

Yritysturvallisuusselvitykset Puolustusvoimissa

19. Turvallisuusjohdon koulutusohjelma.

Lopputyöraportti

Markus Koskivirta

Puolustusvoimat

Helsingissä 9.2.2026

Aalto University Executive Education and Professional Development

Tiivistelmä

Teos toimii perehdytysoppaana ja jatko-osa vuoden 2017 projektityölle, ja se käsittelee Pääesikunnan (PE DSA) tekemiä kansallisia yritysturvallisuusselvityksiä. Teoksen tarkoituksena on kuvata turvallisuusselvityslain (726/2014) mukaiset prosessit, toimintaperiaatteet ja viranomaisroolit. Teos toimii perehdytysoppaana yritysturvallisuusselvityksien peruseriaatteista ja selvityksiin liittyviin prosesseihin sekä asiakirjoihin. Yritysturvallisuusselvityksissä arvioidaan yrityksen tietoturvan tasoa, sitoumuksenhoitokykyä ja vastuuhenkilöiden nuhteettomuutta.

Sisällysluettelo

Yritysturvallisuusselvitykset Puolustusvoimissa	1
1 Johdanto	1
2 Määritelmät, rajausta ja käsitteet	4
2.1 Määritelmät	4
2.2 Tutkimuskysymykset	4
2.3 Rajausta	5
2.4 Käsitteet.....	5
3 Yritysturvallisuusmalli.....	7
4 Toimivaltaiset viranomaiset.....	9
4.1 Kansallinen turvallisuusviranomainen, NSA	9
4.2 Pääesikunta, PE DSA	9
4.3 Suojelupoliisi, SUPO DSA	9
4.4 Liikenne- ja viestintävirasto Traficom, NCSA	10
4.5 Puolustusministeriö, PLM DSA.....	10
4.6 Ohjaavat asiakirjat.....	10
4.6.1 Yleiset	10
4.6.2 Puolustusvoimat.....	11
5 Yritysturvallisuusselvitys.....	12
5.1 Tarkoitus.....	12
5.2 Kohde	13
5.3 Hakija	13
5.4 Hakemus (liitteet 4 ja 5).....	14
5.5 Selvitystyö.....	16
5.6 Selvitystyön valmistuminen	17
5.7 Luovutustilaisuus	18
5.8 Voimassaolo ja päättäminen.....	18
5.9 Yritysturvallisuusselvityksen seuranta.....	18
5.10 Kielteinen päätös	19
6 Yritysturvallisuusselvitystodistus ja siihen liittyvät asiakirjat.....	20
6.1 Yritysturvallisuusselvitystodistus (liite 1).....	20
6.2 Yritysturvallisuusselvityksen loppuraportti (liite 2)	20
6.3 Sitoumus (liite 3).....	20
7 Yritysturvallisuusselvityksen eri laajuudet	21
7.1 Henkilöturvallisuusselvitykset	21
7.2 Suppea tai FSC without safeguards (w/o).....	21
7.3 Perusmuotoinen tai FSC with safeguards.....	21
7.4 Laaja tai FSC with safeguards including CIS	21

8	Yritysturvallisuusselvityksiin liittyvät tarkastukset (auditoinnit)	23
8.1	Katakri – auditointityökalu	23
8.2	Tilaturvallisuus (toimitilaturvallisuus)	23
8.2.1	Hallinnollinen alue	23
8.2.2	Turva-alue	24
8.2.3	Teknisesti suojattu turva-alue.....	24
8.3	Tekninen tietoturvatarkastus (CIS).....	24
8.4	Turvallisuustarkastaja (auditoija)	26
9	Yritysturvallisuusselvityksiin liittyvät edut, tavoitteet ja rajoitteet	27
9.1	Yritysturvallisuusselvityksen edut.....	27
9.2	Keskeiset tavoitteet ja käyttötarkoitukset	27
9.3	Yritysturvallisuusselvitykseen liittyvät rajoitteet	28
10	Yritysturvallisuusselvityksien maksullisuus	29
11	Johtopäätökset	31

1 Johdanto

Turvallisuusselvityslaki (726/2014) ja siihen liittyvät säädökset tulivat voimaan 1.1.2015. Sillä kumottiin vuonna 2002 säädetty laki turvallisuusselvityksistä (177/2002).

Turvallisuusselvityslain tarkoituksena on parantaa mahdollisuuksia ennakolta ehkäistä toimintaa, joka voi vahingoittaa valtion turvallisuutta, maanpuolustusta, Suomen kansainvälisiä suhteita, yleistä turvallisuutta tai muuta niihin verrattavaa yleistä etua taikka erittäin merkittävää yksityistä taloudellista etua taikka tällaisten etujen suojaamiseksi toteutettavia turvallisuusjärjestelyjä. Lain avulla on pyritty luomaan tehokas menettely henkilöiden ja yritysten taustojen selvittämiseksi. Sen avulla osana yleisen edun suojaa turvataan turvallisuutta ja yhteiskunnan toimivuuden kannalta kriittisen infrastruktuurin toimivuutta riippumatta siitä, onko kysymys julkishallinnossa vai yksityissektorilla hoidettavasta tehtävästä. Turvallisuusselvityslain tarkoituksena on lähentää alan lainsäädäntöä vastaamaan kansainvälisesti yleisesti noudatettavia sääntöjä ja käytäntöjä. Lakia säädettäessä on kuitenkin otettu huomioon suomalaisen yhteiskunnan erityispiirteet, kuten henkilön tunnistettavuus henkilötunnuksen avulla ja erilaisten tietojärjestelmien kattavuus samoin kuin muu työnhakijan taustatietojen hankintaa koskeva lainsäädäntö. Turvallisuusselvityslaille lisätään myös avoimuutta ja vuorovaikutteisuutta turvallisuusselvitysmenettelyssä sekä varmistetaan menettelyn tehokkuutta ja yhdenmukaisuutta lain soveltamisessa¹.

Turvallisuusselvitysten avulla selvitetään joko luonnollisten henkilöiden (henkilöturvallisuusselvitys) tai yritysten (yritysturvallisuusselvitys) taustoja näiden luotettavuuden varmistamiseksi. Selvitysmenettelyt kohdistuvat hen-

¹ Oikeusministeriön yleisesittely turvallisuusselvityslaista 16.12.2014

Johdanto

kilöihin ja yrityksiin, jotka pääsevät turvallisuuden kannalta kriittisiin tietoihin tai tehtäviin ja joissa edellytetään erityistä luotettavuutta tehtävien hoidossa².

Pääesikunta päättää yritysturvallisuusselvityksen tekemisestä yrityksestä, joka hoitaa tai jonka on tarkoitus hoitaa puolustusvoimien antamaa tehtävää, taikka yrityksestä, joka liittyy Puolustusvoimien hankintoihin. Yritysturvallisuusselvitys tehdään niiltä sidosryhmiltä, jotka käsittelevät tai joille luovutetaan Puolustusvoimien turvallisuusluokan III (luottamuksellinen), turvallisuusluokan II (salainen) ja turvallisuusluokan I (erittäin salainen) tietoa. Toimintaa valvova viranomaisen voi pyytää yritysturvallisuusselvitystä myös niistä sidosryhmistä, jotka käsittelevät tai joille luovutetaan Puolustusvoimien turvallisuusluokan IV (käyttö rajoitettu) tietoa. Tarve yritysturvallisuusselvitykseen ja sen perusteella myönnetylle todistukselle voi liittyä myös kansainvälisiin tietoturvallisuusvelvoitteisiin. Selvitys on aina harkinnanvarainen.

Tässä teoksessa pääpaino on kuvata Pääesikunnan määrätyn turvallisuusviranomaisen tekemien yritysturvallisuusselvityksien perusperiaatteet ja toimintatavat.

