HE 4/2023 vp

Hallituksen esitys eduskunnalle tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdyn sopimuksen ja turvallisuussääntöjen hyväksymiseksi ja voimaansaattamiseksi sekä Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen irtisanomiseksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan, että eduskunta hyväksyisi tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdyn sopimuksen ja turvallisuussäännöt sekä lain, jolla saatetaan voimaan sopimuksen ja turvallisuussääntöjen lainsäädännön alaan kuuluvat määräykset. Esityksessä ehdotetaan myös, että eduskunta antaisi suostumuksensa siihen, että Suomi irtisanoo Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen.

Pohjois-Atlantin sopimuksen osapuolten välillä tehty tietoturvallisuussopimus on osa Pohjois-Atlantin liiton (Nato) oikeudellisesti sitovaa sopimuskehikkoa, johon Pohjois-Atlantin sopimukseen liittyvien uusien jäsenmaiden edellytetään sitoutuvan. Sopimus sisältää Pohjois-Atlantin sopimuksen osapuolten välillä sovellettavat määräykset turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja turvaamisesta. Monenvälinen sopimus korvaa Suomen kahdenväliset tietoturvallisuusjärjestelyt Pohjois-Atlantin liiton kanssa.

Sopimus tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä on tehty Brysselissä 6.3.1997 ja se on tullut kansainvälisesti voimaan 16.8.1998. Sopimus tulee Suomen osalta voimaan kolmenkymmenen päivän kuluttua siitä päivästä, kun Suomi tallettaa tietoturvallisuussopimusta koskevan liittymiskirjansa Amerikan yhdysvaltojen hallituksen huostaan. Sopimuksen ja turvallisuussääntöjen voimaansaattamislaki on tarkoitettu tulemaan voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samaan aikaan, kun sopimus tulee Suomen osalta voimaan. Laki Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain kumoamisesta on tarkoitettu tulemaan voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samanaikaisesti, kun kyseisten sopimusten irtisanominen tulee voimaan.

———

SISÄLLYS

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Sopimus Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta

Pohjois-Atlantin sopimuksen osapuolten välillä vuonna 1997 tietoturvallisuudesta tehdyn sopimuksen (jäljempänä myös tietoturvallisuussopimus) mukaan tehokas poliittinen neuvottelu, yhteistyö ja suunnittelu puolustusasioissa sopimuksen tavoitteiden saavuttamiseksi edellyttävät turvallisuusluokitellun tiedon vaihtamista osapuolten välillä. Tiedon vaihtamiseksi tarvitaan määräyksiä sellaisen turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja turvaamisesta. Sopimuksen tarkoituksena on asettaa turvallisuusvaatimuksille ja menettelyille yleiset puitteet. Sopimus ei aseta osapuolille velvoitteita luovuttaa tällaista tietoa.

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.

Tietoturvallisuussopimuksessa määritellään Naton ja sen jäsenvaltioiden turvallisuusluokiteltu tieto, johon sopimusta sovelletaan. Sopimuksen keskeinen lähtökohta on, että osapuolet säilyttävät tiedon turvallisuusluokituksen ja pyrkivät kaikin keinoin turvaamaan tietoa. Tietoa ei luovuteta kolmansille osapuolille ilman tiedon luovuttajan suostumusta. Sopimuksen toimeenpanoa varten osapuolilla tulee olla kansallinen turvallisuusviranomainen. Sopimuksen mukaan luottamuksellista (CONFIDENTIAL) ja sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa käsittelevillä henkilöillä tulee olla asianmukainen turvallisuusselvitys.

Sopimuksen mukaan osapuolet laativat turvallisuusvaatimuksia, joilla varmistetaan turvallisuusluokitellun tiedon yhteinen suojauksen taso. Naton turvallisuussääntöjen vaatimukset koskevat henkilöstöturvallisuutta, tietoaineistoturvallisuutta, toimitilaturvallisuutta, viestintä- ja tietojärjestelmien turvallisuutta sekä yritysturvallisuutta.

Vuonna 1997 tehdyllä sopimuksella on korvattu osapuolten välillä vuonna 1952 tehty turvallisuussopimus. Pohjois-Atlantin liiton kaikki nykyiset jäsenvaltiot ovat tietoturvallisuussopimuksen osapuolia.

1.2 Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehty hallinnollinen järjestely ja Pohjois-Atlantin liiton kanssa tehty tietoturvallisuussopimus

Suomen ja Pohjois-Atlantin liiton välinen tietoturvallisuussopimus (*Security Agreement between Finland and the North Atlantic Treaty Organization*) allekirjoitettiin 22.9.1994 Suomen liityttyä Naton rauhankumppanuusohjelmaan (*Partnership for Peace, PfP*). Sopimuksessa sovittiin turvallisuusluokitellun aineiston vaihtamisesta ja suojaamisesta.

Suomen ja Naton välisellä tietoturvallisuussopimuksella Suomi sitoutui luokittelemaan ja suojaamaan rauhankumppanuusohjelman puitteissa Natolta saadun aineiston sekä laatimaan turvallisuusselvityksen niistä henkilöistä, joilla on pääsy suojattuun aineistoon. Sopimuksen liitteenä

oli selvitys Naton käyttämästä asiakirjojen turvallisuusluokittelusta sekä tiettyjen hallinnollisten kysymysten järjestämisestä sopimuksen toimeenpanemiseksi.

Samassa yhteydessä allekirjoitettiin Naton tilojen käyttöä koskeva käyttäytymissääntö (*Code of Conduct*), joka liittyi Suomen edustajien lisääntyvään liikkumiseen Naton tiloissa. Käyttäytymissäännön allekirjoittamalla Suomi sitoutui olemaan käyttämättä Naton tiloja epäasialliseen toimintaan. Lisäksi ulkoasiainministeriön 13.9.1994 tekemällä päätöksellä hyväksyttiin tietoturvallisuussopimukseen liittyvät kaksi hallinnollisluonteista asiakirjaa (turvallisuusluokiteltua tietoa koskevat minimistandardit ja toimeenpanojärjestely) ja nimettiin sopimuksessa edellytetyksi informaatio- ja asiakirjaturvallisuuskysymyksistä vastaavaksi hallintoviranomaiseksi ulkoasiainministeriö. Päätöksen esittelymuistiossa hallintoviranomaisen tehtävät yksilöidään viittaamalla kansallisen sopimuksessa tarkoitetun turvallisuusviranomaisen tehtäviin sekä keskusrekisteriin (*Central Registry)*.

Sopimus katsottiin voitavan tehdä tuolloin voimassa olleen valtiosäännön mukaisesti viranomaisten välisenä, niin sanottuna kansainvälisenä hallintosopimuksena, koska asiakirjaturvallisuutta koskeva sopimus luonnehdittiin käytännön yhteistyöhön liittyväksi hallinnollisluonteiseksi asiakirjaksi. Sopimuksen liitteineen ei katsottu olevan ristiriidassa Suomen lainsäädännön kanssa. Tämän johdosta päätös sopimuksen ja käyttäytymissäännön allekirjoittamisesta tehtiin lausuntokierroksen jälkeen ulkoasiainministeriössä ja sopimuksen allekirjoitti Suomen edustaja Natossa.

Vuonna 2004 Suomessa säädettiin laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), jota 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. Lakia voidaan soveltaa vain, jos kansainvälinen sopimus on saatettu Suomessa voimaan perustuslaissa säädetyllä tavalla tai jos kysymys on Suomea muutoin sitovasta kansainvälisestä velvoitteesta.

Vuonna 2012 valtioneuvoston yleisistunto asetti valtuuskunnan neuvottelemaan vuoden 1994 tietoturvallisuussopimusta täydentävän hallinnollisen järjestelyn, jonka tarkoituksena oli ajantasaistaa vuoden 1994 sopimus siten, että siinä otetaan huomioon kansainvälisistä tietoturvallisuusvelvoitteista annetun lain säännökset sekä ajantasaistetut turvallisuusmääräykset. Tämän mukaisesti osapuolet neuvottelivat keväällä 2012 sopimusta täydentävän järjestelyn, joka allekirjoitettiin Helsingissä 3.7.2012. Hallinnollinen järjestely sisältää muun muassa määräykset turvallisuusluokitellun tiedon merkitsemisestä, tiedon suojaamisesta ja pääsystä tietoon, turvallisuusvaatimusten yksityiskohdista ja turvallisuustarkastuksista. Hallinnollisen järjestelyn kansallisen hyväksymisen yhteydessä saatettiin kansallisesti voimaan myös vuonna 1994 tehty Suomen ja Naton välinen tietoturvallisuussopimus (SopS 7 ja 8/2013). Hallinnollisen järjestelyn sekä vuonna 1994 tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta 21.12.2012 annettu laki (945/2012) tuli voimaan 1.2.2013. Suomen liittyessä Naton monenväliseen tietoturvallisuussopimukseen nämä kahdenväliset tietoturvallisuusjärjestelyt on tarkoitus irtisanoa sekä niiden voimaansaattamislaki kumota.

1.3 Valmistelu

Sopimuksen valmistelu

Tasavallan presidentti päätti 17.5.2022 valtioneuvoston esityksestä, että Suomi ilmoittaa Pohjois-Atlantin liitolle kiinnostuksesta käydä keskustelut Natoon liittymisestä ja nimitti Suomen

valtuuskunnan liittymiskeskusteluihin. Suomen kiinnostuksenosoitus esitettiin Naton pääsihteerille ulkoministerin kirjoittamalla kirjeellä, joka luovutettiin Brysselissä 18.5.2022. Naton jäsenvaltioiden päämiehet kutsuivat Suomen liittymiskeskusteluihin 29.6.2022 Madridin huippukokouksen yhteydessä.

Suomen ja Naton väliset liittymiskeskustelut käytiin Naton päämajassa Brysselissä 4.7.2022. Liittymiskeskusteluissa katettiin viisi osa-aluetta: 1) poliittiset kysymykset ja terrorismin torjunnan politiikkaan liittyvät kysymykset, 2) puolustus- ja sotilaalliset kysymykset, 3) resurssikysymykset, 4) tietoturvallisuuteen liittyvät kysymykset ja 5) oikeudelliset kysymykset. Liittymiskeskustelujen mukaan Suomen tulee liittyä seuraaviin kuuteen Naton sopimukseen 12 kuukauden sisällä Pohjois-Atlantin sopimusta koskevan Suomen liittymiskirjan tallettamisesta: sopimus Pohjois-Atlantin sopimuksen sopimuspuolten välillä niiden joukkojen asemasta (Nato SOFA), pöytäkirja Pohjois-Atlantin sopimuksen mukaisesta perustettujen kansainvälisten sotilasesikuntien asemasta (Pariisin pöytäkirja), sopimus teknisten tietojen välittämisestä puolustustarkoituksiin, sopimus puolustukseen liittyvien, patentoitavaksi haettujen keksintöjen salassapidon vastavuoroiseksi turvaamiseksi, sopimus Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta sekä Pohjois-Atlantin osapuolten välinen sopimus ydinpuolustustietoja koskevasta yhteistyöstä.

