HE 164/2012 vp

Hallituksen esitys eduskunnalle turvallisuustoimenpiteistä turvallisuusluokitellun tiedon suojaamiseksi Suomen ja Yhdysvaltojen välillä tehdyn sopimuksen hyväksymisestä sekä laiksi sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan, että eduskunta hyväksyisi Suomen ja Yhdysvaltojen välisen sopimuksen turvallisuustoimenpiteistä turvallisuusluokitellun tiedon suojaamiseksi sekä lain sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.

Sopimuksen tarkoituksena on varmistaa Suomen ja Yhdysvaltojen välisessä yhteistyössä luottamuksellisesti vaihdettavan turvallisuusluokitellun tiedon suojaaminen erityisesti ulko-, puolustus-, turvallisuus-, poliisi-, tiede- ja yritysasiossa. Sopimuksella osapuolet sitoutuvat suojaamaan toiselta osapuolelta suoraan tai välillisesti saamansa turvallisuusluokitellut tiedot sopimuksessa määrättyjen vaatimusten sekä lakiensa ja asetustensa mukaisesti.

Sopimus tulee voimaan toisen kuukauden ensimmäisenä päivänä sen jälkeen, kun Suomi on ilmoittanut Yhdysvalloille, että kaikki sopimuksen voimaan saattamiseksi Suomessa tarvittavat kansalliset menettelyt on saatettu päätökseen. Sopimuksen voimaansaattamislaki on tarkoitettu tulemaan voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samaan aikaan kuin sopimus tulee Suomen osalta voimaan.

296180

SISÄLLYSLUETTELO

YLEISPERUSTELUT

1 Johdanto

Tietoturvallisuudella tarkoitetaan kaikkia sellaisia menettelyjä, joiden avulla turvataan informaation sisällön suojaaminen ulkopuolisilta (tiedon luottamuksellisuus), tiedon muuttumattomuus (tiedon eheys) sekä tiedon käytettävyys. Tietoturvallisuuden varmistamiseksi käytetään erilaisia keinoja, joista tavallisimmat ovat henkilöstön luotettavuuden ja toimitilojen turvallisuuden varmistaminen, salassapitosäännökset ja tietojen käytön rajoittaminen vain sovittuun tarkoitukseen sekä erilaiset tietojen käsittelyyn ja siirtoon liittyvät menettelytapavaatimukset. Tietoturvallisuusvaatimukset kattavat informaation koko elinkaaren sisältäen tietojen hankkimisen, muokkaamisen, käytön, luovutuksen, arkistoinnin ja hävittämisen.

Kansainväliseen yhteistyöhön liittyviin asiakirjoihin sisältyy sellaisia salassa pidettäviä tietoja, joiden luvaton paljastuminen voi aiheuttaa merkittävää ja laajalle ulottuvaa vahinkoa keskeisille yleisille eduille. Tällaisten aineistojen asianmukaisesta käsittelystä on sen vuoksi pidettävä erityistä huolta. Kysymys on Suomen luotettavuudesta kansainvälisen yhteistyön osapuolena. Kansainvälinen tietoturvallisuusyhteistyö, johon Suomikin osallistuu, käsittää perinteisesti diplomaattiseen toimintaan samoin kuin puolustus- ja poliisihallintojen väliseen yhteistyöhön liittyvän ei-julkisen tiedonvaihdon suojaamisen. Välittömän valtiovastuun piiriin kuuluvien kysymysten lisäksi kansainvälisillä tietoturvallisuusvelvoitteilla on kuitenkin kasvava merkitys myös taloudellisen, teollisen ja teknologisen yhteistyön kannalta, joiden puitteissa yhä useammat yritystason hankkeet edellyttävät turvallisuussuojatun tiedon hyödyntämistä. Näin etenkin silloin, kun kyse on sellaisesta viranomaisen hankinnasta, jossa valtion suojattuja tietoja on annettava yritykselle kaupallisen sopimuksen toteuttamista varten. Tällaisia ovat perinteisesti olleet erityisesti puolustusalan hankinnat.

Pyrkimyksistä huolimatta ei kuitenkaan ole osoittautunut mahdolliseksi toteuttaa tietoturvallisuusalan monenkeskistä yleissopimusta. Pääasiallinen syy tähän ovat kansallisten lainsäädäntöjen ja hallintorakenteiden ja -tapojen eroavaisuudet, jotka puolestaan heijastelevat tietoturvallisuuden sensitiivisyyttä osana kansallista kokonaisturvallisuutta. Edellä sanotusta poikkeuksena on kuitenkin Tanskan, Suomen, Islannin, Norjan ja Ruotsin välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja vaihtamisesta tehty yleinen turvallisuussopimus (SopS 128 ja 129/2010).

Yleissopimuksen puuttuminen on pakottanut valtiot, Suomi mukaan luettuna, etsimään kahdenvälisiä sopimusratkaisuja. Suomi on tehnyt ensimmäisen kahdenvälisen tietoturvallisuussopimuksensa Saksan liittotasavallan kanssa vuonna 2004. Sopimus tuli voimaan 16 päivänä heinäkuuta 2004 (SopS 96 ja 97/2004). Vuotta myöhemmin allekirjoitettiin Suomen ja Ranskan välinen sopimus, joka puolestaan tuli voimaan 1 päivänä elokuuta 2005 (SopS 66 ja 67/2005). Kumpikin suuri Euroopan unionin (EU) jäsen on Suomelle tärkeä yhteistyökumppani niin turvallisuushallinnon kuin taloudellisen vuorovaikutuksenkin aloilla. Tietoturvallisuustarpeiden painottumista enenevässä määrin myös taloudelliseen toimintaan ilmentää Suomen ja Euroopan Avaruusjärjestön (ESA) välinen yhteistyösopimus, jäljempänä ESA:n tietoturvallisuussopimus, niin ikään vuodelta 2004 (SopS 94 ja 95/2004). Sopimuksen eräs keskeinen tavoite on turvata Suomen elinkeinoelämän mahdollisuudet osallistua tasavertaisesti muiden jäsenmaiden kanssa ESA:n turvallisuusluokiteltuihin tarjouskilpailuihin. Tietoturvallisuussopimus on tehty myös Länsi-Euroopan unionin (WEU) kanssa (SopS 41 ja 42/1998) ja Eurooppalaisen puolustusmateriaaliyhteistyöjärjestön (OCCAR) kanssa (SopS 109 ja 110/2008). Mainittujen sopimusten lisäksi Suomi on tehnyt voimassaolevan tietoturvallisuussopimuksen Slovakian (SopS 116 ja 117/2007), Viron (SopS 12 ja

13/2008), Italian (SopS 23 ja 24/ 2008), Latvian (SopS 33 ja 34/2008), Puolan (SopS 46 ja 47/2008), Bulgarian (SopS 116 ja 117/2008), Slovenian (SopS 22 ja 23/2009), Tšekin (SopS 53 ja 54/2009) ja Espanjan (SopS 38 ja 39/2010) kanssa sekä edellä mainitun pohjoismaisen tietoturvallisuussopimuksen, jota sovelletaan tällä hetkellä väliaikaisesti Suomen, Ruotsin, Norjan ja Tanskan välillä (SopS 130/2010 ja 20/2012). Suomi on 10 päivänä toukokuuta 2012 hyväksynyt EU:n jäsenvaltioiden välillä toukokuussa 2011 allekirjoitetun sopimuksen turvallisuusluokitellun tiedon suojaamisesta, mutta sopimus ei ole toistaiseksi tullut voimaan. Suomi on omalta osaltaan hyväksynyt Luxemburgin kanssa tehdyn tietoturvallisuussopimuksen 19 päivänä lokakuuta 2012. Naton kanssa tehtyä hallinnollista tietoturvallisuusjärjestelyä koskeva hallituksen esitys on annettu eduskunnalle syksyllä 2012 (HE 139/2012 vp). Kesäkuussa 2012 Suomi allekirjoitti tietoturvallisuussopimuksen Iso-Britannian kanssa. Suomi on lähiaikoina allekirjoittamassa tietoturvallisuussopimuksen myös Sveitsin kanssa. Kaikkiin edellä mainittujen sopimusten nojalla vastaanotettuihin turvallisuusluokiteltuihin tietoihin sovelletaan lakia kansainvälisistä tietoturvallisuusvelvoitteista.

2 Nykytila

2.1 Laki kansainvälisistä tietoturvallisuusvelvoitteista

Lain yleinen soveltamisala

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) säädettiin osana Suomen ja Saksan välisen tietoturvallisuussopimuksen sekä ESA:n tietoturvallisuussopimuksen voimaansaattamista. Laki katsottiin tarpeelliseksi muun ohella sen vuoksi, että kansainvälisten sopimusten panemiseksi täytäntöön on tarve poiketa asiakirjajulkisuuteen ja -turvallisuuteen perustuvista kansallisista järjestelyistä, jotka perustuvat pääosin viranomaisten toiminnan julkisudesta annettuun lakiin (621/1999), jäljempänä *julkisuuslaki*.

Lakia kansainvälisistä tietoturvallisuusvelvoitteista sovelletaan erityissuojattaviin tietoaineistoihin. Näillä tarkoitetaan salassa pidettäviä asiakirjoja ja materiaaleja, jotka on toimitettu Suomen viranomaiselle ja joiden lähettäjä on kansainvälisen, Suomea sitovan sopimuksen tai muun kansainvälisen velvoitteen mukaisesti tehnyt niihin turvallisuusluokkaa koskevan merkinnän. Määräysvalta luovutettuun tietoon säilyy luovutuksen jälkeenkin aineiston luovuttaneella valtiolla. Lakia voidaan soveltaa vain, jos kansainvälinen sopimus on saatettu Suomessa voimaan perustuslaissa säädetyllä tavalla tai jos kysymys on Suomea muutoin sitovasta kansainvälisestä velvoitteesta.

Lain soveltamisalan piiriin kuuluvia erityissuojattavia tietoaineistoja ovat lisäksi Suomen viranomaisen tai lain soveltamisalan piiriin kuuluvan elinkeinonharjoittajan laatimat asiakirjat, joista ilmenee Suomeen toimitettuihin asiakirjoihin sisältyviä tai materiaalista saatavissa olevia tietoja. Lain soveltamisalan piiriin kuuluvat niin ikään asiakirjat ja materiaalit, jotka on Suomessa tuotettu erityissuojattavan tietoaineiston pohjalta.

Laissa säädettyjä turvallisuusvelvoitteita sovelletaan silloinkin, kun sopimus tai säädös, johon säännösten soveltaminen perustuu, ei enää ole voimassa (15 §). Soveltaminen jatkuu niin kauan kuin se turvallisuusluokituksen perusteena olevan yleisen edun vuoksi on tarpeen.

Lain suhde julkisuuslainsäädäntöön

Kansainvälisistä tietoturvallisuusvelvoitteista annettuun lakiin sisältyy kansallisten asiakirjojen tietoturvallisuudesta annetuista säännöksistä poikkeavia säännöksiä. Laissa on kuitenkin yleinen viittaussäännös julkisuuslakiin. Niiltä osin kuin suomalaisten viranomaisten asiakirjoihin sisältyy muita kuin kansainvälisten tietoturvallisuusvelvoitteiden piiriin kuuluvia tietoja kansainvälisestä yhteistyöstä, on sovellettava julkisuuslain ja sen nojalla annettuja säännöksiä. Laissa on myös erityissäännös, joka koskee päätöksentekovaltaa siinä tilanteessa, että tietoja pyydetään julkisuuslain nojalla erityissuojattavasta aineistosta. Julkisuuslain mukaan tie-

donsaantia koskevan pyynnön voi käsitellä ja ratkaista se viranomainen, jonka hallussa asiakirja on. Tiedonsaantipyyntö voidaan kuitenkin siirtää toisen viranomaisen ratkaistavaksi julkisuuslain 15 §:ssä säädetyissä tilanteissa.

Lain soveltaminen elinkeinonharjoittajiin

Lakia sovelletaan viranomaisten lisäksi myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on osapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana (1 §:n 2 momentti).

Turvallisuusluokitellulla sopimuksella tarkoitetaan sopimusta, jonka toisen valtion viranomainen tai siinä kotipaikkaansa pitävä yritys taikka kansainvälinen järjestö tai toimielin aikoo tehdä tai on tehnyt kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitetulla tavalla Suomessa kotipaikkaansa pitävän elinkeinonharjoittajan kanssa, jos tarjouskilpailuun osallistuminen tai sopimuksen toteuttaminen voi edellyttää pääsyä erityissuojattavaan tietoaineistoon (2 §:n 3 kohta).

Elinkeinonharjoittaja voi pyytää yhteisöturvallisuusselvityksen ja arvion tekemistä voidakseen osallistua toisen valtion viranomaisen tai siinä kotipaikkaansa pitävän yrityksen järjestämään tarjouskilpailuun (12 §:n 2 momentti). Säännöksen tarkoituksena on turvata suomalaisten yritysten kilpailumahdollisuudet hankinnoissa silloinkin, kun hankintaan sovellettavissa olevaa kansainvälistä tietoturvallisuussopimusta ei ole. Useimmat valtiot kuitenkin edellyttävät kahdenvälisen tietoturvallisuussopimuksen olemassa oloa ulkomaisen turvallisuustodistuksen hyväksymiseksi.

Elinkeinonharjoittajalla ja tämän palveluksessa tai toimeksiannosta toimivalla on erityissuojattavia tietoaineistoja koskeva salassapitovelvollisuus (6 §). Elinkeinonharjoittajalla on myös velvollisuus kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi antaa toimivaltaiselle turvallisuusviranomaiselle tietoja sekä sallia viranomaisen ja kansainvälisen toimielimen tai sopimusvaltion edustajan tutustuminen turvallisuusjärjestelyihinsä ja toimitiloihinsa (16 §:n 2 momentti ja 18 §:n 2 momentti).

Lain täytäntöönpanoviranomaiset

Laissa on säännökset (4 §) niistä viranomaisista, jotka huolehtivat kansainvälisten tietoturvallisuusvelvoitteiden hoitamisesta. Kansallisena turvallisuusviranomaisena (National Security Authority, NSA) kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseen liittyvissä tehtävissä toimii ulkoasiainministeriö. Puolustusministeriö, pääesikunta, Suojelupoliisi ja Viestintävirasto toimivat määrättyinä turvallisuusviranomaisina (Designated Security Authority, DSA). Näille viranomaisille voi kuulua muun ohella tarjous- ja hankintamenettelyihin liittyvien asiakirjojen turvallisuusluokittelu.

Henkilöstöturvallisuuteen liittyvien turvallisuusselvitysten laadinnasta huolehtivat Suojelupoliisi ja pääesikunta (11 §). Yhteisöturvallisuusselvityksen laadinta kuuluu lain mukaan Suojelupoliisille, paitsi silloin, kun kyse on puolustukseen liittyvästä hankinnasta, jolloin selvitysten tekemisestä huolehtii pääesikunta (12 §). Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 5 §:n 2 momentin mukaan kansallinen turvallisuusviranomainen ja tehtävään määrätyt turvallisuusviranomaiset voivat sen estämättä, mitä muun muassa toimivallasta yhteisöturvallisuusselvitysten laadinnasta säädetään, sopia tietyn tehtävän tai tehtäväkokonaisuuden hoitamisesta toisen turvallisuusviranomaisen lukuun, jos järjestely on tarpeen tehtävien hoitamiseksi tarkoituksenmukaisesti, taloudellisesti ja joutuisasti. Viestintävirasto on lain 4 §:n 1 momentissa (885/2010) määrätty turvallisuusviranomaiseksi, jonka tehtävänä on arvioida tietojärjestelmien ja tietoliikennejärjestelyjen turvallisuutta.

Laissa kansainvälisistä tietoturvallisuusvelvoitteista on säännökset viranomaisia ja elinkeinonharjoittajaa koskevasta tiedonantovelvollisuudesta (16 §). Säännösten tarkoituksena on varmistaa, että toimivaltaiset turvallisuusviranomaiset voisivat saada niille kuuluvien tehtävien hoitamiseksi tarpeelliset tiedot. Viranomaiset voivat myös salassapi-

tovelvollisuuden estämättä antaa kansainväliseen tietoturvallisuusvelvoitteeseen perustuvaa yhteistyötä varten salassa pidettäviä tietoja ulkomaiselle sopimuspuolelle (17 §). Viranomaisella on myös oikeus sallia kansainväliseen tietoturvallisuusvelvoitteeseen perustuva kansainvälisen järjestön, toimielimen tai sopimusvaltion edustajan tutustuminen viranomaisen toteuttamiin turvallisuusjärjestelyihin ja toimitiloihin riippumatta siitä, mitä turvallisuusjärjestelyjen salassapidosta säädetään taikka säädetään tai määrätään pääsystä tiloihin, joissa käsitellään tai säilytetään salassa pidettäviä tietoja (18 §).

Kansallisen turvallisuusviranomaisen on lain mukaan ilmoitettava kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitetuissa tapauksissa toiselle sopimuspuolelle tietoonsa tulleesta turvallisuusluokiteltujen tietojen suojan vaarantumisesta ja tietoturvallisuutta koskevan määräyksen loukkaamisesta sekä ryhdyttävä toimenpiteisiin asian selvittämiseksi samoin kuin rangaistavaan tekoon syyllistyneen syytteeseen saattamiseksi (19 §).

