvioinnista ja hyväksynnästä, mutta jossa turvallisuusviranomaisilla on mahdollisuus sopia tehtävien hoitamisesta.

Traficomilla ja Pääesikunnan määrätyllä turvallisuusviranomaisella on toimivat käytännöt yhteistyöstä kansainvälisten tietoturvallisuusvelvoitteiden suhteen ja niiden pohjalta voidaan sujuvasti rakentaa myös kansallista arviointitehtävää koskeva yhteistyö. Traficom korostaa 4 b §:ssä ehdotettuja arviointiviranomaisten yhteistyötä, tiedonvaihtoa ja yhteistä soveltamiskäytäntöä koskevien ehdotusten tärkeyttä ja välttämättömyyttä tehokkaan ja tarkoituksenmukaisen viranomaistoiminnan kannalta.

Traficom toteaa, että Traficomin tehtävien priorisointiperusteiden täydennykset 4 §:n 3 momentissa parantavat priorisoinnin läpinäkyvyyttä ja tukevat rajallisten resurssien priorisoinnissa tarvittavaa harkintaa. Traficom ehdottaa, että luettelon kohdassa 8 oleva käytettävissä olevien voimavarojen huomioiminen siirrettäisiin selvyyden vuoksi johtolauseeseen, sillä luettelon 1-7 kohtien perusteella harkitaan juuri voimavarojen jakamista eri tehtäviin.

Traficom katsoo, että 6 §:n tiedonsaanti-, pääsy- ja tarkastusoikeuksien täydennykset tarkentavat arviointien toteuttamiseksi välttämättömiä oikeuksia. Täydennykset tukevat erityisesti turvallisuuskriittisten ratkaisujen valmistajien hyväksyntähakemusten käsittelyssä tarvittavia arviointitoimenpiteitä. Traficom katsoo, että 6 §:n 2 momenttia, joka koskee Traficomin hyväksymien hajasäteilyratkaisuja tarjoavien valmistajien valvontaa, tulisi täydentää siten, että myös

Pääesikunnan määrätyllä turvallisuusviranomaisella olisi osaltaan säännöksessä tarkoitetut oikeudet, jos Traficom ja Pääesikunnan määrätty turvallisuusviranomainen ovat sopineet 4 b §:n nojalla valvontaa tukevasta selvitystehtävästä. Säännösehdotuksen mukaan tällaiset oikeudet koskisivat nyt vain lain 4 a §:n mukaista avustavaa ulkopuolista asiantuntijaa. Traficom ja Pääesikunnan määrätty turvallisuusviranomainen voivat ehdotetun 4 b §:n 2 momentin perusteella "sopia tietyn tässä laissa säädetyn tehtävän tai sen osan hoitamisesta toisen arviointiviranomaisen lukuun, jos järjestely on tarpeen tehtävien hoitamiseksi tarkoituksenmukaisesti, taloudellisesti ja joutuisasti." Tämän menettelyn hyödyntäminen myös hyväksytyn hajasäteilysuojausratkaisuja tarjoavan yrityksen valvonnassa voi olla tarkoituksenmukaista ja välttämätöntä arviointiviranomaisten resurssien ja kyvykkyyksien valossa ja käytännössä hajasäteilysuojaukseen liittyviä ratkaisuja tarjoava yritys voi olla Puolustusvoimille keskeinen toimija. Valvontaa tukevan tehtävän hoitaminen ei luonnollisesti vaikuta siihen, että Traficomin vastaa valvontaviranomaisena mahdollisen valvontaprosessin käynnistämisestä, sisällöstä ja selvityksen perusteella tehtävistä ratkaisuista.

Traficom ehdottaa vielä harkittavaksi arviointiviranomaisten välistä tiedonvaihtoa koskevassa 4 b §:n 1 momentissa ja valtiovarainministeriön pyynnöstä tehtävien selvitysten tiedonvaihtoa koskevassa 5 §:n 2 momentissa, onko viranomaisten välillä tarpeen säätää tiedonvaihto-oikeudesta "muiden tiedon luovuttamista koskevien rajoitusten estämättä". Traficomin käsityksen mukaan viranomaisen on aina arvioitava viranomaistehtävissään saamiensa tai laatimiensa asiakirjojen ja tietojen luovutus salassapitosäännösten mukaisesti viranomaisten toiminnan julkisuudesta annetun lain (621/1999), kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n tai muun säädöksen mukaan, eikä viranomaisella voi olla tehtävissään muita oikeudellisesti sitovia tiedon luovuttamista koskevia rajoituksia kuin salassapitosäännökset. Sen sijaan ehdotetussa 6 §:n 1 momentissa, joka koskee myös yritysten tiedonluovutusta viranomaiselle, "muiden tiedon luovuttamista koskevien rajoitusten estämättä" on hyvä ja tarpeellinen lisäys, sillä yrityksillä voi olla esimerkiksi sopimuksiin perustuvia salassapitositoumuksia.

Huomiot ehdotetusta uudesta turvallisuuskriittisten ratkaisujen ja niiden valmistuksen arviointien kokonaisuudesta/ Kommentarer om de nya bestämmelserna om bedömningen av säkerhetskritiska lösningar och produktionen av dem:

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Arviointiviranomaisena Traficom korostaa, että turvallisuuskriittisen ratkaisun valmistajalle säädettävä mahdollisuus hakea arviointia ja hyväksyntää Traficomilta on tärkeä muutos, joka parantaa ja selkeyttää elinkeinotoiminnan edellytyksiä.

Arviointilain ehdotetut muutokset suomalaisen valmistajan itsenäisestä oikeudesta hakea hyväksyntää ja arviointiperusteita sekä hyväksyntää koskevat säännösehdotukset luovat tarpeellisen sääntelyperustan kansallisen turvallisuusluokitellun tiedon suojaamisessa käytettävien ratkaisujen hyväksyntään ja mahdollistavat samalla kansainvälisten, erityisesti EU:n ja/tai Naton, vaatimusten huomioimisen. Investointien, kaupallisten ja asiakkaiden tarpeiden kannalta valmistuksessa tähdätään yleensä sekä kansallisten että kansainvälisten vaatimusten arviointiin ja täyttämiseen. Sääntely tukee osaltaan suo-malaisten valmistajien mahdollisuuksia EU:n ja Naton yhteydessä sekä

erilaisissa valtioiden kahden- tai monenvälisissä hankkeissa. Erityisen tärkeä mahdollistava vaikutus ehdotetulla sääntelyllä on suomalaisiin hajasäteilyratkaisujen valmistajiin, sillä se mahdollistaisi niiden hyväksynnän, ohjauksen ja valvonnan kansallisesti sekä EU:n ja Naton sääntelykehysten mukaisella tavalla. Traficom tarkastelee vaikutusarviointia enemmän sitä koskevan kysymyksen kohdalla.