Liittymiskeskustelujen jälkeen tasavallan presidentti päätti 4.7.2022 valtioneuvoston ratkaisuehdotuksesta, että Suomi toimittaa Pohjois-Atlantin liitolle aiekirjeen liittymisestä Pohjois-Atlantin sopimukseen. Aiekirje toimitettiin Natolle 5.7.2022, ja Pohjois-Atlantin sopimuksen osapuolet allekirjoittivat Suomen liittymispöytäkirjan samana päivänä.

Kansallinen valmistelu

Valtioneuvoston yleisistunto asetti 15.9.2022 koordinaatioryhmän ja sen alatyöryhmät valmistelemaan hallituksen esitystä Pohjois-Atlantin sopimuksen hyväksymisestä. Hallituksen esitys eduskunnalle Pohjois-Atlantin sopimuksen sekä Pohjois-Atlantin liiton, kansallisten edustajien ja kansainvälisen henkilöstön asemasta tehdyn sopimuksen hyväksymiseksi ja voimaansaattamiseksi (HE 315/2022 vp) annettiin 5.12.2022. Eduskunta hyväksyi esityksen 1.3.2023 (EV 327/2022 vp) ja tasavallan presidentti 23.3.2023. Suomen liittymiskirja on talletettu Yhdysvaltojen hallituksen huostaan 4.4.2023 ja sopimus (SopS 17 ja 18/2023) on tullut Suomen osalta voimaan samana päivänä.

Edellä mainitut kuusi sopimusta päätettiin valmistella ja esittää hyväksyttäviksi erillisinä hallituksen esityksinä. Ulkoministeriö asetti 5.12.2022 työryhmän valmistelemaan hallituksen esitystä Naton tietoturvallisuussopimuksen hyväksymisestä. Työryhmässä olivat edustettuina ulkoministeriö, puolustusministeriö, oikeusministeriö, Suojelupoliisi ja Liikenne- ja viestintävirasto Traficom. Pääesikunnan edustaja osallistui työhön pysyvänä asiantuntijana. Työryhmä kokoontui yhteensä 11 kertaa. Työryhmä kuuli valmistelun aikana tasavallan presidentin kansliaa ja ministeriöitä, joilla ei ollut edustajaa työryhmässä. Valtioneuvoston kanslia, valtiovarainministeriö, työ- ja elinkeinoministeriö, sosiaali- ja terveysministeriö sekä maa- ja metsätalousministeriö osallistuivat kuulemiseen.

Työryhmä sai hallituksen esityksen muotoon laaditun mietintönsä valmiiksi 22.3.2023.

Hallituksen esitysluonnoksesta pyydettiin lausuntoa muun muassa ministeriöiltä ja muilta viranomaisilta, elinkeinoelämän edustajilta sekä järjestöiltä ajalla 24.3.–21.4.2023 Lausuntopalvelu.fi –palvelun kautta. Annetut lausunnot sekä lausuntoyhteenveto ovat saatavilla valtioneuvoston hankesivuilla hankenumerolla UM001:00/2023.

Tietoturvallisuussopimuksen ruotsinkielisen käännöksen valmistelussa on tehty yhteistyötä Ruotsin kanssa.

2 Voimassa oleva lainsäädäntö ja sen arviointi

2.1 Laki kansainvälisistä tietoturvallisuusvelvoitteista

2.1.1 Lain yleinen soveltamisala

Lakia kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) sovelletaan erityissuojattaviin tietoaineistoihin. Näillä tarkoitetaan 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. Määräysvalta erityissuojattavaan tietoaineistoon säilyy luovutuksen jälkeenkin aineiston luovuttaneella valtiolla, kansainvälisellä järjestöllä tai toimielimellä. Lakia voidaan soveltaa vain, jos kansainvälinen sopimus on saatettu Suomessa voimaan perustuslaissa säädetyllä tavalla tai jos kysymys on Suomea muutoin sitovasta kansainvälisestä tietoturvallisuusvelvoitteesta.

Lain soveltamisalan piiriin kuuluvia erityissuojattavia tietoaineistoja ovat lisäksi Suomen viranomaisen tai lain soveltamisalan piiriin kuuluvan elinkeinonharjoittajan laatimat asiakirjat, joista ilmenee Suomeen toimitettuihin erityissuojattaviin tietoaineistoihin sisältyviä tai tällaisista saatavissa olevia tietoja. Lakia ei sovelleta asiakirjojen tai niiden osien salassapitoon tai luokitukseen, jos asiakirjat sisältävät vain Suomen kansallista tietoa.

Laissa on säännökset henkilöturvallisuusselvitystodistuksen (*Personnel Security Clearance, PSC*) ja yritysturvallisuusselvitystodistuksen (*Facility Security Clearance, FSC*) myöntämisestä. Henkilö- tai yritysturvallisuusselvityksen laatineen viranomaisen on salassapitosäännösten estämättä toimitettava todistuksen antamista ja siihen liittyvää harkintaa varten kansalliselle turvallisuusviranomaiselle tieto kaikista selvityksen laadinnassa ilmi tulleista selvityksen kohdetta koskevista seikoista (11 §:n 1 momentti ja 12 §:n 1 momentti).

Todistuksen antamista koskevaan arvioon sekä todistuksen voimassaoloon ja peruuttamiseen sovelletaan turvallisuusselvityslakia (726/2014) (kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n 2 momentti ja 12 §:n 2 momentti). Jos kansallinen turvallisuusviranomainen kieltäytyy antamasta henkilö- tai yritysturvallisuusselvitystodistusta, sen tulee ilmoittaa syyt tähän selvityksen hakijalle ja sen kohteelle annettavassa kirjallisessa päätöksessä (kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n 3 momentti ja 12 §:n 3 momentti). Muutoksenhausta säädetään lain 20 a §:ssä.

Kansainvälisistä tietoturvallisuusvelvoitteista annettua lakia on tarkistettu sen säätämisen jälkeen tähän mennessä kuusi kertaa. Laki tarjoaa asianmukaisen säädöskehikon edelleen myös Naton tietoturvallisuussopimuksen täytäntöönpanolle Suomessa. Tietoturvallisuussopimus ei edellytä lain muuttamista, mutta lain 20-vuotisen soveltamiskäytännön valossa on jatkossa hyödyllistä arvioida mahdollisia tarkistustarpeita.

2.1.2 Lain suhde julkisuus- ja tiedonhallintalainsäädäntöön

Perustuslain (731/1999) sananvapautta ja julkisuutta koskevan 12 §:n mukaan viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi erikseen rajoitettu, ja jokaisella on oikeus saada tieto julkisesta asiakir-

jasta ja tallenteesta. Julkisuusperiaatetta vahvistettiin Suomen valtiosäännössä perusoikeusuudistuksen yhteydessä, kun silloiseen hallitusmuotoon otettiin säännös oikeudesta saada tieto viranomaisen hallussa olevasta asiakirjasta ja muusta tallenteesta (HE 309/1993 vp, s. 58 ja PeVM 25/1994 vp, s. 9). Perustuslain 12 §:n 2 momentista johdettavaa julkisuusperiaatetta ilmentää viranomaisten toiminnan julkisuudesta annetun lain (621/1999, jäljempänä julkisuuslaki) 1 §. Julkisuuslain 1 §:n 1 momentin mukaan viranomaisten asiakirjat ovat julkisia, jollei julkisuuslaissa tai muussa laissa erikseen toisin säädetä. Julkisuuslain esitöiden mukaan säännös vahvistaa julkisuusperiaatetta keskeisenä julkishallinnon periaatteena Suomessa. Pykälän tarkoitus on myös painottaa, että julkisuusperiaate on pääsääntö, josta voidaan poiketa vain lailla.

Naton asiakirjoihin ei lähtökohtaisesti järjestön omien säännösten tai käytäntöjen perusteella sovelleta julkisuusperiaatetta, eikä järjestön osalta ole säädetty yleisestä lähtökohtaisesta tiedonsaantioikeudesta sen asiakirjoihin.

Suomen viranomaisten hallussa oleviin asiakirjoihin sovelletaan julkisuuslakia, jollei laissa toisin säädetä. Julkisuuslain mukaan viranomaisen asiakirjoja ovat viranomaisen toimialalla tehtäviä hoidettaessa laaditut ja viranomaiselle toimitetut asiakirjat, jotka ovat viranomaisen hallussa (5 §). Toisin sanoen sekä viranomaisen itsensä laatimat Nato-yhteistyötä koskevat asiakirjat että viranomaisen hallussa olevat muut asiakirjat, jotka on saatu Nato-yhteistyön puitteissa, ovat julkisuuslaissa tarkoitettuja viranomaisen asiakirjoja. Naton turvallisuusluokiteltuihin asiakirjoihin sovelletaan kansainvälisistä tietoturvallisuusvelvoitteista annetun lain erityissäännöstä ehdottomasta salassapidosta, eikä näihin asiakirjoihin kohdistu julkisuuslain mukaista salassapidon vahinkoedellytyslausekkeiden mukaista arviointia. Naton turvallisuusluokitellut asiakirjat on siten pidettävä salassa, jollei niitä koskevista sopimuksista tai säännöistä muuta johdu.

Viranomaisen laatimat asiakirjat tulevat julkisuuslain mukaisen tiedonsaantioikeuden piiriin, kun asian käsittelyssä on saavutettu julkisuuslain 6 §:ssä säädetty ajankohta. Vastaavasti viranomaiselle toimitettujen asiakirjojen julkisuus alkaa siitä hetkestä, kun ne ovat saapuneet viranomaiselle (7 §). Mainittujen ajankohtien jälkeen tieto on annettava asiakirjasta, jollei salassapitosäännöksistä tai muista tiedon saantia rajoittavista säännöksistä muuta johdu. Tiedon antaminen sisällöltään julkisesta asiakirjasta ennen julkiseksi tulemisen ajankohtaa on viranomaisen harkinnassa (9 §).