Pääesikunnan työjärjestys määrittää toimivaltaisen viranomaisen (PE DSA, Designated Security Authority) roolin Pääesikunnan tiedusteluosastolle (PE TIEDOS).

Teos on tarkoitettu esimerkiksi perehdytysoppaaksi kuvaamaan yritysturvallisuusselvityksien tarkoitusta, toimintaperiaatteita sekä prosesseja Puolustusvoimissa.

Yritysturvallisuusselvitykset – aihetta on käsitelty aikaisemmin Aalto PRO:n 14. turvallisuusjohdon koulutusohjelman projektityössä vuonna 2017 (Yritysturvallisuusselvitykset, Reijo Kaariste, Puolustusvoimat). Aiheeseen niinkään liittyvä teos ”Sitoumuksen valvontakyvyn hallintamalli Puolustusvoimien sidosryhmille” on laadittu 18. Turvallisuusjohdon koulutusohjelmassa (Jani Rantanen, Puolustusvoimat). Rantasen teos käsittelee aihekokonaisuutta miten toimivaltaisen viranomaisen ja määrätyn turvallisuusviranomaisen tulisi osana puolustusjärjestelmän suojaamista, turvallisuusselvityslain

² Oikeusministeriön yleisesittely turvallisuusselvityslaista 16.12.2014

(726/2014) 40 §:n mukaisesti valvoa yritykselle myönnetyn yritysturvallisuusselvitystodistuksen sitoumuksen hoitokykyä ja siinä tapahtuvia muutoksia³.

Tämän nyt tehdyn teoksen on tarkoitus toimia jatko-osana Kaaristeiden työlle. Tässä teoksessa paneudutaan enemmän itse selvitysprosessiin ja sen käytänteisiin, joita on opittu vuosien aikana selvitystyötä tehtäessä.

³ 18. Turvallisuusjohdon koulutusohjelman lopputyöraportti (Jani Rantanen).

2 Määritelmät, rajaus ja käsitteet

2.1 Määritelmät

Teosta varten tutustuin yritysturvaluusselvityksestä kirjoitettuun aineistoon. Aiheesta on lainsäädäntöä ja rajallinen määrä viranomaisten ohjeita ja normeja. Kirjallisuuskatsauksen⁴ tapaan päädyttiin käytettävään lähdeaineistoon, joka suurelta osin on edellä kuvattua lainsäädäntöä, ohjeita ja normeja. Teos ei sinällään ole tutkimustyö, mutta teoksessa pyritään käsittelemään aihetta laadullisella⁵ tutkimusotteella. Aineistoa käsiteltäessä käytettiin teorialähtöistä sisällönanalyysiä⁶. Sisällönanalyysissä aineisto järjestetään tiiviiseen muotoon, siten että aineiston informaatio ei katoa. Analysoinnin tarkoituksena on lisätä informaatioarvoa, niin että laajasta aineistosta saadaan yhtenäinen, selkeä informaatiokokonaisuus. Aiheesta kerrotaan perusteet ja prosessit. Tarkoituksena on jättää lukijalle selkeä kuvaus miksi ja miten yritysturvaluusselvityksiä laaditaan Puolustusvoimissa.

2.2 Tutkimuskysymykset

Pääkysymys:

1. Mikä on yritysturvaluusselvitys?

Alakysymykset:

1. Miten yritysturvaluusselvitykset tehdään Puolustusvoimissa?
2. Mitä asioita tulee huomioida yritysturvaluusselvityksen tekemisessä?
3. Mitä lakeja, ohjeita ja asiakirjoja yritysturvaluusselvityksiin liittyy?

⁴ Hirsjärvi S. et al, Tutki ja kirjoita, 11. painos s.111

⁵ Hirsjärvi S. et al, Tutki ja kirjoita, 11. painos s.152

⁶ www.fsd.uta.fi/menetelmaopetus/kvali/L7_3_2.html (30.3.2017)

2.3 Rajaus

Teos on rajattu käsittelemään vain Pääesikunnan laatimia kansallisia yritysturvallisuusselvityksiä. Henkilöturvallisuusselvityksiä käsitellään ainoastaan kohdissa, jossa ne liittyvät yrityksen vastuuhenkilöistä tehtäviin turvallisuusselvityksiin. Teoksessa käsitellään muita viranomaisia vain niiltä osin kuin se on tarkoituksenmukaista teoksen kokonaisuuden ymmärtämiseksi.

2.4 Käsitteet

Yritysturvallisuudella yrityksen kaikkien toimintojen turvallisuutta.

Yritysturvaluustoiminnalla, toimia, joilla voidaan suojata yritysten tärkeitä arvoja kuten henkilöitä, tietoa, mainetta, omaisuutta ja ympäristöä.

Yritysturvaluusselvityksellä yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumuksenhoitokyvyn arvioimiseksi laadittavaa selvitystä.

Henkilöturvallisuusselvityksellä henkilön nuhteettomuuden ja luotettavuuden varmistamiseksi laadittavaa selvitystä.

Henkilöturvallisuusselvitystodistus (Personal Security Clearance, PSC)

Turvallisuusselvityksellä henkilöturvallisuusselvitystä ja yritysturvaluusselvitystä.

Yrityksen vastuuhenkilöllä henkilöä, joka merkitään viranomaisen julkiseen rekisteriin yhtiömiehenä, vastuullisena yhtiömiehenä, toimitusjohtajana, yrityksen hallituksen puheenjohtajana, hallituksen jäsenenä tai varajäsenenä tai henkilöä, jolla on prokuura- ja nimenkirjoitusoikeus.

Yritysturvaluusselvityshakemuksella viranomaisen laatimaa määrämukoista hakemusta.

Kansallinen yritysturvaluusselvitystodistuksella viranomaisen yritysturvaluusselvityksen perusteella yritykselle myöntämää todistusta.

Kansainvälisellä yritysturvaluusselvitystodistuksella (FSC, Facility Security Clearance) kansallisen turvallisuusviranomaisen myöntämää todistusta

Määritelmät, rajaus ja käsitteet

Viestintä- ja tietojärjestelmät (CIS, Communications and Information Systems)

Kansallisella turvallisuusviranomaisella (NSA, National Security Authority) kansainvälisistä tietoturvallisuusvelvoitteista annetulla lailla (588/2004) määrättyä ulkoasiainministeriössä toimivaa turvallisuusviranomaista.

Kansallisella tietoturvallisuusviranomaisella (NCSA, National Communications Security Authority) Liikenne – ja viestintäviraston (Traficom) Kyber-
turvallisuuskeskuksessa toimivaa turvallisuusviranomaista, joka vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja –käsittelyyn liittyvistä turvallisuusasioista.

Määrätyllä turvallisuusviranomaisella (DSA, Designated Security Authority) kansainvälisistä tietoturvallisuusvelvoitteista annetulla lailla (588/2004) määrättyä puolustusministeriössä (PLM DSA), suojelupoliisissa (SUPO DSA), pääesikunnassa (PE DSA) tai Traficomissa (NCSA) toimivaa turvallisuusviranomaista.

Toimivaltainen viranomainen, viranomainen, joka hoitaa kansalliseen turvallisuuteen liittyviä tehtäviä

PSCIS, Personal Security clearance information sheet

Turvallisuusselvitysrekisteri, Turvallisuusselvitysrekisteriin tallennetaan tiedot henkilöistä sekä yrityksistä (tai yhteisö), joista on tehty turvallisuusselvityslain mukainen turvallisuusselvitys tai yritysturvallisuusselvitys

Yrityksen yhteyshenkilö, henkilö, joka on merkitty yritysturvallisuusselvityshakemuksessa kohteena olevan yrityksen vastuuhenkilöksi.

Katakri 2020, on Suomen kansallisen turvallisuusviranomaisen (Ulkoministeriö) ylläpitämä auditointityökalu, jolla arvioidaan organisaation kykyä suojata turvallisuusluokiteltua tietoa.