Traficom katsoo, että turvallisuuskriittisten ratkaisujen ehdotettu määritelmä on yhteensopiva kansainvälisten tietoturvallisuusvelvoitteiden ja riittävän joustava ja teknologianeutraali siten, että määritelmä kestää aikaa, kv-tietoturvallisuuskehysten muutoksia ja mahdollisten kansallisten tarpeiden huomioimista. Traficom ehdottaa harkittavaksi kielellistä tarkennusta säännöksen (2 § 9 kohta) määritelmään, jotta tuote, toteutus ja palvelu viittaavat selvästi myös salaus- ja hajasäteilysuojausratkaisuihin: "turvallisuuskriittisellä ratkaisulla salaus-[ratkaisua], hajasäteilysuojaus-[ratkaisua] ja muuta tieto- ja viestintäteknistä ratkaisua, tuotetta, toteutusta tai palvelua, jolla suojataan turvallisuusluokiteltua tietoa tietojärjestelmissä ja tietoliikennejärjestelyissä." Turvallisuuskriittisen ratkaisun valmistajan määritelmä huomioi ratkaisujen luotettavuuden kannalta tarpeellisella tavalla ratkaisujen elinkaaren.

Traficom toteaa, että turvallisuuskriittisten ratkaisujen valmistuksen luotettavuus on olennainen osa ratkaisujen luotettavuutta. Traficom pitää ehdotettuja edellytyksiä julkiseen luetteloon hyväksyttäville ratkaisuille tarkoituksenmukaisina: hyväksynnän hakeminen olisi mahdollista Suomeen sijoittautuneille valmistajille ja Suomessa valmistetuille ratkaisuille ja turvallisuusselvityslain mukaisella yritysturvallisuusselvityksellä voitaisiin varmistaa valmistajan luotettavuus. Edellytysten tarkasteluun liittyy luonnollisesti toimeenpanossa tulkinnanvaraa, mutta ehdotettu sääntely luo asianmukaisen ja riittävän joustavan perustan oikeudelliselle harkinnalle ja tukee sääntelyn ennakoitavuutta, läpinäkyvyyttä ja oikeusvarmuutta valmistajien kannalta.

Traficom pitää ehdotettua 4 b §:ää arviointiviranomaisten yhteistyöstä, tiedonvaihdosta ja yhtenäisestä soveltamiskäytännöstä tärkeänä turvallisuuskriittisten ratkaisujen valmistajien kannalta ja viranomaistoiminnan tehokkuuden kannalta. Valmistajille on tärkeää, että arviointiviranomaisten tulkinnat eivät eriydy. Sujuva tiedonvaihto ja yhtenäinen soveltamiskäytäntö säästää arviointiviranomaisia tarpeettomalta päällekkäiseltä työltä. Esimerkiksi Pääesikunnan määrätyn turvallisuusviranomaisen 4 §:n 1 momentin ja 3 d §:n mukaisesti tekemää arviointia ratkaisun käytöstä Puolustusvoimien tietojär-jestelmässä voidaan hyödyntää Traficomin arvioinnissa, jos samaa tuotetta halutaan käyttää jonkun muun viranomaisen järjestelmässä. Jos valmistus täyttää julkiseen luetteloon hyväksynnän edellytykset, Traficom voi ottaa siinä huomioon tiettyjä järjestelmiä varten tehdyn arvioinnin. Soveltamiskäytännön yhdenmukaisuus ei estä sitä, että arvioinneissa koordinoidaan myös tietoa Puolustusvoimien mahdollisista toiminnallisista erityistarpeista ja valmistaja voi ottaa ne huomioon.

Traficom pitää Teknologian tutkimuskeskus VTT Oy:n avustavan tehtävän säätämistä ja kyvykkyyden ohjausta ja kehittämistä arviointiviranomaisten yhteistyössä tärkeänä erityisesti Suomen kansallisten salaustuotekyvykkyyksien kannalta. Tehtävän sitominen toimivaltaisen viranomaisen ohjaukseen ja siten kehitys- ja arviointitoimintaan liittyvä valtiollinen kontrolli on osa AQUA-maan edellytyksiä.

Traficom pitää hyväksyttyjen turvallisuuskriittisten ratkaisujen julkisesta luettelosta säätämistä tarkoituksenmukaisena ja hyödyllisenä sekä valmistajille että näiden mahdollisille asiakkaille. Säädettyyn luetteloon merkintä osoittaa, että ratkaisujen tietoturvallisuuteen vaikuttavat riskit ja niiltä suojaavat ominaisuudet on arvioitu ja todennettu kattavasti. Tärkeää on myös, että luettelossa informoidaan mahdollisista rajoituksista ja käyttöpolitiikasta, sillä luotettavakaan tuote ei itsessään takaa turvallisuutta, jos sen turvallinen käyttötapa laiminlyödään.

Viranomaisten riittävällä tiedonvaihdolla voidaan edesauttaa arviointitietojen hyödyntämistä silloinkin, kun arviointi tehdään vain järjestelmäkohtaista käyttöä varten, koska julkiseen luetteloon hyväksyntään ei ole edellytyksiä tai tarvetta.

Huomiot ehdotetuista siirtymäsäännöksistä ja -ajoista/ Kommentarer om de föreslagna övergångsbestämmelserna och övergångstiderna:

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Valtionhallinnon viranomaisena ja tiedonhallintayksikkönä Traficom katsoo, että siirtymäajat ovat tasapainossa turvallisuustarpeiden ja arvioinnin edellyttämien resurssien kannalta. Ehdotetun arviointivelvoitteen soveltaminen julkista tietoa käsitteleviin järjestelmiin voi kaivata soveltamisohjeita. Jos kaikki viranomaiset jättävät riippumattoman arvioinnin hankkimisen määräajan viime hetkeen, arviointilaitoksille ja Traficomin arviointiviranomaiselle voi toki muodostua ruuhkaa.

Muut arviointilakia koskevat huomiot, pyydämme yksilöimään pykälän/ Övriga kommentarer om bedömningslagen (specificera vilken paragraf som avses):

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Traficom nostaa tässä kohdassa esille eräitä arviointitoiminnan sujuvuuden kannalta keskeisiä kannatettavia muutosehdotuksia ja ehdottaa joitakin selkeyttäviä täydennyksiä yleisperusteluihin ja säännöskohtaisiin perusteluihin.

Suhde lakiin kansainvälisistä tietoturvallisuusvelvoitteista

Traficom kannattaa 1 §:n 2 momentin ehdotusta suhteesta lakiin kansainvälisistä tietoturvallisuusvelvoitteista (588/2004, kv-titulaki). Ehdotus selkeyttää pyyntöjen käsittelyä, kun Traficom voi kv-titulain 4 §:n mukaisissa tehtävissään soveltaa arviointilain menettelysäännöksiä. Tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnin tai hyväksynnän pyytäjillä ja turvallisuuskriittisten ratkaisujen valmistajilla on usein tarve saada samanaikaisesti vireille ja käsittelyyn kansallisen ja kansainvälisen sääntelykehyksen mukainen arviointi.