Naton turvallisuussäännöstön mukaan Naton julkista tietoa on sellainen Naton tieto, jota ei ole turvallisuusluokiteltu ja jonka asiasta vastuussa oleva Naton toimielin tai virasto saattaa julkiseksi. Naton sisäiseen käyttöön tarkoitettu tieto, jota ei ole turvallisuusluokiteltu, merkitään NATO UNCLASSIFIED (NU). Tällaista tietoa saa luovuttaa turvallisuussäännöstön mukaan vain henkilöille, joilla on tarve tietoon (need-to-know). Asiakirjan ollessa Suomen viranomaisen hallussa, arvioidaan kunkin asiakirjan julkisuutta tapauskohtaisesti julkisuuslain perusteella.

Julkisuuslain lähtökohtana on, että asiakirjan salassapito perustuu laissa säädettyihin salassapitoperusteisiin, ja tieto julkisesta asiakirjasta voidaan luovuttaa ilman, että arvioidaan tiedon pyytäjän tarvetta pyydettyyn tietoon. Tietojensaantioikeutta voidaan perustuslain mukaan rajoittaa vain laissa määriteltyjen, välttämättömäksi katsottujen etujen turvaamiseksi. Julkisuuslain 24 §:ään sisältyvät yleiset säännökset asiakirjojen salassapitovelvoitteista. Nato-yhteistyöhön liittyvien asiakirjojen julkisuuden määräytymisen kannalta keskeisin salassapitosäännös on lain 24 §:n 1 momentin 2 kohta. Lainkohdassa tarkoitetut asiakirjat ovat salassa pidettäviä, jos tiedon antaminen niistä aiheuttaisi vahinkoa tai haittaa Suomen kansainvälisille suhteille tai edellytyksille toimia kansainvälisessä yhteistyössä. Lainkohdan perusteella salassa pidettäviä voivat olla

esimerkiksi kansainvälisen yhteisön tai toimielimen laatimat asiakirjat, jos ne yhteisössä tai toimielimessä ovat salassa pidettäviä (HE 30/1998 vp). Muita kyseeseen tulevia salassapitosäännöksiä voivat olla julkisuuslain 24 §:n 1 momentin 1 ja 7-10 kohdat.

Kansainvälisistä tietoturvallisuusvelvoitteista annettuun lakiin sisältyy kansallisten asiakirjojen tietoturvallisuudesta annetuista säännöksistä poikkeavia säännöksiä. Lain 3 §:n 1 momentissa on kuitenkin yleinen viittaussäännös julkisuuslakiin sekä julkisen hallinnon tiedonhallinnasta annettuun lakiin (906/2019, jäljempänä tiedonhallintalaki). Niiltä osin kuin suomalaisten viranomaisten asiakirjoihin sisältyy kansainvälisten tietoturvallisuusvelvoitteiden piiriin kuuluvia tietoja kansainvälisestä yhteistyöstä, on näihin tietoihin sovellettava kansainvälisistä tietoturvallisuusvelvoitteista annetun lain säännöksiä. Muilta osin sovelletaan julkisuus- ja tiedonhallintalakia ja niiden nojalla annettuja säännöksiä. Kuten edellä on todettu, julkisuuslaissa säädetään muun muassa oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä viranomaisessa toimivan vaitiolovelvollisuudesta ja asiakirjojen salassapidosta. Tiedonhallintalaissa puolestaan säädetään viranomaisten tietoaineistojen tiedonhallinnasta ja tietojärjestelmien käytöstä. Tiedonhallintalain 4 luvussa säädetään yleisistä tietoturvallisuustoimenpiteistä, jotka liittyvät kansainvälisiä tietoturvallisuusvelvoitteita mukaillen erityistä luotettavuutta edellyttävien tehtävien tunnistamiseen ja luotettavuudesta varmistumiseen (12 §), tietoaineistojen ja tietojärjestelmien tietoturvallisuuteen (13 §), tietojen siirtämiseen tietoverkossa (14 §), tietoaineistojen turvallisuuden varmistamiseen (15 §), tietojärjestelmien käyttöoikeuksien hallintaan (16 §), lokitietojen keräämiseen (17 §) ja asiakirjojen turvallisuusluokitteluun valtionhallinnossa (18 §).

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 8 §:n mukaan erityissuojattavaan tietoaineistoon on siitä riippumatta, mitä julkisen hallinnon tiedonhallinnasta annetussa laissa tai sen nojalla säädetään, tehtävä kansainvälisessä tietoturvallisuusvelvoitteessa määritelty luokittelumerkintä sen osoittamiseksi, minkälaisia tietoturvallisuusvaatimuksia sen käsittelyssä on noudatettava. Merkintä voidaan tehdä myös asiakirjaan liitettävälle lomakkeelle, joka sisältää asiakirjan yksilöintitiedot. Tiedonhallintalain 19 §:n mukaan tietoaineiston sähköiseen muotoon muuttamisesta ja säilyttämisestä voidaan poiketa, jos se on välttämätöntä esimerkiksi turvallisuusluokiteltavien asiakirjojen käsittelyä koskevien vaatimusten vuoksi. Kansainvälisten turvallisuusluokiteltujen tietoaineistojen säilytystarpeet määräytyvät pääsääntöisesti kansainvälisen velvoitteen nojalla. Tiedonhallintalain 25 ja 26 §:ssä säädetään asiarekisteristä ja siihen rekisteröitävistä tiedoista. Kansainvälisissä tietoturvallisuusvelvoitteissa määrätään keskusrekisteritoiminnoista ja rekisteröintivaatimuksista asiakirjan seuraamiseksi turvallisuustarkoituksia varten.

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 3 §:n 2 momentin mukaan julkisuuslakiin tai muuhun lakiin perustuvan pyynnön saada tieto erityissuojattavasta tietoaineistosta käsittelee ja ratkaisee se viranomainen, jolle tietoaineisto on toimitettu taikka jonka käsiteltäväksi asia kokonaisuudessaan kuuluu. Mainitun lain 6 §:n 1 momentissa säädetään erityisestä salassapitoperusteesta, jonka mukaan erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu. Lain 7 §:n 2 momentin mukaan viranomaiseen palvelussuhteessa olevan ja viranomaisessa muutoin toimivan samoin kuin viranomaisen toimeksiannosta toimivan ja tämän palveluksessa olevan vaitiolovelvollisuudesta sekä siihen liittyvästä hyväksikäyttökiellosta on voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa säädetään. Lain 8 §:n 1 momentin mukaan erityissuojattavaan tietoaineistoon on siitä riippumatta, mitä julkisen hallinnon tiedonhallinnasta annetussa laissa tai sen nojalla säädetään, tehtävä kansainvälisessä tietoturvallisuusvelvoitteessa määritelty luokittelumerkintä sen osoittamiseksi, minkälaisia tietoturvallisuusvaatimuksia sen käsittelyssä on noudatettava.

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain säännöksiä sovelletaan niin kauan kuin se turvallisuusluokituksen perusteena olevan yleisen edun vuoksi on tarpeen silloinkin, kun sopimus tai säädös, johon säännösten soveltaminen perustuu, ei enää ole voimassa (15 §). Salassapitovelvollisuuden lakkaamisesta on voimassa mitä julkisuuslaissa säädetään. Julkisuuslain 31 §:n 2 momentin mukaan viranomaisen asiakirjan salassapitoaika on 25 vuotta, jollei toisin ole säädetty. Julkisuuslain 31 §:n 3 momentin mukaan asiakirjan salassapito voi jatkua 25 vuoden jälkeenkin, mikäli asiakirja sisältää kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan turvallisuusluokiteltua tietoa ja mikäli tiedon antaminen asiakirjasta aiheuttaisi julkisuuslain 24 §:n 1 momentin 2, 7, 8 tai 10 kohdassa tarkoitetun seurauksen. Tällaiset asiakirjat tulevat julkisuuslain 31 §:n 3 momentin mukaan julkisiksi, kun turvallisuusluokitus on kumottu.

Lisäksi julkisuuslain 30 §:ssä säädetään, että sen lisäksi, mitä laissa erikseen säädetään, viranomainen voi antaa salassa pidettävästä asiakirjasta tiedon ulkomaan viranomaiselle tai kansainväliselle toimielimelle, jos ulkomaan ja Suomen viranomaisen välisestä yhteistyöstä määrätään Suomea sitovassa kansainvälisessä sopimuksessa tai säädetään Suomea velvoittavassa säädöksessä ja tieto asiakirjasta voitaisiin tämän lain mukaan antaa yhteistyötä Suomessa hoitavalle viranomaiselle. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 17 §:n mukaan Suomen viranomaisilla on vastaavalla tavalla oikeus antaa toiselle sopimuspuolelle kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi välttämättömiä asiakirjoja ja tietoja sen estämättä, mitä asiakirjojen ja tietojen salassapidosta Suomen lainsäädännössä säädetään.

2.1.3 Lain soveltaminen elinkeinonharjoittajiin

Kansainvälisistä tietoturvallisuusvelvoitteista annettua 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 siellä 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 1 momentin 3 kohta).

Elinkeinonharjoittajalla ja tämän palveluksessa tai toimeksiannosta toimivalla on erityissuojattavia tietoaineistoja koskeva salassapitovelvollisuus, velvollisuus käyttää tällaista tietoaineistoa vain siihen tarkoitukseen, jota varten se on annettu sekä velvollisuus pitää huolta siitä, että tietoaineistoon on pääsy vain niillä, jotka tarvitsevat tietoa tehtävän hoitamisessa (6 §). Elinkeinonharjoittajalla on myös velvollisuus antaa toimivaltaiselle turvallisuusviranomaiselle tietoja kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi sekä sallia viranomaisen ja kansainvälisen toimielimen tai sopimusvaltion edustajan tutustuminen turvallisuusjärjestelyihinsä ja toimitiloihinsa (16 §:n 2 momentti ja 18 §:n 2 momentti).

2.1.4 Lain täytäntöönpanoviranomaiset

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:ssä on säännökset niistä viranomaisista, jotka huolehtivat kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisesta. Kansallisena turvallisuusviranomaisena (National Security Authority, NSA) kansainvälisten tieto-

turvallisuusvelvoitteiden toteuttamiseen liittyvissä tehtävissä toimii ulkoministeriö. Puolustusministeriö, Pääesikunta, Suojelupoliisi sekä Liikenne- ja viestintävirasto toimivat kansainvälisissä tietoturvallisuusvelvoitteissa tarkoitettuina määrättyinä turvallisuusviranomaisina (Designated Security Authority, DSA).