Tietojen salassapito ja käytön sääntely

Erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu (6 §:n 1 momentti). Salassapitovelvollisuus koskee myös elinkeinonharjoittajaa tämän olleessa osapuolena turvallisuusluokitellussa sopimuksissa. Suomen tekemissä, käytännössä kahdenvälissä sopimuksissa, jotka koskevat eri maiden viranomaisten välistä salassa pidettävien tietojen vaihtoa, on säännönmukaisesti määräys, joka rajoittaa luovutettujen tietojen käyttöä. Tämän mukaisesti erityissuojattavaa tietoaineistoa saa käyttää ja luovuttaa vain siihen tarkoitukseen, jota varten se on annettu, jollei se, joka on määritellyt aineiston turvallisuusluokan, ole antanut muuhun suostumustaan. Erityissuojattavien tietoaineistojen käyttöä koskee siten vahva käyttötarkoitussidonnaisuus.

Turvallisuusluokittelu ja -toimenpiteet

Laissa säädetään velvollisuudesta merkitä erityissuojattavaan tietoaineistoon sen turvallisuusluokka. Tietoaineistoon tehty merkintä turvallisuusluokasta osoittaa, minkälaisia toimenpiteitä on toteutettava aineistoa käsiteltäessä (8 §). Mitä korkeampaan turvallisuusluokkaan aineisto kuuluu, sitä tiukempia tietoturvallisuustoimenpiteitä edellytetään. Laissa on yleinen velvoite toteuttaa tietoaineiston käsittelyssä sen turvallisuusluokkaa koskevia käsittelymääräyksiä sekä valtuus säätää erityissuojattavan tietoaineiston käsittelyssä noudatettavista turvallisuusluokitusta vastaavista teknisistä turvallisuustoimenpiteistä valtioneuvoston asetuksella (9 §). Tietoturvallisuudesta valtionhallinnossa annetun valtioneuvoston asetuksen (681/2010), jäljempänä *tietoturvallisuusasetus*, 11 §:ssä on säädetty turvallisuusluokitusmerkintää koskevista erityissäännöksistä ja 12 §:ssä turvallisuusluokituksen vastaavuudesta.

Turvallisuusluokiteltuja aineistoja käsiteltäessä on lain mukaan huolehdittava siitä, että tietoja säilytetään asianmukaisissa tiloissa. Tilojen turvallisuusvaatimuksista on säädetty tietoturvallisuusasetuksen 14 §:ssä.

Turvallisuusluokiteltuja tietoja viranomaisissa käytettäessä on noudatettava pidättyvyyttä ja sen vuoksi lakiin kansainvälisistä tietoturvallisuusvelvoitteista on kirjattu kansainvälisissä sopimuksissa oleva yleinen vaatimus siitä, että tietoihin annetaan pääsy vain niille, jotka tarvitsevat tietoja tehtäviensä hoitamisessa. Nämä henkilöt on nimettävä etukäteen, jos sopimuksessa tätä edellytetään. Sama koskee myös 1 §:n 2 momentissa tarkoitettua elinkeinonharjoittajaa (6 §:n 3 momentti).

Henkilöstöturvallisuus

Kansainvälisessä tietoturvallisuusvelvoitteessa edellytetty henkilöstöturvallisuutta koskeva turvallisuusselvitys tehdään siten kuin turvallisuusselvityksistä annetussa laissa (177/2002) ja sen nojalla säädetään. Siten esimerkiksi selvityksen kohteena olevan henkilön oikeudet määräytyvät sanotun lain mukaisesti.

Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa on kuitenkin kaksi säännöstä, jotka ovat erityissäännöksiä suhteessa turvallisuusselvityksistä annettuun la-

kiin. Suppea turvallisuusselvitys on mahdollista laatia muissakin kuin turvallisuusselvityksistä annetun lain 19 §:ssä luetelluissa tapauksissa, jos se on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi (11 §:n 1 momentti). Toinen erityissäännös koskee viranomaisten toimivaltaa. Turvallisuusselvityksen tekee pääesikunta silloin kun turvallisuusselvityksen laatiminen on tarpeen puolustushallintoa tai puolustushankintoja koskevan kansainvälisen velvoitteen toteuttamiseksi. Muissa tapauksissa henkilöön liittyvien turvallisuusselvitysten laadinnasta huolehtii Suojelupoliisi (11 §:n 2 momentti). Turvallisuusselvityksistä annetun lain 10 §:n 2 momentin mukaan turvallisuusselvitykseen ei saa sisällyttää selvityksen laatineen viranomaisen arviota selvityksen kohteena olevan henkilön luotettavuudesta tai sopivuudesta virkaan tai tehtävään, ellei lain 9 §:ssä tarkoitettu valtiosopimus tai muu kansainvälinen velvoite tätä edellytä. Koska pääsääntönä on, että turvallisuusselvitys ei sisällä arviota henkilön luotettavuudesta, laissa kansainvälisistä tietoturvallisuusvelvoitteista on erikseen säädetty henkilön luotettavuuden arvioinnista. Tällaisen arvion tekee turvallisuusselvityksen perusteella kansallinen turvallisuusviranomainen tai, jos turvallisuusviranomaisten välillä on niin sovittu, tehtävään määrätty turvallisuusviranomainen (11 §:n 3 momentti).

Arvioinnin perusteella annetaan henkilöstöturvallisuutta koskeva todistus (Personnel Security Clearance Certificate). Se toimitetaan tavanomaisimmin sopimuspuolen turvallisuusviranomaiselle sopimuksen osoittamalla tavalla. Laissa on myös säännökset todistuksen antamisesta henkilölle itselleen (14 §).

Yhteisöturvallisuusselvitys

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 §:ssä säädetään yhteisöturvallisuusselvityksistä ja arvioista. Yhteisöturvallisuusselvityksellä varmistetaan elinkeinonharjoittajan toimitilojen ja käsittelykäytäntöjen asianmukaisuus sekä henkilöstön osaaminen. Elinkeinonharjoittajan luotettavuuden arvioinnilla varmistutaan erityisesti siitä, kuinka hyvin tämä pystyy huolehtimaan turvallisuusluokiteltujen tietojen suojaamisesta. Yhteisöturvallisuusmenettely ja siihen perustuva arvio toteutetaan pääosin elinkeinonharjoittajalta itseltään saatujen tietojen perusteella sekä tämän toimitilojen turvallisuuden kartoituksella, ja tarvittavista toimenpiteistä huolehditaan elinkeinonharjoittajan kanssa tehtävän sopimuksen avulla. Selvityksen laatii Suojelupoliisi. Pääesikunta huolehtii tehtävästä kuitenkin silloin, kun kysymys on puolustukseen liittyvästä hankinnasta. Selvitystä laadittaessa on otettava huomioon laissa yksilöidyt seikat, muun muassa se, miten suojataan turvallisuusluokiteltuja tietoja oikeudettomalta ilmitulolta, muuttamiselta ja hävittämiseltä, ja miten estetään asiaton pääsy tiloihin, joissa turvallisuusluokiteltuja tietoja käsitellään tai joissa harjoitetaan turvallisuusluokitellussa sopimuksessa tarkoitettua toimintaa. Viestintävirasto laatii tarvittaessa osana yhteisöturvallisuusselvitystä selvityksen ja arvion siitä, täyttävätkö elinkeinonharjoittajan tietojärjestelmät ja tietoliikenteen järjestelyt kansainvälisistä tietoturvallisuusvelvoitteista johtuvat vaatimukset.

Määrätyt turvallisuusviranomaiset voivat toimialaansa kuuluvaa yhteisöturvallisuusselvitystä ja sen perusteella annettavaa arviota laatiessaan lain 13 §:n mukaan edellyttää, että elinkeinonharjoittaja sitoutuu huolehtimaan 12 §:n 1 momentissa tarkoitetuista ja muista kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi tarpeellisista toimenpiteistä. Sitoumuksessa voidaan yksityiskohtaisemmin määritellä ne toimenpiteet, jotka elinkeinonharjoittaja toteuttaa täyttääkseen kansainvälisistä tietoturvallisuusvelvoitteista johtuvat vaatimukset. Sitoumuksessa elinkeinonharjoittaja sitoutuu myös tekemään ne mahdolliset tarkistukset toimintaansa, jotka toiminnan turvallisuuskartoituksessa on havaittu. Turvallisuusselvityksen ja mahdollisen sitoumuksen jälkeen Suojelupoliisi tai pääesikunta voi tehdä arvion elinkeinonharjoittajan luotettavuudesta ja antaa tätä koskevan turvallisuustodistuksen (Facility Security Clearance Certificate).

2.2 Turvallisuusselvityksiä koskeva lainsäädäntö

Henkilöstöturvallisuuteen liittyvistä turvallisuusselvityksistä säädetään turvallisuusselvityksistä annetussa laissa. Lain tarkoituksena on turvallisuusselvitysmenettelyä käyttämällä parantaa mahdollisuuksia ennakolta estää rikokset, jotka vakavasti vahingoittaisivat keskeisiä yleisiä tai yksityisiä etuja taikka erittäin merkittävää tietoturvallisuutta.

Turvallisuusselvitys voidaan tehdä virkaan tai tehtävään hakeutuvasta, tehtävään tai koulutukseen otettavasta taikka virkaa tai tehtävää hoitavasta henkilöstä, ja se voi olla perusmuotoinen, laaja tai suppea. Turvallisuusselvitys tehdään laissa määritellyissä tapauksissa, kuten silloin, kun Suomea sitova valtiosopimus tai muu kansainvälinen velvoite edellyttää turvallisuusselvityksen tekemistä tai sen perusteella laaditun todistuksen esittämistä.

Yksityisyyden suojan perusoikeusluonteen vuoksi turvallisuusselvitysmenettely on tarkan muotosidonnaista. Turvallisuusselvitys voidaan tehdä vain selvityksen kohteena olevan henkilön etukäteen antaman, nimenomaisen ja kirjallisen suostumuksen perusteella. Myös turvallisuusselvitysmenettelyssä käytettävät rekisterit on laissa lueteltu tyhjentävästi.

Jokaisella on oikeus saada tieto siitä, onko hänestä tehty turvallisuusselvitys tiettyä tehtävää varten. Selvityksen kohteella on myös oikeus pyynnöstä saada toimivaltaiselta viranomaiselta perusmuotoisen tai laajan turvallisuusselvityksen tiedot. Tiedonsaantioikeus ei kuitenkaan koske sellaisesta rekisteristä peräisin olevaa tietoa, johon rekisteröidyllä ei ole tarkastusoikeutta.

Turvallisuusselvityslain kokonaistarkistusta varten asetettu työryhmä on luovuttanut mietintönsä oikeusministerille 31 päivänä tammikuuta 2011. Työryhmälle annettuun tehtävään kuului turvallisuusselvityslain kehittäminen siten, että se vastaa Suomea sitovia velvoitteita ja kansainvälisesti yleisesti sovellettavia käytäntöjä. Uudistettua turvallisuusselvityslakia koskeva hallituksen esitys on tarkoitus antaa syysistuntokaudella 2012.

3 Esityksen tavoitteet ja keskeiset ehdotukset

Esityksen tavoitteena on saattaa voimaan Suomen ja Yhdysvaltojen välinen tietoturvallisuussopimus ja sillä tavoin parantaa maiden välistä yhteistyötä sekä turvata suomalaisten yritysten mahdollisuudet osallistua sellaisiin kansainvälisiin sekä Suomen ja Yhdysvaltojen välisiin hankkeisiin, joiden toteuttaminen saattaa edellyttää turvallisuusluokiteltujen tietojen vaihtoa. Tietoturvallisuussopimus tukee myös muiden Suomen ja Yhdysvaltojen välillä tehtyjen sopimusten täytäntöönpanoa. Suomen ja Yhdysvaltojen välillä on tehty vuonna 1991 sotilastiedon turvallisuutta koskeva sopimus, joka lakkaa olemasta voimassa tämän sopimuksen tullessa voimaan.

4 Esityksen vaikutukset

4.1 Vaikutukset kansalaisiin

Sopimuksen voimaansaattamisen myötä Yhdysvalloista Suomeen toimitettuihin turvallisuusluokiteltuihin tietoihin ja materiaaleihin sovellettaisiin lakia kansainvälisistä tietoturvallisuusvelvoitteista. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukainen salassapito on riippuvainen sopimuksen määräyksistä, mikä merkitsee yleensä kattavampaa salassapitovelvoitetta kuin julkisuuslain säännökset. Suomen ja Yhdysvaltojen välisessä sopimuksessa on kysymys asiakirjoista, joita toinen osapuoli pitää salassa pidettävinä ja jotka se on määritellyt ja merkinnyt korkean tietoturvallisuuden tasoa edellyttäviksi. Sopimuksen 7 artiklassa määrätään turvallisuusluokitellun tiedon salassapidosta. Artiklan a kohdan mukaan osapuolet eivät salli kolmansien osapuolten saada turvallisuusluokiteltua tietoa ilman lähettäjän kirjallista ennakkolupaa. Tämä merkitsee poikkeusta julkisuuslain yleistä etua koskevista salassapitosäännöksistä, joissa salassapito on useimmissa tapauksissa riippuvainen siitä, minkälaisia vaikutuksia tietojen antamisella olisi suojattavalle edulle. Tällaisia asiakirjoja on säännönmukaisesti pidettävä salaisina myös julkisuuslain 24 §:n 1 momentin 2 kohdan mukaan. Merkittävimpänä erona on

se, että viranomaisella ei olisi kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitettuun asiakirjaan kohdistuvaa tiedonsaantipyyntöä ratkaistessaan velvollisuutta erikseen perustella tiedon antamisesta aiheutuvaa vahinkoa. Tiedonsaantipyyntö olisi muutoin käsiteltävä julkisuuslain mukaisesti. Jos luokituksen oikeellisuudesta tai siitä, minkä asiakirjan tietojen vuoksi luokitusmerkintä on tehty, syntyy epäselvyyttä, viranomaisen on otettava yhteyttä asiakirjan laatineeseen osapuoleen. Edellä olevan perusteella voidaan arvioida, että Suomen ja Yhdysvaltojen välisen tietoturvallisuussopimuksen voimaansaattamista koskeva lakiehdotus ei asiallisesti vaikuta kansalaisten tiedonsaantia vähentävästi suhteessa siihen, mitä tiedonsaanti yleisen lainsäädännön mukaan on.

Henkilöstöturvallisuus on keskeinen tietoturvallisuuden osa-alue. Koska laki kansainvälisistä tietoturvavelvoitteista edellyttää turvallisuusselvityksistä annetun lain mukaisen menettelyn käyttämistä henkilöstön luotettavuuden varmistamisesta, ehdotetun voimaansaattamislain hyväksyminen ei tarkoittaisi sitä, että kansalaisten yksityisyyselämän ja henkilötietojen suojaa kavennettaisiin aikaisempaan verrattuna.

4.2 Vaikutukset elinkeinoelämään

Sopimus antaa suomalaiselle teollisuudelle mahdollisuuden saada sellaisia tilauksia tai osallistua sellaisiin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Yhdysvaltojen turvallisuusluokiteltuihin tietoihin. Vastaavasti sopimus antaa Yhdysvaltojen teollisuudelle mahdollisuuden saada sellaisia tilauksia tai osallistua sellaisiin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Suomen turvallisuusluokiteltuun tietoon.

4.3 Taloudelliset vaikutukset

Esityksellä ei ole vaikutusta valtion talousarvioon eikä muitakaan vähäistä merkittävämpiä taloudellisia vaikutuksia.

4.4 Vaikutukset hallintoon

Esitykseen sisältyvän sopimuksen ja lain hyväksymisestä ei aiheudu hallintoa koskevia muutosvelvoitteita tai -tarpeita. Sopimus lisää jonkin verran kansallisen turvallisuusviranomaisen ja määrättyjen turvallisuusviranomaisten niitä tehtäviä, jotka kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaisesti kuuluvat näille viranomaisille.

5 Asian valmistelu

Hallituksen esitys on valmisteltu ulkoasiainministeriössä. Sopimuksen valmisteluun ja neuvotteluihin on osallistunut edustajia ulkoasiainministeriöstä, oikeusministeriöstä, puolustusministeriöstä, työ- ja elinkeinoministeriöstä, Säteilyturvakeskuksesta, Viestintävirastosta ja Suojelupoliisista. Esityksestä on pyydetty lausunnot oikeusministeriöltä, puolustusministeriöltä, sisäasiainministeriöltä, valtiovarainministeriöltä, liikenne- ja viestintäministeriöltä, työ- ja elinkeinoministeriöltä, Suojelupoliisilta ja Viestintävirastolta. Lausunnoissa on puollettu sopimuksen pikaista hyväksymistä ja voimaansaattamista.

YKSITYISKOHTAISET PERUSTELUT

1 Sopimuksen sisältö ja suhde Suomen lainsäädäntöön

1 artikla. Seuraanto. Sopimuksen tullessa voimaan Suomen hallituksen ja Yhdysvaltojen hallituksen 11 päivänä lokakuuta 1991 allekirjoittama sotilastiedon turvallisuutta koskeva sopimus lakkaa olemasta voimassa. Artiklan 2 kohdan mukaan aiemmin välitetyt turvallisuusluokitellut tiedot suojataan tämän sopimuksen mukaisesti ja kaikki viittaukset tietoturvallisuussopimukseen katsotaan viittaukseksi tähän sopimukseen.