Tekninen turvatarkastus eli TSCM (*Technical Surveillance Countermeasures*) on toimenpidekokonaisuus, jolla varmistetaan, ettei tilassa ole luvattomia kuuntelu-, katselu- tai lähetinlaitteita.

3 Yritysturvallisuusmalli

Elinkeinoelämän keskusliitto (EK) on määritellyt, että yritysturvallisuuden keskeinen tehtävä on edistää yrityksen kilpailukykyä ja parantaa tuottavuutta. Turvallisuusjohtaminen on osa normaalia yrityksen johtamista. Tavoitteena ei ole erillinen turvallisuustoiminto, vaan yrityksen toiminnan jatkuvuuden, turvallisuuden ja vaatimustenmukaisuuden varmistaminen kaikissa tilanteissa, luonnollisena osana yrityksen riskienhallinnan kokonaisuutta. Yritysturvallisuuden keskeinen tehtävä on edistää yrityksen kilpailukykyä ja parantaa tuottavuutta. Turvallisuusjohtaminen on osa normaalia yrityksen johtamista. Tavoitteena ei ole erillinen turvallisuustoiminto, vaan yrityksen toiminnan jatkuvuuden, turvallisuuden ja vaatimustenmukaisuuden varmistaminen kaikissa tilanteissa, luonnollisena osana yrityksen riskienhallinnan kokonaisuutta⁷.

⁷ <https://ek.fi/hyotytietoa-yrityksille/yritysturvallisuus/>



Kuva 1 Elinkeinoelämässä on kehitetty yritysturvallisuusmalli (ek.fi)

Yritysturvallisuus selvityksellä (Turvallisuus selvityslaki 726/2014 3§ 1 mom. 2 k.) tarkoitetaan yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumustenhoitokyvyn arvioimiseksi turvallisuus selvityslain mukaisesti laadittavaa selvitystä. Selvitystyössä käytetään turvallisuus selvityslain mukaisia rekisteritarkastuksia sekä tilojen auditointiin Katakri 2020 – auditointikriteeristöä (tietoturvallisuuden auditointityökalua viranomaisille).

Selvitys kattaa laajasti yrityksen turvallisuuteen vaikuttaviin tekijöihin. Elinkeinoelämän keskusliiton yritysturvallisuus – määritelmään turvallisuus selvityslain mukaisesti määritelty yritysturvallisuus selvitys ei ota kantaa työ-, ympäristö- ja tuotannon ja toiminnan turvallisuuteen. Yritysturvallisuus mallissa (kuva 1.) yritysturvallisuus selvitys ottaa kantaa pelastusturvallisuuteen turvatilojen osalta sekä varautumiseen ja kriisinhallintaan turvaluokiteltujen tietojen ja tilojen osalta.

4 Toimivaltaiset viranomaiset

4.1 Kansallinen turvallisuusviranomainen, NSA

Suomessa kansallisena turvallisuusviranomaisena toimii ulkoministeriössä toimiva erillinen yksikkö NSA (National Security Authority) joka ohjaa kansallista toimintaa ja vastaa muun muassa kansainvälisten tietoturvallisuusso-
pimusten valmistelusta⁸.

NSA:n tehtävänä on erityisesti ohjata ja valvoa, että kansainväliset turvallisuusluokitellut tietoaineistot suojataan ja niitä käsitellään asianmukaisesti sekä viranomaisissa että yrityksissä. NSA myöntää kansainvälisten tietotur-
vallisuusvelvoitteiden edellyttämät henkilö (PSC) - ja yritysturvallisuustodis-
tukset (FSC). Lisäksi NSA koordinoi määrättyjen turvallisuusviranomaisten
toimintaa ja edustaa Suomea kansainvälisissä turvallisuuskomiteoissa ja –
työryhmissä sekä johtaa kahden- ja monenvälisten tietoturvallisuusso-
pimusten neuvotteluja. NSA huolehtii myös kansainväliseen turvallisuusluokitel-
tuun tietoon kohdistuvien tietoturvallisuusrikkomusten selvittämisestä⁹.

4.2 Pääesikunta, PE DSA

Pääesikunta päättää turvallisuusselvityksen tekemisestä silloin, kun selvityk-
sen kohteen on tarkoitus toimia puolustusvoimissa tai hoitaa puolustusvoi-
mien antamaa tehtävää taikka jos turvallisuusselvitys liittyy puolustusvoi-
mien toimintaan tai hankintoihin. Pääesikunta toimii lisäksi suojelupoliisin
tapaan määrättyinä turvallisuusviranomaisena (Designated Security Autho-
rity, DSA) kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa.

4.3 Suojelupoliisi, SUPO DSA

Suojelupoliisi on turvallisuusselvityslaisissa (726/2014) tarkoitettu toimivaltai-
nen viranomainen, jolla on yleinen toimivalta päättää turvallisuusselvitysten

⁸ <https://um.fi/kansallinen-turvallisuusviranomainen>

⁹ Turvallisuusviranomaisten käsikirja yrityksille, 2021

tekemisestä. Suojelupoliisi päättää henkilöturvallisuusselvityksen ja yritysturvallisuusselvityksen laatimisesta, ellei tehtävä kuulu Pääesikunnalle.

Suojelupoliisi toimii myös määrättyinä turvallisuusviranomaisena (Designated Security Authority, DSA) ja kansallisen turvallisuusviranomaisen asiantuntijana kansainvälisten tietoturvaluusvelvoitteiden toteuttamisessa erityisesti henkilöstö-, yritys- ja toimitilaturvallisuutta koskevissa asioissa.

4.4 Liikenne- ja viestintävirasto Traficom, NCSA

Liikenne- ja viestintävirasto Traficom voi laatia yritysturvallisuusselvityksen *osana* tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvaluuden tasoa koskevan arvioinnin. Liikenne- ja viestintävirasto toimii kansallisena tieto- ja tietoliikenneturvaluudesta vastaavana viranomaisena (National Communications Security Authority, NCSA).

NCSA:n tehtäviin kuuluu kansainvälistä turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien hyväksyntä (Security Accreditation Authority, SAA), minkä lisäksi se toimii kansallisen turvallisuusviranomaisen asiantuntijana tietojärjestelmien ja tietoliikennejärjestelyjen turvallisuutta koskevissa asioissa.

4.5 Puolustusministeriö, PLM DSA

Puolustusministeriö toimii määrättyinä turvallisuusviranomaisena (Designated Security Authority, DSA (Israel) ja osallistuu kansainväliseen yhteistyöhön omalla hallinnonalallaan. Puolustusministeriö on itsenäinen toimija, joka tekee yhteistyötä muiden maiden DSA-viranomaisten kanssa puolustusmateriaalihankkeissa

4.6 Ohjaavat asiakirjat

4.6.1 Yleiset

1. Turvaluususselvityslaki 726/2014
2. Laki kansainvälisistä tietoturvaluusvelvoitteista 588/2004
3. Laki sotilaskurinpidoista ja rikostorjunnasta puolustusvoimissa 89/2025
4. Voimassa olevat tietoturvaluusussopimukset (<https://um.fi/voimassa-olevat-tietoturvaluusussopimukset>)
5. Traficom / Kyberturvaluusukeskus (NCSA | Kyberturvaluusukeskus)

6. Hyväksytyt tietoturvallisuuden arviointilaitokset (<https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta/hyvaksytyt-tietoturvallisuuden-arviointilaitokset?toggle=Laki%20tietoturvallisuuden%20arviointilaitoksista>)
7. Katakri – tietoturvallisuuden auditointityökalu viranomaisille (<https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille>)
8. Aluevalvontalaki 755/200 -> Laki aluevalvontalain muuttamisesta 85/2025 (19 §)
9. Luvan myöntämisen ja peruuttamisen edellytykset)
10. Puolustusministeriön asetus Puolustusvoimien maksullisista suoritteista vuosina 2026 ja 2027 (18.12.2025)
11. Turvallisuusviranomaisten käsikirja yrityksille (2021)