Traficom ehdottaa hyväksyntätilanteita koskevan 3 c §:n perustelujen selkeyttämistä ja täydentämistä seuraavasti:

Pykälän 1 kohdassa tarkoitettu kansainvälinen tietoturvallisuusvelvoite voi perustua esimerkiksi EU:n tai Naton turvallisuussääntöihin tai Suomen tietoturvallisuussopimusten sopimusmääräyksiin. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaan tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevat asiat ovat määrättynä turvallisuusviranomaisena Liikenne- ja viestintäviraston tehtäviä. Kansainväliseen tietoturvallisuusvelvoitteen perusteella kyseeseen voi tulla tarve osallistua yhteisen järjestelmän hyväksyntään, hyväksyä valtioiden rajat ylittävä sähköinen tiedonsiirtomenettely tai esittää hyväksyntä jostain kansallisesta järjestelmästä. Esimerkiksi EU:n ja Naton turvallisuusluokitellun tiedon käsittelyyn käytettävät tietojärjestelmät on turvallisuussääntöjen mukaan etukäteen akkreditoitava, ja myös tietyt osa-alueet tai elementit on etukäteen arvioitava ja hyväksyttävä. Tietoturvallisuussopimuksissa puolestaan määrätyn turvallisuusviranomaisen hyväksyntää edellyttävien sopimusmääräysten ala on yleensä kapeampi ja muutoin sovelletaan vastavuoroisuusperiaatetta eli vastaavan turvallisuusluokan kansallisia tietoturvallisuusvaatimuksia. Suomessa sääntelyn mukaan tiedonhallintayksikkö vastaa tietoturvallisuudestaan ja arviointivelvoitteet ja arviointimenettelyt määrittyisivät tämän lain ehdotetun 3 a § ja 3 b §:n mukaisesti.

Pykälän kohdassa 2 tarkoitettu muun kansainvälisen yhteistyön tilanne voi syntyä esimerkiksi, kun toisen valtion kanssa ei ole tietoturvallisuussopimusta eikä siten valtiosopimukseen perustuvaa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain tarkoittamaa kansainvälistä tietoturvallisuusvelvoitetta, mutta riippumaton arviointi ja tietoturvallisuusvaatimusten täyttymisen toteaminen on käytännössä välttämätöntä kansainvälisen yhteistyön onnistumiseksi. Tällöin pääesikunnan määrätty turvallisuusviranomainen Puolustusvoimien pyynnöstä ja Liikenne- ja viestintävirasto muun viranomaisen pyynnöstä voisi tarvittaessa laatia hyväksynnän, jota kansainvälisessä yhteistyössä välttämättä edellytetään.

Pykälän kohdassa 3 tarkoitettuja säädettyjä vaatimuksia ei tällä hetkellä ole siitä, että vaatimustenmukaisuus olisi osoitettava arviointiviranomaisen hyväksynnällä.

Traficom ehdottaa lisäksi 4 §, 8 § ja 10 § säännöskohtaisten perustelujen selkeyttämistä seuraavasti: 4 §:n (s. 39), 8 §:n (s. 47), 10 §:n (s. 49) perusteluihin olisi hyvä lisätä maininta, että kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaan tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevat asiat ovat määrättynä turvallisuusviranomaisena Liikenne- ja viestintäviraston tehtäviä.

Traficom ehdottaa yleisperustelujen nykytilakuvauksessa (s. 5) olevan EU:n ja Naton turvallisuussääntöjä koskevan tekstikappaleen palauttamista työryhmän HE-luonnoksessa esitettyyn muotoon, jotta se kuvaisi kyseisten kansainvälisten tietoturvallisuusvelvoitteiden perusteita.

Riskiarviointien ja -päätösten selkeyttäminen laissa (3 a §, 7 § ja 8 §)

Traficom pitää hyvänä muutoksena sitä, että riskiarvioinnista säädettäisiin nimenomaisesti laissa arvioinnin tekijän valinnassa sekä arvioinnin kohteen ja arviointikriteerien määrittelyssä. Riskiperusteisuus voidaan usein kapeasti mieltää tunnettujen tai tuntemattomien poikkeamien ja uhkien aiheuttamien riskien hyväksymiseksi, mutta lakiluonnos selkeyttää sitä, että kysymys on johdonmukaisesta uhkien ja niiltä suojaavien toimenpiteiden ja tosiallisen suojautumiskyvyn tarkastelusta ja arvioinnin avulla saatuun tietoon pohjautuvasta riskeihin liittyvästä päätöksenteosta. Arvioinnin ja hyväksynnän erottaminen laissa selkeyttää vastuuta riskipäätöksen tekemisestä. Arviointi tehdään vain tiettynä ajanhetkenä, mutta kun arvioinnissa huomioidaan kohteen kyky havainnoida mahdollisia poikkeamia ja reagoida niihin, arviointi tukee kohteen tietoturvallisuutta sen elinkaaren aikana.

Traficom kannattaa 3 a §:n ehdotusta riskiarvioinnista valittaessa arviointimenettelyä eli arvioinnin tekijää. Laissa säädettäisiin sitovasti arvioinnin tekijä TL I ja TL II -tietojen käsittelyssä, mutta muutoin valinta perustuisi viranomaisen tekemään riskiarvioon. Tämä mahdollistaa tarpeellisen tapauskohtaisen harkinnan. Traficom pitää tärkeänä, että laissa edellytetään TL III-järjestelmissä riskiarvioon perustuvaa päätöstä, jos viranomainen päätyy tekemään arvioinnin itsearviointina eikä käytä hyväksyttyä tietoturvallisuuden arviointilaitosta tai pyydä arviointia arviointiviranomaiselta. Edelleen Traficom pitää tärkeänä, että kun ehdotuksen mukaan TL IV-järjestelmien arvioinnin voi hankkia myös muulta yritykseltä kuin hyväksytyltä tietoturvallisuuden arviointilaitokselta, riskiarvioinnissa ja yrityksen luotettavuuden varmistamisessa otetaan huomioon kansallisen turvallisuuden tarpeet.

Traficom kannattaa 7 §:n 2 momentin ehdotusta, jonka mukaan arvioinnin kohteen ja arviointiperusteiden määrittämisessä on huomioitava säädetyt vaatimukset ja riskiarvioinnin perusteella valitut vaatimukset. Teknisten toteutusten yksityiskohdat ja muuttuvat uhkat vaikuttavat tietojärjestelmien, tietoliikennejärjestelyjen ja turvallisuuskriittisten ratkaisujen tietoturvallisuuteen. Säädöksiä ei ole mahdollista tai tarkoituksenmukaista laatia ja päivittää niin yksityiskohtaisella tasolla, että pykälissä säädetyt vaatimukset yksinään toimisivat arviointikriteereinä ja kohteen teknisen rajauksen määrittelyssä. Jotta riskiarvioinnissa pystytään huomioimaan yleisesti tunnetut uhkat ja kohteen erityiset uhkat, kriteerien valinnassa ja kohteen kattavuuden määrittämisessä on tarpeen hyödyntää kohteen omaa tuntemusta, arviointikriteeristöjä ja muita ohjeita ja suosituksia sekä arvioinnin tekijän ammattiosaamista. Kun kysymys on hyväksyntää edellyttävästä tilanteesta, hyväksyntää koskevat vaatimukset kuten EU:n neuvoston tai Naton turvallisuussäännöt sitovat myös riskiarvioinnin tekemistä.