Sopimuksen 1 artiklan 3 kohdassa asetetaan soveltamisalaa koskeva rajoitus. Sopimusta ei sovelleta Yhdysvaltojen vuoden 1954 atomienergialaissa tarkoitettuun käytöltään rajoitettuun tietoon (Restricted Data) eikä entiseen käytöltään rajoitettuun tietoon (Formerly Restricted Data), joka on poistettu atomienergialain käytöltään rajoitetun tiedon luokasta, mutta jonka Yhdysvallat katsoo edelleen puolustustiedoksi.

2 artikla. Sitoumus turvallisuusluokitellun tiedon suojaamiseen. Artiklan 1 kohdan mukaan kumpikin osapuoli suojaa toiselta osapuolta suoraan tai välillisesti saamansa turvallisuusluokitellut tiedot sopimuksessa määrättyjen vaatimusten sekä lakiensa ja määräystensä mukaisesti. Sopimuksen johdannossa osapuolten välisinä yhteistyöaloina luetellaan ulko-, puolustus-, turvallisuus-, poliisi-, tiede- elinkeino- ja teknologia-asiat. Turvallisuusluokitellun tiedon suojaamista koskevat keskeiset vaatimukset sisältyvät sopimuksen 7 artiklaan.

Artiklan 2 kohdan mukaan osapuolten tulee ilmoittaa toisilleen lakeihinsa ja määräyksiinsä ehdotetuista muutoksista, jotka vaikuttaisivat turvallisuusluokitellun tiedon suojaamiseen. Tällaisessa tapauksessa osapuolet neuvottelevat keskenään käsitelläkseen tähän sopimukseen mahdollisesti tehtävistä muutoksista.

3 artikla. Määritelmät. Artiklassa määritellään sopimuksen soveltamisen kannalta keskeiset käsitteet seuraavasti:

Artiklan a alakohdassa on turvallisuusluokitellun tiedon määritelmä. Sopimus koskee tietoa, jonka Suomen tai Yhdysvaltojen hallitus tuottaa tai joka tuotetaan näiden hallitusten puolesta tai joka kuuluu jommankumman hallituksen lainkäyttö- tai määräysvaltaan ja joka on suojattava kansallisen turvallisuuden vuoksi ja on osoitettu sellaiseksi tiedoksi kyseisen hallituksen määräämällä turvallisuusluokituksella. Tieto voi olla suullisessa, visuaalisessa, elektronisessa tai asiakirjan muodossa tai se voi olla aineiston, kuten laitteiden tai teknologian, muodossa. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 1 kohdan kanssa.

Artiklan b alakohdan mukaan turvallisuusluokitellulla sopimuksella tarkoitetaan sopimusta joka edellyttää tai tulee edellyttämään hankeosapuolen tai sen työntekijöiden pääsyä turvallisuusluokiteltuun tietoon. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 3 kohdan kanssa.

Artiklan c alakohdan mukaan hankeosapuolella tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, jolla on oikeudellinen kelpoisuus tehdä sopimuksia, ja/tai tämän sopimuksen mukaista turvallisuusluokitellun sopimuksen osapuolta.

Artiklan d alakohdassa määritellään yhteisöturvallisuusselvitys (Facility Security Clearance, FSC). Yhteisöturvallisuusselvityksellä tarkoitetaan toimivaltaisen turvallisuusviranomaisen hankeosapuolen organisaatiolle antamaa todistusta, josta ilmenee, että organisaatiosta on tehty turvallisuusselvitys ja että se on toteuttanut asianmukaiset turvallisuustoimet turvallisuusluokiteltujen tietojen suojaamiseksi. Todistus merkitsee myös sitä, että hankeosapuoli suojaa turvallisuusluokiteltua tietoa tämän sopimuksen mukaisesti ja että toimivaltainen turvallisuusviranomainen

valvoo ja varmistaa, että hankeosapuoli noudattaa tätä sopimusta. Yhteisöturvallisuusselvitystä ei vaadita KÄYTTÖ RAJOITETTU -tasolla. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 §:n kanssa.

Artiklan e alakohdassa määritellään henkilöturvallisuusselvitys (Personnel Security Clearance, PSC). Henkilöturvallisuusselvityksellä tarkoitetaan toimivaltaisen turvallisuusviranomaisen antamaa todistusta osapuolen lainkäyttövaltaan kuuluvan valtion viraston tai hankeosapuolen organisaation palveluksessa olevan luonnollisen henkilön henkilöturvallisuusselvityksen tasosta. Henkilöturvallisuusselvityksellä tarkoitetaan myös henkilön kansalaisuusvaltion toimivaltaisen turvallisuusviranomaisen antamaa lausuntoa henkilön edellytyksistä saada turvallisuusselvitys, jos henkilön on määrä työskennellä toisen osapuolen tai sen hankeosapuolen palveluksessa. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n kanssa.

Artiklan f alakohdassa on määritelty tiedonsaantitarve. Tiedonsaantitarpeella tarkoitetaan turvallisuusluokitellun tiedon haltijan päätöstä, jonka mukaan tiedon mahdollinen vastaanottaja tarvitsee pääsyn tiettyyn turvallisuusluokiteltuun tietoon toimiakseen laillisessa ja sallitussa valtion tehtävässä tai avustaakseen siinä. Vastaavan tyyppinen määritelmä sisältyy myös kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 3 momenttiin.

4 artikla. Turvallisuusviranomaiset. Artiklan mukaan osapuolet ilmoittavat toisilleen kirjallisesti ne turvallisuusviranomaiset, jotka vastaavat sopimuksen täytäntöönpanosta, sekä näiden turvallisuusviranomaisten mahdolliset myöhemmät muutokset.

Suomessa mainittuna viranomaisena toimii kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaan ulkoasiainministeriö, jossa tehtävää hoitaa Kansallinen turvallisuusviranomainen. Tämän lisäksi puolustusministeriö, pääesikunta, Suojelupoliisi ja Viestintävirasto toimivat määrättyinä turvallisuusviranomaisina.

5 artikla. Turvallisuusluokiteltujen tietojen merkitseminen. Artiklan 1 kohdan mukaan turvallisuusluokiteltuun tietoon merkitään toisiaan vastaavasti kansalliset turvallisuusluokat artiklassa esitetyn taulukon mukaisesti.

Korkein, ankarimpia tietoturvallisuustoimenpiteitä vaativa luokka on "ERITTÄIN SALAINEN" (TOP SECRET). Suomessa tähän luokkaan luetaan kuuluviksi tiedot, joiden luvaton ilmitulo voi aiheuttaa erittäin suurta vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille.

Toiseksi korkein turvallisuusluokka on "SALAINEN" (SECRET). Tähän kuuluvat Suomessa tiedot, joiden luvaton ilmitulo voi aiheuttaa merkittävää vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille.

Kolmanneksi korkein turvallisuusluokka on "LUOTTAMUKSELLINEN" (CONFIDENTIAL), jolla tarkoitetaan Suomessa tietoja, joiden luvaton ilmitulo voi aiheuttaa vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille.

Neljänteen asiakirjaluokkaan "KÄYTTÖ RAJOITETTU" kuuluvat tiedot, joiden luvaton ilmitulo voi aiheuttaa haittaa yleisille eduille tai heikentää viranomaisen toimintaedellytyksiä. Yhdysvalloissa ei ole käytössä vastaavaa luokkaa. Turvallisuusluokiteltuja tietoja, joihin on merkitty suomenkielinen turvallisuusluokka KÄYTTÖ RAJOITETTU, käsitellään Yhdysvalloissa siten, kuin sopimuksen liitteessä ”Turvallisuusluokkaan KÄYTTÖ RAJOITETTU (Restricted) kuuluvan suomalaisen turvallisuusluokitellun tiedon käsittelymenettely Yhdysvalloissa” määrätään. Turvallisuusluokiteltuja tietoja, joihin on merkitty suomenkielinen turvallisuusluokka KÄYTTÖ RAJOITETTU, käsitellään Yhdysvalloissa samoin kuin Yhdysvaltojen luokittelemattomia (U.S. UNCLASSIFIED) tietoja, jotka yhden tai useamman Yhdysvaltojen lain mukaan eivät ole julkisia. Kyseiset lait on mainittu 5 artiklan 1 kohdan kolmannessa alaviitteessä.

Kaikki asiakirjat tai aineisto, joissa on Yhdysvaltojen merkintä siitä, että se on valvottua luokittelematonta tietoa (Controlled Unclassifed Information, CUI), merkitään, käsi-

tellään, siirretään ja säilytetään Suomessa kuten turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluva tieto.

Suomenkielisiä turvallisuusluokitusmerkintöjä vastaavat ruotsinkieliset merkinnät on lueteltu sopimuksen 5 artiklan 1 kohtaa koskevassa ensimmäisessä alaviitteessä.

Suomen kansainvälisiä suhteita suojaavat julkisuuslain 24 §:n 1 momentin 1 ja 2 kohta, maanpuolustusta momentin 10 kohta ja turvallisuutta momentin 5, 8 ja 9 kohdat. Muita julkisuuslaissa tarkoitettuja yleisiä etuja voivat olla esimerkiksi valtionjohdon ja valtiovieraiden sekä tietojärjestelmien turvallisuusjärjestelyjen suojaaminen (24 § 1 momentin 7 kohta) sekä kansantalouden toimivuus (24 § 1 momentin 11 ja 12 kohta). Julkisuuslain 25 §:ssä on yleiset säännökset salassapito- ja luokitusmerkinnän tekemisestä viranomaisen asiakirjaan. Lain 25 §:n 3 momentin mukaan asiakirjaan voidaan tehdä merkintä sen osoittamiseksi, minkälaisia tietoturvallisuusvaatimuksia asiakirjaa käsiteltäessä noudatetaan. Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitettuihin asiakirjoihin on tehtävä turvallisuusluokituksesta merkintä siten kuin mainitussa laissa säädetään. Turvallisuusluokituksesta on tehtävä merkintä myös, jos valtioneuvoston antamalla asetuksella niin säädetään.

Artiklan 2 kohdan mukaan kumpikin osapuoli leimaa, merkitsee tai liittää kaikkiin toiselta osapuolelta saamiinsa turvallisuusluokiteltuihin tietoihin tiedot luovuttaneen hallituksen nimen. Tietoihin leimataan, merkitään tai liitetään vastaanottavan osapuolen kansallinen turvallisuusluokka, joka ei saa olla alhaisempi kuin tiedot luovuttaneen hallituksen määräämä vastaava turvallisuusluokka ja joka antaa vähintään samantasoisen suojan kuin tiedot luovuttaneen osapuolen määräämä turvallisuusluokka.

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 8 §:n mukaan erityissuojattavaan tietoaineistoon on siitä riippumatta, mitä viranomaisen toiminnan julkisuudesta annetussa laissa tai sen nojalla säädetään, tehtävä kansainvälisessä tietoturvallisuusvelvoitteessa määritelty luokitusmerkintä sen osoittamiseksi, minkälaisia tietoturvallisuusvaatimuksia sen käsittelyssä on noudatettava. Turvallisuusluokitusmerkintää koskevat erityissäännökset sisältyvät tietoturvallisuusasetuksen 11 §:ään, ja merkintöjen vastaavuudesta kansainvälisten tietoturvallisuusvelvoitteiden luokkien kanssa on säädetty asetuksen 12 §:ssä. Asetuksen 11 §:n 1 momentissa säädetään, milloin salassa pidettävään asiakirjaan voidaan tehdä turvallisuusluokitusmerkintä. Asetuksen 11 §:n 3 momentin mukaan turvallisuusluokitusmerkintää ei saa käyttää muissa kuin 1 momentissa tarkoitetuissa tapauksissa, ellei merkinnän tekeminen ole tarpeen kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi tai asiakirja muutoin liity kansainväliseen yhteistyöhön. Ruotsinkielisistä turvallisuusluokitusmerkinnöistä on erityissäännös asetuksen 11 §:n 4 momentissa.

6 artikla. *Vastuu turvallisuusluokitellusta tiedosta*. Artiklan mukaan kumpikin osapuoli on vastuussa kaikista toisen osapuolen turvallisuusluokitelluista tiedoista sinä aikana, jona tiedot ovat sen lainkäyttöalueella ja määräysvallassa. Tietojen kuljetuksen aikana tiedot lähettänyt osapuoli on vastuussa kaikista turvallisuusluokitelluista tiedoista, kunnes tiedot ovat virallisesti siirtyneet toisen osapuolen hallintaan.

7 artikla. *Turvallisuusluokitellun tiedon suojaaminen*. Artikla sisältää keskeiset turvallisuusluokitellun tiedon suojaamista koskevat velvoitteet.

Artiklan ensimmäisen kappaleen mukaan luonnollisella henkilöllä ei ole oikeutta päästä toiselta osapuolelta saatuihin turvallisuusluokiteltuihin tietoihin pelkästään arvonsa, asemansa tai turvallisuusselvityksensä perusteella. Pääsy turvallisuusluokiteltuihin tietoihin sallitaan ainoastaan niille henkilöille, joiden viralliset tehtävät edellyttävät sitä, ja joista on tehty henkilöturvallisuusselvitys osapuolten ennalta määräämien vaatimusten mukaisesti.

Määräys on sopusoinnussa kansainvälisen tietoturvallisuusvelvoitteista annetun lain 6 §:n 3 momentin kanssa, jossa sallitaan tietoaineistoon pääsy vain niille henkilöille, jotka tarvitsevat tietoja tehtävänsä hoitamiseen. Kansainvälisen tietoturvallisuusvelvoitteen edellyttämä henkilöiden luotettavuuden varmistaminen toteutetaan Suomessa turvalli-

suusselvityksistä annetun lain sekä kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n mukaisesti.

Artiklan a alakohdan mukaan turvallisuusluokitellun tiedon vastaanottaja ei saa antaa tietoa kolmannen valtion hallitukselle, henkilölle, yritykselle, laitokselle, järjestölle tai muulle yhteisölle ilman tiedon luovuttaneen osapuolen kirjallista ennakkolupaa. Kohta velvoittaa osapuolet noudattamaan luovuttajan suostumuksen periaatetta. Määräys on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 1 kohdan kanssa, jonka mukaan erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisistä tietoturvallisuusvelvoitteista muuta johdu.

Artiklan b alakohdassa on ilmaistu turvallisuusluokiteltujen tietojen vastavuoroista suojaamista koskeva määräys. Alakohdan mukaan osapuolet varmistavat, että turvallisuusluokitellun tiedon vastaanottava osapuoli antaa tälle tiedolle samantasoisen suojan kuin luovuttanut osapuoli.

Artiklan c alakohdan mukaan turvallisuusluokitellun tiedon vastaanottava osapuoli ei saa käyttää tietoa eikä salli sitä käytettävän muuhun kuin siihen tarkoitukseen, jota varten tieto on luovutettu, ilma luovuttaneen osapuolen kirjallista ennakkolupaa. Velvoitetta vastaava säännös on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 2 momentissa.

Artiklan d alakohta koskee turvallisuusluokiteltuihin tietoihin sisältyviä tai liittyviä yksityisiä oikeuksia kuten patentteja, tekijänoikeuksia tai liikesalaisuuksia. Vastaanottavan osapuolen tulee kunnioittaa näitä yksityisiä oikeuksia eikä saa luovuttaa, käyttää, vaihtaa tai paljastaa turvallisuusluokiteltua tietoa, johon liittyy immateriaalioikeuksia, ennen kuin näiden oikeuksien omistajalta on saatu siihen nimenomainen kirjallinen lupa. Immateriaalioikeuksien suojasta säädetään muun muassa patenttilaissa (550/1967) ja tekijänoikeuslaissa (404/1961).

Artiklan e alakohdan mukaan jokaisen turvallisuusluokiteltua tietoa käsittelevän organisaation tai laitoksen on pidettävä luetteloa niistä henkilöistä, joilla on lupa päästä turvallisuusluokiteltuun tietoon. Määräys on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 3 momentin kanssa.

Artiklan f alakohdan mukaan osapuolten on varmistettava, että luodaan vastuu- ja valvontamenettelyt turvallisuusluokitellun tiedon levityksen ja tähän tietoon pääsyn hallintaa varten. Suomessa kunkin viranomaisen on huolehdittava muun muassa asiakirjojen suojaamisesta ja eheydestä julkisuuslain 18 §:n perusteella. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 § 2 momentin mukaan kansallisen turvallisuusviranomaisen tehtävänä on erityisesti ohjata ja valvoa, että erityissuojattavat tietoaineistot suojataan ja niitä käsitellään asianmukaisesti.