4.6.2 Puolustusvoimat

1. Puolustusvoimien Sidosryhmäturvallisuus, HS511, liite 2. (30.6.2022), TLIV
2. Henkilöturvallisuusselvitys- ja todistusmenettely sekä vierailuluvat ulkomaille suuntautuviissa vierailuissa, HK735 (16.1.2015)
3. Turvallisuusjärjestelyiden varmistaminen Puolustusvoimien ja sidosryhmien välisessä yhteistyössä, HN555 (23.10.2017)
4. Puolustusvoimien toiminta yhteistoimintaosapuolten kanssa, HR187 (11.4.2022), TLIV
5. Tilaturvallisuusnormi, HQ2 (28.5.2020), TLIV

5 Yritysturvallisuusselvitys

5.1 Tarkoitus

Turvallisuusselvityslain (726/2014 1§) tarkoituksena on parantaa mahdollisuuksia ennakolta ehkäistä toimintaa, joka voi vahingoittaa valtion turvallisuutta, maanpuolustusta, Suomen kansainvälisiä suhteita, yleistä turvallisuutta tai muuta niihin verrattavaa etua taikka erittäin merkittävää yksityistä taloudellista etua taikka edellä tarkoitettujen etujen suojaamiseksi toteutettavia turvallisuusjärjestelyjä.

Yritysturvallisuusselvityksellä (Turvallisuusselvityslaki 726/2014 3§ 1 mom. 2 k.) tarkoitetaan yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumustenhoitokyvyn arvioimiseksi turvallisuusselvityslaisissa säädetyllä tavalla laadittavaa selvitystä.

Yritysturvallisuusselvitystodistusta edellytetään¹⁰ niiltä sidosryhmiltä, jotka käsittelevät tai joille luovutetaan puolustusvoimien turvallisuusluokan III (luottamuksellinen), turvallisuusluokan II (salainen) ja turvallisuusluokan I (erittäin salainen) tietoa.

Toimintaa valvova viranomainen voi pyytää yritysturvallisuusselvitystä myös niistä sidosryhmistä, jotka käsittelevät tai joille luovutetaan puolustusvoimien turvallisuusluokan IV (käyttö rajoitettu) tietoa.

Tarve yritysturvallisuusselvitykseen ja sen perusteella myönnetylle todistukselle voi liittyä myös kansainvälisiin tietoturvelvoitteisiin. Kansainvälisiin tietoturvelvoitteisiin liittyen todistuksen myöntää Kansallinen turvallisuusviranomainen (NSA) kansallisen yritysturvallisuustodistuksen perusteella. Vastuuviranomaisena voi toimia SUPO DSA tai PE DSA.

¹⁰ Puolustusvoimien Sidosryhmäturvallisuus, HS511, Liite 2.

Pääesikunnan tiedusteluosastolle (PETIEDOS) on määrätty Pääesikunnan työjärjestyksessä toimivaltaisen viranomaisen rooli (PE DSA) joka vastaa yritysturvallisuusselvityksien tekemisestä.

Pääesikunnan operatiivinen osasto (PEOPOS) toimii Puolustusvoimien kumppanien osalta pääasiallisena hakijana yritysturvallisuusselvityksissä.

5.2 Kohde

Selvityksen kohteella tarkoitetaan yritystä tai yhteisöä, josta turvallisuusselvitystä on haettu.

5.3 Hakija

Yritysturvallisuusselvitystä voi hakea turvallisuusselvityslain mukaan¹¹:

- 1) se, joka tarvitsee selvitystä laissa tai sen nojalla säädetyn taikka kansainvälisestä tietoturvallisuusvelvoitteesta johtuvan velvoitteen toteuttamiseksi;
- 2) viranomainen, jonka on tarkoitus tehdä sopimus selvityksen kohteen kanssa, jos sopimuksen yhteydessä yritykselle annetaan tai sopimuksen johdosta syntyy turvallisuusluokkaan I–III kuuluvaksi luokiteltuja asiakirjoja tai muita salassa pidettäviä asiakirjoja, jos näihin asiakirjoihin sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitettulle yleiselle tai yksityiselle edulle;
- 3) 2 kohdassa tarkoitetuissa tilanteissa viranomaisen toimeksiannosta valtionhallinnon hankinnoista vastaava yksikkö taikka valtionhallinnolle yhteisiä tai laajaan käyttöön tarkoitettuja tieto- ja viestintekniikkapalveluja tuottava yksikkö;
- 4) 21 §:n 1 momentin 5 ja 6 kohdassa tarkoitettua toimintaa valvova viranomainen.

¹¹ Tursel 726/2014 5 luku 33 §

Yritysturvallisuusselvitys

Yritysturvallisuusselvitys voidaan tehdä selvityksen kohteen pyynnöstä 36 §:n 2 momentissa tarkoitetuissa tapauksissa.

Puolustusvoimat käyttää hakiessaan pääsääntöisesti kohdassa 2. mainittuja asioita. PV:n yritysturvallisuusselvityksissä pääsääntöisesti hakijana toimii Pääesikunnan operatiivinen osasto koska suurin osa haettavista selvityksistä liittyy PV:n turvallisuussopimuskumppaneihin. Pv:n sisäinen määräys Puolustusvoimien Sidosryhmäturvallisuus (käsky HS511, 30.6.2022, TLIV) – asiakirjan liitteen 2 kohdassa 5.3 käsketään seuraavasti:

Yritysturvallisuusselvitystodistusta edellytetään niiltä sidosryhmiltä, jotka käsittelevät tai joille luovutetaan puolustusvoimien turvallisuusluokan III (luottamuksellinen), turvallisuusluokan II (salainen) ja turvallisuusluokan I (erittäin salainen) tietoa.

5.4 Hakemus (liitteet 4 ja 5)

Yritysturvallisuusselvityksen laatimista koskevasta hakemuksesta¹² tulee ilmetä:

- 1) selvityksen kohteen nimi ja muut tunnistetiedot sekä yhteystiedot;
- 2) ne alihankkijat, joiden kanssa selvityksen kohde aikoo tehdä sopimuksen yritysturvallisuusselvityksen perusteena olevan hankkeen toteuttamisesta, aliurakoitsijan osuus hankkeen toteuttamisessa sekä alihankkijaa koskevat 1 kohdassa tarkoitetut tiedot;
- 3) selvitys yritysturvallisuusselvityksen laatimiselle 36 §:ssä säädettyjen edellytysten täyttymisestä;
- 4) tieto siitä, onko yritysturvallisuusselvityksen avulla tarkoitus osoittaa yrityksen täyttävän määrätty tietoturvallisuuden taso ja jos on, mikä on käytettävä arviointiperuste;
- 5) tieto siitä, onko yrityksen tai sen alihankkijana toimivan toimitiloista, tietojärjestelmistä ja muista turvallisuusjärjestelyistä laadittu tietoturvallisuuden arviointilaitoksista annetussa laissa tarkoitetun hyväksytyt arviointilaitoksen

¹² Tursel 726/2014 5 luku 33 §

laatima arviointi ja jos on, kopio arvioinnin perusteella annetusta todistuksesta.

Hakemukseen tulee liittää asiakirja, josta ilmenee yrityksen suostumus yritysturvallisuusselvityksen laatimiseen, jollei yritys itse tee hakemusta.