Traficom kannattaa 8 §:n ehdotusta arviointiraportin ja hyväksyntäpäätöksen ja -lausunnon eriyttämisestä. Ehdotus selkeyttää tarpeellisella tavalla arviointien ja hyväksyntöjen eroa. Kansallisen turvallisuusluokitellun tai julkisen tai salassa pidettävän tiedon käsittelyn tietoturvallisuuden ja varautumisen arvioinnista säädetään annettavaksi vain arviointiraportti. Tämä selkeyttää sitä, että arviointiviranomaisen tehtävä on tuottaa tiedonhallintayksikölle riippumatonta, ammattitaitoisesti tuotettua ja realistista tietoa tietoturvallisuustoimenpiteiden tosiasiallisesta toteutumisesta ja tarpeista. Tiedon perusteella tehtävät päätökset riskinhallinnasta ovat tiedonhallintalain 13 §:n

mukaisesti tiedonhallintayksikön vastuulla. Tiedonhallintayksikön liikkumavara riskinhallintapäätöksissä on puolestaan merkittävästi kapeampi niissä 3 c §:n mukaisissa tilanteissa, joissa arviointiviranomainen antaa 8 §:n mukaan hyväksyntäpäätöksen tai -lausunnon vaatimusten täyttymisestä.

Suhde kyberturvallisuuteen 7 §:n perusteluissa

HE-luonnoksessa todetaan 7 §:n 1 momentin 1 kohdan perusteluissa (s. 44) seuraavaa: "Pykälän 1 momentin arviointiperusteiden luettelon tarkoituksena olisi mahdollistaa laajasti eri arviointiperusteiden käyttäminen. Momentin 1 kohtaan lisättäisiin kyberturvallisuus- ja varautumisvaatimukset tietoturvallisuusvaatimusten lisäksi. Viranomaisten toiminalle on asetettu tietoturvallisuusvaatimusten rinnalle myös kyberturvallisuusvaatimuksia, jotka olisi tarkoituksenmukaista huomioida osana tietojärjestelmien ja tietoliikennejärjestelyjen arviointeja. "

Traficom kiinnittää huomiota siihen, että arviointilain soveltamisalana ei ole kyberturvallisuuden arviointi vaan tietoturvallisuuden ja varautumisen arviointi. Traficom katsoo kuitenkin, että perustelun toteamus kyberturvallisuusvaatimusten arvioinnista ei aiheuttane varsinaista sisällöllistä ristiriitaa lain soveltamisalaan nähden. Tietoturvallisuuden ja kyberturvallisuuden vaatimukset ovat usein varsin samanlaisia ja niitä voi olla vaikeakin eritellä, ja siten kyberturvallisuuden soveltuvia kriteereitä voi olla tarkoituksenmukaista käyttää arvioinnissa. Eri viranomaistehtäviensä kannalta Traficom katsoo, että tiedonhallintalain 4 a luvussa Traficomille säädetty valvontaviranomaisen tehtävä julkishallinnon kyberturvallisuusvelvoitteiden valvonnassa ei vaikuta siihen, että arviointilain mukaisessa arviointitehtävässä Traficomin rooli on tuottaa tiedonhallintayksikölle tietoa, ei valvoa tai velvoittaa tiedonhallintayksikköä, saati käynnistää valvontaprosesseja. Viranomaisten päällekkäisen työn välttämiseksi ja resurssien tehokkaan käytön varmista-miseksi kaikilta osin tiedonhallintayksikkö ja Traficom voivat hyödyntää mahdollisessa valvonnassa tuotettua aineistoa arvioinnissa ja toisaalta arvioinnissa laadittua aineistoa, jos tiedonhallintayksikköön kohdistuu valvontaa.

Traficom ehdottaa 7 §:n 1 momentin 1 kohdan perusteluja täydennettäväksi ja selvennettäväksi kyberturvallisuusvaatimusten osalta esimerkiksi seuraavasti: Tietoturvallisuuden ja kyberturvallisuuden vaatimukset ovat usein varsin samankaltaisia. On huomattava, että julkishallinnolle tiedonhallintalain 4 a luvussa säädettyihin kyberturvallisuusvaatimuksiin liittyvä Liikenne- ja viestintäviraston valvontatehtävä ei vaikuta viraston tässä laissa säädettyyn arviointitehtävään, jonka tarkoitus on tuottaa tietoa arviointia pyytäneelle viranomaiselle, ei käynnistää valvontaprosesseja tai velvoittaa tiedonhallintayksikköä johonkin. Viranomaisresurssien tehokkaan käytön varmistamiseksi tiedonhallintayksikkö ja Liikenne- ja viestintävirasto voivat kuitenkin hyödyntää mahdollisessa valvonnassa tuotettua aineistoa arvioinnissa ja toisaalta arvioinnissa laadittua aineistoa, jos tiedonhallintayksikköön kohdistuu valvontaa.

Yleisperustelut

HE-luonnoksen luku 2.1 Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointi, Arviointiperusteet ja -kriteerit (s. 9)

Nykytilakuvauksessa todetaan, että "(Katakri), jota kansallisen turvallisuusviranomaisen antaman ohjeen mukaisesti sovelletaan kansainvälisten tietoturvallisuusvelvoitteiden hoitamisessa". Traficom ehdottaa selvyyden vuoksi täydennettäväksi tosiasiallista nykytilaa kuvaavan tiedon, joka oli mukana työryhmän laatimassa HE-luonnoksessa: "Katakrissa on huomioitu EU:n ja Naton turvallisuusluokitellun tiedon käsittelyn vaatimukset sekä tiedonhallintalain ja turvallisuusluokitteluasetuksen vaatimukset, joten sitä voidaan hyödyntää monissa tilanteissa. Katakria käytetään etenkin kansainvälisiin velvoitteisiin liittyvissä arvioinneissa, mutta myös monissa kansallisissa tilanteissa, kuten lain julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015) mukaisten palveluiden arvioinneissa ja yritysturvallisuusselvityksiin liittyvissä arvioinneissa."