Artiklan g alakohdan mukaan turvallisuusluokitellun tiedon vastaanottavan osapuolen tulee noudattaa kaikkia lisärajoituksia, jotka tiedon luovuttanut osapuoli mahdollisesti määrää tiedon käytölle, paljastamiselle tai luovuttamiselle tai tietoon pääsylle. Käytön osalta tällaisia lisärajoituksia voivat olla muun muassa kopiointia ja kääntämistä koskevat rajoitukset, käytön ajallista kestoa koskevat rajoitukset sekä sähköisen käsittelyn rajoittaminen. Luovuttamisen ja paljastamisen osalta rajoitukset voivat koskea muun muassa ulkoistamista ja alihankkijoiden käyttöä. Pääsyn osalta lisärajoitukset voivat koskea henkilömäärän rajaamista ja tiedon luovuttamista vain nimetyille henkilöille.

8 artikla. *Henkilöturvallisuusselvitys*. Artiklan 1 kohdan mukaan kumpikin osapuoli suorittaa asianmukaisen ja riittävän yksityiskohtaisen tutkinnan päättääkseen, onko henkilöllä edellytykset päästä turvallisuusluokiteltuun tietoon. Päätös henkilöturvallisuusselvityksen myöntämisestä tehdään kansallisten lakien ja määräysten mukaisesti. Artiklan 2 kohdan mukaan ennen kuin osapuolen edustaja luovuttaa turvallisuusluokiteltua tietoa toisen osapuolen työntekijälle tai edustajalle, tiedon vastaanottava osapuoli antaa tiedon luovuttavalle osapuolelle vakuutuksen siitä, että kyseisestä työntekijästä tai edustajasta on tehty tarvittavan tason turvallisuusselvitys, että hän tarvitsee pääsyä turvallisuusluokiteltuun tietoon virallisessa tehtävässään ja että osapuoli suojaa tiedon. Kansainvälisen tietoturvallisuusvelvoitteen edellyt-

tämä henkilöiden luotettavuuden varmistaminen toteutetaan Suomessa turvallisuusselvityksistä annetun lain sekä kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n mukaisesti. Henkilöturvallisuusselvityksen laatii pääesikunta silloin, kun kysymys on puolustushallintoon liittyvästä asiasta, muutoin Suojelupoliisi. Turvallisuustodistuksista säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 14 §:ssä.

9 artikla. *Turvallisuusluokitellun tiedon luovuttaminen hankeosapuolille*. Artiklassa määrätään toimenpiteistä, jotka turvallisuusluokitellun tiedon vastaanottavan osapuolen on tehtävä ennen toiselta osapuolelta saadun turvallisuusluokitellun tiedon luovuttamista hankeosapuolelle tai mahdolliselle hankeosapuolelle. Vastaanottavan osapuolen tulee varmistaa, että hankeosapuolella on valmiudet suojata turvallisuusluokiteltu tieto (a alakohta) ja antaa hankeosapuolen organisaatiolle asianmukainen yhteisöturvallisuusselvitys (b alakohta) sekä henkilöturvallisuusselvitykset henkilöille, joiden tehtävät edellyttävät pääsyä turvallisuusluokiteltuun tietoon (c alakohta). Lisäksi vastaanottavan osapuolen tulee varmistaa, että henkilöille on selvitetty heidän velvollisuutensa suojata turvallisuusluokiteltua tietoa (d alakohta). Vastaanottavan osapuolen tulee suorittaa määräaikaistarkastuksia turvallisuusselvityksen saaneessa yrityksessä (e alakohta) ja varmistaa, että pääsy turvallisuusluokiteltuun tietoon rajoitetaan vain niihin henkilöihin, joilla on tiedonsaantitarve (f alakohta). Määräyksen suhdetta Suomen lainsäädäntöön on selostettu tarkemmin 10 artiklan perustelujen yhteydessä.

10 artikla. *Turvallisuusluokitellut sopimukset*. Artikla koskee turvallisuusluokitellun sopimuksen tekemisestä jommankumman osapuolen alueella.

Artiklan 1 kohdan mukaan se osapuoli, joka aikoo tehdä tai valtuuttaa hankeosapuolensa tekemään toisen osapuolen hankeosapuolen kanssa sopimuksen, johon liittyy turvallisuusluokkaan LUOTTAMUKSELLINEN/CONFIDENTIAL tai sitä ylempään turvallisuusluokkaan kuuluvaa tietoa, pyytää vakuutuksen siitä, että toisen osapuolen toimivaltaiset turvallisuusviranomaiset ovat antaneet yhteisöturvallisuusselvityksen.

Artiklan 2 kohdan mukaan turvallisuusluokiteltuun sopimukseen tai tarjouspyyntöön tulee sisällyttää asianmukaiset turvallisuuslausekkeet sekä muut asianmukaiset määräykset, myös turvallisuuskustannuksia koskevat määräykset.

Sopimuksen 9 ja 10 artiklaan sisältyviä määräyksiä on tarkasteltava kokonaisuutena. Turvallisuusluokitellun tiedon luovuttamista hankeosapuolille ja turvallisuusluokiteltuja sopimuksia koskevat kansalliset säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 1 § 2 momenttiin (soveltaminen elinkeinonharjoittajaan), 2 §:n 2 kohtaan (erityissuojattava tietoaineisto), 7 §:ään (vaitiolovelvollisuus ja hyväksikäyttökielto) sekä 12 §:ään (yhteisöturvallisuusselvitys), 13 §:ään (sitoumus turvallisuustoimenpiteiden suorittamisesta) ja 14 §:ään (turvallisuustodistus). Kansallinen sääntely vastaa sopimusvelvoitteen vaatimuksia. Velvoitteiden täyttämiseksi tarpeellisesta suomalaisen viranomaisen tietojenanto-oikeudesta säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 17 §:ssä.

11 artikla. *Vastuu organisaatiosta*. Artiklan mukaan kumpikin osapuoli vastaa kaikkien sellaisten valtion ja yksityisten organisaatioiden ja laitosten turvallisuudesta, joissa säilytetään toisen osapuolen turvallisuusluokiteltua tietoa, ja varmistaa, että kuhunkin tällaiseen organisaatioon nimetään pätevät henkilöt, joilla on vastuu tiedon valvonnasta ja suojaamisesta ja valtuudet siihen. Tietoturvallisuusasetuksessa on säädetty muun muassa valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista. Yksityiset organisaatiot ja laitokset voidaan kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 13 §:n 1 momentin mukaan sitouttaa kansainvälisessä tietoturvallisuusvelvoitteessa edellytettyihin tarpeellisiin toimenpiteisiin tämän artiklan määräysten täyttämiseksi. Yhteisöturvallisuustodistuksen myöntämisen edellytyksenä on, että yrityksessä on turvallisuusvastaava, joka huolehtii sitoumuksesta johtuvista velvoitteista.

12 artikla. *Turvallisuusluokitellun tiedon säilyttäminen*. Artiklan mukaan turvallisuusluokiteltu tieto säilytetään siten, että siihen pääsevät vain ne henkilöt, joilla on siihen lupa. Velvollisuudesta pitää huolta erityissuojattavan tietoaineiston suojaamisesta sen turvallisuusluokkaa vastaavalla tavalla sitä luotaessa, kopioitaessa, siirrettäessä, jaettaessa, säilytettäessä, hävitettäessä tai muutoin käsiteltäessä on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 9 §:n 1 momentissa. Pykälän 2 momentissa on annettu valtuus säätää valtioneuvoston asetuksella (tietoturvallisuusasetus) eri turvallisuusluokkia vastaavista turvallisuustoimenpiteistä. Asiakirjojen säilyttämistä ja käsittelyä koskevista turvallisuusvaatimuksista säädetään tietoturvallisuusasetuksen 14 §:ssä. Säilytystä koskevat määräykset ovat siten Suomessa säädetty asetuksentasoisena.

13 artikla. *Turvallisuusluokitellun tiedon välittäminen*. Artikla sisältää yksityiskohtaiset määräykset menettelyistä siirrettäessä turvallisuusluokiteltuja asiakirjoja ja aineistoja osapuolten kesken sekä sähköistä tiedonsiirtoa koskevat määräykset. Määräykset ovat sopusoinnussa asiakirjojan välittämistä ja sähköistä siirtämistä koskevien tietoturvallisuusasetuksen 18 ja 19 §:n kanssa.

14 artikla. *Vierailut*. Artiklaa sovelletaan vierailuihin, jotka edellyttävät pääsyä turvallisuusluokiteltuihin tietoihin, tai vierailuihin, joissa pääsy vierailun kohteeseen edellyttää turvallisuusselvitystä. Artiklan 1 kohdan mukaan tällaiset vierailut rajoitetaan virallisen tarkoituksen kannalta välttämättömiin vierailuihin.

Artiklan 2 kohdan mukaan vierailuluvan voi myöntää vain se osapuoli, jonka alueella vierailukohde sijaitsee, tai tämän osapuolen nimeämät valtion viranomaiset. Vierailuluvan myöntävä osapuoli vastaa siitä, että ehdotetun vierailun kohteena olevalle organisaatiolle tai laitokselle tiedotetaan vierailusta sekä vieraalle mahdollisesti annettavan turvallisuusluokitellun tiedon laajuudesta ja korkeimmasta turvallisuusluokasta. Artiklan 3 kohdan mukaan vierailulupapyynnöt esitetään suomalaisten vieraiden ollessa kyseessä Suomen Washingtonin-suurlähetystölle ja yhdysvaltalaisten vieraiden kyseessä ollessa Yhdysvaltojen Helsingin-suurlähetystölle.

15 artikla. *Turvallisuusvierailut*. Artiklan mukaan sopimuksessa mainittujen turvallisuusvaatimusten täytäntöönpanoa voidaan edistää osapuolten turvallisuushenkilöstön keskinäisillä vierailuilla. Turvallisuusedustajien sallitaan vierailla toisen osapuolen luona keskustelemassa ja tarkkailemassa täytäntöönpanomenettelyjä. Vierailuja koskevat säännökset ovat kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 18 §:ssä.

16 artikla. *Turvallisuusstandardit*. Artiklan mukaan kumpikin osapuoli antaa toiselle osapuolelle tietoja omista turvallisuusluokitellun tiedon suojaamiseen soveltamistaan turvallisuusstandardeista, -menettelyistä ja -käytännöistä.

17 artikla. *Turvallisuusluokitellun tiedon kopiointi.* Artiklan mukaan kun turvallisuusluokiteltuja asiakirjoja tai muita turvallisuusluokiteltua tietoa sisältäviä tietovälineitä kopioidaan, kaikki niissä olleet alkuperäiset turvallisuusmerkinnät kopioidaan tai merkitään myös jokaiseen kopioon. Tällaisia kopioituja asiakirjoja tai tietovälineitä valvotaan samalla tavalla kuin alkuperäisiä asiakirjoja tai tietovälineitä. Kopioiden lukumäärä rajoitetaan viralliseen tarkoitukseen vaadittavaan määrään. Tietoturvallisuusasetuksen 17 §:ssä säädetään asiakirjan kopioimisesta.

18 artikla. *Turvallisuusluokitellun tiedon hävittäminen*. Artiklan 1 kohdan mukaan toiselta osapuolelta saadut turvallisuusluokitellut asiakirjat ja muut turvallisuusluokiteltua tietoa sisältävät tietovälineet hävitetään polttamalla, silppuamalla, sulputtamalla tai muulla tavalla, joka estää niiden sisältämän turvallisuusluokitellun tiedon palauttamisen ennalleen. Artiklan 2 kohdan mukaan turvallisuusluokiteltua tietoa sisältävä turvallisuusluokiteltu aineisto, laitteet mukaan luettuna, hävitetään siten, ettei se enää ole tunnistettavissa, ja siten, että estetään kaiken siirretyn turvallisuusluokitellun tiedon tai sen osan palauttaminen ennalleen. Tietoturvallisuusasetuksen 21 §:ssä säädetään asiakirjan arkistoimisesta ja hävittämisestä. Käsittelyä koskevat määräykset ovat siten Suomessa säädetty asetuksentasoisina.

19 artikla. *Turvallisuusluokituksen alentaminen tai poistaminen*. Artiklan 1 kohdan mukaan turvallisuusluokiteltu tieto olisi luokiteltava alempaan turvallisuusluokkaan tai sen turvallisuusluokitus olisi poistettava heti, kun tietoa koskeva suojaamisvaatimus lievenee tai tietoa ei enää tarvitse suojata millään tavoin luvattomalta paljastamiselta. Artiklan 2 kohdan mukaan tiedon luovuttaneella osapuolella on täysi harkintavalta oman turvallisuusluokitellun tietonsa turvallisuusluokituksen alentamiseen tai poistamiseen nähden. Vastaanottava osapuoli ei saa alentaa toiselta osapuolelta saadun turvallisuusluokitellun tiedon turvallisuusluokitusta ilman tiedon luovuttaneen osapuolen kirjallista ennakkosuostumusta.

20 artikla. *Tiedon katoaminen tai vaarantuminen*. Artiklan mukaan tiedon luovuttaneelle osapuolelle ilmoitetaan viipymättä kaikesta sen turvallisuusluokitellun tiedon todetuista tai mahdollisesta katoamisesta tai vaarantumisesta, ja tiedon vastaanottava osapuoli käynnistää tutkinnan tapauksen tosiseikkojen selvittämiseksi. Tiedot luovuttaneelle osapuolelle ilmoitetaan tutkinnan tulokset sekä tiedot tilanteen uusiutumisen estämiseksi toteutetuista toimenpiteistä. Tämän artiklan velvoitteisiin liittyvät säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ään.

21 artikla. *Riidat*. Artiklan mukaan sopimuksesta johtuvat tai siihen liittyvät osapuolten väliset riidat ratkaistaan osapuolten välisillä neuvotteluilla, eikä niitä saateta kansallisen eikä kansainvälisen tuomioistuimen eikä muun henkilön tai yhteisön ratkaistavaksi.

22 artikla. *Kulut*. Artiklan mukaan kumpikin osapuoli vastaa omista kuluistaan, jotka aiheutuvat tämän sopimuksen täytäntöönpanosta.

23 artikla. *Loppumääräykset*. Artiklassa on sopimuksen voimaantuloa, täydentäviä järjestelyjä, irtisanomista ja voimassaoloaikaa koskevat määräykset sekä irtisanomisesta johtuvat velvollisuudet. Osapuolten toimivaltaiset viranomaiset voivat tehdä täydentäviä järjestelyjä tämän sopimuksen mukaisesti. Suomen ja Yhdysvaltojen turvallisuusviranomaisten välillä on tarkoitus neuvotella järjestely sopimuksen tarkemmasta täytäntöönpanosta. Sopimus on voimassa kaksikymmentäviisi vuotta ja sen jälkeen ilman eri toimenpiteitä viisi vuotta kerrallaan. Osapuoli voi irtisanoa sopimuksen ilmoittamalla asiasta kirjallisesti toiselle osapuolelle diplomaattiteitse yhdeksänkymmentä päivää etukäteen.

2 Lakiehdotuksen perustelut

1 §. Säännöksellä saatettaisiin voimaan sopimuksen lainsäädännön alaan kuuluvat määräykset. Lainsäädännön alaan kuuluvia määräyksiä selostetaan jäljempänä eduskunnan suostumuksen tarpeellisuutta koskevassa jaksossa.

2 §. Pykälässä ehdotetaan kumottavaksi Amerikan Yhdysvaltojen kanssa tehdyn sotilastiedon turvallisuutta koskevan sopimuksen voimaansaattamisesta 21 päivänä marraskuuta 1991 annettu tasavallan presidentin asetus (1359/1991). Kyseinen sopimus lakkaa olemasta voimassa sopimuksen 1 artiklan 1 kohdan mukaan uuden sopimuksen tullessa voimaan. Tämän vuoksi vuoden 1991 sopimuksen voimaansaattamisasetus on tarpeen kumota uuden sopimuksen voimaansaattamisen yhteydessä.

3 §. Sopimuksen muiden kuin lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta ja lain voimaantulosta säädettäisiin valtioneuvoston asetuksella. Laki on tarkoitus saattaa voimaan samanaikaisesti kuin sopimus tulee Suomen osalta voimaan.

3 Voimaantulo

Suomen ja Yhdysvaltojen välisen sopimuksen 23 artiklan 1 kohdan mukaan sopimus tulee voimaan toisen kuukauden ensimmäisenä päivänä sen jälkeen, kun Suomen tasavallan hallitus on ilmoittanut Amerikan Yhdysvaltojen hallitukselle diplomaattiteitse, että kaikki sopimuksen voimaan saattamiseksi Suomessa tarvittavat kansalliset menettelyt on saatettu päätökseen. Sopimuksen voimaansaattamislaki on tarkoitettu tulemaan voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samaan aikaan kuin sopimus tulee Suomen osalta voimaan.

Sopimuksen 1 artiklan 1 kohdassa määrätään, että sopimuksen tullessa voimaan Suomen hallituksen ja Yhdysvaltojen hallituksen 11 päivänä lokakuuta 1991 allekirjoittama sotilastiedon turvallisuutta koskeva sopimus (SopS 95/1991) lakkaa olemasta voimassa. Vuoden 1991 sopimus on aikanaan voimaansaatettu tasavallan presidentin asetuksella. Asetus on tarpeen kumota sopimuksen voimaansaattamisen yhteydessä.