2.1.5 Tietojen salassapito ja käytön sääntely

Erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu (6 §:n 1 momentti). Salassapitovelvollisuus koskee myös elinkeinonharjoittajaa tämän ollessa osapuolena turvallisuusluokitellussa sopimuksessa. Suomen tekemissä sopimuksissa, jotka koskevat eri valtioiden viranomaisten välistä salassa pidettävien tietojen vaihtoa ja suojaamista, on säännönmukaisesti määräys, joka rajoittaa luovutettujen tietojen käyttöä. Kyseisen määräyksen 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.

2.1.6 Turvallisuusluokittelu ja suojaamistoimenpiteet

Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään velvollisuudesta merkitä erityissuojattavaan tietoaineistoon sen turvallisuusluokka. Erityissuojattavaan tietoaineistoon on tehtävä luokittelumerkintä, joka osoittaa, minkälaisia tietoturvallisuusvaatimuksia sen käsittelyssä on noudatettava (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 eri turvallisuusluokkia vastaavista turvallisuustoimenpiteistä valtioneuvoston asetuksella (9 §). Asiakirjojen turvallisuusluokittelusta valtionhallinnossa annetun valtioneuvoston asetuksen (1101/2019, jäljempänä turvallisuusluokitteluasetus) 4 §:ssä säädetään turvallisuusluokituksen vastaavuudesta kansainvälisiä tietoturvallisuusvelvoitteita toteutettaessa. Säännöstä sovelletaan, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu.

Erityissuojattava tietoaineisto on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 10 §:n mukaan säilytettävä tiloissa, joissa asiakirjojen ja materiaalien sekä niihin sisältyvien tietojen suojaamisesta voidaan huolehtia kansainvälisessä tietoturvallisuusvelvoitteessa edellytetyllä tavalla. Tilojen turvallisuusvaatimuksista säädetään turvallisuusluokitteluasetuksen 9 ja 10 §:ssä.

Lakiin kansainvälisistä tietoturvallisuusvelvoitteista on kirjattu kansainvälisissä sopimuksissa oleva yleinen vaatimus siitä, että erityissuojattavaan tietoaineistoon annetaan pääsy vain niille, jotka tarvitsevat tietoja tehtäviensä hoitamisessa. Nämä henkilöt on nimettävä etukäteen, jos kansainvälisessä tietoturvallisuusvelvoitteessa tätä edellytetään (lain 6 §:n 3 momentti). Sama koskee myös 1 §:n 2 momentissa tarkoitettua elinkeinonharjoittajaa.

2.1.7 Tietojärjestelmäturvallisuus

Liikenne- ja viestintävirasto toimii kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaan kansallisen turvallisuusviranomaisen asiantuntijana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa ja vastaa muun muassa kansainvälisten tietoturvallisuusvelvoitteiden edellyttämistä tietojärjestelmien arvioinnista ja hyväksyntätehtävistä (akkreditointi). Viranomaisten tietojärjestelmien tietoturvallisuuden arviointia koskevasta menettelystä ja Liikenne- ja viestintäviraston tietoturvallisuuden arviointitehtävästä säädetään

viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetussa laissa (1406/2011, jäljempänä arviointilaki). Viranomaiset voivat käyttää tietojärjestelmäarvioinneissa myös laissa tietoturvallisuuden arviointilaitoksista (1405/2011) tarkoitettuja Liikenne- ja viestintäviraston hyväksymiä arviointilaitoksia. Toistaiseksi arviointilaitoksia ei ole hyväksytty tekemään EU:n tai Naton turvallisuusluokiteltuja tietoja käsittelevien tietojärjestelmien arviointeja. Yritysten tietojärjestelmien arvioinnista osana yritysturvallisuusselvitystä säädetään turvallisuusselvityslaissa.

2.2 Turvallisuusselvityslaki

2.2.1 Lain tarkoitus ja soveltamisala

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

Laissa säädetään henkilö- ja yritysturvallisuusselvityksen laadinnassa noudatettavasta menettelystä. Laki sisältää säännökset turvallisuusselvityksen laatimisen edellytyksistä sekä sitä laadittaessa käytettävistä tiedoista, selvityksen kohteen suostumuksesta ja tiedonsaantioikeuksista, selvityksen hakijan ja selvityksen kohteen tiedonantovelvollisuuksista sekä turvallisuusselvityksen ja sen perusteella annetun todistuksen voimassaolosta ja todistuksen peruuttamisesta sekä henkilörekisterien yhdistämisestä selvityksen kohteen nuhteettomuuden ja luotettavuuden seuraamiseksi ja sen johdosta suoritettavista toimenpiteistä (2 §). Turvallisuusselvitys voidaan tehdä vain selvityksen kohteen etukäteen antaman kirjallisen suostumuksen perusteella (5 §).

2.2.2 Henkilöstöturvallisuus

Henkilöturvallisuusselvityksellä tarkoitetaan turvallisuusselvityslain 3 §:n 1 momentin 1 kohdan mukaisesti henkilön nuhteettomuuden tai luotettavuuden varmistamiseksi turvallisuusselvityslaissa säädetyllä tavalla laadittavaa selvitystä henkilön taustasta. Lain 23 §:n mukaan henkilöturvallisuusselvitys tehdään tarkistamalla henkilöä koskevat rekisteritiedot lain 4 luvussa säädetyllä tavalla sekä tarvittaessa selvityksen kohdetta haastattelemalla hänen yleisistä olosuhteistaan, ulkomailla oleskelustaan ja hänen suhteistaan muiden maiden kansalaisiin sekä muista sellaisista seikoista, joilla on erityistä merkitystä arvioitaessa hänen luotettavuuttaan selvityksen perustana olevan tehtävän kannalta.

Lain 14 §:n mukaan henkilöturvallisuusselvitys voidaan laatia suppeana, perusmuotoisena tai laajana. Turvallisuusselvitys tehdään laissa määritellyissä tapauksissa, kuten silloin, kun Suomea sitova valtiosopimus tai muu kansainvälinen velvoite edellyttää turvallisuusselvityksen tekemistä tai sen perusteella laaditun todistuksen esittämistä.

Jokaisella on oikeus saada tieto siitä, onko hänestä tehty turvallisuusselvitys tiettyä tehtävää varten. Selvityksen kohteella on myös oikeus pyynnöstä saada toimivaltaiselta viranomaiselta turvallisuusselvityksen tiedot. Tiedonsaantioikeus ei kuitenkaan koske sellaisesta rekisteristä peräisin olevaa tietoa, johon rekisteröidyllä ei ole tarkastusoikeutta (6 §).

Turvallisuusselvitysmenettelyssä käytetyt rekisterit on laissa lueteltu tyhjentävästi. Turvallisuusselvityksessä voidaan käyttää myös tiettyjä ulkomaan viranomaisen rekistereihin talletettuja tietoja (25 §).

Turvallisuusselvityslain 43 §:n 2 momentin mukaan kansallinen turvallisuusviranomainen antaa kansainvälisen tietoturvallisuusvelvoitteiden toteuttamiseksi tarpeellisen henkilöturvallisuusselvitystodistuksen siten kuin kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään. Henkilöturvallisuusselvityksen laatii suojelupoliisi, taikka pääesikunta, jos selvityksen kohde toimii tai hänen on tarkoitus toimia puolustusvoimissa tai hoitaa puolustusvoimien antamaa tehtävää taikka jos turvallisuusselvitys liittyy puolustusvoimien toimintaan tai hankintoihin.

2.2.3 Yritysturvallisuus

Yritysturvallisuusselvityksellä tarkoitetaan turvallisuusselvityslain 3 §:n 1 momentin 2 kohdan mukaisesti yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumustenhoitokyvyn arvioimiseksi turvallisuusselvityslaissa säädetyllä tavalla laadittavaa selvitystä yrityksestä. Selvitys voidaan laatia, jos selvitystä edellytetään kansainvälisen järjestön tai toimielimen säännöissä tai toisen valtion laissa ja jos se on tarpeen sen vuoksi, että selvityksen kohde voi tulla valituksi kansainvälisen järjestön tai toimielimen järjestämään tai näiden muutoin organisoimaan hankkeeseen taikka toisessa valtiossa järjestettävään hankintakilpailuun tai aloittaa yritystoiminnan toisessa valtiossa (36 § 2 momentti). Yritysturvallisuusselvitys voidaan laatia selvityksen kohteen pyynnöstä 36 §:n 2 momentissa tarkoitetuissa tapauksissa.

Selvityksen laatii turvallisuusselvityslain 9 §:n mukaan Suojelupoliisi. Pääesikunta huolehtii yritysturvallisuusselvityksen laatimisesta kuitenkin silloin, kun kysymys on yrityksestä, joka hoitaa tai jonka on tarkoitus hoitaa puolustusvoimien antamaa tehtävää, taikka yrityksestä, joka liittyy puolustusvoimien hankintoihin. Liikenne- ja viestintäviraston tehtävänä on huolehtia yrityksen tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista.

Yritysturvallisuusselvitystä laadittaessa selvitetään hakemuksessa esitettyjen tietojen ja 37 §:ssä tarkoitettujen tietolähteiden sekä yrityksen toimitilojen ja tietojärjestelmien tarkastuksen avulla, miten yritys huolehtii tietojen suojaamisesta, asiattoman pääsyn estämisestä tiloihin ja henkilöstön koulutuksesta (38 §:n 1 momentti). Lain 38 §:n mukaan yritysturvallisuusselvitys voidaan tehdä myös osittaisena, jos se on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai muutoin perusteltua.

Toimivaltainen viranomainen voi turvallisuusselvityslain 40 §:n mukaan yritysturvallisuusselvitystä ja sen perusteella annettavaa todistusta laatiessaan edellyttää yritykseltä sitoumusta, jonka mukaan elinkeinonharjoittaja sitoutuu huolehtimaan tietoturvallisuustason säilyttämisestä sekä ilmoittamaan muutoksista, joilla on siihen vaikutuksia sekä antamaan tietoturvallisuustason säilyttämisen valvomiseksi viranomaiselle luvan päästä yrityksen tiloihin sekä antamaan seurannassa tarvittavia tietoja.

Lain 46 §:n 2 momentin mukaan kansallinen turvallisuusviranomainen antaa kansainvälisen tietoturvallisuusvelvoitteiden toteuttamiseksi tarpeellisen yritysturvallisuusselvitystodistuksen siten kuin kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään.