Luku 5.1 Vaihtoehdot ja niiden vaikutukset (s. 27)

Traficom ehdottaa tarkennusta yleisperustelujen lukuun 5.1 Vaihtoehdot ja niiden vaikutukset. Luvun lopussa todetaan: "[p]ohditut sääntelyn tarkennukset koskivat muun muassa valtiovarainministeriön ohjausta ja ohjeistusta koskien viranomaisten pyytämiä ja hankkimia arviointeja, arvioinnissa käytettäviä todentamis- eli tarkastusmenetelmiä, arviointikriteeristöjä, arviointien voimassaoloaikoja, viranomaisten velvollisuuksia tietojärjestelmien poikkeamien havainnoinnissa ja niihin reagoimisessa sekä viranomaisten viestintävelvoitetta toteutetuista arvioinneista julkiselle hallinnolle. Näiden tarkennusten osalta todettiin, että valtiovarainministeriön yleistoimivalta on riittävä ohjauksen ja ohjeistuksen antamiselle."

Traficom kiinnittää huomiota siihen, että valtiovarainministeriön yleistoimivalta ei koske Pääesikunnan määrätyn turvallisuusviranomaisen ja Liikenne- ja viestintäviraston toimia riippumattomana arviointiviranomaisena tai Liikenne- ja viestintäviraston tehtäviä hyväksytyn tietoturvallisuuden arviointilaitoksen hyväksymisessä, ohjauksessa ja valvonnassa. Traficom ehdottaa kohtaa selkeytettäväksi ja tarkennettavaksi siten, että valtiovarainministeriön yleistoimivalta on riittävä julkishallinnon TVT-ohjauksen ja ohjeistuksen antamiselle.

Huomiot ehdotetusta tietoturvallisuuden arviointilaitosten luotettavuuden varmistamista koskevista muutoksista (4–5 §)/ Kommentarer om de föreslagna ändringarna angående säkerställandet av tillförlitligheten hos bedömningsorganen för informationssäkerhet (4–5 §):

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Tietoturvallisuuden arviointilaitosten hyväksyntä- ja valvontaviranomaisena Traficom kannattaa kaikilta osin 4 §:ään ja 5 §:ään ehdotettuja muutoksia.

Voimassa olevan lain 4 §:n mukaan Liikenne- ja viestintäviraston on varattava suojelupoliisille tilaisuus lausua arviointilaitoksen vastuuhenkilöiden luotettavuudesta ja sen toimitilojen turvallisuudesta. Nämä seikat kuuluvat arviointilaitolakia myöhemmin säädetyn

turvallisuusselvityslain (726/2014) mukaiseen yritysturvallisuusselvitykseen, johon kuitenkin kuuluu myös muita selvitettäviä ja seurattavia asioita yrityksen luotettavuudesta. Olisi perusteltua hyödyntää täysimääräistä turvallisuusselvityslain mukaista menettelyä siinä tapauksessa, että arviointilaitoksen pätevyys koskee turvallisuusluokitellun tiedon käsittelyä ja arviointilaitos arvioi useiden viranomaisten tai näille palveluita tuottavien yritysten turvallisuusluokitellun tiedon käsittelyä. Ehdotetut 5 §:n 1 momentin 4 kohdan muutokset mahdollistavat yritysturvallisuusselvityksessä ilmenneistä seikoista kokonaisharkinnan, mikä on tärkeää elinkeinotoiminnan mahdollisuuksien ja asiakkaiden luottamuksen punninnan kannalta. Muiden kuin turvallisuusluokitellun tiedon käsittelyyn liittyvien pätevyyksien suhteen on alalle tulon kynnyksen takia perusteltua, ettei yritysturvallisuusselvitystä edellytetä, vaan toimitilojen ja vastuuhenkilöiden luotettavuuden varmistaminen riittää.

Lain 5 §:n 1 momentin 4 kohtaan ehdotetaan myös lisättäväksi, että laitoksella on oltava menetelmä henkilökunnan luotettavuuden varmistamiseen. Tämä henkilöstöturvallisuutta koskeva lisäys on tarpeellinen ja tavanomainen osa tietoturvallisuuden kokonaisuutta.

Huomiot ehdotetusta tietoturvallisuuden arviointilaitosten lisäpätevyyksien hyväksymisprosessista (5 § 3 mom)/ Kommentarer om processen för godkännande av bedömningsorganens specialbehörigheter (5 § 3 mom.):

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Traficom pitää tietoturvallisuuden arviointilaitosten hyväksyntä- ja valvontaviranomaisena lisäpätevyyden hyväksyntämenettelyä koskevaa muutosta tärkeänä, jotta arviointilaitoksilla olisi nykyistä joustavammin mahdollisuus hakea ja saada lisäpätevyyksiä ilman, että FINASin akkreditointi ja akkreditoinnin ylläpito pätevyydelle olisi aina pakollinen. Traficom pitää hyvänä, että tietoturvallisuuden arviointilaitoksen hyväksyntä ensi vaiheessa edellyttäisi jatkossakin aina jonkin pätevyyden akkreditointia, sillä akkreditointimenettely varmistaa osaltaan tietoturvallisuuden arviointilaitoksen kyvyn noudattaa johdonmukaisesti tasalaatuisuuden ja vertailukelpoisuuden turvaavia toimintaprosesseja. Lisäpätevyystarpeet liittyvät kuitenkin usein säädöksiin ja säädösten soveltamista koskeviin viranomaisohjeisiin ja -menettelyihin, joiden erityisasiantuntemusta on lähinnä kapealla joukolla toimivaltaisia viranomaistoimijoita. FINASin kansainvälisiin akkreditointistandardeihin perustuva prosessi, joka soveltuu erityyppisten markkinatoimijoiden tasalaatuisen ja vertailukelpoisen arvioinnin pätevyyksiin, ei tue lisäpätevyyksien erityispiirteitä siinä määrin, että se välttämättä toisi lisäarvoa viranomaisselvitykseen verrattuna. Traficom pitää kuitenkin hyvänä, että sääntely mahdollistaa myös FINASin akkreditoinnin käyttämisen lisäpätevyyden osoittamisessa. Näin sääntely on riittävän joustavaa tulevaisuudessa syntyvien tarpeiden ja erilaisten pätevyysalueiden varalta.

Traficom pitää tärkeänä, että sääntelyssä tuodaan selkeästi esille se, että niissä tapauksissa, joissa FINAS ei ole akkreditoinut pätevyyttä, FINASilla ei ole myöskään pätevyyden seurantaan, ohjaukseen tai valvontaan liittyviä vastuita.

Muut arviointilaitoslakia koskevat huomiot, pyydämme yksilöimään pykälän/ Övriga kommentarer om lagen om bedömningsorgan (specificera vilken paragraf som avses):

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Traficom pitää tärkeänä viraston tiedonsaanti- ja tarkastusoikeuksiin ehdotettuja muutoksia (7 §), jotka osaltaan mahdollistavat tietoturvallisuuden arviointilaitosten sekä niiden alihankkijoiden toiminnan riittävän ja uskottavan valvonnan.