4 Eduskunnan suostumuksen tarpeellisuus ja käsittelyjärjestys

4.1 Eduskunnan suostumuksen tarpeellisuus

Perustuslain 94 §:n 1 momentin mukaan eduskunta hyväksyy sellaiset valtiosopimukset ja muut kansainväliset velvoitteet, jotka sisältävät lainsäädännön alaan kuuluvia määräyksiä. Perustuslakivaliokunnan tulkintakäytännön mukaan määräys on luettava lainsäädännön alaan kuuluvaksi, jos se koskee jonkin perustuslaissa turvatun perusoikeuden käyttämistä tai rajoittamista, jos määräys muutoin koskee yksilön oikeuksien ja velvollisuuksien perusteita, jos määräyksen tarkoittamasta asiasta on perustuslain mukaan säädettävä lailla tai jos määräyksessä tarkoitetusta asiasta on jo voimassa lain säännöksiä taikka siitä on Suomessa vallitsevan käsityksen mukaan säädettävä lailla. Perustuslakivaliokunnan mukaan kansainvälisen velvoitteen määräys kuuluu näiden perusteiden mukaan lainsäädännön alaan siitä riippumatta, onko määräys ristiriidassa vai sopusoinnussa Suomessa lailla annetun säännöksen kanssa (kts. esimerkiksi PeVL 11/2000 vp ja PeVL 12/2000 vp).

Edellä mainituilla perusteilla esitykseen sisältyvässä sopimuksessa on lukuisia eduskunnan hyväksymistä edellyttäviä määräyksiä.

Sopimuksen 1 artiklan 1 kohdassa määrätään, että sopimuksen tullessa voimaan Suomen hallituksen ja Yhdysvaltojen hallituksen 11 päivänä lokakuuta 1991 allekirjoittama sotilastiedon turvallisuutta koskeva sopimus (SopS 94/1991) lakkaa olemasta voimassa. Perustuslain 94 §:n 1 momentin mukaan eduskunnan hyväksyminen vaaditaan sellaisen valtiosopimuksen ja muun kansainvälisen velvoitteen irtisanomiseen, joka sisältää lainsäädännön alaan kuuluvia määräyksiä. Perustuslakivaliokunta on sopimuksen voimassaolon lakkauttamista koskevassa tulkintakäytännössään katsonut, että vaikka sopimuksen lakkauttamisessa ei ole muodollisesti kysymys sopimuksen irtisanomisesta, vaikutuksiltaan sopimuksen kansainvälisoikeudellisen voimassaolon lakkauttaminen rinnastuu velvoitteen irtisanomiseen (PeVL 18/2002 vp ja PeVL 32/2006 vp). Perustuslakivaliokunta on perustuslakiuudistuksen yhteydessä katsonut, että eduskunnan hyväksyminen vaaditaan myös sellaisen kansainvälisen velvoitteen irtisanomiseen, jonka eduskunta on hyväksynyt ennen uuden perustuslain voimaantuloa. Hyväksymisvaatimus ulottuu lisäksi irtisanomistapauksiin, joissa velvoitetta ei ole alun perin hyväksytty eduskunnassa, mutta joissa velvoite uuden perustuslain sisällön perusteella arvioituna olisi tullut saattaa hyväksyttäväksi eduskunnassa (PeVM 10/1998 vp ja PeVL 18/2002 vp). Vuoden 1991 sopimuksen on aikaisemman valtiosäännön mukaisesti hyväksynyt tasavallan presidentti ja se on saatettu voimaan tasavallan presidentin asetuksella (1359/1991). Koska sopimus sisältää lainsäädännön alaan kuuluvia määräyksiä - esimerkiksi turvallisuusluokiteltujen tietojen salassapitoa ja suojaamista koskeva 1 artikla sekä turvallisuusluokitellun tiedon määritelmää ja turvallisuusluokitusmerkintöjä koskeva 2 artikla - sopimuksen lakkauttaminen edellyttää nykyisen perustuslain mukaan eduskunnan suostumusta.

Sopimuksen 2 artiklan 1 kohdassa määrätään, että kumpikin osapuoli suojaa toiselta osapuolelta suoraan tai välillisesti saamansa turvallisuusluokitellut tiedot tässä sopimuksessa määrättyjen vaatimusten sekä lakiensa ja asetustensa mukaisesti. Sopimuksen 2 artiklan 1 kohta yhdessä turvallisuusluokiteltujen tietojen suojaamista koskevan 7 artiklan kanssa muodostavat sopimuksen lainsäädännön alaan kuuluvat keskeiset määräykset. Sopimuksen 3 artiklassa määritellään, mitä tarkoitetaan turvallisuusluokitellulla tiedolla ja turvallisuusluokitelluilla sopimuksilla.

Koska nämä määritelmät vaikuttavat joko suoraan tai välillisesti sopimuksen lainsäädännön alaan kuuluvien aineellisten määräysten tulkintaan ja soveltamiseen, ne edellyttävät eduskunnan hyväksymistä (PeVL 6/2001 vp).

Sopimuksen 5 artiklassa on määräykset turvallisuusluokiteltujen tietojen merkitsemisestä ja turvallisuusluokkien vastaavuudesta. Yleisesti sovellettavat säännökset salassapito- ja luokitusmerkinnästä on säädetty julkisuuslain 25 §:ssä. Lain 25 §:n mukaan salassa pidettävään viranomaisen asiakirjaan on tehtävä merkintä asiakirjan salassa pitämisestä, kun tällainen asiakirja annetaan asianosaiselle ja kun asiakirja on pidettävä salassa toisen tai yleisen edun vuoksi. Muihin salaisiin asiakirjoihin tehtävä merkintä on harkinnanvarainen. Lisäksi kansainvälisistä tietoturvavelvoitteista annetun lain 8 §:ssä on säännökset turvallisuusluokan merkitsemisestä erityissuojattavaan tietoaineistoon. Sen mukaisesti erityissuojattavaan tietoaineistoon on julkisuuslain säännöksistä riippumatta tehtävä kansainvälisessä tietoturvallisuusvelvoitteessa määritelty merkintä sen osoittamiseksi, millaisia tietoturvallisuusvaatimuksia käsittelyssä on noudatettava. Määräys kuuluu lainsäädännön alaan.

Sopimuksen 7 artiklassa on sopimuksen soveltamisalan piiriin kuuluvan turvallisuusluokitellun tiedon suojaamista koskevat määräykset, jotka rajoittavat turvallisuusluokitellun tiedon luovuttamista sekä sen käyttämistä, välittämistä ja pääsyä siihen. Sopimuksen 7 artiklan a alakohdassa on kyse salassapitoa koskevasta sopimuksen ydinmääräyksestä, jonka perusteella Suomi voi suojata sopimuksen perusteella vaihdettua turvallisuusluokiteltua tietoa ilman julkisuuslaissa säädettyä vahinkoedellytysarviointia. Tähän suojaan liittyy myös b alakohta, jonka mukaan osapuolet varmistavat, että turvallisuusluokitellun tiedon vastaanottanut osapuoli antaa tiedolle samantasoisen suojan kuin luovuttanut osapuoli. Suomessa viranomaisten asiakirjojen julkisuus on pääsääntö. Jokaisella on perustuslain 12 §:n 2 momentin mukaan oikeus saada tieto viranomaisen julkisesta asiakirjasta. Tätä oikeutta voidaan rajoittaa välttämättömistä syistä vain lailla. Julkisuuslain säännöksistä poiketen kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 1 momentin mukaan erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisistä tietoturvallisuusvelvoitteesta muuta johdu. Sopimuksen 7 artiklan ensimmäisessä kappaleessa on ilmaistu turvallisuusluokiteltua tietoa saavia henkilöitä koskeva rajoitus, jonka mukaan pääsy turvallisuusluokiteltuihin tietoihin sallitaan ainoastaan niille henkilöille, joiden viralliset tehtävät edellyttävät sitä ja joista on tehty henkilöturvallisuusselvitys osapuolten ennalta määräämien vaatimusten mukaisesti. Velvoitetta vastaava säännös on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 3 momentissa. Sopimuksen 7 artiklan c alakohdan mukaan turvallisuusluokiteltua tietoa saa käyttää ainoastaan siihen tarkoitukseen, jota varten se on luovutettu. Velvoitetta vastaava säännös on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 2 momentissa. Sopimuksen 7 artiklan d alakohta koskee turvallisuusluokiteltuihin tietoihin sisältyviä tai liittyviä yksityisiä oikeuksia kuten patentteja, tekijänoikeuksia tai liikesalaisuuksia. Vastaanottavan osapuolen tulee kunnioittaa näitä yksityisiä oikeuksia eikä saa luovuttaa, käyttää, vaihtaa tai paljastaa turvallisuusluokiteltua tietoa, johon liittyy immateriaalioikeuksia, ennen kuin näiden oikeuksien omistajalta on saatu siihen nimenomainen kirjallinen lupa. Immateriaalioikeuksien suojasta säädetään muun muassa patenttilaissa (550/1967) ja tekijänoikeuslaissa (404/1961). Sanotut määräykset kuuluvat siten lainsäädännön alaan ja edellyttävät eduskunnan suostumusta voimaantullakseen.

Sopimuksen 8 artiklassa on määräykset henkilöturvallisuusselvityksistä. Artiklan 1 kohdan mukaan kumpikin osapuoli suorittaa asianmukaisen ja riittävän yksityiskohtaisen tutkinnan päättääkseen, onko henkilöllä edellytykset päästä turvallisuusluokiteltuun tietoon. Päätös henkilöturvallisuusselvityksen myöntämisestä tehdään kansallisten lakien ja määräysten mukaisesti. Turvallisuusselvitysten laadinnassa on otettava huomioon perustuslain 10 §:n 1 momentissa säädetty yksityiselämän suoja ja velvollisuus säätää henkilötietojen suojasta lailla. Suomessa turvalli-

suusselvityksen kohteena olevista henkilöistä sekä selvityksessä sovellettavasta menettelystä on säädetty turvallisuusselvityksistä annetussa laissa. Määräys kuuluu siten lainsäädännön alaan ja edellyttää eduskunnan suostumusta voimaantullakseen.

Sopimuksen 9 artiklassa on määräykset turvallisuusluokiteltujen tietojen luovuttamisesta hankeosapuolille ja 10 artiklassa on määräykset turvallisuusluokitelluista sopimuksista ja niitä tekevien yritysten turvallisuusselvityksistä. Yhteisöturvallisuusselvitystä koskevat säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 ja 13 §:ään. Sopimuksen 9 ja 10 artiklan määräykset kuuluvat lainsäädännön alaan.

Sopimuksen 15 artiklassa on määräykset osapuolten turvallisuusviranomaisten välisistä vierailuista. Osapuolten turvallisuusviranomaisten edustajien vierailuiden tarkoituksena on edistää sopimuksessa määrättyjen turvallisuusvaatimusten täytäntöönpanoa. Tähän vierailuoikeuteen ei sisälly sellaista julkista vallan käyttöä ja tarkastusoikeutta, joka olisi ristiriidassa perustuslain kanssa (PeVL 39/1997). Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 18 §:ssä on vastaavat säännökset vierailuja koskevan sopimusmääräyksen täytäntöönpanoon liittyvistä seikoista. Artiklan määräykset kuuluvat näin ollen lainsäädännön alaan.

Sopimuksen 20 artiklassa edellytetään, että tiedon luovuttaneelle osapuolelle ilmoitetaan viipymättä kaikesta sen turvallisuusluokitellun tiedon todetusta tai mahdollisesta katoamisesta tai vaarantumisesta, ja tiedon vastaanottava osapuoli käynnistää tutkinnan tapauksen tosiseikkojen selvittämisesi. Tiedon luovuttaneelle osapuolelle ilmoitetaan tutkinnan tulokset sekä tiedot tilanteen uusiutumisen estämiseksi toteutetuista toimenpiteistä. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ssä säädetään kansalliselle turvallisuusviranomaiselle kuuluvista velvoitteista sopimusmääräyksissä tarkoitetuissa tilanteissa. Artiklan määräykset kuuluvat näin ollen lainsäädännön alaan.

4.2 Käsittelyjärjestys

Turvallisuusluokitellun tietoaineiston salassapidosta on annettu yleiset säännökset laissa kansainvälisistä tietoturvallisuusvelvoitteista. Sen 6 §:n 1 momentin mukaan erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu. Lain 6 §:n 2 momentin mukaan erityissuojattavaa tietoaineistoa saa käyttää ja luovuttaa vain siihen tarkoitukseen, jota varten se on annettu, jollei se, joka on määritellyt aineiston turvallisuusluokan, ole antanut muuhun suostumustaan. Edelleen lain 6 §:n 3 momentin mukaan erityissuojattavaa tietoaineistoa käsittelevän viranomaisen on pidettävä huolta siitä, että tietoaineistoon on pääsy vain niillä, jotka tarvitsevat tietoja tehtävänsä hoitamisessa. Nämä henkilöt on nimettävä etukäteen kansainvälisessä tietoturvallisuusvelvoitteessa edellytetyissä tapauksissa. Sama koskee myös 1 §:n 2 momentissa tarkoitettua elinkeinonharjoittajaa. Erityissuojattavalla tietoaineistolla tarkoitetaan laissa sellaisia salassa pidettäviä asiakirjoja ja materiaaleja sekä asiakirjoista ja materiaaleista saatavissa olevia tietoja sekä näiden perusteella tuotettuja asiakirjoja ja materiaaleja, jotka kansainvälisen tietoturvallisuusvelvoitteen mukaisesti on turvallisuusluokiteltu. Käsillä olevan sopimuksen 7 artiklan määräykset eivät laajenna salassapitovelvollisuutta siitä, mitä salassapidosta on säädetty sanotun lain 6 §:ssä. Määräykset eivät siten vaikuta sopimuksen käsittelyjärjestykseen.

Suomen ja Yhdysvaltojen välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja vaihtamisesta tehtyyn sopimukseen ei voida katsoa sisältyvän sellaisia määräyksiä, jotka koskisivat perustuslakia sen 94 §:n 2 momentissa ja 95 §:n 2 momentissa tarkoitetulla tavalla. Hallituksen näkemyksen mukaan sopimus voitaisiin näin ollen hyväksyä äänten enemmistöllä ja ehdotus sen lainsäädännön alaan kuuluvien sopimusmääräysten voimaansaattamiseksi tavallisen lain säätämisjärjestyksessä.

Edellä olevan perusteella ja perustuslain 94 §:n mukaisesti esitetään, että

eduskunta hyväksyisi turvallisuustoimenpiteistä turvallisuusluokitellun tiedon suojaamiseksi Suomen tasavallan ja Amerikan Yhdysvaltojen välillä Helsingissä 27 päivänä kesäkuuta 2012 tehdyn sopimuksen.

Koska sopimus sisältää määräyksiä, jotka kuuluvat lainsäädännön alaan, annetaan samalla eduskunnan hyväksyttäväksi seuraava lakiehdotus:

Lakiehdotus

Laki

turvallisuustoimenpiteistä turvallisuusluokitellun tiedon suojaamiseksi Yhdysvaltojen kanssa tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Turvallisuustoimenpiteistä turvallisuusluokitellun tiedon suojaamiseksi Suomen tasavallan hallituksen ja Amerikan Yhdysvaltojen hallituksen välillä Helsingissä 27 päivänä kesäkuuta 2012 tehdyn sopimuksen lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

2 §

Tällä lailla kumotaan Amerikan Yhdysvaltojen kanssa tehdyn sotilastiedon turvallisuutta koskevan sopimuksen voimaansaattamisesta annettu tasavallan presidentin asetus (1359/1991).

3 §

Sopimuksen muiden määräysten voimaansaattamisesta ja tämän lain voimaantulosta säädetään valtioneuvoston asetuksella.

Helsingissä 22 päivänä marraskuuta 2012

Pääministerin sijainen, valtiovarainministeri

JUTTA URPILAINEN

Ulkoasiainministeri *Erkki Tuomioja*

Sopimusteksti

**SOPIMUS
SUOMEN TASAVALLAN HALLITUKSEN
JA
AMERIKAN YHDYSVALTOJEN
HALLITUKSEN VÄLILLÄ
TURVALLISUUSTOIMENPITEISTÄ
TURVALLISUUSLUOKITELLUN TIEDON SUOJAAMISEKSI**

Johdanto

Suomen tasavallan hallitus ja Amerikan yhdysvaltojen hallitus (jäljempänä "osapuolet"), jotka

ottavat huomioon, että osapuolet toimivat yhteistyössä esimerkiksi, mutta eivät yksinomaan, ulko-, puolustus-, turvallisuus-, poliisi-, tiede-, elinkeino- ja teknologia-asioissa varmistaakseen sellaisten turvallisuusluokiteltujen tietojen suojaamisen, joita vaihdetaan luottamuksellisesti suoraan osapuolten välillä, ja

jakavat yhteisen edun, joka liittyy turvallisuusluokitellun tiedon suojaamiseen,
ovat sopineet seuraavasta:

1 artikla

Seuraanto

1. Suomen hallituksen ja Yhdysvaltojen hallituksen 11 päivänä lokakuuta 1991 allekirjoittama sotilastiedon turvallisuutta koskeva sopimus (“tietoturvallisuussopimus”) lakkaa olemasta voimassa sinä päivänä, jona tämä sopimus tulee voimaan.