2.3 Henkilötietojen käsittelyä koskeva lainsäädäntö

Käsitellessään hallituksen esitystä Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamisesta tehdyn hallinnollisen järjestelyn hyväksymisestä sekä laiksi järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta (HE 139/2012 vp) eduskunnan puo-

lustusvaliokunta kiinnitti huomiota julkisuuden ja salassapitokysymysten ohella esityksen henkilötietojen suojaa koskeviin vaatimuksiin. Valiokunta totesi tuolloin saamansa selvityksen perusteella, että Suomen ja Naton väliseen hallinnolliseen järjestelyyn sisältyvät määräykset loivat riittävästi edellytyksiä henkilötietojen suojaa koskevien vaatimusten huomioimiselle julkisuus- ja salassapitonäkökohtien ohella. Valiokunta korosti, että hallinnollisen järjestelyn artikloja tulkittaessa ja sovellettaessa tulee huomioida perustuslain 12 §:ssä turvattu julkisuus ja 10 §:ssä suojattu henkilötietojen suoja siltä osin kuin turvallisuusluokiteltuihin tietoihin sisältyy henkilötietoja (PuVM 5/2012 vp).

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 17 §:n mukaan Suomen viranomaisilla on oikeus antaa toiselle sopimuspuolelle kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi välttämättömiä asiakirjoja ja tietoja sen estämättä, mitä asiakirjojen ja tietojen salassapidosta Suomen lainsäädännössä säädetään. Sanottu ei koske yksityisyyden suojan vuoksi salassa pidettäviksi säädettyjä tietoja. Turvallisuusselvityslain 26 §:ssä säädetään mahdollisuudesta hankkia kansainvälisen sopimuksen nojalla tietoja ulkomaan viranomaisen ylläpitämistä rekistereistä, 57 §:ssä viranomaisten tiedonsaantioikeudesta ja 59 §:ssä tietojen salassapitovelvollisuudesta.

Henkilötietojen käsittelyn yhteydessä on merkitystä sillä, että suurin osa Naton jäsenistä on myös yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä tehdyn Euroopan neuvoston yleissopimuksen (tietosuojayleissopimus, SopS 35 ja 36/1992) osapuolia. Yleissopimusta on muutettu pöytäkirjalla nro 223, joka ei kuitenkaan ole vielä voimassa.

Kansalliseen turvallisuuteen liittyvä henkilötietojen käsittely jää nimenomaisten EU:n yleisen tietosuoja-asetuksen (EU) 2016/679 ja rikosasioiden tietosuojadirektiivin (EU) 2016/680 säännösten perusteella niiden soveltamisalan ulkopuolelle. Sopimuksessa tarkoitettuja turvallisuusluokiteltuja tietoja käsitteleviä viranomaisia voivat olla esimerkiksi ministeriöt. Näiden viranomaisten suorittamaan henkilötietojen käsittelyyn sovelletaan tietosuojalain (1050/2018) 2 §:n 1 momentin mukaisesti EU:n yleistä tietosuoja-asetusta ja kansallista tietosuojalakia. Jos tietosuoja-asetuksen soveltamisalalla toimivat viranomaiset luovuttavat henkilötietoja Natolle tai tietoturvallisuussopimuksen osapuolille, jotka eivät ole EU:n jäsenvaltioita, henkilötietojen siirtoihin sovelletaan tietosuoja-asetuksen V lukua.

Suomessa rikosasioiden tietosuojadirektiivi on pantu täytäntöön lailla henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018, jäljempänä rikosasioiden tietosuojalaki). Rikosasioiden tietosuojadirektiivin soveltamisalarajoituksesta huolimatta rikosasioiden tietosuojalain soveltamisalaa on ulotettu koskemaan henkilötietojen käsittelyä kansallisen turvallisuuden ja puolustuksen yhteydessä. Näin ollen Naton asiakirjojen sisältämien henkilötietojen käsittelyyn sovelletaan lähtökohtaisesti rikosasioiden tietosuojalakia silloin kun käsittely kuuluu lain 1 §:n 2 momentin soveltamisalaan. Rikosasioiden tietosuojalain 1 §:n 2 momentin mukaan sen lisäksi, mitä 1 momentissa säädetään, lakia sovelletaan

1) Puolustusvoimien suorittamaan ja Puolustusvoimien lukuun suoritettavaan henkilötietojen käsittelyyn, kun tietoja käsitellään puolustusvoimista annetun lain (551/2007) 2 §:n 1 momentin 1 kohdassa, 2 kohdan a alakohdassa tai 3 ja 4 kohdassa säädettyjen tehtävien hoitamiseksi, sekä Puolustusvoimien pääesikunnan suorittamaan henkilötietojen käsittelyyn turvallisuusselvityslain 9 §:n 3 momentissa tarkoitettujen tehtävien hoitamiseksi;

2) poliisin suorittamaan henkilötietojen käsittelyyn, kun tietoja käsitellään sellaisessa poliisilain (872/2011) 1 luvun 1 §:n 1 momentissa tarkoitetussa tehtävässä, joka liittyy kansallisen turvallisuuden suojaamiseen, sekä turvallisuusselvityslain 9 §:n 1 momentissa tarkoitetuissa tehtävissä;

3) Rajavartiolaitoksen suorittamaan henkilötietojen käsittelyyn, kun tietoja käsitellään sellaisessa rajavartiolain (578/2005) 3 §:n 2 ja 3 momentissa tarkoitetussa tehtävässä, joka liittyy kansallisen turvallisuuden suojaamiseen.

Rikosasioiden tietosuojalain 7 luvussa säädetään toimivaltaisen viranomaisen suorittamasta henkilötietojen siirrosta kolmansiin maihin ja kansainvälisille järjestöille. Henkilötietojen käsittelystä Puolustusvoimissa annetun lain (332/2019) 2 §:n 1 momentissa on rajattu Puolustusvoimien suorittama tiedonvaihto rikosasioiden tietosuojalain 7 luvun soveltamisen ulkopuolelle. Puolustusvoimien suorittamasta henkilötietojen luovuttamisesta ulkomaille ja kansainvälisille järjestöille säädetään henkilötietojen käsittelystä Puolustusvoimissa annetun lain 4 luvussa.

Lisäksi Naton asiakirjojen sisältämien henkilötietojen käsittelyyn voidaan soveltaa rikosasioiden tietosuojalakia täydentäviä säädöksiä, kuten henkilötietojen käsittelystä poliisitoimessa annettua lakia (616/2019) ja henkilötietojen käsittelystä Puolustusvoimissa annettua lakia.

Kansainvälisesti erityissuojattavien tietoaineistojen siirtämiseen viestintäverkoissa voi liittyä tiettyjä erityiskysymyksiä esimerkiksi tietosuojan osalta. Henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla säädetään yleisen tietosuoja-asetuksen ohella Euroopan unionin sähköisen viestinnän tietosuojadirektiivissä (ns. ePrivacy-direktiivi 2002/58/EY). Direktiivi on pantu täytäntöön suurelta osin sähköisen viestinnän palveluista annetulla lailla (917/2014). Sääntelyä sovelletaan muun muassa välitystietoihin. Välitystietojen osalta on otettava muutoinkin huomioon sähköisen viestinnän palveluista annetussa laissa säädetty sekä perustuslain 10 §:ssä turvattu luottamuksellisen viestin salaisuus, josta poikkeaminen edellyttää lailla säätämistä.

2.4 Eduskunnan tiedonsaantioikeus

Eduskunnan tietojensaanti- ja osallistumisoikeus Nato-asioissa turvataan perustuslain ja muun lainsäädännön nojalla. Valtiosäännön perusta on perustuslaissa säädetty kansanvallan periaate (2 § 1 momentti), jonka mukaan eduskunta on ylin valtioelin myös kansainvälisissä asioissa. Eduskunnan asema ylimpänä valtioelimenä saa tässä suhteessa konkreettista sisältöä menettelystä presidentin ja valtioneuvoston välisen näkemyseron ratkaisemisessa (58 § 2 momentti). Eduskunnan vaikutusmahdollisuudet tulee turvata myös ennakoivalla tavalla.

Valtioneuvosto on kokonaisvastuussa eduskunnan tiedonsaannista sekä osallistumismahdollisuuksien turvaamisesta. Parlamentaarisen hallitustavan periaatteen ja perustuslain 58 §:n ja 93 §:n säännösten perusteella valtioneuvosto on myös kokonaisvastuussa asioiden valmistelusta.

Eduskunnalla on perustuslain 47 §:n mukaan oikeus saada valtioneuvostolta asioiden käsittelyssä tarvitsemansa tiedot. Säännös sisältää yhtäältä valtioneuvoston velvollisuuden oma-aloitteisesti toimittaa eduskunnan tarvitsemat tiedot ja toisaalta velvollisuuden toimittaa eduskunnan pyytämät tiedot (HE 1/1998 vp, s. 97). Asianomaisen ministerin tulee huolehtia siitä, että valiokunta tai muu eduskunnan toimielin saa viipymättä tarvitsemansa viranomaisen hallussa olevat asiakirjat ja muut tiedot. Ulkoasiainvaliokunnalle annetaan selvityksiä ulko- ja turvallisuuspolitiikkaa koskevista asioista perustuslain 97 §:n nojalla. Ulkoasiainvaliokunta voi saamiensa

selvitysten perusteella tarvittaessa antaa oma-aloitteisen lausunnon valtioneuvostolle. Perustuslakivaliokunnan mukaan selvityksenantovelvollisuus myös presidentin ulkopoliittisesta toiminnasta on eduskunnan luottamuksen varassa toimivalla valtioneuvostolla (PeVM 9/2010 vp). Eduskunta on korostanut, että valtioneuvoston tulee oma-aloitteisesti pitää ulkoasiainvaliokunta informoituna oikea-aikaisesti ja säännönmukaisesti kansainvälisistä asioista. Eduskunnan rooli mahdollisena ristiriidan ratkaisijana edellyttää laaja-alaista tiedottamista myös asioiden valmistelu- ja keskusteluvaiheesta (PeVM 9/2010 vp ja UaVL 5/2010 vp).