Yritysturvallisuusselvityksen laatimisen edellytykset:

Yritysturvallisuusselvitys voidaan laatia¹³, jos selvitys on tarpeen yrityksen arvioimiseksi, kun:

- 1) yritysturvallisuusselvitys on laadittava tai voidaan laatia lain tai sen nojalla annetun säännöksen mukaan taikka kansainvälisen tietoturvaluottamukseen toteuttamiseksi;
- 2) viranomainen on tekemässä yrityksen kanssa sopimusta, jonka yhteydessä yritykselle luovutetaan viranomaisen salassa pidettäviä asiakirjoja;
- 3) toimintaa valvova viranomainen pyytää yritysturvallisuusselvitystä sellaisesta yrityksestä, joka harjoittaa 21 §:n 1 momentin 5 tai 6 kohdassa tarkoitettua toimintaa tai on osallistumassa aliurakoitsijana hankkeeseen, jossa sillä tai sen työntekijöillä on pääsy mainituissa lainkohdissa tarkoitettuihin tietoihin taikka tiloihin tai alueelle.

Yritysturvallisuusselvitys voidaan laatia, jos turvallisuusselvitystä edellytetään kansainvälisen järjestön tai toimielimen säännöissä tai toisen valtion laissa ja jos se on tarpeen sen vuoksi, että selvityksen kohde voi:

- 1) tulla valituksi kansainvälisen järjestön tai toimielimen järjestämään tai näiden muutoin organisoimaan hankkeeseen taikka toisessa valtiossa järjestettävään hankintakilpailuun;
- 2) aloittaa yritystoiminnan toisessa valtiossa.

Yritysturvallisuusselvitys voidaan ulottaa koskemaan myös selvityksen kohteen alihankkijana toimivaa yritystä niiltä osin kuin 1 momentissa säädetty edellytykset täyttyvät myös alihankkijaa koskevana ja toimivaltainen viranomainen katsoo sen tarpeelliseksi.

¹³ Tursel 726/2014 5 luku 36 §

Yritysturvallisuusselvitys

Valtioneuvoston asetuksella voidaan säätää, että yritysturvallisuusselvitys voidaan laatia myös yrityksen sellaisten liikesalaisuuksien tai teknologista kehittämistyötä koskevien tietojen suojaamiseksi, joiden oikeudeton käyttö, käsittely ja luovuttaminen aiheuttaisivat yritykselle merkittävää taloudellista vahinkoa tai joiden suojaamisella on merkitystä yleisen edun kannalta.

5.5 Selvitystyö

Yritysturvallisuusselvityksessä selvitetään yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumuksenhoitokyvyn arvioimiseksi turvallisuusselvityslaisissa säädetyllä tavalla.

Yritysturvallisuusselvitys kirjataan Suojelupolisiin ylläpitämään valtakunnalliseen turvallisuusselvitysrekisteriin, joka toimii virallisena rekisterinä henkilö- ja yritysturvallisuusselvityksille.

Turvallisuusselvitysrekisterissä on käytössä automaattinen nuhteettomuuden seuranta (automaattinen tieto rikosepäilystä).

Henkilöturvallisuusselvitys on voimassa toistaiseksi, enintään kuitenkin viisi vuotta. Henkilöturvallisuusselvitys voidaan peruuttaa, mikäli nuhteettomuusseurannan perusteella havaitaan kohteen syyllistyneen tekoon, joka olisi ollut esteenä todistuksen myöntämiselle.

Yritysturvallisuusselvityksessä tehdään aina vaikuttavuuden arviointia yksittäisen yrityksen vastuuhenkilön henkilöturvallisuusselvityksessä ilmenneistä asioista selvityksen kohteena olevan yrityksen selvitykseen.

Yrityksen taustat tarkastetaan luotettavuuden ja sitoumuksenhoitokyvyn arvioimiseksi turvallisuusselvityslaisissa mainituista lähteistä.

Henkilöturvallisuusselvityksillä varmistetaan yrityksen vastuuhenkilöiden nuhteettomuuden ja luotettavuuden varmistamista laatimalla selvitys henkilön taustasta.

Henkilöturvallisuusselvitys tehdään tarkistamalla henkilöä koskevat rekisteritiedot turvallisuusselvityslaisissa säädetyllä tavalla sekä tarvittaessa selvityksen kohdetta haastatteleamalla hänen yleisistä olosuhteistaan, ulkomailla oleskelustaan, ulkomaansidonnaisuuksistaan ja muista sellaisista seikoista, joilla

on erityistä merkitystä arvioitaessa hänen riippumattomuuttaan ja luotettavuuttaan toimiessaan yrityksen vastuuhenkilönä.

Yritysturvallisuusselvityksen yhteydessä yrityksen vastuuhenkilöistä tehdään aina perusmuotoinen henkilöturvallisuusselvitys sekä ulkomaalaisidonnaisuuksien selvittäminen (UMS).

Yrityksen vastuuhenkilöt ovat ne, joka merkitään viranomaisen julkiseen rekisteriin yhtiömiehenä, vastuullisena yhtiömiehenä, toimitusjohtajana, yrityksen hallituksen jäsenenä tai varajäsenenä tai henkilönä, jolla on prokuura- ja nimenkirjoitusoikeus.

Yrityksen ulkomaalaisista vastuuhenkilöistä selvitetään, onko hänelle myönnetty oman maan viranomaisten toimesta turvallisuusselvitystodistus (PSC) tai tehty turvallisuusselvitys.

Ensisijaisesti kohde (yritys) selvittää asian. Mikäli yritys ei saa selvitettyä niin kohdehenkilöstä tehdään PSCIS (Personal Security Clearance Information Sheet) -kysely PE DSA:n toimesta NSA - yksikön kautta kohdemaan NSA - viranomaiselta.

Kyselyssä pyydetään myös käynnistämään prosessi, jos henkilölle ei ole voimassa olevaa PSC-todistusta. Käytänteet vaihtelevat eri maissa.

Mikäli viranomainen ei saa kohtuullisessa ajassa vastausta niin tästä tehdään kirjaus yritysturvallisuusselvityksen loppuraporttiin. Käytännössä se tarkoittaa sitä, että kyseinen henkilö ei saa perehtyä yritysturvallisuusselvitykseen myönnetyn turvaluokan (TLIII/TLII) mukaiseen aineistoon.

Yritysturvallisuusselvityksen voimassaoloaika on määräajan 5 vuotta kuten henkilöturvallisuusselvityksetkin. Kohteena olevan yrityksen tai yhteisön on pidettävä huolta, että vastuuhenkilöiden turvallisuusselvitykset ovat katkeamatta voimassa koko yritysturvallisuusselvityksen voimassaoloajan.

5.6 Selvitystyön valmistuminen

Yritysturvallisuusselvitystodistuksen myöntämisestä menee aina kirjallinen (sähköposti) ilmoitus kohteelle. Ilmoituksen yhteydessä sovitaan ajankohta,

milloin todistus luovutetaan kohteelle. Toimivaltainen viranomainen menee käytännössä aina kohteena olevan yrityksen tai yhteisön toimipaikalle noin yhden tunnin mittaiseen todistuksen luovutustilaisuuteen.

5.7 Luovutustilaisuus

Tilaisuudessa esittäytyään ja yritys tai yhteisö pitää lyhyen esittelyn. Ohjelmaan kuuluu todistuksen luovutus, sitoumuksen allekirjoittaminen sekä niin sanottu vapaa sana, jonka aikana voidaan keskustella ajankohtaisista asioista, menneistä ja tulevista asioista.

Selvityksen tekijän puolelta pääsääntöisesti osallistuu selvityksen valmistelijaksi ja kohteen puolelta nimenkirjoituksen (prokuura) omaava henkilö, joka on hyvin usein toimitusjohtaja sekä turvallisuudesta vastaava henkilö ja/tai yhteyshenkilö (ellei sama) sekä mahdollisesti muita yrityksen henkilöitä, joiden on katsottu yrityksen toimesta tärkeä olla tilaisuudessa mukana.