2. Tietoturvallisuussopimuksen voimassaolon päätyttyä tiedot, jotka ovat olleet suojattuina tietoturvallisuussopimuksen mukaisesti, suojataan tämän sopimuksen mukaisesti. Kaikki osapuolten välillä voimassa olevissa sopimuksissa tai järjestelyissä esiintyvät viittaukset tietoturvallisuussopimukseen katsotaan viittauksiksi tähän sopimukseen.

**AGREEMENT BETWEEN
THE GOVERNMENT OF THE REPUBLIC
OF FINLAND
AND
THE GOVERNMENT OF THE UNITED
STATES OF AMERICA
CONCERNING SECURITY MEASURES
FOR THE PROTECTION OF
CLASSIFIED INFORMATION**

Preamble

The Government of the Republic of Finland and the Government of the United States of America (hereinafter referred to as "the Parties"),

Considering that the Parties cooperate in matters such as, but not limited to, foreign affairs, defense, security, police, science, industry and technology, in order to ensure the protection of any Classified Information exchanged in confidence directly between the Parties; and

Having a mutual interest in the protection of Classified Information;
Have agreed as follows:

Article 1

Succession

1.The General Security of Military Information Agreement signed on October 11, 1991 between the Government of Finland and the Government of the United States (“the Security Agreement”) shall terminate on the date that this Agreement enters into force.

2. Following termination, any information that was protected in accordance with "the Security Agreement” shall continue to be protected in accordance with this Agreement. Any reference in an existing agreement or arrangement between the Parties to "the Security Agreement" shall be considered to be a reference to this Agreement.

3. Tätä sopimusta ei sovelleta sellaisen käytöltään rajoitetun tiedon (Restricted Data) vaihtoon, joka on määritelty Yhdysvaltojen vuoden 1954 atomienergialaissa (Atomic Energy Act of 1954, AEA), sellaisena kuin se on muutettuna, eikä entiseen käytöltään rajoitettuun tietoon (Formerly Restricted Data), joka on poistettu käytöltään rajoitetun tiedon luokasta atomienergialain mukaisesti mutta jonka Yhdysvaltojen hallitus edelleen katsoo puolustustiedoksi.

3. This Agreement shall not apply to the exchange of Restricted Data, as defined in the U.S. Atomic Energy Act of 1954, as amended (AEA), or to Formerly Restricted Data, which is data removed from the Restricted Data category in accordance with the AEA but still considered defense information by the Government of the United States of America.

2 artikla

Sitoumus turvallisuusluokitellun tiedon suojaamiseen

1. Kumpikin osapuoli suojaa toiselta osapuolelta suoraan tai välillisesti saamansa turvallisuusluokitellut tiedot tässä sopimuksessa määrättyjen vaatimusten sekä lakiensa ja määräystensä mukaisesti.

2. Kumpikin osapuoli ilmoittaa toiselle osapuolelle viipymättä lakeihinsa tai määräyksiinsä ehdotetuista muutoksista, jotka vaikuttaisivat tämän sopimuksen mukaiseen turvallisuusluokitellun tiedon suojaamiseen. Tällaisessa tapauksessa osapuolet neuvottelevat keskenään käsitelläkseen tähän sopimukseen mahdollisesti tehtäviä muutoksia. Tänä aikana turvallisuusluokitellut tiedot suojataan edelleen tässä sopimuksessa kuvatulla tavalla, elleivät osapuolet sovi kirjallisesti toisin.

Article 2

Commitment to the Protection of Classified Information

1. Each Party shall protect Classified Information received directly or indirectly from the other Party according to the terms set forth herein and in accordance with its laws and regulations.

2. Each Party shall promptly notify the other of any changes to its laws and regulations that would affect the protection of Classified Information under this Agreement. In such case, the Parties shall consult to consider possible amendments to this Agreement. In the interim Classified Information shall continue to be protected as described herein, unless agreed otherwise in writing by the Parties.

3 artikla

Määritelmät

Tässä sopimuksessa sovelletaan seuraavia määritelmiä:

a. Turvallisuusluokiteltu tieto: Tieto, jonka Suomen tasavallan hallitus tai Yhdysvaltojen hallitus tuottaa tai joka tuotetaan näiden hallitusten puolesta tai kuuluu jommankumman hallituksen lainkäyttövaltaan tai määräysvaltaan ja joka on suojattava kyseisen hallituksen kansallisen turvallisuuden vuoksi ja on osoitettu sellaiseksi tiedoksi kyseisen hallituksen määräämällä turvallisuusluokituksella. Tieto voi olla suullisessa, visuaalisessa, elektronisessa tai asiakirjan muodossa, tai se voi

Article 3

Definitions

For the purpose of this Agreement:

a. Classified Information: Any information that is generated by or for the Government of the Republic of Finland or the Government of the United States of America or that is under the jurisdiction or control of one of them, and which requires protection in the interests of national security of that government and that is so designated by the assignment of a security classification by that government. The information may be in oral, visual, electronic, or documentary form, or in the form

olla aineiston, kuten laitteitten tai teknologian, muodossa.

b. Turvallisuusluokiteltu sopimus: Sopimus, joka edellyttää tai tulee edellyttämään hankeosapuolen tai sen työntekijöiden pääsyä turvallisuusluokiteltuihin tietoihin sopimusta täytäntöön pantaessa.

c. Hankeosapuoli: Luonnollinen henkilö tai oikeushenkilö, jolla on oikeudellinen kelpoisuus tehdä sopimuksia, ja/tai tämän sopimuksen mukaisen turvallisuusluokitellun sopimuksen osapuoli.

d. Yhteisöturvallisuusselvitys (Facility Security Clearance, FSC): Toimivaltaisen turvallisuusviranomaisen lainkäyttövaltaansa kuuluvalle hankeosapuolen organisaatiolle antama todistus, josta ilmenee, että organisaatiosta on tehty tietyn tason turvallisuusselvitys ja että se on myös toteuttanut asianmukaiset tietyn tason turvallisuustoimet turvallisuusluokiteltujen tietojen suojaamiseksi. Todistus merkitsee myös sitä, että hankeosapuoli, jolle on myönnetty yhteisöturvallisuusselvitys, suojaa turvallisuusluokkaan LUOTTAMUKSELLINEN/CONFIDENTIAL tai sitä ylempään turvallisuusluokkaan kuuluvat tiedot tämän sopimuksen määräysten mukaisesti ja että toimivaltainen turvallisuusviranomainen valvoo ja varmistaa, että hankeosapuoli noudattaa tätä sopimusta. Hankeosapuolelta ei vaadita yhteisöturvallisuusselvitystä sellaisten turvallisuusluokiteltujen sopimusten täytäntöönpanoa varten, jotka edellyttävät käytöltään rajoitetun (Restricted) turvallisuusluokitellun tiedon vastaanottamista tai tuottamista.

e. Henkilöturvallisuusselvitys (Personnel Security Clearance, PSC):

(1) Toimivaltaisen turvallisuusviranomaisen antama todistus sellaisen luonnollisen henkilön henkilöturvallisuusselvityksen tasosta, joka on osapuolen lainkäyttövaltaan kuuluvan valtion viraston tai hankeosapuolen organisaation palveluksessa.

(2) Jos luonnollinen henkilö on yhden osapuolen kansalainen mutta hänen on määrä työskennellä toisen osapuolen tai sen hankeosapuolten palveluksessa, kyseisen henkilön kansalaisuusvaltion toimivaltaisen turvallisuusviranomaisen antama lausunto tämän henkilön edellytyksistä saada henkilöturvallisuusselvitys kyseisen osapuolen lainkäyttövaltaan kuuluvan valtion viraston tai hankeosapuolen organisaation palveluksessa.

of material including, equipment or technology.

b. Classified Contract: A contract that requires, or will require, access to Classified Information by a Contractor or by its employees in the performance of a contract.

c. Contractor: An individual or a legal entity possessing the legal capacity to conclude contracts and/or a party to a Classified Contract under the provisions of this Agreement.

d. Facility Security Clearance (FSC): A certification provided by the relevant security authority for a Contractor facility under its jurisdiction that indicates the facility is security cleared to a specified level and also has suitable security safeguards in place at a specified level to safeguard Classified Information. The certification also signifies that Classified Information LUOTTAMUKSELLINEN/CONFIDENTIAL or above will be protected by the Contractor for which the FSC is provided in accordance with the provisions of this Agreement and that compliance shall be monitored and enforced by the responsible security authority. An FSC is not required for a Contractor to undertake Contracts that require the receipt or production of Classified Information at the KÄYTTÖ RAJOITETTU (Restricted) level.

e. Personnel Security Clearance (PSC):

(1) A certification provided by the relevant security authority concerning the level of personnel security clearance held by the individual, who is employed by a government agency or Contractor facility under the jurisdiction of a Party.

(2) In the case of an individual who is a citizen of one Party but is to be employed by the other Party or its Contractors, a statement provided by the relevant security authority of the individual's country of citizenship concerning the individual's eligibility for a personnel security clearance at a level specified

suusselvitys, joka vastaa tätä selvitystä pyytävän osapuolen ilmoittamaa tasoa.

f. Tiedonsaantitarve: Turvallisuusluokitellun tiedon valtuutetun haltijan päätös, jonka mukaan tiedon mahdollinen vastaanottaja tarvitsee pääsyä tiettyyn turvallisuusluokiteltuun tietoon toimiakseen laillisessa ja sallitussa valtion tehtävässä tai avustaakseen siinä.

by the requesting Party.

f. Need to Know: A determination made by an authorized holder of Classified Information that a prospective recipient requires access to specific Classified Information in order to perform or assist in a lawful and authorized governmental function.

4 artikla

Turvallisuusviranomaiset

Article 4

Security Authorities

Osapuolet ilmoittavat toisilleen kirjallisesti ne turvallisuusviranomaiset, jotka vastaavat tämän sopimuksen täytäntöönpanosta, sekä näiden turvallisuusviranomaisten mahdolliset myöhemmät muutokset.

The Parties shall inform each other in writing of the security authorities responsible for implementation of this Agreement and any subsequent changes to these security authorities.

5 artikla

Turvallisuusluokiteltujen tietojen merkitseminen

Article 5

Marking of Classified Information

1. Turvallisuusluokiteltuun tietoon merkitään toisiaan vastaavat kansalliset turvallisuusluokat seuraavasti

1. Classified Information shall be marked with corresponding national security classifications as follows:

*Suomi/Finland**	*United States/Yhdysvallat*
ERITTÄIN SALAINEN	TOP SECRET
SALAINEN	SECRET
LUOTTAMUKSELLINEN	CONFIDENTIAL
** KÄYTTÖ RAJOITETTU	*** No equivalent/Ei vastaavaa

* Ruotsiksi kirjoitetuissa tai käännetyissä asiakirjoissa voi olla ruotsinkieliset turvallisuusluokitusmerkinnät. Ruotsinkielisiä turvallisuusluokitusmerkintöjä voidaan käyttää myös muissa tapauksissa, jos Suomen valtion viranomainen katsoo sen tarpeelliseksi. Suomenkielisiä turvallisuusluokitusmerkintöjä vastaavat ruotsinkieliset merkinnät ovat seuraavat: "YTTERST HEMLIG", joka vastaa luokkaa ERITTÄIN SALAINEN, "HEMLIG", joka vastaa luokkaa SALAINEN, "KONFIDENTIELL", joka vastaa luokkaa LUOTTAMUKSELLINEN ja "BEGRÄNSAD TILLGÅNG", joka vastaa luokkaa KÄYTTÖ RAJOITETTU.

** Kaikki asiakirjat tai aineisto, joissa on Yhdysvaltojen merkintä siitä, että se on valvottua luokittelematonta tietoa (Controlled Unclassified Information, CUI), merkitään, käsitellään, siirretään ja säilytetään Suomessa kuten turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluva tieto.

*** Turvallisuusluokiteltuja tietoja, joihin on merkitty suomenkielinen turvallisuusluokka KÄYTTÖ RAJOITETTU, käsitellään Yhdysvalloissa samoin kuin Yhdysvaltojen luokittelemattomia (U.S. UNCLASSIFIED) tietoja, jotka yhden tai useamman Yhdysvaltojen lain mukaan eivät ole julkisia. Näihin lakeihin kuuluvat tiedonvapauslaki (Freedom of Information Act, FOIA) ja Yhdysvaltojen lakikokoelman 10 osan §130c, joka koskee salassa pidettäviä tietoja sekä ulkomaisia hallituksia ja kansainvälisiä järjestöjä koskevia tiettyjä arkaluonteisia tietoja (Title 10 U.S.C. §130c "Nondisclosure of Information: Certain Sensitive Information of Foreign Government and International Organizations"). Turvallisuusluokitelluiksi merkityt tiedot käsitellään, siirretään ja säilytetään asianmukaisin suojaustoimin, jotka estävät luvattomien henkilöiden pääsyn tietoihin. Tämän sopimuksen liite sisältää Yhdysvalloissa noudatettavat määräykset suomalaisista turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluvista tiedoista.

2. Kumpikin osapuoli leimaa, merkitsee tai liittää kaikkiin toiselta osapuolelta saamiinsa turvallisuusluokiteltuihin tietoihin tiedot luovuttaneen hallituksen nimen. Tietoihin leimataan, merkitään tai liitetään vastaanottavan osapuolen kansallinen turvallisuusluokka, joka ei saa olla alhaisempi kuin tiedot luovuttaneen hallituksen määräämä vastaava turvallisuusluokka ja joka antaa vähintään samantasoisen suojan kuin tiedot luovuttaneen osapuolen määräämä turvallisuusluokka.

* Security classification markings in Swedish may appear on documents written in or translated into Swedish. Security classification markings in Swedish also may appear in other cases if the Finland State authority considers it necessary. The equivalents in Swedish of the Finnish security classification are as follows: "YTTERST HEMLIG" for ERITTÄIN SALAINEN, "HEMLIG" for SALAINEN, "KONFIDENTIELL" for LUOTTAMUKSELLINEN and "BEGRÄNSAD TILLGÅNG" for KÄYTTÖ RAJOITETTU.

** Any document or material bearing a U.S. marking indicating it is Controlled Unclassified Information (CUI) shall be marked, handled, transmitted, and stored as KÄYTTÖ RAJOITETTU in Finland.

*** Classified Information bearing the Finnish classification KÄYTTÖ RAJOITETTU shall be handled in the United States as U.S. UNCLASSIFIED information that is exempt from public release under one or more U.S. laws. These laws include the Freedom of Information Act (FOIA) and Title 10 U.S.C. §130c, "Nondisclosure of Information: Certain Sensitive Information of Foreign Government and International Organizations." Classified Information so marked shall be handled, transmitted and stored affording appropriate protection that will prevent access by unauthorized personnel. The Appendix to this Agreement contains provisions for Finnish Classified Information at the KÄYTTÖ RAJOITETTU level in the United States.

2. Each Party shall stamp, mark or designate the name of the originating government on all Classified Information received from the other Party. The information shall be stamped, marked or designated with a national security classification marking of the receiving Party no lower than the corresponding classification specified by the originating government that will afford a degree of protection at least equivalent to that afforded to it by the releasing Party.

6 artikla

Vastuu turvallisuusluokitellusta tiedosta

Kumpikin osapuoli on vastuussa kaikista toisen osapuolen turvallisuusluokitelluista tiedoista sinä aikana, jona tiedot ovat sen lainkäyttöalueella ja määräysvallassa. Tietojen kuljetuksen aikana tiedot lähettänyt osapuoli on vastuussa kaikista turvallisuusluokitelluista tiedoista, kunnes tiedot ovat virallisesti siirtyneet toisen osapuolen hallintaan.

7 artikla

Turvallisuusluokitellun tiedon suojaaminen

Luonnollisella henkilöllä ei ole oikeutta päästä toiselta osapuolelta saatuihin turvallisuusluokiteltuihin tietoihin pelkästään arvonsa, asemansa tai turvallisuusselvityksensä nojalla. Pääsy turvallisuusluokiteltuihin tietoihin sallitaan ainoastaan niille henkilöille, joiden viralliset tehtävät edellyttävät sitä ja joista on tehty henkilöturvallisuusselvitys osapuolten ennalta määräämien vaatimusten mukaisesti. Osapuolet varmistavat, että:

a. turvallisuusluokitellun tiedon vastaanottava osapuoli ei anna tätä tietoa kolmannen valtion hallitukselle, henkilölle, yritykselle, laitokselle, järjestölle tai muulle yhteisölle ilman tiedon luovuttaneen osapuolen kirjallista ennakkolupaa;

b. turvallisuusluokitellun tiedon vastaanottava osapuoli antaa tälle tiedolle samantasoisen suojan kuin luovuttanut osapuoli;

c. turvallisuusluokitellun tiedon vastaanottava osapuoli ei käytä tätä tietoa eikä salli sitä käytettävän muuhun kuin siihen tarkoitukseen, jota varten tieto on luovutettu, ilman luovuttaneen osapuolen kirjallista ennakkolupaa;

d. turvallisuusluokitellun tiedon vastaanottava osapuoli kunnioittaa tähän tietoon sisältyviä tai liittyviä yksityisiä oikeuksia, kuten patentteja, tekijänoikeuksia tai liikesalaisuuksia, eikä luovuta, käytä, vaihda tai paljasta turvallisuusluokiteltua tietoa, johon liittyy immateriaalioikeuksia, ennen kuin näiden oi-

Article 6

Responsibility for Classified Information

Each Party shall be responsible for all Classified Information of the other Party while the information is under its jurisdiction and control. While in transit, the sending Party shall be responsible for all Classified Information until custody of the information is formally transferred to the other Party.