Perustuslakivaliokunnan tulkinnan mukaan valiokunnan tietojensaantioikeuteen ei vaikuta se, että valiokunnan tarvitsemat tiedot olisivat esimerkiksi oikeudelliselta luonteeltaan salassa pidettäviä (PeVL 30/2020 vp s. 3). Myös eduskunnan ulkoasiainvaliokunta on korostanut, että eduskunnan tiedonsaantioikeus ulottuu myös salassa pidettäviin asiakirjoihin (UaVL 4/2020 vp s. 2). Eduskunnan tarkastusvaliokunta on todennut, että perusteet, joilla ministeriö voisi olla antamatta joitain tietoja eduskunnalle, voivat olla hyvin vähälukuisia ja etupäässä liittyä sellaisiin seikkoihin kuin tiedon ilmeisen selvä epäolennaisuus ja epäluotettavuus, spekulatiivisuus ja vanhentuneisuus. Joissain tilanteissa kansainväliseen yhteistyöhön liittyviin asiakirjoihin voi sisältyä sellaisia tietoja, joiden paljastuminen voi aiheuttaa merkittävää ja laajalle ulottuvaa vahinkoa keskeisille yleisille eduille, kuten Suomen suhteille ulkovaltoihin. Tällaisten aineistojen asianmukaisesta käsittelystä on pidettävä erityistä huolta, koska kysymys on Suomen luotettavuudesta kansainvälisen yhteistyön osapuolena. Tällaistenkin tietojen suhteen on ensisijainen menettelytapa perustuslain kannalta se, että valiokunnan jäseniltä edellytetään vaiteliaisuutta sen sijaan, ettei tietoa lainkaan anneta eduskunnalle. Perustuslaki ei tunne mahdollisuutta, että esim. turvallisuusluokiteltu tieto jätettäisiin antamatta eduskunnalle. (TrVM 2/2013 vp s. 3)

Sääntelyä valiokunnan jäsenten vaitiolovelvollisuudesta on perustuslain 50 §:n 2 ja 3 momentissa sekä eduskunnan työjärjestyksen 43 a–43 c §:ssä (PeVL 30/2020 vp, s. 3). Työjärjestyksen 43 c §:n 1 momentin mukaan valiokunnan jäsen tai virkamies ei saa paljastaa asiakirjan salassa pidettävää sisältöä tai tietoa, joka asiakirjaan merkittynä olisi salassa pidettävä, taikka sellaista seikkaa, josta valiokunta on tehnyt perustuslain 50 §:n 3 momentin mukaisen vaitiolopäätöksen. Vaiteliaisuus merkitsee siis myös sitä, että vaiteliaisuuden alaista asiaa käsittelevän valiokunnan jäsen ei voi vapaasti keskustella asiasta esimerkiksi ryhmäkokouksessa (PeVL 30/2020 vp, s. 18). Perustuslakivaliokunta on korostanut, että vaiteliaisuuden ala tulee rajata laajuudeltaan ja kestoltaan vain välttämättömään (PeVL 16/2020 vp s. 5–6). Valiokunnan jäsen tai virkamies ei saa myöskään käyttää salassa pidettäviä tietoja omaksi taikka toisen hyödyksi tai toisen vahingoksi. Rangaistus salassapitorikoksesta ja salassapitorikkomuksesta säädetään rikoslain 38 luvun 1 ja 2 §:ssä.

Naton turvallisuusluokitellun tiedon käsittelyä koskevat säännökset on otettava huomioon myös tietojen käsittelyssä eduskunnassa. Tämä tarkoittaa esimerkiksi Naton turvallisuussääntöjen mukaisia toimintamalleja (sisältäen tila-, henkilö- ja tiedonhallintaratkaisut sekä niihin liittyvät tekniset ratkaisut) ja henkilöturvallisuusselvitystodistusten myöntämistä soveltuvin osin. Valtioneuvoston oikeuskansleri on ottanut muistiossaan OKV/3212/24/2021 kantaa erityissuojattavia tietoaineistoja koskevaan eduskunnan tiedonsaantioikeuteen hävittäjien hankintaa koskevassa asiassa. Muistiossa todetaan, että kansainvälisissä tietoturvallisuusvelvoitteissa on usein keskeistä luovutettujen tietojen tiukka käyttötarkoitussidonnaisuus, jonka mukaan tiedot ovat käytettävissä vain tiettyyn nimenomaiseen tarkoitukseen. Tietojen käyttö muuhun tarkoitukseen edellyttää tiedot antaneen tahon suostumusta. Lisäksi sopimuksissa on sovittu erityissuojattavan aineiston suojaamista koskevista erityisistä menettelyistä ja suojatoimista. Nykyisessä kansainvälisessä yhteistyössä tietoturvallisuutta koskevien velvoitteiden noudattamiseen kiinnitetään paljon huomiota ja tietoturvallisuusvelvoitteiden asianmukainen kunnioittaminen on keskeinen osa valtion mahdollisuuksia toimia kansainvälisessä yhteistyössä ja saada tietoja muilta valtioilta.

Eduskunnan asemasta ylimpänä valtioelimenä sekä lainsäädäntövaltaa ja valtiontaloudellista valtaa käyttävänä valtioelimenä seuraa, että eduskunnan on saatava luotettavat ja kattavat tiedot päätöksentekonsa perustaksi. Tämä on perustuslaissa säädettyjen kansanvaltaisen hallitusmuodon perusteiden toteuttamisen välttämätön edellytys. Parlamentaarisen järjestelmän toimintaan kuuluu välttämättömänä elementtinä tiedonkulku eduskunnan ja hallituksen välillä. Eduskunnan laaja tiedonsaantioikeus turvaa myös valtioneuvoston parlamentaarista valvontaa (PeVL 30/2020 vp s. 2–3).

3 Kansainvälinen kehitys sekä ulkomaiden ja EU:n lainsäädäntö

Turvallisuusluokiteltujen tietojen käsittelyä koskevissa kansainvälisissä sopimuksissa ja järjestelyissä on luotu pitkälti vakiintuneet menettelyt ja säännöt kansainvälisen luokitellun tiedon käsittelyssä. Suomella on tällä hetkellä tietoturvallisuussopimus 20 valtion kanssa sekä Pohjoismaiden, Euroopan unionin jäsenvaltioiden, Euroopan avaruusjärjestön, Euroopan puolustusmateriaalijärjestö OCCARin sekä Pohjois-Atlantin liiton kanssa. Suomi osallistuu myös Naton jäsenmaiden vuonna 1985 perustamaan monenväliseen epävirallliseen yritysturvallisuustyöryhmään (Multinational industrial security working group, *MISWG*), jossa valmistellaan yhteisiä menettelyitä ja sääntöjä turvallisuusluokiteltujen tietojen vaihdon käsittelyssä.

Euroopan unionissa avoimuus ja tiedonsaantioikeus on yksi keskeisistä periaatteista, kun taas Naton asiakirjoihin ei järjestön omien säännösten tai käytäntöjen perusteella sovelleta lähtökohtaisesti julkisuusperiaatetta. Turvallisuusluokiteltujen tietojen käsittelyssä Euroopan unionissa on omaksuttu Naton järjestelmää läheisesti muistuttavat menettelyt ja säännöt. Neuvoston osalta ne sisältyvät neuvoston päätökseen EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä (2013/488/EU). Päätöksen lisäys sisältää jäsenmaiden turvallisuusluokkien vastaavuudet. Neuvostossa kokoontuneet Euroopan unionin jäsenvaltiot tekivät vuonna 2015 sopimuksen Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta (SopS 76 ja 77/2015). Komissio antoi 22.3.2022 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi tietoturvallisuudesta unionin toimielimissä, elimissä ja laitoksissa (COM(2022) 119 final), jonka käsittely neuvostossa ja Euroopan parlamentissa on kesken. Euroopan unioni on tehnyt vuonna 2003 Naton kanssa tietoturvallisuutta koskevan sopimuksen (2003/211/YUTP, EUVL L 80, 27.3.2003, s. 36).

Euroopan unionin jäsenvaltiot ovat osapuolina edellä mainitussa neuvostossa kokoontuneiden Euroopan unionin jäsenvaltioiden välisessä sopimuksessa Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta. Kaikki nykyiset Naton jäsenvaltiot ovat osapuolina nyt hyväksyttävänä olevassa Naton tietoturvallisuussopimuksessa. Pohjoismaat ovat tehneet lisäksi sopimuksen Tanskan, Suomen, Islannin, Norjan ja Ruotsin välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja vaihtamisesta (SopS 10-12/2013). Näin ollen Suomen viiteryhmän maiden kansainväliset velvoitteet ovat yhteneväiset.

Kansallisten turvallisuusviranomaisten järjestäytyminen vaihtelee historiallisista syistä maittain. Esimerkiksi Ruotsissa kansallinen turvallisuusviranomainen (NSA) sijaitsee Suomen tavoin ulkoministeriössä, Tanskassa NSA sijaitsee tiedustelupalvelussa ja Norjassa kansallinen turvallisuusviranomainen (NSM) on poikkisektoraalinen ammatti- ja valvontaviranomainen, joka on järjestetty puolustusministeriön alaisuuteen, mutta raportoi siviilisektorin osalta oikeusministeriölle. Alankomaissa on kaksi kansallista turvallisuusviranomaista, AIVD ja MIVD. AIVD on osa sisäministeriötä. Sillä on yleisenä tiedustelu- ja turvallisuuspalveluna koordinoiva rooli, mutta molemmat on epävirallisesti nimetty kansalliseksi turvallisuusviranomaiseksi (NSA).

4 Sopimuksen tavoitteet

Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta tehdyn sopimuksen johdannon mukaan tehokas poliittinen neuvottelu, yhteistyö ja suunnittelu puolustusasioissa sopimuksen tavoitteiden saavuttamiseksi edellyttävät turvallisuusluokitellun tiedon vaihtamista osapuolten välillä. Sen mahdollistaminen edellyttää määräyksiä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja turvaamisesta. Sopimuksen tarkoituksena on luoda turvallisuusvaatimuksille ja menettelyille yleiset puitteet.

5 Keskeiset ehdotukset

Esityksessä ehdotetaan, että eduskunta hyväksyisi Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta tehdyn sopimuksen ja turvallisuussäännöt. Esitys sisältää myös ehdotuksen niin sanotuksi blankettilaiksi, jolla saatetaan voimaan sopimuksen ja turvallisuussääntöjen lainsäädännön alaan kuuluvat määräykset. Lisäksi ehdotetaan, että eduskunta antaisi suostumuksensa siihen, että Suomi irtisanoo Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen. Esitys sisältää ehdotuksen laiksi, jolla kumotaan kyseisten sopimusten lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annettu laki (945/2012).