5.8 Voimassaolo ja päättäminen

Yritysturvallisuusselvitys(todistus) on voimassa määräajan 5 vuotta. Yritysturvallisuusselvityksen todistus voidaan päättää joko myöntäjän (toimivaltainen viranomainen) tai kohteen (yrityksen) toimesta. Tyypillinen tapa selvityksen päättymiselle on joko sen vanhentuminen ja/tai uuden selvitysprosessin käynnistäminen. Uuden selvitykseen tekemiseen tarvitaan aina kohteen suostumus. Yritysturvallisuusselvitystodistus voidaan myös päättää, mikäli selvityksen kohde ei täytä selvitykseen vaadittavia vaatimuksia tai kohde ei täytä sitoumuksen (kts. kohta sitoumus) ehtoja.

5.9 Yritysturvallisuusselvityksen seuranta

Yritys sitoutuu todistuksen voimassaolo ajan noudattamaan sitoumuksessa (liite 3) mainituista velvoitteista. Tällaisia velvoitteita ovat mm. vastuuhenkilömuutokset ja esimerkiksi toimitiloissa tapahtuneita muutoksia (auditoidut turvatilat). Edellä mainitut muutokset eivät vaikuta todistuksen voimassaoloaikaan. Tiedot päivitetään selvityksen loppuraporttiin, jonka päivittäminen ei vaikuta itse todistukseen voimassaoloaikaan. Isommat muutokset, jossa esimerkiksi yrityksen y-tunnus, yrityksen koko tai omistusrakenne muuttuvat merkittävästi, tehdään aina tapauskohtainen arvio selvityksen mahdollisesta uusimisesta.

Toimivaltainen viranomainen voi tarkastaa tarvittavassa laajuudessa yrityksen toimitilojen, tietojärjestelmien ja tietoliikennejärjestelyjen suojaamiseksi toteutetut sekä muut turvallisuusjärjestelyt. Tarkastusta ei saa suorittaa pysyväisluonteiseen asumiseen käytetyissä tiloissa¹⁴.

5.10 Kielteinen päätös

Kohteelle voidaan antaa yritysturvallisuusselvityksestä kielteinen päätös eli kohteelle ei voida myöntää yritysturvallisuusselvitystodistusta.

Kielteiseen päätökseen voi johtaa esimerkiksi että kohteesta ei ole saatavilla riittäviä tietoja tai kohde ei täytä sille annettuja vaatimuksia¹⁵.

¹⁴ Tursel 726/2014 5 luku 39 §

¹⁵ Tursel 726/2014 5 luku 36 § ja 37 §

6 Yritysturvallisuusselvitystodistus ja siihen liittyvät asiakirjat

Yritysselvitystodistus koostuu kolmesta eri asiakirjasta:

6.1 Yritysturvallisuusselvitystodistus (liite 1)

Yritysturvallisuusselvitystodistus on julkinen, yhden sivun mittainen todistus, josta selviää kohde, selvityksen taso, voimassaoloaika sekä myöntäjä. Todistusta saa käyttää kohteen omalla päätöksellä ns. julkisena referenssinä.

6.2 Yritysturvallisuusselvityksen loppuraportti (liite 2)

Yritysturvallisuusselvityksen ns. loppuraportti on salassa pidettävä (SALPID) dokumentti. Loppuraportin pituus riippuu selvityksen kohteen auditointujen tilojen määrästä.

Loppuraportissa kerrotaan selvityksen taso, yhteyshenkilöt (kohde, myöntäjä), sähköisen käsittelyn taso, kansainvälisen tiedon käsittelyn taso (paperinen, sähköinen), mahdollisen NSCA-viranomaisen hyväksymän tietojärjestelmän taso, voimassaoloaika sekä hyväksymistiedot. Loppuraportissa ilmoitetaan, onko selvityksen yhteydessä toimivaltaisen viranomaisen toimesta tehty harkintaa saatujen tietojen perusteella liittyen esimerkiksi yrityksen taustatietoihin tai vastuuhenkilöiden turvallisuusselvityksiin liittyen yleisellä tasolla.

6.3 Sitoumus (liite 3)

Yritysturvallisuusselvitystodistuksen luovutuksen yhteydessä kohteelta otetaan käytännössä aina sitoumus, joka on vakiomuotoinen asiakirja niistä velvoitteista, joita kohteelta edellytetään yritysturvallisuusselvityksen voimassaoloajalta.

7 Yritysturvallisuusselvityksen eri laajuudet

7.1 Henkilöturvallisuusselvitykset

Henkilöturvallisuusselvitys laaditaan yritysturvallisuusselvitykseen liittyen aina perusmuotoisena ja johon liitetään ulkomaalaissidonnaisuuksien selvittäminen (UMS).

Yritysturvallisuusselvityksistä käytetään alla olevia määritelmiä, joita ei ole virallisesti turvallisuusselvityslaisissa määritelty.

7.2 Suppea tai FSC without safeguards (w/o)

Yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumustenhoitokyvyn arvioimiseksi turvallisuusselvityslaisissa säädetyllä tavalla.

Yrityksen toimitilojen auditointi ei sisälly selvitykseen. Yritys ei voi käsitellä turvaluokiteltua tietoa yrityksen tiloissa (tiloja ei ole auditoitu).

7.3 Perusmuotoinen tai FSC with safeguards

Yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumustenhoitokyvyn arvioimiseksi.

Yrityksen toimitilojen auditointi sisältyy selvitykseen. Yritys voi käsitellä toimitiloissaan turvaluokiteltua tietoa selvityksessä ilmoitetulla turvaluokalla.

7.4 Laaja tai FSC with safeguards including CIS

Yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumustenhoitokyvyn arvioimiseksi.

Yritysturvallisuusselvityksen eri laajuudet

Yrityksen toimitilojen auditointi sisältyy selvitykseen. Yritys voi käsitellä toimitiloissaan turvaluokiteltua tietoa selvityksessä ilmoitetulla turvaluokalla.

Selvitykseen sisältyy sähköisen turvaluokitellun tiedon käsittelyn tason (CIS) joko erilliskoneratkaisuna tai tietojärjestelmänä.

8 Yritysturvallisuusselvityksiin liittyvät tarkastukset (auditoinnit)

8.1 Katakri – auditointityökalu

Katakri 2020 on Suomen kansallisen turvallisuusviranomaisen (Ulkoministeriö) ylläpitämä auditointityökalu, jolla arvioidaan organisaation kykyä suojata turvallisuusluokiteltua tietoa. Se perustuu kansalliseen lainsäädäntöön ja kansainvälisiin tietoturvelvoitteisiin. Katakri – auditointityökalua käytetään yritysturvallisuusselvityksissä kohteen toimitilojen auditointiin sekä osana tietoturvallisuuden arviointiin.

Kriteeristö on jaettu kolmeen pääosa-alueeseen, jotka kattavat turvallisuuden eri puolet:

- T: Turvallisuusjohtaminen (Hallinnollinen turvallisuus): Organisaation turvallisuuspolitiikka, vastuut, koulutus ja riskienhallinta.
- F: Fyysinen turvallisuus: Toimitilojen suojaaminen, pääsynvalvonta ja turvallisuusalueet.
- I: Tekninen tietoturvallisuus: Tietojärjestelmien, verkkojen ja viestinnän tekninen suojaaminen.

Katakri 2020:n liite IV (ns. NATO-liite) on erityinen lisäosa, jota käytetään, kun arvioidaan organisaation valmiutta käsitellä Naton turvallisuusluokiteltua aineistoa.

8.2 Tilaturvallisuus (toimitilaturvallisuus)

Tilaturvallisuudessa noudatetaan seuraavaa jaottelua:

8.2.1 Hallinnollinen alue

Hallinnollisella alueella tarkoitetaan normaaliin työskentelyyn tarkoitettuja alueita ja tiloja, kuten toimistotilaa tai useista eri toimistotiloista muodostuvaa kokonaisuutta. Turvallisuusluokitellun tiedon

omistaja varmistaa, että niihin on itsenäinen pääsy ainoastaan ennalta valtuutetuilla henkilöillä.

