

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

Maanmittauslaitos kiittää mahdollisuudesta lausua valtiovarainministeriön lausuntopyyntöön ehdotuksesta viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisesta annetun lainsäädännön muuttamisesta.

Maanmittauslaitos tuo esiin asiassa seuraavaa.

Maanmittauslaitos pitää soveltamisalan laajentamista varautumisen arviointiin (1 §, 2 § 6-kohta, 7 §) lähtökohtaisesti kannatettavana. Varautumisen tuominen lain tasolle selkeyttää velvoitteita ja parantaa jatkuvuudenhallinnan yhdenmukaisuutta.

Muutosvaikutusten arviointi: (i) varautumisen vaatimukset on johdettava järjestelmätasolle (RTO/RPO, toipumisharjoitukset, riippuvuuksien hallinta), (ii) evidenssiä varautumisen toimivuudesta on kerättävä ja esitettävä arviointiraporteissa, (iii) yhteistyö palveluntuottajien kanssa tiivistyy.

Edellytys varautumisen todentamisesta kasvattaa auditointi- ja testauskapasiteetin tarvetta ja vaatii entistä tiiviimpää yhteistyötä eri sidosryhmien ja palveluntuottajien kanssa.

Ehdotuksena muutoksesta on, että VM tai Traficom laatii yhteiset varautumisen arviointiperusteet ja mallit tai tarkastuslistat, joita virastot voivat soveltaa järjestelmäkohtaisesti. Em. voivat olla ohjeistuksena, jotta helpotetaan yhdenmukaista valmistautumista ottaen huomioon, että yksityiskohtien tarve vaihtelee virastoittain.

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

Maanmittauslaitos suhtautuu kokonaisuuteen myönteisesti. Arviointipolku on selkeä, mutta edellyttää: (i) systemaattista turvallisuusluokittelua, (ii) vuosittaista arviointisuunnitelmaa ja (iii) päätösperiaatteita III-luokan ollessa kysymyksessä.

Lakiin ja ohjeisiin on tehtävä täsmennys, että III-luokan riskiperusteinen poikkeaminen ulkoisesta arvioinnista dokumentoidaan johdon päätöksellä ja liitetään arviointiraporttiin (8 §) jäännösriskin käsittelyn näkyväksi tekemiseksi.

Itsearviointin osaamista on vahvistettava, jotta mallit, kriteeristöt ja tekniset todentamismenetelmät vastaavat arviointimenettelyjen edellytyksiä.

Hankintadokumenteissa on varmistettava mahdollisuus arviointeihin ja auditointeihin, sisällytettävä tiedon suojaaminen, salassapito- ja tietoturva vaatimukset sekä tarvittaessa henkilöstön turvallisuusselvitykset.

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

Traficom ja Pääesikunnan DSA:n roolien selkeyttäminen on kannatettavaa. Välttämättömyyskriteeri tiedonsaannissa (6 §) on perusteltu.

Laitoksen näkökulmasta korostuu tarkastuksiin valmistautuminen: tarvittava dokumentaatio ja tekniset näytöt (esim. tarvittavat logit, skannaukset, konfiguraatiodiedot), tilojen ja järjestelmien pääsyjärjestelyt (edellyttää myös sopimuksellista varmistusta palveluntuottajien tiloihin ja järjestelmiin). Myös tietojen luovutuksen politiikka ja salassapidon käytännöt tarkastustilanteita varten on ohjeistettava ja varmistettava.

Ehdotetaan, että Traficom julkaisee tarkastusten vähimmäisdokumentaatiolistan ja tekniset todentamismenetelmät (ohje), jotta virastot voivat valmistautua mahdollisiin tarkastuksiin yhdenmukaisesti.

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

Maanmittauslaitos pitää myönteisenä, että Traficom voi arvioida kotimaisia salaus-, TEMPEST- ja muita turvallisuuskriittisiä ratkaisuja sekä julkaista hyväksytyjen luettelon (8 c §). Tämä nopeuttaa tuotekohtaista arviointia ja hankintoja.

Hyväksyntäpäätösten liitteenä voisi julkaista lyhyen turvallisen käytön käyttöpolitiikan, jotta virastot voivat varmistaa käyttöympäristönsä riittävyden.

Maanmittauslaitoksen kannalta valmistuksen arviointi ulottuu alihankkijoihin, jolloin hankintasopimuksissa on edellytettävä riittäviin tietoihin ja muihin kokonaisuuden arvioinnin kannalta oleellisiin ratkaisuihin pääsyä.