6 Esityksen vaikutukset

6.1 Taloudelliset vaikutukset

Natoon liittymisestä johtuvia vaikutuksia on selvitetty hallituksen esityksessä HE 315/2022 vp. Natoon liittyminen aiheuttaa kertaluonteisia lisäkustannuksia ja pysyviä kiinteitä kustannuksia mm. tietoturvallisuusratkaisuihin ja toimitilaturvallisuuteen sekä järjestelmien tarkastus- ja hyväksyntätyöhön liittyen. Natoon liittyvän tiedon käsittelyn mahdollistavan ja korkeaa turvallisuutta edellyttävän tietojenkäsittely-ympäristön jatkokehittämiskustannusten arvioidaan tällä hetkellä olevan noin 20 miljoonaa euroa vuosina 2023-2025. Kulut koostuvat henkilöstö-, laite- ja ohjelmistomenoista. Korkeaa turvallisuutta edellyttävän tietojenkäsittelyratkaisun jatkokehittämiselle on varattu rahoitus vuosien 2022 ja 2023 talousarvioissa. Lisäksi tietojenkäsittelytiloihin vaadittavat suojaukset tulevat aiheuttamaan uusia kustannuksia arviolta noin kuusi miljoonaa euroa kohdistuen pääsääntöisesti vuokrauskustannuksiin. Tehtävät investoinnit tulevat aiheuttamaan noin kolmen miljoonan euron ylläpitokustannukset vuodesta 2026 lähtien.

Investointi- ja ylläpitorahoituksen lopullinen tarve tarkentuu suunnittelun ja toteutuksen edetessä. Välillisesti Nato-jäsenyydestä aiheutuvat tiloihin kohdistuvat kustannukset tarkentuvat vuoden 2023 aikana tehtävässä kartoituksessa. Muut mahdolliset lisäkustannukset, ml. tiedonvälitykseen ja toimitilaturvallisuuteen liittyen, selkiytyvät usean vuoden kuluessa. Nato-jäsenyyden myötä voi korkeaa turvallisuutta edellyttävän tiedonkäsittelyn määrän lisääntymisellä olla vaikutuksia Nato-tiedonkäsittelyn kustannuksiin. Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta tehty sopimus ei kuitenkaan suoranaisesti lisää valtion yhteisen korkeaa turvallisuutta edellyttävän tietojenkäsittely ympäristön kustannuksia, koska vastaavat vaatimukset ovat olleet voimassa jo kumppanuusaikana.

Nato-jäsenyyden myötä lisääntyvästä Puolustusvoimien ja Naton välisestä suorasta tietojenkäsittelystä aiheutuvat lisäkustannukset sisältyvät Puolustusvoimien talousarvio- ja kehysesitykseen. Puolustusvoimien lisäkustannukset johtuvat välillisesti tietoturvallisuusvelvoitteiden toteuttamisesta, mutta suoranaisesti pääosin itse Nato-jäsenyydestä.

Taloudellisia vaikutuksia eri hallinnonalaoille aiheutuu muun muassa tietojärjestelmien muutoksista, mahdollisten uusien tietojärjestelmien käyttöönotosta ja toimitilaratkaisuista ja tietojärjestelmistä sekä niiden auditoinneista sekä koulutuksesta. Myös järjestelmien suunnittelun tuesta ja sujuvan akkreditointiprosessin etenemisestä sekä järjestelmien tarkastuksesta ja hyväksynnästä (akkreditointi) aiheutuu kansallisena akkreditointiviranomaisena toimivalle Liikenne- ja viestintävirastolle lisäresurssitarpeita. Kaikkia kustannusvaikutuksia eri hallinnonaloilla ei ole mahdollista arvioida yksityiskohtaisesti tässä vaiheessa. Jäsenyydestä aiheutuvat eri hallinnonalojen lisämäärärahatarpeet tullaan esittämään vuosittaisen julkisen talouden suunnitelman sekä talous- ja lisätalousarvioiden valmistelun yhteydessä niiden käyttötarkoituksen mukaisilta momenteilta.

6.2 Vaikutukset viranomaistoimintaan

Nato-jäsenyyden myötä keskeisimmät vaikutukset kansalliseen tietoturvallisuuteen syntyvät eri toimintojen järjestämisestä Naton tietoturvallisuusvaatimusten edellyttämälle tasolle. Suomi on tehnyt Naton kanssa turvallisuusluokitellun tiedon suojaamista koskevan sopimuksen ja sitä täydentävän hallinnollisen järjestelyn, minkä johdosta Suomi suojaa ja käsittelee Naton turvallisuusluokiteltua tietoa jo tällä hetkellä Naton turvallisuussääntöjen vähimmäisvaatimusten ja perusperiaatteiden mukaisesti. Vaatimukset koskevat henkilöstöturvallisuutta, tietoaineistoturvallisuutta, toimitilaturvallisuutta, viestintä- ja tietojärjestelmien turvallisuutta sekä yritysturvallisuutta. Naton tietoturvallisuussopimukseen sitoutuminen ei muuta nykytilannetta merkittävästi. Rauhankumppanuuden ja jäsenyyden aikana sovellettavien tietoturvallisuusvaatimusten vähäisiä eroja selostetaan jaksossa 8.2. Rauhankumppanuuden aikana vakiintuneet tietoturvallisuusprosessit muodostavat toimivan perustan myös niitä koskevalle kehitystyölle jäsenyyden alkaessa. Jäsenyyden myötä Naton turvallisuusluokiteltujen tietojen määrät kasvavat ja käsittelytarve laajenee eri viranomaisiin ja ministeriöihin sekä yrityksiin. Asiakirjojen määrän kasvua ja lisäystä eri hallinnonaloilla on kuitenkin vaikea arvioida ennen jäsenyyden alkua. Jäsenyyden myötä Suomi voi saada myös Naton korkeimman turvaluokan (COSMIC TOP SECRET) asiakirjoja, joita ei pääsääntöisesti luovuteta jäsenvaltioiden ulkopuolisille tahoille. Asiakirjojen määrän kasvu, asiakirjojen vastaanottajien piirin laajentuminen ja päätöksenteon nopeudelle asetettavat vaatimukset on otettava huomioon kehitystyössä.

Naton turvallisuustoimisto teki Suomeen 3.-6.5.2022 tarkastusvierailun, jossa arvioitiin Naton turvallisuusluokitellun tiedon suojaamista. Tarkastuksen johtopäätösten mukaan viranomaisten tulee arvioida ja tarvittavilta osin lisätä Naton luokitellun tiedon suojaamista koskevia resursseja. Tämä koskee nimenomaisesti kansallista turvallisuusviranomaista ja henkilöturvallisuusselvityksiä, kirjaamohenkilökuntaa, tietojärjestelmien ja sähköisten käsittely-ympäristöjen hyväksymisprosessia, toimitilaturvallisuutta ja yritysturvallisuutta. Pääesikunnassa on tunnistettu tarve vahvistaa asiantuntijaresursseja edellä mainituilla osa-alueilla. Puolustusvoimissa kasvaa tarve perusmuotoisille ja erityisesti laajoille henkilöturvallisuusselvityksille. Myös tarve Pääesikunnan laatimille yritysturvallisuusselvityksille voi kasvaa. Nämä lisäävät Pääesikunnan henkilöresursointitarvetta.

Nato-jäsenyys tulee lisäämään Naton turvallisuusluokitellun tiedon määrää Suomessa. Nato suosittelee turvallisuusluokiteltujen tietojen suojaamisessa ensisijaisesti sähköistä tiedonsiirtoa ja käsittelyä. Sähköinen tiedonsiirto on myös kansallisesta näkökulmasta operatiivisen yhteistyön ja päätöksenteon oikea-aikaisuuden varmistamiseksi välttämätöntä. Sähköisten tietojenkäsittely-ympäristöjen suunnittelussa ja toteuttamisessa tulee ottaa huomioon eri ministeriöiden, Suomen ulkomaan edustustojen, tasavallan presidentin kanslian sekä virastojen ja erityisesti Puolustusvoimien tarpeet. Asiakirjajakelut tulevat kohdentumaan eri hallinnonaloille, mutta erityisesti määrän kasvu näkyy Puolustusvoimissa sekä ulko- ja puolustusministeriöissä. Sellaisen kansallisen TLII-ympäristön kehittäminen, joka on hyväksytty myös NATO SECRET -tason

turvallisuusluokitellun tiedon käsittelyyn, on välttämätöntä mahdollisimman nopealla aikataululla. Sähköisen käsittely-ympäristön toteutus nojaa osin päätökseen, kuinka rekisteritoiminnot kansallisesti toteutetaan. Sähköisen tietojenkäsittely-ympäristön toteutusmalleja ja rekisteröintitoimintojen kehittämisestä on linjattu valtioneuvoston kanslian, ulkoministeriön ja valtiovarainministeriön kesken.

Naton tietoturvallisuusvaatimusten mukaan turvallisuusluokiteltua tietoa NATO CONFIDENTIAL tasolta alkaen voi käsitellä ja säilyttää vain kulunvalvonnan piirissä olevalla ja fyysisesti suojatulla viranomaisen hyväksymällä turva-alueella. NATO RESTRICTED tason tietoa on käsiteltävä viranomaisen hyväksymällä hallinnollisella alueella. Fyysisten käsittely-ympäristöjen toteuttamiseen kohdistuu merkittäviä kustannuksia koko valtionhallinnossa.

Naton turvallisuussääntöjen mukaan kaikkien Naton turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien on läpikäytävä hyväksymisprosessi. Tämä koskee Naton Suomelle toimittamia järjestelmiä ja Suomen kansallisia järjestelmiä, joissa käsitellään Naton turvallisuusluokiteltua tietoa. Naton toimittamien järjestelmien osalta Liikenne- ja viestintävirasto vastaa järjestelmän kansallisen käyttöpisteen akkreditoinnista ja toimittaa sitä koskevan lausunnon (Statement of Compliance) Naton turvallisuushyväksyntälautakunnalle. Naton turvallisuusluokiteltua tietoa käsittelevien kansallisten tietojärjestelmien hyväksyntäprosessi koostuu riskiarvioinnista, järjestelmäkohtaisten vaatimusten määrittelystä, tarkastuksesta ja akkreditoinnista, jäännösriskin hyväksymisestä annetun akkreditointilausunnon pohjalta sekä käyttöluvan antamisesta. Akkreditointilausunto on voimassa kolme vuotta. Naton turvallisuusluokiteltua tietoa käsittelevien järjestelmien tarkastus- ja hyväksyntätyön on arvioitu edellyttävän Liikenne- ja viestintävirastossa pysyvästi lisäresursointitarpeita.