Myös lain 2 §:ään ehdotettu vaatimus Suomeen sijoittautumisesta varmistaa, että arviointilaitosten toiminta on Suomen lainkäyttövallan piirissä ja hyväksyntä, ohjaus ja valvonta voidaan tehdä lainsäädännön edellyttämällä tavalla.

Traficom pitää tietoturvallisuuden arviointilaitosten hyväksyntä- ja valvontaviranomaisena arviointilaitoslain 9 a §:n ehdotusta alihankinnan reunaehtojen säätämisestä tarpeellisena. Asiaan on liittynyt verraten paljon tulkintakysymyksiä ja sääntely selkeyttää yritystoiminnan suunnittelua ja tukee asiakkaiden luottamusta arviointilaitoksiin.

Arviointilaitosten hyväksyttynä arviointilaitoksena hoitamat tehtävät ovat julkisia hallintotehtäviä ja Traficom katsoo, että lain 13 §:ään ehdotetut täydennykset virkavastuuta ja hyvää hallintoa koskevien säännösten soveltamisesta vastaavat julkisen hallintotehtävän hoitamiselta edellytettäviä seikkoja.

Arviointilaitosten julkinen hallintotehtävä on eräiltä osin rinnakkainen arviointilain mukaisen arviointiviranomaisen tehtävän kanssa. Siksi on tärkeää, että arviointilaki ja arviointilaitoslaki ovat yhdenmukaiset esimerkiksi mahdollisten arviointiperusteiden osalta.

Perustelujen täydennykset

7 §:n perustelut (s. 53)

Liikenne- ja viestintäviraston tarkastusoikeus ehdotetaan 7 §:ssä ulotettavaksi koskemaan myös arviointilaitoslain 9 a §:ssä tarkoitettua arviointilaitoksen alihankkijaa. Traficom ehdottaa, että myös 7 §:n säännöskohtaisia perusteluja täydennetään vastaavasti: Pykälän 1 momenttia muutettaisiin siten, että pykälässä säädetty tarkastusoikeus ulotettaisiin koskemaan myös arviointilaitoksen alihankkijan tiloja ja se koskisi Liikenne- ja viestintäviraston lisäksi, sen toimeksiannosta toimivan asiantuntijan sijaan, sitä avustavaa asiantuntijaa. Muutos vastaisi 4 §:n 2 momenttiin ehdotettavaa

mahdollisuutta antaa vain avustavia tehtäviä ulkopuoliselle asiantuntijalle. Avustavassa tehtävässä toimivaa ulkopuolista asiantuntijaa voitaisiin käyttää tietoturvallisuuden arviointilaitoksen ja sen 9 a §:ssä tarkoitetun alihankkijan toimitiloja ja menetelmiä koskevassa tarkastuksessa.

Perustelujen luku 10 suhde perustuslakiin ja säätämisjärjestys (s. 61)

Traficom ehdottaa perusteluihin täydennystä kotirauhan osalta, koska Liikenne- ja viestintäviraston tarkastusoikeutta ehdotetaan laajennettavan arviointilaitosten alihankkijoihin: Arviointilaitoslain 7 §:n 1 momentin Liikenne- ja viestintäviraston ja sitä avustavan asiantuntijan oikeutta tarkastaa hyväksyntää hakevan ja hyväksytyn tietoturvallisuuden arviointilaitoksen tilat ja menetelmät ulotettaisiin koskemaan myös arviointilaitoslain 9 a §:ssä tarkoitettua arviointilaitoksen alihankkijaa. Tarkastusta ei ole tarkoitus eikä tarpeen näiltäkään osin ulottaa kotirauhan piiriin kuuluviin tiloihin.

Pätevyysalueen hyväksynnän perustelut (3 §:n muutos)

Traficom ehdottaa lain perusteluja tarkennettavaksi siten, että mahdollisuutta hakea hyväksyntää pätevyysalueelle ja siten myös lisäpätevyyksiä ei kuvata lain muutoksena vaan selkeyttämisenä. Näin esimerkiksi 3 §:n säännöskohtaisissa perusteluissa. Hyväksynnän hakeminen uudelle pätevyydelle on ollut mahdollista ja vallitseva käytäntö jo nykyisen lain perusteella. Arviointilaitokset ovat lain voimassa ollessa hakeneet eri aikoina esimerkiksi ISO/IEC 27001-standardin, VAHTI-ohjeiden ja Katakrin eri versioiden ja eri turvallisuusluokkien mukaisia lisäpätevyyksiä. On hyvä selkeyttää lakia siten, että mainitaan mahdollisuus hakea hyväksyntää arvioinnin pätevyysaluetta varten, mutta kysymyksessä ei ole varsinainen laitosten oikeuteen vaikuttava muutos. Sen sijaan uuden pätevyysalueen hyväksyntämenettelyn muutoksesta säädettäisiin 5 §:ssä.

Perustelut, luku 10 Suhde perustuslakiin ja säätämisjärjestys, Elinkeinovapaus (s. 61)

Koska 3 §:ssä ei ole kysymys muutoksesta laitosten oikeuksiin vaan informatiivisesta selkeytyksestä, muutoksen arvioiminen perustuslain ja säätämisjärjestyksen kannalta elinkeinovapauden näkökulmasta ei Traficomin käsityksen mukaan olisi tarpeen ja seuraavan virkkeen voisi poistaa: "Nyt ehdotettavassa arviointilaitoslain muutoksessa arviointilaitoslain 3 §:ään lisättäisiin mahdollisuus hakea hyväksyntä toiminnan lisäksi yksittäiselle pätevyysalueelle. Ehdotuksen on tarkoitus laajentaa arviointilaitosten toimintamahdollisuuksia."

Perustelut, luku 10 Suhde perustuslakiin ja säätämisjärjestys, Julkinen hallintotehtävä (s. 59)

Traficom ehdottaa, että arviointilaitosten alihankintaan liittyvää perusoikeusulottuvuuteen liittyvää tarkastelua harkitaan täydennettäväksi kohdassa julkinen hallintotehtävä. Vastaavaan alihankintajärjestelyyn on hiljattain otettu kantaa eräistä paloturvallisuuslaitteista annettua lakia (191/2024) koskevassa hallituksen esityksessä HE 106/2023, johon tukeutuen perusteluja voisi täydentää esimerkiksi seuraavasti: Arviointilaitoslain ehdotetun 9 a §:n mukaan hyväksytty tietoturvallisuuden arviointilaitos voisi käyttää alihankkijaa sille kuuluvien tehtävien suorittamiseen. Yksityiselle siirretyn julkisen hallintotehtävän edelleen siirtämiseen (subdelegointiin) on perustuslakivaliokunnan käytännössä suhtauduttu lähtökohtaisesti kielteisesti. Ehdotonta kieltoa tällaiselle siirtämiselle ei kuitenkaan ole ollut osoitettavissa tilanteissa, joissa on kyse teknisluonteisesta tehtävästä ja joissa alihankkijaan kohdistuvat samat laatuvaatimukset ja vastaava valvonta kuin alkuperäiseen palveluntuottajaan (PeVL 26/2017 vp, s. 51, PeVL 6/2013 vp, s. 4). Ehdotetun sääntelyn mukaan hyväksytty tietoturvallisuuden arviointilaitos olisi velvollinen antamaan alihankinnasta selvityksen Liikenne- ja viestintävirastolle, joka valvoisi, että alihankkija täyttää soveltuvin osin laissa säädetyt arviointilaitoksen hyväksymisen edellytykset. Hyväksytty tietoturvallisuuden arviointilaitos olisi myös oikeudellisessa vastuussa alihankkijalla toteuttamastaan työstä ja sillä olisi kokonaisvastuu asiakkaaseen nähden. Alihankkijoiden käytön ei siten nähdä muodostavan ehdotetun lain yhteydessä perustuslain 124 §:n kannalta sellaista subdelegointia, että se olisi perustuslain kannalta ongelmallinen, koska kyse on teknisluonteisista tehtävistä ja alihankkijaa koskevat samat vaatimukset kuin hyväksyttyä tietoturvallisuuden arviointilaitostakin.