Article 7

Protection of Classified Information

No individual shall be entitled to access to Classified Information received from the other Party solely by virtue of rank, appointment, or security clearance. Access to the Classified Information shall be granted only to those individuals whose official duties require such access and who have been granted a Personnel Security Clearance in accordance with the prescribed standards of the Parties. The Parties shall ensure that:

a. The receiving Party shall not release the Classified Information to a government, person, firm, institution, organization or other entity of a third country without the prior written approval of the releasing Party;

b. The receiving Party shall afford the Classified Information a degree of protection equivalent to that afforded it by the releasing Party;

c. The receiving Party shall not use or permit the use of the Classified Information for any other purpose than that for which it was provided without the prior written approval of the releasing Party;

d. The receiving Party shall respect private rights, such as patents, copyrights, or trade secrets, that are included or involved in the Classified Information and not release, use, exchange or disclose Classified Information in which intellectual property rights exist, until the specific written -authorization of the

keuksien omistajalta on ensin saatu siihen nimenomainen kirjallinen lupa;

e. jokainen turvallisuusluokiteltua tietoa käsittelevä organisaatio tai laitos pitää luetteloa niistä organisaation tai laitoksen henkilöistä, joilla on lupa päästä kyseiseen tietoon;

f. luodaan vastuu- ja valvontamenettelyt turvallisuusluokitellun tiedon levityksen ja tähän tietoon pääsyn hallintaa varten; ja

g. turvallisuusluokitellun tiedon vastaanottava osapuoli noudattaa kaikkia lisärajoituksia, jotka tämän tiedon luovuttanut osapuoli mahdollisesti määrää tiedon käytölle, paljastamiselle tai luovuttamiselle tai tietoon pääsylle.

8 artikla

Henkilöturvallisuusselvitys

1. Kumpikin osapuoli suorittaa asianmukaisen ja riittävän yksityiskohtaisen tutkinnan päättääkseen, onko henkilöllä edellytykset päästä turvallisuusluokiteltuun tietoon. Päätös henkilöturvallisuusselvityksen myöntämisestä tehdään osapuolen kansallisten lakien ja määräysten mukaisesti.

2. Ennen kuin osapuolen edustaja luovuttaa turvallisuusluokiteltua tietoa toisen osapuolen työntekijälle tai edustajalle, tiedon vastaanottava osapuoli antaa tiedon luovuttavalle osapuolelle vakuutuksen siitä, että kyseisestä työntekijästä tai edustajasta on tehty tarvittavan tason turvallisuusselvitys, että hän tarvitsee pääsyä turvallisuusluokiteltuun tietoon virallisessa tehtävässään ja että toinen osapuoli suojaa tiedon.

9 artikla

Turvallisuusluokitellun tiedon luovuttaminen hankeosapuolille

Ennen toiselta osapuolelta saadun turvallisuusluokitellun tiedon luovuttamista hankeosapuolelle tai mahdolliselle hankeosapuolelle vastaanottava osapuoli.

a. varmistaa, että kyseisellä hankeosapuolella tai mahdollisella hankeosapuolella ja

owner of these rights has first been obtained;

e. Each facility or establishment that handles Classified Information shall maintain a list of individuals at the facility or establishment who are authorized to have access to such Classified Information;

f. Accountability and control procedures shall be established to manage the dissemination of and access to the Classified Information; and

g. The receiving Party shall comply with any additional limitations on the use, disclosure, release and access to the Classified Information which may be specified by the originating Party.

Article 8

Personnel Security Clearances

1. Each Party shall conduct an appropriate investigation, in sufficient detail to determine an individual's suitability for access to Classified Information. The determination on the granting of a Personnel Security Clearance will be made in accordance with national laws and regulations of the Party.

2. Before a representative of a Party releases Classified Information to an officer or representative of the other Party, the receiving Party shall provide to the releasing Party an assurance that the officer or representative possesses the necessary level of security clearance and requires access for official purposes, and that the Classified Information will be protected by the other Party.

Article 9

Release of Classified Information to Contractors

Prior to the release to a Contractor or prospective Contractor of any Classified Information received from the other Party, the receiving Party shall:

a. Ensure that such Contractor or prospective Contractor and the Contractor's facility

hankeosapuolen organisaatiolla on valmiudet suojata turvallisuusluokiteltu tieto;

b. antaa hankeosapuolen organisaatiolle asianmukaisen yhteisöturvallisuusselvityksen;

c. antaa asianmukaiset henkilöturvallisuusselvitykset kaikille henkilöille, joiden tehtävät edellyttävät pääsyä kyseiseen turvallisuusluokiteltuun tietoon;

d. varmistaa, että kaikille henkilöille, joilla on pääsy turvallisuusluokiteltuun tietoon, on selitetty heidän velvollisuutensa suojata tämä tieto sovellettavien lakien ja määräysten mukaisesti;

e. suorittaa turvallisuusselvityksen saaneessa organisaatiossa määräaikaisia turvallisuustarkastuksia varmistaakseen, että turvallisuusluokiteltu tieto suojataan tässä sopimuksessa määrättyjen vaatimusten mukaisesti; ja

f. varmistaa, että pääsy turvallisuusluokiteltuun tietoon rajoitetaan vain niihin henkilöihin, joilla on tiedonsaantitarve virallisia tarkoituksia varten.

have the capability to protect the Classified Information;

b. Grant to the facility an appropriate Facility Security Clearance;

c. Grant appropriate Personnel Security Clearances for all individuals whose duties require access to the Classified Information;

d. Ensure that all individuals having access to the Classified Information are informed of their responsibilities to protect the Classified Information in accordance with applicable laws and regulations;

e. Carry out periodic security inspections of cleared facilities to ensure that the Classified Information is protected as required herein; and

f. Ensure that access to the Classified Information is limited to those persons who have a Need to Know for official purposes.

10 artikla

Turvallisuusluokitellut sopimukset

1. Kun osapuoli aikoo tehdä tai valtuuttaa valtiossaan toimivan hankeosapuolen tekemään toisen osapuolen valtiossa toimivan hankeosapuolen kanssa sopimuksen, johon liittyy turvallisuusluokkaan LUOTTAMUKSELLINEN/CONFIDENTIAL tai sitä ylempään turvallisuusluokkaan kuuluvaa tietoa, se osapuoli, joka tekee tai valtuuttaa hankeosapuolen tekemään sopimuksen, pyytää vakuutuksen siitä, että toisen osapuolen toimivaltaiset turvallisuusviranomaiset ovat antaneet yhteisöturvallisuusselvityksen. Vakuutukseen liittyy vastuu siitä, että yhteisöturvallisuusselvityksen saaneen hankeosapuolen turvallisuustoiminnassa noudatetaan kansallisia turvallisuuslakeja ja -määräyksiä ja että toimivaltaiset turvallisuusviranomaiset valvovat sitä.

2. Sen osapuolen vastuuviranomainen, joka on ryhtynyt neuvottelemaan toisessa valtiossa täytäntöön pantavasta turvallisuusluokitellusta sopimuksesta, ja jokainen hankeosapuoli, jonka kanssa on tehty toisessa valtiossa täytäntöön pantava turvallisuusluokiteltu sopi-

Article 10

Classified Contracts

1. When a Party proposes to place, or authorizes a Contractor in its country to place, a Contract involving Classified Information that is classified at the LUOTTAMUKSELLINEN/ CONFIDENTIAL level or above with a Contractor in the country of the other Party, the Party that is to place or authorize the Contractor to place such Contract will request an assurance that a Facility Security Clearance has been issued from the appropriate security authorities of the other Party. The assurance will carry a responsibility that the security conduct by the cleared Contractor will be in accordance with national security laws or regulations and be monitored by appropriate security authorities.

2. The responsible authority of the Party in the process of negotiating a Classified Contract to be performed within the other country, and every Contractor in receipt of a Classified Contract or in the process of negotiating a classified subcontract to be performed

mus tai joka on ryhtynyt neuvottelemaan toisessa valtiossa täytäntöön pantavasta turvallisuusluokitellusta alihankintasopimuksesta, sisällyttää sopimukseen, tarjouspyyntöön tai alihankintasopimusta koskevaan asiakirjaan asianmukaiset turvallisuuslausekkeet sekä muut asianmukaiset määräykset, myös turvallisuuskustannuksia koskevat määräykset.

within the other country, shall incorporate in the contract, request for proposal or subcontract document, appropriate security clauses as well as other relevant provisions, including costs for security.

11 artikla

Vastuu organisaatioista

Kumpikin osapuoli vastaa kaikkien sellaisten valtion ja yksityisten organisaatioiden ja laitosten turvallisuudesta, joissa säilytetään toisen osapuolen turvallisuusluokiteltua tietoa, ja varmistaa, että kuhunkin tällaiseen organisaatioon tai laitokseen nimetään pätevät henkilöt, joilla on vastuu tiedon valvonnasta ja suojaamisesta ja valtuudet siihen.

Article 11

Responsibility for Facilities

Each Party shall be responsible for the security of all government and private facilities and establishments where Classified Information of the other Party is kept and shall ensure for each such facility or establishment that qualified individuals are appointed who shall have the responsibility and authority for the control and protection of the information.

12 artikla

Turvallisuusluokitellun tiedon säilyttäminen

Turvallisuusluokiteltu tieto säilytetään siten, että siihen pääsevät vain ne henkilöt, joilla on siihen lupa.

Article 12

Storage of Classified Information

Classified Information shall be stored in a manner that assures access only by those individuals who have been authorized access.

13 artikla

Turvallisuusluokitellun tiedon välittäminen

1. Turvallisuusluokiteltu tieto välitetään osapuolten välillä hallituskanavien tai etukäteen kirjallisesti sovittujen kanavien kautta.

2. Tietoa välitettäessä noudatetaan seuraavia tiedon turvallisuutta koskevia vähimmäisvaatimuksia:

a. Asiakirjat:

(1) Turvallisuusluokiteltua tietoa sisältävät asiakirjat tai muut tietovälineet välitetään kaksinkertaisissa, suljetuissa postikuorissa. Sisimpään postikuoreen merkitään vain asiakirjojen tai muiden tietovälineiden turvallisuusluokka ja aiotun vastaanottajan organisaation osoite, ja uloimpaan postikuoreen merkitään vastaanottajan organisaation osoite sekä lähettäjän organisaation osoite ja rekiste-

Article 13

Transmission

1. Classified Information shall be transmitted between the Parties through government-to-government channels or channels mutually approved in advance in writing.

2. The minimum requirements for the security of the information during transmission shall be as follows:

a. Documents:

(1) Documents or other media containing Classified Information shall be transmitted in double, sealed envelopes, the innermost envelope bearing only the classification of the documents or other media and the organizational address of the intended recipient, the outer envelope bearing the organizational address of the recipient, the organizational address of the sender, and the registry number,

rinumero, jos sellainen on olemassa.

(2) Uloimpaan postikuoreen ei tehdä mitään merkintää postikuoressa olevien asiakirjojen tai muiden tietovälineiden turvallisuusluokasta. Suljettu postikuori kuljetetaan sen jälkeen osapuolten määräämien menettelyjen mukaisesti.

(3) Osapuolten välillä välitettäviin turvallisuusluokiteltuja asiakirjoja tai muita tietovälineitä sisältäviin paketteihin liitetään tositteet, ja lopullinen vastaanottaja allekirjoittaa paketin sisältämiä asiakirjoja tai muita tietovälineitä koskevan tositteen ja palauttaa sen lähettäjälle.

b. Turvallisuusluokiteltu aineisto:

(1) Turvallisuusluokiteltu aineisto, mukaan lukien laitteisto, kuljetetaan suljetuissa, peitetyissä ajoneuvoissa, tai se pakataan tai suojataan muutoin huolellisesti siten, että sen yksityiskohtien tunnistaminen estetään, ja sitä valvotaan jatkuvasti, jotta luvattomat henkilöt eivät pääse siihen.

(2) Turvallisuusluokiteltu aineisto, mukaan lukien laitteisto, jota on säilytettävä väliaikaisesti kuljetusta odotettaessa, sijoitetaan suojatulle varastoalueelle. Tällaisilla alueilla on oltava tunkeutumisenhavaitsemislaitteet tai turvallisuusselvityksen saaneet vartijat, jotka valvovat varastoalueita jatkuvasti. Vain asianmukaisen turvallisuus-selvityksen saaneilla valtuutetuilla henkilöillä saa olla pääsy varastoalueille.

(3) Jokaisesta tapahtumasta, jossa turvallisuusluokiteltu aineisto, laitteisto mukaan lukien, siirretään toiselle haltijalle kuljetuksen aikana, on saatava tosite, ja lopullinen vastaanottaja allekirjoittaa tositteen ja palauttaa sen lähettäjälle.

c. Sähköinen tiedonsiirto:

(1) Sähköisesti siirrettävä turvallisuusluokkaan LUOTTAMUKSELLINEN/ CONFIDENTIAL tai sitä ylempään turvallisuusluokkaan kuuluva tieto lähetetään turvallisin menetelmin, jotka kummankin osapuolen viestintäturvallisuusviranomaiset ovat hyväksyneet.

(2) Turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluva tieto lähetetään Yhdysvalloissa liitteessä olevien määräysten mukaisesti.

if applicable.

(2) No indication of the classification of the enclosed documents or other media shall be made on the outer envelope. The sealed envelope shall then be transmitted according to the prescribed procedures of the Parties.

(3) Receipts shall be prepared for packages containing classified documents or other media that are transmitted between the Parties, and a receipt for the enclosed documents or media shall be signed by the final recipient and returned to the sender.

b. Classified material:

(1) Classified material, including equipment, shall be transported in sealed, covered vehicles, or otherwise be securely packaged or protected in order to prevent identification of its details, and kept under continuous control to prevent access by unauthorized persons.

(2) Classified material, including equipment, which must be stored temporarily awaiting shipments shall be placed in protected storage areas. The areas shall be protected by intrusion-detection equipment or guards with security clearances who shall maintain continuous surveillance of the storage areas. Only authorized personnel with the requisite security clearance shall have access to the storage areas.

(3) Receipts shall be obtained on every occasion when classified material, including equipment, changes hands en route, and a receipt shall be signed by the final recipient and returned to the sender.

c. Electronic transmissions:

(1) Classified Information that is classified at the LUOTTAMUKSELLINEN/ CONFIDENTIAL level or above that is to be transferred electronically shall be transmitted using secure means that have been approved by both Parties' communications security authorities.

(2) Classified Information that is classified at the KÄYTTÖ RAJOITETTU level will be transmitted in the U.S. in accordance with the provisions contained in the Appendix.

14 artikla

Vierailut

1. Sellaiset osapuolen edustajien vierailut toisen osapuolen organisaatioihin ja laitoksiin, jotka edellyttävät pääsyä turvallisuusluokiteltuihin tietoihin, tai vierailut, joissa pääsy vierailun kohteeseen edellyttää turvallisuusselvitystä, rajoitetaan virallisen tarkoituksen kannalta välttämättömiin vierailuihin. Vierailulupa annetaan vain edustajille, joilla on voimassa oleva turvallisuusselvitys.

2. Vierailuluvan organisaatioihin ja laitoksiin myöntävät vain se osapuoli, jonka alueella vierailun kohteena oleva organisaatio tai laitos sijaitsee, tai tämän osapuolen nimeämät valtion viranomaiset. Vierailun kohteena oleva osapuoli tai sen nimeämät viranomaiset vastaavat siitä, että ehdotetun vierailun kohteena olevalle organisaatiolle tai laitokselle tiedotetaan ehdotetusta vierailusta sekä vieraalle mahdollisesti annettavan turvallisuusluokitellun tiedon laajuudesta ja korkeimmasta turvallisuusluokasta.

3. Osapuolten edustajien vierailupyynnöt esitetään suomalaisten vieraiden kyseessä ollessa Suomen Washingtonin-suurlähetystölle ja yhdysvaltalaisten vieraiden kyseessä ollessa Yhdysvaltojen Helsingin-suurlähetystölle.

Article 14

Visits

1. Visits by representatives of one Party to facilities and establishments of the other Party that require access to Classified Information or visits in which a security clearance is required to permit access, shall be limited to those necessary for official purposes. Authorization shall only be granted to representatives who possess a valid security clearance.

2. Authorization to visit the facilities and establishments shall be granted only by the Party in whose territory the facility or establishment to be visited is located or by government officials designated by that Party. The visited Party, or its designated officials, shall be responsible for advising the facility or establishment of the proposed visit, and the scope and highest level of Classified Information that may be furnished to the visitor.

3. Requests for visits by representatives of the Parties shall be submitted through the Embassy of the United States in Helsinki, in the case of United States visitors, and through the Embassy of Finland in Washington D.C, in the case of Finnish visitors.