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

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Siirtymäajat ovat realistisia, mutta edellyttävät myös arviointiviranomaisten kapasiteetin suunnittelua. Etusijalla on oltava I-II luokat, sitten III ja muun portfolion kohdalla sen jälkeen.

Valtionhallinnon tasolla edellytetään toimijaa, joka koordinoi valtionhallinnon yhteistä aikataulutusta, jotta kriittisimmät järjestelmät priorisoidaan ja arviointijonot pysyvät hallittuina.

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

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Seuraavat havainnot:

3 § 2 mom: Palveluntarjoaja-arvioinneissa Maanmittauslaitoksen on ennalta varmistettava palveluntuottajan luotettavuus (tausta, henkilöstö, omistus, tietojenkäsittelyn suoja). Tämä vaatii valmiin menettelyn ja hankintasopimukseen vahvat tietoturva- ja salassapitoehdot.

7 § 2 mom: Arviointiperusteet ja kohderajaus riskiperusteisesti: hyvä, että arviointiviranomainen asettaa perusteet kuullen hakijaa. Tämä vähentää väärinymmärryksiä auditointikriteereistä.

8 §: Todistuskäytännön korvaaminen arviointiraportilla ja tarvittaessa hyväksyntäpäätöksellä/lausunnolla parantaa johdon jäännösriskipäätösten laatua.

12 §: Neuvonta tulee maksulliseksi eli jos Maanmittauslaitos tarvitsee Traficomien ohjausta suunnitteluvaiheessa, tämä vaatii erillisrahoitusta.

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

Esitetty parantaa luottamusta ulkoisiin arviointeihin ja vähentää tarvetta Maanmittauslaitoksen omille, päällekkäisille taustaselvityksille. Suomeen sijoittautumisen vaatimus valvonnan toimivuuden varmistamiseksi on kannatettavaa.

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

Joustavampi lisäpätevyyksien hyväksyntä voi lisätä arviointikapasiteettia. Traficom voisi julkaista kriteerit ja vertailuperusteet, jotta hankkijat voivat arvioida ko. lisäpätevyyksien soveltuvuuden omiin tarpeisiin.

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

Seuraavat huomiot:

7 §: Arviointi voi edellyttää tietojen saantia myös Maanmittauslaitoksen asiakkaalta.

9 a §: Alihankinta turvallisuusluokitellun tiedon arvioinnissa vain asiakkaan nimenomaisella suostumuksella on kannatettavaa.

13 §: Kun arviointilaitoksen henkilöstö ja asiantuntijat toimivat rikosoikeudellisella virkavastuulla, tämä parantaa oikeusturvaa ja toiminnan laatuvaatimuksia.

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

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Vaikutusarviot ovat pääosin realistisia. Arviointien lisääntyminen kasvattaa kustannuksia lyhyellä aikavälillä. Jos Maanmittauslaitos voi kehittää omaa itsearviointikyvykkyyttään riittävästi, tämä voi tuoda kokonaissäästöjä. Toisaalta arvioinnit myös vähentävät tietoturvapoikkeamien riskiä ja em. aiheutuvia suoria ja epäsuoria kustannuksia ja maine- tai luottamusriskiä.

Kokonaisuus edellyttää Maanmittauslaitokselta järjestelmien säännöllistä inventointia ja tietovirtojen luokittelua sekä em. pohjalta arviointimenettelyjä (ulkoinen vs. itsearviointi). Itsearviointikyvykkyyden luominen tarkoittaa soveltuvien kriteeristöjen (mm. Julkri, NIS2 käytännöt) osaamista, teknisten todentamismenetelmien hyödyntämistä (mm. skannaukset) sekä arviointiraporttien dokumentointimallin systematisointia. Budjetoinnissa on tarvittaessa varauduttava ulkoisiin arviointeihin ja Traficomın maksulliseen neuvontaan.

Hankintasopimuksissa palveluntarjoajia on arvioitava ja tehtävä tarpeelliset taustaselvitykset, varmistuttava tiedon suojaamisen ehdoista sekä audit- ja pääsyoikeuksista.

Valtionhallinnon tasolta esim. VM tai Traficom voisivat tukea virastoja itsearviointikyvykkyyden rakentamisessa (esim. koulutuspaketit, malliraportit, teknisen todentamisen suositukset).

Mikkonen Soile

Maanmittauslaitos - Pääjohtajan sijaisena ylijohtaja Petri Korpinen ja
maanmittausneuvos Markku Markkula