8.2.2 Turva-alue

Turva-alueella tarkoitetaan organisaation työskentelyyn tarkoitettuja, hallinnollista aluetta paremmin suojattuja alueita ja tiloja, joissa turvallisuusluokiteltuja tietoja käsitellään ja säilytetään. Turva-alue voidaan tilapäisesti perustaa hallinnolliselle alueelle turvallisuusluokiteltua kokousta tai muuta vastaavaa tarkoitusta varten.

8.2.3 Teknisesti suojattu turva-alue

Teknisesti suojattua turva-aluetta ei ole määritelty kansallisesti (1101/2019, 9 §), mutta alue on osa Euroopan neuvoston ja Naton turvallisuussäntöjen määrittelemiä turva-alueita. Alue voidaan perustaa EU:n ja Naton turvallisuusluokiteltujen tietojen suojaamiseksi.

8.3 Tekninen tietoturvatarkastus (CIS)

Sähköinen turvaluokitellun tiedon käsittely jakaantuu erilliskone- ja tietojärjestelmä -ratkaisuihin. Tarkastuksiin sisältyy aina myös käytettävät oheislaitteet.

Hyväksynnästä käytetään yleisesti termiä sähköinen käsittely tai CIS (Communications and Information Systems) erityisesti kansainvälisen yritysturvallisuusselvityksen (FSC) yhteydessä. Suoraan ei voi päätellä onko kyseessä erilliskone - vai tietojärjestelmä – hyväksyntä. Ratkaisu on aina selvitettävä erikseen.

Yritysturvallisuusselvityksen osana tehtävä tietojärjestelmätarkastus on prosessi, jolla varmistetaan, että yrityksen IT-infrastruktuuri täyttää viranomaisvaatimukset turvallisuusluokitellun tiedon käsittelyyn. Tarkastuksesta vastaa yleensä NCSA (Traficom), usein yhteistyössä puolustusvoimien kanssa. Traficom noudattaa arvioinnissa soveltuvien osin edellä kuvattua hyväksyntäprosessia. Esimerkiksi järjestelmäkohtaisen turvallisuusvaatimusmäärittelyn laadinnassa sovelletaan suoraan Katakri -arviointityökalua. Traficom antaa arviointinsa perusteella Pääesikunnalle tietojärjestelmien tietoturvallisuuden ta-soa koskevan selvityksen. Selvityslausuntoon liitetään arviointiraportti. Lausunto ja raportti toimitetaan myös asianosaiselle yritykselle. On huomattava,

että lausunto tai raportti eivät ole Traficomın hyväksyntä järjestelmälle, vaan ainoastaan osaselvitys pääesikunnan päätökseen (yritysturvallisuusselvitys), jota tehtäessä myös näiden viranomaisten vastuulla olevat osa-alueet huomioidaan¹⁶.

Erilliskone -ratkaisu on nimensä mukaisesti erillinen kone, teknisesti ja fyysisesti irrotettu kaikista verkkoyhteysistä. Koneita voi olla yksi tai useampi. Tarkastukseen ja/tai ratkaisun hyväksyntään kuuluu tarvittavat oheislaitteet.

Yritysturvallisuusselvityksiin liittyen tarkastuksen ja hyväksynnän erilliskoneista voi tehdä myös toimivaltainen turvallisuustarkastaja (Puolustusvoimat) viiteasiakirjan mukaisesti¹⁷.

Tarkastus ja hyväksyntä tehdään yritysturvallisuusselvityksiin liittyen aina turvaluokan LUOTTAMUKSELLINEN (TLIII) tai SALAINEN (TLII) tason tietoa käsittelevistä kokonaisuuksista.

Pyynnön tarkastuksesta yritysturvallisuusselvitykseen liittyen tekee toimivaltainen viranomainen (PE DSA).

Mikäli yrityksellä on perusteltu tarve käsitellä sähköisesti EU CONFIDENTAL tai SECRET (EU-C/S) ja/tai NATO CONFIDENTAL tai SECRET (NC/S) tietoja, järjestelmän tarkastaa ja hyväksyy eli akkreditoi aina Traficom PE DSA:n pyynnöstä.

Fyysiset tilaturvallisuusauditoinnit tekevät Puolustusvoimissa toimivaltaiset turvallisuustarkastajat. Auditointityö tehdään pääsääntöisesti PV:n sopimus-kumppanien osalta yhteistyöhön liittyviin turvatiloihin. Näitä auditointiraportteja hyödynnetään Pääesikunnan tekemissä yritysturvallisuusselvityksissä tilojen osalta.

¹⁶ Liikenne- ja viestintäviraston ohje tietojärjestelmien tietoturvallisuuden arviointi- ja hyväksyntäprosesseista (Dnro TRAFICOM/1061/09.04.00/2023)

¹⁷ Ohje erillistyöasemien tietoturvallisuuden varmistamisesta (Traficom/17011/09.04.00/2023)

8.4 Turvallisuustarkastaja (auditoija)

Pääesikunnan toimivaltaisen viranomaisen (PE DSA) laatimissa yritysturvallisuusselvityksissä tukeudutaan pääsääntöisesti Puolustusvoimien toimivaltaisiin turvallisuustarkastajiin, jotka on koulutettu ja hyväksytty Puolustusvoimien sisäisessä tarkastaja – koulutuksessa turvallisuustarkastajiksi. Turvallisuustarkastajat ylläpitävät Puolustusvoimien kumppaniyrityksien kanssa tehtyjä turvallisuussopimuksia, joihin liittyy yrityksen toimitilojen auditoinnit. PE DSA ei itsessään tee auditointeja yrityksen toimitiloihin vaan yritysturvallisuusselvityksessä hyödynnetään edellä mainittua auditointityötä osana selvitystyötä.

Puolustusvoimien toimivaltaisen turvallisuustarkastajan oikeus edellyttää vuosittaista osaamisen ja ammattitaidon ylläpitoa.

Toimivaltaiseksi turvallisuustarkastajaksi voidaan nimetä Puolustusvoimien virassa oleva henkilö, joka on suorittanut turvallisuustarkastajan koulutusohjelman hyväksytysti.

Yritysturvallisuusselvityksistä vastaavan (PE DSA/yritysturvallisuus) tai vastaavien henkilöiden tulee olla Puolustusvoimien hyväksymä toimivaltaisen turvallisuustarkastaja

9 Yritysturvallisuusselvityksiin liittyvät edut, tavoitteet ja rajoitteet

9.1 Yritysturvallisuusselvityksen edut

Yritysturvallisuusselvityksen päätarkoitus on varmistaa yrityksen ja sen toiminnan luotettavuus ja turvallisuuden taso, erityisesti kun on kyse arkaluonteisten tietojen tai kriittisten toimintojen käsittelystä. Selvityksellä pyritään estämään ulkopuolisten uhkien, kuten vakoilun tai sisäpiirikollisuuden, aiheuttamat vahingot.

9.2 Keskeiset tavoitteet ja käyttötarkoitukset

Valtion turvallisuuden varmistaminen:

Selvitys on valtion turvallisuusjärjestelmän työkalu, jolla pyritään estämään epäluotettavien tahojen pääsy tehtäviin, joissa he voisivat uhata valtion turvallisuutta.

Arkaluonteisten tietojen suojaaminen:

Viranomaisen edellyttää yritysturvallisuusselvitystä yleensä silloin, kun se aikoo tehdä yrityksen kanssa sopimuksen, jossa käsitellään turvallisuusluokiteltuja (salassa pidettäviä) asiakirjoja.

Kriittisen infrastruktuurin ja toimialojen turvaaminen:

Selvitys vaaditaan yrityksiltä, joiden toiminta liittyy esimerkiksi ydinlaitoksiin, ydinaineiden tai räjähdysaineiden kuljetukseen tai valmistukseen.