Huomiot esityksen vaikutusten arvioinnista/ Kommentarer om bedömningen av propositionens konsekvenser:

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Traficom on saanut olla mukana HE-luonnoksen työryhmävalmistelussa ja sihteeristössä ja Traficomin käsitys on, että yleisesti ottaen keskeiset vaikutukset elinkeinotoimintaan ja viranomaisiin on sinänsä huomioitu asianmukaisesti. Viraston resurssien kannalta Traficom nostaa joitain esitykseen liittyviä huomioita ja viittaa muutoin Liikenne- ja viestintäministeriön lausuntoon.

Turvallisuuskriittisten ratkaisujen valmistus ja hyväksyntä

Turvallisuuskriittisten ratkaisujen valmistajien kannalta arviointi- ja hyväksyntätehtävän ja -perusteiden sääntelyperustan luominen ja itsenäinen mahdollisuus hakea hyväksyntöjä esitetyllä tavalla parantaa elinkeinotoiminnan edellytyksiä ja ennakoitavuutta olennaisesti. Ehdotettu sääntely tukee osaltaan hallitusohjelman tavoitteita salaustuotteiden arvioinnin nopeuttamisesta ja Suomen AQUA-maan aseman saavuttamisesta.

Esityksessä ei ehdoteta lisäresursseja arviointiviranomaisen toimintaan, mutta aivan kuten HE-luonnoksen vaikutusarvioinnissa todetaan, "arvioinnissa käytettävissä olevat resurssit vaikuttavat kuitenkin siihen, kuinka nopeasti ja tehokkaasti Liikenne- ja viestintävirasto pystyy tukemaan arvioinneilla ja hyväksynnöillä suomalaisia valmistajia ja kuinka laajasti vastaamaan viranomaisten pyyntöihin erilaisten tuotteiden ja ratkaisujen arvioinnissa." Salausratkaisujen ja turvallisuuskriittisten tuotteiden kysynnän nähdään kasvavan, mutta valmistajat tarvitsevat EU- ja

Nato-markkinoilla Liikenne- ja viestintäviraston hyväksynnän ratkaisuilleen ja suomalaiset yritykset voivat menettää merkittäviä liiketoimintamahdollisuuksia, koska Liikenne- ja viestintäviraston nykyinen resursointi ei riitä vastaamaan valmistajien tarpeisiin. Resurssipula johtaa pitkiin odotusaikoihin ja samoista arviointiresursseista on osoitettava asiantuntijat myös suomalaisten viranomaisten kiireellisimmin tarvitsemien tuotteiden järjestelmäkohtaisiin arviointeihin. Viraston rajalliset resurssit hidastavat yritysten vientimahdollisuuksia ja markkinoille tuloa ja heikentävät niiden kilpailuasemaa. Pahimmillaan tämä voi johtaa yritysten toimintojen siirtämiseen pois Suomesta. Lisäresursointi tehostaisi arviointitoimintaa, mahdollistaisi useamman tuotteen arvioinnin rinnakkain ja lyhentäisi arviointien kestoa, mikä parantaisi suomalaisten yritysten vientimahdollisuuksia. Arviointitoiminnan tehostaminen vahvistaisi myös Suomen asemaa NATO-maana turvallisuuskriittisten ratkaisu-jen valmistajana ja hyväksyjämaana.

EU:n kansainvälisiä tietoturvahyväksyntöjä myöntävän maan aseman (ns. AQUA-status) saaminen edellyttää, että Liikenne- ja viestintävirastolla on kansainväliset vaatimukset täyttävä kansallinen kyvykkyys arvioida algoritmeja ja salaustuotteita kansainväliselle SECRET-turvallisuusluokitustasolle asti. Salaustuotteiden täysimääräinen arviointikyvykkyys on osa kokonaisturvallisuutta ja kansallista huoltovarmuutta ja luo elinkeinoelämälle kilpailukykyä kansainvälisillä markkinoilla. AQUA-mailla tulee olla resursointi ja osaaminen arvioida kotimaisten salaustuotteiden lisäksi myös muiden maiden arvioimia salaustuotteita niin sanotussa Second Party Evaluator -roolissa.

Tietoturvallisuuden arviointilaitokset

Tietoturvallisuuden arviointilaitosten elinkeinotoiminnan edellytyksiin liittyy vaikutusarvioinnissa todetusti sekä heikentäviä että parantavia muutoksia. Kokonaisuutena vaikutusarviointiin voi siten liittyä epävarmuuksia. Julkishallinnon hankinta- ja sopimusmenettelyjen vaikutusta markkinoille pääsyyn ei ole arvioitu, mutta viranomaisten hankintajärjestelyillä ja pitkäaikaisilla hankintasopimuksilla voi olettaa olevan vain tilapäisesti uusien toimijoiden markkinoille pääsyä heikentävä vaikutus. Sen sijaan TL IV-arviointien tekijän valinnanvapauden ja yhteisten palveluiden arviointimenettelyjen vaikutus kysynnän muutoksiin ei ole vielä selvillä.