15 artikla

Turvallisuusvierailut

Sopimuksessa määrättyjen turvallisuusvaatimusten täytäntöönpanoa voidaan edistää osapuolten turvallisuushenkilöstön keskinäisillä vierailuilla. Sen vuoksi kummankin osapuolen turvallisuusedustajien sallitaan ennakkoneuvottelujen jälkeen vierailla toisen osapuolen luona keskustelemassa ja tarkkailemassa toisen osapuolen täytäntöönpanomenettelyjä, jotta turvallisuusjärjestelmät saataisiin vastaamaan toisiaan kohtuullisessa määrin. Kumpikin osapuoli auttaa turvallisuusedustajia määrittämään, suojataanko toiselta osapuolelta saatua turvallisuusluokiteltua tietoa riittävästi.

Article 15

Security Visits

Implementation of the security requirements set out in the Agreement can be advanced through reciprocal visits by security personnel of the Parties. Accordingly, security representatives of each Party, after prior consultation, shall be permitted to visit the other Party to discuss and observe the implementing procedures of the other Party in the interest of achieving reasonable comparability of the security systems. Each Party shall assist the security representatives in determining whether Classified Information received from the other Party is being adequately protected.

16 artikla

Turvallisuusstandardit

Kumpikin osapuoli antaa toiselle osapuolelle pyydettäessä tietoja omista turvallisuusluokitellun tiedon suojaamiseen soveltamistaan turvallisuusstandardeista, -menettelyistä ja -käytännöistä.

17 artikla

Turvallisuusluokitellun tiedon kopiointi

Kun turvallisuusluokiteltuja asiakirjoja tai muita turvallisuusluokiteltua tietoa sisältäviä tietovälineitä kopioidaan, kaikki niissä olleet alkuperäiset turvallisuusmerkinnät kopioidaan tai merkitään myös jokaiseen kopioon. Tällaisia kopioituja asiakirjoja tai tietovälineitä valvotaan samalla tavoin kuin alkuperäisiä asiakirjoja tai tietovälineitä. Kopioiden lukumäärä rajoitetaan viralliseen tarkoitukseen vaadittavaan määrään.

18 artikla

Turvallisuusluokitellun tiedon hävittäminen

1. Toiselta osapuolelta saadut turvallisuusluokitellut asiakirjat ja muut turvallisuusluokiteltua tietoa sisältävät tietovälineet hävitetään polttamalla, silppuamalla, sulputtamalla tai muulla tavalla, joka estää niiden sisältämän turvallisuusluokitellun tiedon palauttamisen ennalleen.

2. Turvallisuusluokiteltua tietoa sisältävä turvallisuusluokiteltu aineisto, laitteet mukaan luettuina, hävitetään siten, ettei se enää ole tunnistettavissa, ja siten, että estetään kaiken siirretyn turvallisuusluokitellun tiedon tai sen osan palauttaminen ennalleen.

19 artikla

Turvallisuusluokituksen alentaminen tai poistaminen

1. Osapuolet sopivat, että turvallisuusluokiteltu tieto olisi luokiteltava alempaan turvallisuusluokkaan tai sen turvallisuusluokitus olisi

Article 16

Security Standards

On request, each Party shall provide the other Party with information about its security standards, procedures and practices for safeguarding of Classified Information.

Article 17

Reproduction of Classified Information

When classified documents or other media containing Classified Information are reproduced, all original security markings thereon shall also be reproduced or marked on each copy. Such reproduced documents or media shall be placed under the same controls as the original document or media. The number of copies shall be limited to that required for official purposes.

Article 18

Destruction of Classified Information

1. Classified documents and other media containing Classified Information received from the other Party shall be destroyed by burning, shredding, pulping, or other means preventing reconstruction of the Classified Information contained therein.

2. Classified material, including equipment, containing Classified Information shall be destroyed so that it is no longer recognizable and so as to preclude reconstruction of the transmitted Classified Information in whole or in part.

Article 19

Downgrading and Declassification

1. The Parties agree that Classified Information should be downgraded to a lower classification level or it should be declassi-

poistettava heti, kun tietoa koskeva suojaamisvaatimus lievenee tai tietoa ei enää tarvitse suojata millään tavoin luvattomalta paljastamiselta.

2. Tiedon luovuttaneella osapuolella on täysi harkintavalta oman turvallisuusluokitellun tietonsa turvallisuusluokituksen alentamiseen tai poistamiseen nähden. Vastaanottava osapuoli ei saa alentaa toiselta osapuolelta saadun turvallisuusluokitellun tiedon turvallisuusluokitusta ilman tiedon luovuttaneen osapuolen kirjallista ennakkosuostumusta.

fied as soon as information requires a lower degree of protection or requires no further protection against unauthorized disclosure.

2. The originating Party has complete discretion concerning downgrading or declassification of its own Classified Information. The receiving Party shall not downgrade the security classification of Classified Information received from the other Party without the prior written consent of the originating Party.

20 artikla

Tiedon katoaminen tai vaarantuminen

Tiedon luovuttaneelle osapuolelle ilmoitetaan viipymättä kaikesta sen turvallisuusluokitellun tiedon todetusta tai mahdollisesta katoamisesta tai vaarantumisesta, ja tiedon vastaanottava osapuoli käynnistää tutkinnan tapauksen tosiseikkojen selvittämiseksi. Tiedon luovuttaneelle osapuolelle ilmoitetaan tutkinnan tulokset sekä tiedot tilanteen uusiutumisen estämiseksi toteutetuista toimenpiteistä.

Article 20

Loss or Compromise

The originating Party shall be informed immediately of all losses or compromises, as well as possible losses or compromises, of its Classified Information, and the receiving Party shall initiate an investigation to determine the circumstances. The results of the investigation and information regarding measures taken to prevent recurrence shall be forwarded to the originating Party.

21 artikla

Riidat

Tästä sopimuksesta johtuvat tai siihen liittyvät osapuolten väliset riidat ratkaistaan osapuolten välisillä neuvotteluilla, eikä niitä saateta kansallisen eikä kansainvälisen tuomioistuimen eikä muun henkilön tai yhteisön ratkaistavaksi.

Article 21

Disputes

Disagreements between the Parties arising under or relating to this Agreement shall be settled through consultations between the Parties and shall not be referred to a national court, to an international tribunal, or to any other person or entity for settlement.

22 artikla

Kulut

Kumpikin osapuoli vastaa omista kuluistaan, jotka aiheutuvat tämän sopimuksen täytäntöönpanosta.

Article 22

Costs

Each Party shall be responsible for meeting its own costs incurred in implementing this Agreement.

23 artikla

Loppumääräykset

1. Kun kumpikin osapuoli on allekirjoittanut tämän sopimuksen, sopimus tulee voimaan toisen kuukauden ensimmäisenä päivänä sen jälkeen, kun Suomen tasavallan hallitus on ilmoittanut Amerikan Yhdysvaltojen hallitukselle diplomaattiteitse, että kaikki sopimuksen voimaan saattamiseksi Suomessa tarvittavat kansalliset menettelyt on saatettu päätökseen.

2. Osapuolten toimivaltaiset turvallisuusviranomaiset voivat tehdä täydentäviä järjestelyjä tämän sopimuksen mukaisesti.

3. Kumpi tahansa osapuoli voi irtisanoa tämän sopimuksen ilmoittamalla aikomuksestaan irtisanoa sopimus toiselle osapuolelle kirjallisesti diplomaattiteitse yhdeksänkymmentä päivää etukäteen.

4. Ellei tätä sopimusta irtisanota tämän artiklan 3 kohdan mukaisesti, sopimus pysyy voimassa kaksikymmentäviisi vuotta ja sen jälkeen ilman eri toimenpiteitä viisi vuotta kerrallaan.

5. Tämän sopimuksen irtisanomisen estämättä kaikki tämän sopimuksen mukaisesti luovutettu turvallisuusluokiteltu tieto suojataan edelleen tämän sopimuksen määräysten mukaisesti.

Tämän vakuudeksi allekirjoittaneet, hallitustensa siihen asianmukaisesti valtuuttamina, ovat allekirjoittaneet tämän sopimuksen.

Tehty Helsingissä 27 päivänä kesäkuuta 2012 kahtena kappaleena suomen ja englannin kielellä, molempien tekstien ollessa yhtä todistusvoimaiset. Jos syntyy tulkintaeroja, englanninkielinen teksti on ratkaiseva.

Suomen tasavallan hallituksen puolesta

ulkoasiainministeri
Erkki Tuomioja

Amerikan yhdysvaltojen hallituksen puolesta

ulkoministeri
Hillary Clinton

Article 23

Final Provisions

1. Following signature by both Parties, this Agreement shall enter into force on the first day of the second month after the date that the Government of the Republic of Finland notifies the Government of the United States of America through diplomatic channels that all domestic procedures necessary to bring this Agreement into force have been completed.

2. Supplementary arrangements under this Agreement may be concluded by the appropriate security authorities of the Parties.

3. Either Party may terminate this Agreement by notifying the other Party in writing, through the diplomatic channels, ninety days in advance of its intention to terminate the Agreement.

4. Unless terminated in accordance with paragraph 3 of this Article, this Agreement shall remain in force for a period of twenty five years and shall be automatically extended in five year increments thereafter.

5. Notwithstanding the termination of this Agreement, all Classified Information provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

In witness whereof, the undersigned, being duly authorized thereto by their respective Governments, have signed this Agreement.

Done in duplicate at Helsinki this 27 day of June 2012 in the Finnish and English languages, both texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the Government of the Republic of Finland

Minister for Foreign Affairs
Erkki Tuomioja

For the Government of the United States of America

Secretary of State
Hillary Clinton

Liite

Liite

Turvallisuusluokkaan KÄYTTÖ RAJOITETTU (Restricted) kuuluvan suomalaisen turvallisuusluokitellun tiedon käsittelymenettely Yhdysvalloissa

1. Suomalaisia asiakirjoja tai aineistoa, joihin on merkitty turvallisuusluokka KÄYTTÖ RAJOITETTU, käsitellään Yhdysvalloissa samoin kuin Yhdysvaltojen luokittelemattomia (U.S. UNCLASSIFIED) tietoja, jotka yhden tai useamman Yhdysvaltojen lain nojalla eivät ole julkisia. Näihin lakeihin kuuluvat tiedonvapauslaki (Freedom of Information Act, FOIA) ja Yhdysvaltojen lakikokoelman 10 osan §130c, joka koskee salassa pidettäviä tietoja sekä ulkomaisia hallituksia ja kansainvälisiä järjestöjä koskevia tiettyjä arkaluonteisia tietoja (Title 10 U.S.C. §130c "Nondisclosure of Information: Certain Sensitive Information of Foreign Government and International Organizations"). Asiakirjoja tai aineistoa, joihin on tehty tämä merkintä, säilytetään asianmukaisen suojan antavissa lukituissa säiliöissä tai suljetuilla alueilla, joille luvattomat henkilöt eivät pääse.

2. Turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluvia asiakirjoja käsitellään siten, että estetään niiden julkaiseminen tai käyttö ja pääsy niihin muita tarkoituksia kuin Yhdysvaltojen hallituksen tai tiedon luovuttaneen valtion virallisia tarkoituksia varten. Näiden asiakirjojen sisältämä tieto on ei-julkista sovellettavien Yhdysvaltojen tiedonvapauslakien nojalla, ellei Suomen hallitus ole antanut kirjallista ennakkosuostumusta sen julkaisemiseen.

3. Yhdysvaltalaisten hankeosapuolten kanssa tehdyissä sopimuksissa, joihin liittyy turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluvan turvallisuusluokitellun tiedon säilyttämistä tai tuottamista, on oltava turvallisuusvaatimuslauseke, jossa määrätään turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluvan tiedon turvaamiseksi sovellettavista suojatoimista.

4. Ennen kuin minkään viestintä- ja tietojärjestelmän sallitaan tallentaa, käsitellä tai lä-

Appendix

Procedures for handling the Finnish Classified Information at the KÄYTTÖ RAJOITETTU (Restricted) level within the United States

1. Finnish documents or material bearing the classification KÄYTTÖ RAJOITETTU shall be handled in the United States as U.S. UNCLASSIFIED information that is exempt from public release under one or more U.S. laws. These laws include Freedom of Information Act (FOIA) and Title 10 U.S.C. §130c, "Nondisclosure of Information: Certain Sensitive Information of Foreign Governments and International Organizations." Documents or material so marked shall be stored in locked containers affording appropriate protection or closed spaces areas that will prevent access by unauthorized personnel.

2. KÄYTTÖ RAJOITETTU documents shall be handled in a manner that will preclude open publication, access or use for other than official government purposes of the United States or the releasing country. Information contained in these documents shall be exempt from public release under applicable U.S. Freedom of Information laws unless the Government of Finland has granted prior written approval.

3. Contracts placed with U.S. contractors that involve the retention or production of Classified Information at the KÄYTTÖ RAJOITETTU level will include a security requirements clause identifying the protective measures to be applied to safeguard the KÄYTTÖ RAJOITETTU information.

4. Before any communications and information system is allowed to store, process or

hettää edelleen turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluvaa tietoa, sille on saatava turvallisuushyväksyntä, jota kutsutaan akkreditoinniksi. Akkreditointi määritellään viralliseksi lausunnoksi, jolla toimivaltainen viranomainen vahvistaa, että järjestelmän käyttö täyttää asianomaiset turvallisuusvaatimukset eikä aiheuta vaaraa, jota ei voida hyväksyä. Yhdysvaltojen hallituksen ministeriöiden ja virastojen käyttämien pöytätietokoneiden ja kannettavien tietokoneiden osalta järjestelmän rekisteröintiasiakirja yhdessä turvallisuuskäyttöohjeiden kanssa täyttää akkreditointiin liittyvät vaatimukset. Viestintä- ja tietojärjestelmien käytöstä hankeosapuolille annettavat ohjeet sisältyvät sopimuksen turvallisuusvaatimuslausekkeeseen.

5. Turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluvat asiakirjat lähetetään Yhdysvalloissa ensimmäisen luokan postissa yhdessä turvakuoressa. Yhdysvaltojen ulkopuolelle toimitettavat asiakirjat lähetetään kahdessa turvakuoressa, joista sisemmässä on merkintä KÄYTTÖ RAJOITETTU; tällainen lähetys toimitetaan yhdysvaltalaisen turvallisuusluokitellun tiedon kuljetukselle hyväksytyin menetelmin, kansainvälisessä lentopostissa tai kaupallisen lähettipalvelun avulla.

6. Muutoin luokittelemattomissa yhdysvaltalaisissa asiakirjoissa, jotka on alun perin luovuttanut Yhdysvaltojen hallituksen virasto ja jotka sisältävät Suomen turvallisuusluokkaan KÄYTTÖ RAJOITETTU luokittelemaa tietoa, on kansilehdellä ja ensimmäisellä sivulla merkintä "KÄYTTÖ RAJOITETTU – Exempt from Public Disclosure Title 10 U.S.C. §130.c". Asiakirjoihin merkitään, mikä niihin sisältyvä tieto kuuluu turvallisuusluokkaan KÄYTTÖ RAJOITETTU.

7. Turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluva tieto voidaan siirtää tai siihen voi päästä sähköisesti julkisen verkon, kuten Internetin, kautta käyttämällä hallituksen tai kaupallisen toimijan salauslaitteita, jotka molempien osapuolten hallitusten turvallisuusviranomaiset ovat hyväksyneet. Kansainväliset puhelut, videokonferenssit tai faksilähetykset, joissa käsitellään turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluvaa tietoa, saavat olla ilmitekstiä, jos hy-

forward Classified Information at the KÄYTTÖ RAJOITETTU level, it must be given security approval, known as accreditation. An accreditation is defined as a formal statement by appropriate authority confirming that the use of a system meets the appropriate security requirements and does not present unacceptable risk. For standalone desktop PCs and laptop systems utilized in U.S. Government departments or agencies, the system registration document together with the Security Operating Procedures fulfills the role of the required accreditation. For contractors the guidance on the use of communications and information systems will be incorporated within a security requirements clause in the contract.

5. KÄYTTÖ RAJOITETTU documents shall be transmitted by first class mail within the United States in one secure cover. Transmission outside the United States shall be in two secure covers, the inner cover marked KÄYTTÖ RAJOITETTU. Such transmission shall be by one of the means authorized for United States Classified Information, international air mail or commercial courier.

6. Otherwise unclassified U.S. documents originated by U.S. government agencies that contain information that Finland has classified KÄYTTÖ RAJOITETTU shall bear on the cover and the first page the marking "KÄYTTÖ RAJOITETTU – Exempt from Public Disclosure Title 10 U.S.C. §130c." The KÄYTTÖ RAJOITETTU information shall be identified in the documents.

7. KÄYTTÖ RAJOITETTU information may be transmitted or accessed electronically via a public network like the Internet using government or commercial encryption devices mutually accepted by the Parties' government security authorities. International telephone conversations, video conferencing or facsimile transmission containing KÄYTTÖ RAJOITETTU information may be in clear text, if an approved encryption system is not available. Telephone conversa-

väksyttyä salausjärjestelmää ei ole käytettävissä. Yhdysvalloissa käydyt puhelut, videokonferenssit tai faksilähetykset saavat olla ilmitekstiä.

tions, video conferencing or facsimile transmissions within the United States may be in clear text.