Yrityksen maineen ja kilpailukyvyn ylläpito:

Turvallisuusselvitys toimii osoituksena yrityksen kyvystä suojata tietoa ja hoitaa sitoumuksensa luotettavasti, mikä rakentaa uskottavuutta viranomais- ja yrityskumppaneiden silmissä.

Yritysturvallisuusselvityksiin liittyvät edut, tavoitteet ja rajoitteet

Tietoturvallisuuden tason arviointi:

Selvityksen avulla voidaan osoittaa, että yritys täyttää määrätyn tietoturvallisuuden tason vaatimukset.

Yritysturvallisuusselvitystodistusta voi käyttää julkisena referenssinä.

Kansallinen yritysturvallisuusselvitystodistus toimii pohjana kansainväliselle yritysturvallisuusselvitystodistukselle (FSC, Facility Security Clearance).

9.3 Yritysturvallisuusselvitykseen liittyvät rajoitteet

Kohteena oleva yrityksen tai yhteisön tulee täyttää turvallisuusselvityslaisissa kuvatut vaatimukset sekä toimivaltaisen viranomaisen (PE DSA) asettamat vaatimukset.

Rajoitteena voi olla muun muassa, että tietoturvallisuuden turvaluokan taso ei ole riittävä eli yritys ei käsittele riittävän korkeaa turvaluokiteltua tietoa. Lähtökohtana on tietoturvallisuusluokka LUOTTAMUKSELLINEN (TLIII) tai SALAINEN (TLII) tai harkinnanvaraisesti KÄYTTÖ RAJOITETTU (TLIV).

Hakemuksen saapuessa tai selvityksen aikana voidaan haettua tasoa muuttaa turvaluokka -tason, tilojen sekä sähköisen käsittelyn osalta tarkoituksen mukaiseksi.

Kohteena oleva yrityksen tai yhteisön tulee olla myös selvityskelpoinen vastuuhenkilöiden osalta. Kohteella tulee olla selkeä vastuuhenkilörakenne. Mikäli kohteella ei ole vastuuhenkilöitä tulee selvittää mahdollisesti omistusrakenne esimerkiksi tytär -yhtiöihin ja/tai holding-yhtiöihin. Yritysturvallisuushakemukseen tulee tällöin sisällyttää myös edellä mainitut yhtiöt (y-tunnukset).

10 Yritysturvallisuusselvityksien maksullisuus

Puolustusvoimat alkoi periä turvallisuusselvityslain ja valtion maksuperustelain mukaisesti maksua muille laatimistaan turvallisuusselvityksistä 1.1.2026 alkaen. Puolustusvoimissa laadittavista turvallisuusselvityksistä peritään maksu, joka on samasuuruinen kuin Suojelupoliisin samanlaatuisesta suoritteesta perimä maksu¹⁸.

Hinnat (1.1.2026)

Suppea / FSC without safeguards (w/o): 5000 euroa

Yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumustenhoitokyvyn arvioimiseksi turvallisuusselvityksissa säädetyllä tavalla.

Yrityksen toimitilojen auditointi ei sisälly selvitykseen. Yritys ei voi käsitellä turvaluokiteltua tietoa yrityksen tiloissa (tiloja ei ole auditoitu).

Perusmuotoinen / FSC with safeguards: 10 000 euroa

Yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumustenhoitokyvyn arvioimiseksi.

Yrityksen toimitilojen auditointi sisältyy selvitykseen. Yritys voi käsitellä toimitiloissaan turvaluokiteltua tietoa selvityksessä ilmoitetulla turvaluokalla.

¹⁸ Puolustusministeriön asetus (1226/2025) 18.12.2025

Yritysturvallisuusselvityksien maksullisuus

Laaja / FSC with safeguards including CIS: 10 000 euroa + 180 euroa / tunti (Traficom)

Yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumustenhoitokyvyn arvioimiseksi.

Yrityksen toimitilojen auditointi sisältyy selvitykseen. Yritys voi käsitellä toimitiloissaan turvaluokiteltua tietoa selvityksessä ilmoitetulla turvaluokalla.

Selvitykseen sisältyy sähköisen turvaluokitellun tiedon käsittelyn tason joko erilliskoneratkaisuna tai tietojärjestelmänä.

Henkilöturvallisuusselvitykset

Perusmuotoinen henkilöturvallisuusselvitys, joka sisältää ulkomaansidonnaisuuksien selvittämisen 495 euroa.

11 Johtopäätökset

Tämä teos tarjoaa katsauksen yritysturvallisuusselvitysten monimutkaiseen kenttään. Tutkimus on rajattu tietoisesti keskittymään yritysturvallisuuden ytimeen: vaikka henkilöturvallisuusselvitykset on rajattu yleisellä tasolla pois, niitä on käsitelty yrityksen vastuuhenkilöiden osalta kriittisenä osana kokonaisuutta. Samoin muiden viranomaisten, kuten Suojelupoliisin ja Traficomien, sisäisiä toimintatapoja on analysoitu siltä osin kuin se on välttämättömyyttä prosessin kokonaiskuvan ymmärtämiseksi.

Keskeiset havainnot ja teoreettinen viitekehys Teoksen painopiste on kansallisessa sääntelyssä, vaikka kansainvälinen ulottuvuus (FSC) on tunnistettu käsitetasolla. Keskeisenä rakenteellisena määrittelynä teos vahvistaa Pääesikunnan tiedusteluosaston (PE TIEDOS) roolin Suomen kansallisena puolustushallinnon turvallisuusviranomaisena (PE DSA).

Tutkimus osoittaa, että turvallisuusselvityslaki muodostaa vakaan, yhdenmukaisen ja ennakoitavan perustan selvitystoiminnalle sekä julkisella että yksityisellä sektorilla. Teorialähtöinen sisällönanalyysi ja teoksen luonne käytännönläheisenä perehdytysmateriaalina tekevät muuten raskaasta viranomaisprosessista helpommin lähestyttävän lukijalle.

Analyysissä nousi esiin merkittävä havainto viranomaisohjeistuksen ja normiston rajallisuudesta, mikä osaltaan hidastaa prosessien kehittämistä. Tätä tyhjiötä täyttävät DSA-viranomaiset omalla foorumillaan, jossa koordinoidaan linjauksia ja ratkotaan mahdollisia ristiriitoja. Lainsäädäntöä tulisi osaltaan kehittää vastaamaan kyvykkyyksiä sekä ajan vaatimuksia.

Elinkeinoelämän keskusliiton (EK) määritelmän mukaisesti yritysturvallisuuden kytkeminen osaksi yrityksen normaalia johtamista ja kilpailukykyä on avainasemassa. Kun turvallisuus nähdään strategisena etuna eikä pelkkänä

Johtopäätökset

kulueränä, viranomaisvaatimusten jalkauttaminen organisaatioon helpottuu huomattavasti.

Viestintä- ja tietojärjestelmien (CIS) turvallisuus on merkittävä osa selvitysprosessia ja on hyvin usein liiketoiminnan edellytys turvaluokitellun tiedon käsittelyn osalta. Tämä korostaa tietoturvajohdon (CISO) merkitystä organisaatiossa: yritykseltä edellytetään yhä vahvempaa kyvykkyyttä vastata NCSA:n asettamiin tiukkoihin vaatimuksiin sähköisen tiedonsiirron ja tiedon käsittelyn osalta.

Teoksen pohjalta nousee esiin useita merkittäviä jatkotutkimustarpeita:

1. Maksullisuuden vaikutukset yritysturvallisuusselvityksiin; Viranomaisen näkökulmasta sekä selvityksen kohteen näkökulmasta.
2. Yrityksen turvatiloihin laitettujen investointien hyödyt ja haitat.
3. Kansainvälisten tietoturvaluokitusvelvoitteiden vaikutus suomalaisten yritysten globaaliin kilpailukykyyn ja vaadittavat erityiskyvykkyudet.
4. NATO-vaatimukset osana yritysturvallisuusselvitystä.