Arviointilaitoslain muutosten tarkoitus on selkeyttää ja parantaa edellytyksiä harjoittaa arviointilaitostoimintaa ja sitä kautta lisätä pätevien ja luotettavien arviointipalveluiden saatavuutta eri arviointiperusteiden mukaan. Tällöin arvioinnin hankkiva viranomainen ei joudu itse selvittämään arviointitahon luotettavuutta ja osaamista. Tietoturvallisuuden arviointilaitosten arvioinnin saatavuus on toki parantunut muutoinkin. On huomattava, että kuten työryhmän HE-luonnoksen nykytila-arviossa todettiin, vuosina 2021–2022 oli lähes vuoden ajanjakso, jona ajantasaisen Katakri-pätevyyden mukainen arviointi oli saatavilla vain yhdeltä arviointilaitokselta ja tilanteen voidaan arvioida heijastuneen paitsi saatavuuteen myös hinnoitteluun. Sittemmin alkuvuonna 2025 on hyväksytty jo kolmas arviointilaitos tekemään Katakri TL IV ja TL III -arviointeja. Tämän voi olettaa lisäävän kilpailua, mutta viranomaisten pitkäkestoisten hankintasopimusten takia kolmannen tarjoajan vaikutuksia arviointien tarjontaan ja hintoihin ei vielä ole mahdollista todeta. Viranomaisten tarpeiden kannalta kokonaisuutena on kuitenkin huomattava, että kun arviointilaitosten tekemä arviointi kohdistuu Valtorin tuottamiin yhteisiin tieto- ja viestintäteknisiin

palveluihin, yksinomaan arviointilaitosten resurssit eivät vaikuta mahdollisiin pullonkauloihin, vaan on tärkeää, että myös Valtorilla on riittävästi resursseja mahdollistaa arviointeja.

Tempest-arviointi tietojärjestelmän osana (s. 23, toinen kappale)

Traficom ehdottaa vaikutusarvioinnissa seuraavan lausuman palauttamista koskemaan työryhmän HE-luonnoksessa esitetyllä tavalla hajasäteilysuojauksen arviointia osana tietojärjestelmien arviointeja: "Tietojärjestelmän tai tietoliikennejärjestelyn arvioinnin laajentamisella niihin kuuluvan turvallisuuskriittisen ratkaisun tietoturvallisuuden ja varautumisen arviointiin ei ole välitöntä resurssivaikutusta Liikenne- ja viestintävirastolle tai Puolustusvoimille. Viranomaisten ja niiden palveluntuottajina olevien yritysten tietojärjestelmien hajasäteilysuojauksen arviointi on osa tietojärjestelmien tietoturvallisuuden arviointia ja voi perustua joko vyöhykkeisiin tai tilojen tai laitteiden kykyyn estää tahatonta hajasäteilyä. Tehtävistä huolehditaan käytännössä usean viranomaisen yhteistyöllä ja näiden viranomaisten arvion mukaan vyöhyke- ja tilamittauksiin liittyy nähtävissä oleviin operatiivisiin tarpeisiin vastaamiseksi vähäistä henkilöresurssien lisäystä. Salaustuote- ja TEMPEST-tehtäviin liittyy myös laboratoriokyvykkyyden tarve, jonka resurssivaikutukset riippuvat valittavista toteutusmalleista."

Traficom korostaa, että kyseinen kappale ja huomio resursseista kuvaa vain tietojärjestelmien arviointiin korkeimmissa turvallisuusluokissa liittyvien tapauskohtaisten vyöhyke- tai tilamittausten ja niiden analysoinnin tehtäviä ja näihin tehtäviin osallistuvien viranomaisten yhdessä muodostamaa näkemystä vallitsevasta resurssitilanteesta ja -kapeikosta, jolla on käytännön vaikutusta erityisesti arviointien ja kansainvälisten tietoturvallisuusvelvoitteiden tilanteessa hyväksyntöjen aikatauluun. Valtionhallinnon viranomaisille ehdotettavalla tietojärjestelmien arviointivelvoitteella voi olla tarpeisiin jossain määrin vaikutusta korkeimmissa turvallisuusluokissa. Muiden arviointitehtävien, erityisesti turvallisuuskriittisten ratkaisujen mukaan lukien hajasäteilysuojausratkaisujen valmistuksen, vaikutuksia käsitellään lausunnossa edellä ja HE-luonnoksessa muissa kappaleissa.

Julkishallinnon tietoturvallisuus ja varautuminen

Viranomaisvaikutuksista Traficom toteaa, että arviointisääntelyn perustarkoitus on osaltaan vahvistaa julkishallinnossa käytettävän ICT:n tietoturvallisuutta ja varautumista, mikä on sekä yleisesti digitalisaation jatkuvasti lisääntyessä että erityisesti vallitsevassa turvallisuustilanteessa tärkeä tavoite. Arviointimenettelyjen lisääminen ja selkeyttäminen arviointilaissa on kannatettavaa ja sen voidaan nähdä lisäävän arviointeja. Kuten vaikutusarvioinnissa todetaan, arviointien avulla on mahdollista saavuttaa korkeampi tietoturvallisuuden taso ja parantaa varautumista tietoturvahäiriöihin ja -loukkauksiin.

Yhteiset palvelut

Julkishallinnon tietoturvallisuuteen ja varautumiseen kokonaisuutena vaikuttavat olennaisesti myös yhteisesti tuotetut palvelut ja niiden arviointi. HE-luonnos jättää kuitenkin tällä hetkellä tulkinnanvaraiseksi, koskeeko velvollisuus tehdä vähintään itsearviointi myös tiedonhallintayksikön käyttämiä yhteisiä palveluja. Tämän vuoksi on tärkeää, että itsearviointien tekemistä tuetaan toimeenpanovaiheessa ohjeistuksella omissa ja yhteisissä palveluissa niissä tapauksissa, joissa yhteisiä palveluja koskeva sääntely, riskiarvio tai turvallisuusluokittelu ei edellytä muutakin menettelyä kuin itsearviointia. Jatkossakin Valtori ja Hansel voivat hankkia arviointipalveluita tietoturvallisuuden arviointilaitoksilta ja arviointilain 4 §:n 4 momentin valossa ne voivat pyytää arviointia Liikenne- ja viestintävirastolta. Traficom kiinnittää huomiota siihen, että tiedonhallintayksikkö tarvitsee tietoa myös käyttämiensä yhteisten palveluiden tietoturvallisuuden riskeistä ja tietoturvallisuuden varmistamisesta ja esittää, että suhdetta yhteisiin palveluihin selkeytettäisiin soveltuvassa kohdassa lain perusteluissa esimerkiksi kirjauksella, että viranomainen tarvitsee riskinhallinnassaan myös tiedot käyttämiensä yhteisten palveluiden arvioinnista.

HE-luonnoksessa viitataan sääntelyn muiden vaihtoehtojen kuvauksessa (s. 25-26) valtion yhteisten tieto- ja viestintäteknisten palvelujen arvioinnin ja Valtorin roolin osalta erillisen lainsäädännön päivittämiseen. Käynnissä on valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisen (Tori-toiminta) ja turvallisuusverkkotoiminnan (Tuve-toiminta) kehittämishanke (VN/19401/2024-VM-2, T2-hanke). Traficom pitää tärkeänä, että T2-hankkeen edetessä huomioidaan myös arviointien vaikuttavuus viranomaisten toiminnassa käytettävien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuteen ja varautumiseen sekä riskienhallintaan ja riskipäätöksiä koskevaan vastuuseen perustuvat arviointilain periaatteet.

Lohtander Anne
Traficom - Liikenne- ja viestintävirasto