Kansallinen tietojärjestelmäkokonaisuus Naton turvallisuusluokiteltujen tietojen käsittelyyn tulee suunnitella niin, että se täyttää Naton tietojärjestelmäturvallisuutta koskevat vaatimukset. Liikenne- ja viestintävirasto tarjoaa viranomaisille neuvontaa järjestelmien turvallisuusvaatimusten suunnittelussa, mikä tukee hyväksyntäprosessin sujuvaa etenemistä. Kansallisen järjestelmäkokonaisuuden suunnittelun tuki ja arviointiprosessin tehokkaan toteuttamisen varmistaminen edellyttävät virastossa lisäresursointia.

Eduskunnan tiedusteluvaliokunta on kiinnittänyt hallituksen esitystä HE 315/2022 vp käsitellessään huomiota tieto- ja tilaturvallisuudesta huolehtimiseksi vaadittavien toimenpiteiden resursoinnin kannalta kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitettujen kansallisen turvallisuusviranomaisen ja määrättyjen turvallisuusviranomaisten tehtävien lisääntymiseen (TiVL 1/2022 vp, s. 3).

6.3 Vaikutukset elinkeinoelämään

Tietoturvallisuussopimus antaa suomalaisille yrityksille mahdollisuuden tulla valituksi Naton järjestämään tai muutoin organisoimaan hankkeeseen taikka toisessa valtiossa järjestettävään hankintakilpailuun, joka edellyttää Naton turvallisuusluokiteltujen tietojen käsittelyä.

Turvallisuusluokiteltua tietoa sisältäviä hankkeita toteutetaan erityisesti puolustusteollisuuden, turvallisuuden, ydinvoiman, informaatioteknologian ja muun korkean teknologian aloilla sekä tieteen- ja tutkimuksen aloilla. Ilman tietoturvallisuussopimusta suomalaiset yritykset jäisivät Natossa toteutettavien turvallisuusluokiteltua tietoa sisältävien hankkeiden ulkopuolelle. Hankkeeseen valituksi tuleminen voi sopimuksen perusteella edellyttää yritykseltä turvallisuusselvityslain (46 §) mukaista yritysturvallisuusselvitystodistusta. Yritykseltä peritään turvallisuusselvityslain nojalla tehdyistä yritysturvallisuusselvityksistä maksu noudattaen, mitä valtion maksuperustelaissa (150/1992) säädetään.

Sopimuksen tarkoitus on mahdollistaa hankkeisiin osallistuminen ja näin parantaa suomalaisten yritysten kilpailukykyä ja ulkomaankauppaa.

7 Lausuntopalaute

Luonnos hallituksen esitykseksi on ollut lausuntokierroksella 24.3.–21.4.2023. Lausuntoja pyydettiin 24 taholta. Lausuntoja annettiin yhteensä 13 kappaletta. Lausuntopyyntö ja lausunnot ovat saatavilla osoitteessa valtioneuvosto.fi/hankkeet hankenumerolla UM001:00/2023.

Yleistä

Lausunnon jättäneet ministeriöt sekä viranomaiset yhtyvät pääosin hallituksen esitysluonnoksessa esitettyyn ja kannattavat sopimuksen sekä Naton turvallisuussääntöjen hyväksymistä. Sopimuksen sekä turvallisuussääntöjen hyväksymisen katsotaan mahdollistavan sen, että Suomi voi vastaanottaa täysimääräisesti Naton turvallisuusluokiteltua tietoa. Useat lausunnon antaneista pitää tärkeänä myös sitä, että sopimus saatetaan voimaan mahdollisimman pian, jotta Suomi voi osallistua tiedonvaihtoa sisältävään jäsenmaiden väliseen yhteistyöhön.

Lausunnon antaneista neljä ei esitä varsinaisia huomioita hallituksen esityksen sisältöön. Näistä kaksi edustivat ministeriöitä sekä viranomaisia, jotka ovat osallistuneet hallituksen esityksen valmisteluun.

Lainsäädäntö ja sen arviointi

Valtioneuvoston kanslia pitää tärkeänä, että esityksessä kuvataan mahdollisimman selkeästi sopimusvelvoitteiden suhdetta kansalliseen julkisuus- sekä henkilötietojen käsittelyä koskevaan lainsäädäntöön. Valtioneuvoston kanslia pitää olennaisena hahmottaa Nato-järjestelmän ja EU:n oikeusjärjestyksen välinen lähestymistapaero. Naton asiakirjoihin ei lähtökohtaisesti järjestön omien säännösten ja käytäntöjen mukaan sovelleta julkisuusperiaatetta.

Valtioneuvoston kanslia toteaa luokittelemattomien Naton asiakirjojen osalta (NATO UNCLASSIFIED), että julkisuuslaki ei perustu ”need to know basis” –tyyppiseen lähestymistapaan ja siihen, että tiedon luovuttaminen edellyttäisi tiedon pyytäjän osoittavan erityisen, hyväksyttävän tarpeen. Samalla on selvää, että tiedonsaantioikeutta voidaan rajoittaa julkisuuslain 24 §:n mukaisten edellytysten täyttyessä.

Valtioneuvoston kanslia katsoo, että esityksen jaksoa 2.1 kansainvälisistä tietoturvallisuusvelvoitteista annetun lain sekä tiedonhallintalain soveltamisesta olisi hyvä täsmentää. Selvyyden vuoksi esityksen jatkovalmistelussa olisi tarkennettava, miltä osin kansallista tiedonhallintalainsäädäntöä ei sovelleta erityissuojattavaan tietoaineistoon.

Valtioneuvoston kanslia on kiinnittänyt huomiota siihen, että kansainvälisesti erityissuojattavien tietoaineistojen siirtämiseen viestintäverkoissa voi liittyä tiettyjä erityiskysymyksiä esimerkiksi tietosuojan osalta.

Poliisihallitus katsoo, että vaikka Natolta peräisin oleviin asiakirjoihin voidaan soveltaa laajasti salassapitosäännöksiä, tulisi julkisuuslakia tarkistaa Suomen Nato-jäsenyyden myötä. Turvallisuusluokitellun tiedon osalta kansallinen säännöstö tukee Naton asiakirjojen käsittelyä, mutta mahdollisia ongelmia voi syntyä NATO UNCLASSIFIED –asiakirjojen osalta (s. 8) sekä osittain salassa pidettävien asiakirjojen osalta. Naton tietoturvallisuussäännöissä asetetut minimivaatimukset voivat edellyttää myös hankintalainsäädännön uudistamista.

Poliisihallituksen mukaan on syytä arvioida, kuinka laajasti Suomen julkishallinnossa tullaan jatkossa käsittelemään Nato-tietoa ja asiakirjoja. Puolustussuunnittelu on Suomessa koko yhteiskunnan läpileikkaava prosessi. Kansallisten tietoturvallisuuteen liittyvien normien yhdenmukaistaminen Naton säännöstön kanssa helpottaisi Poliisihallituksen mukaan tietoturvallisuutta ylläpitävien toimijoiden tehtäviä ja pienentäisi tietoturvariskejä.

Oikeusministeriö katsoo, että tietoturvallisuussopimuksen ja Naton tietoturvasääntöjen mukaiset velvoitteet suojaisivat oleellisin osin myös henkilötietoja, vaikka kyseessä ei ole sama asia kuin tietosuojalainsäädännössä tarkoitettu tietosuojan tason riittävyys. Henkilötietojen suojan kannalta merkityksellistä on myös se, että sopimus tulisi sovellettavaksi myös sen osapuolten kahden- ja monenvälisessä tiedonvaihdossa.

Oikeusministeriö katsoo, että selkeyden vuoksi tekstissä olisi hyvä täsmentää, voisivatko suojattavat asiakirjat olla muitakin kuin Naton asiakirjoja. Henkilötietojen käsittelyä vaikuttaisi liittyvän tiedonvaihdon lisäksi ainakin sopimuksen 3 artiklan edellyttämiin henkilöturvallisuusselvityksiin sekä niihin liittyvään yhteistyöhön sopimusosapuolten välillä. Oikeusministeriö korostaa myös sitä, että Naton asiakirjoihin sisältyviä henkilötietoja voivat käsitellä myös muut kuin rikosasioiden tietosuojalaissa tarkoitetut toimivaltaiset viranomaiset. Esitysluonnoksen mukaan asiakirjajakelut tulevat kasvamaan määrällisesti erityisesti Puolustusvoimissa sekä ulko- ja puolustusministeriössä. Tekstistä ei kuitenkaan ilmene, voisivatko muut viranomaiset luovuttaa suoraan suojattavaa aineistoa sopimuksen nojalla. Tällä on merkitystä erityisesti tietosuoja-asetuksen V luvun soveltamisen kannalta. Myös valtioneuvoston kanslian lausunnossa pidetään tärkeänä, että henkilötietojen käsittelyä koskeva kuvaus on kirjoitettu täsmällisesti.

Esityksen jaksoja 2.1–2.3 on täydennetty lausunnot huomioon ottaen.

Vaikutusarvioinnit

Valtiovarainministeriö muistuttaa lausunnossaan ministeriöille tiedonhallintalain 5 §:n 3 momentissa ja 8 §:n 2 momentissa säädetystä velvollisuudesta arvioida ehdotettujen säännösten ja muutosten vaikutuksia tietoaineistoihin ja tietojärjestelmiin.

Liikenne- ja viestintäministeriö toteaa esityksen vaikutusten kohdistuvan ministeriön hallinnonalalla erityisesti Liikenne- ja viestintävirastoon, joka toimii kansallisen turvallisuusviranomaisen asiantuntijana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa. Liikenne- ja viestintävirasto on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:ssä tarkoitettu määrätty turvallisuusviranomainen, joka vastaa kansallisena viranomaisena Naton turvallisuussääntöjen edellyttämistä tietojärjestelmäakkreditoinneista osana turvallisuusselvityslain mukaista yritysturvallisuusselvitystä. Ministeriö jakaa esitysluonnoksen vaikutusarvion siitä, että näiden tehtävien arvioidaan edellyttävän Liikenne- ja viestintävirastossa pysyvästi lisäresursointitarpeita ja edellyttää, että Liikenne- ja viestintävirastolle varmistetaan riittävät resurssit sille osoitettavien tehtävien suorittamiseksi asianmukaisesti.

Rajavartiolaitoksen esikunta toteaa Nato-jäsenyyden lisäävän käsiteltävän Nato-turvallisuusluokitellun tiedon määrää myös Rajavartiolaitoksessa, minkä lisäksi tietoturvallisuusjärjestelyjen saattaminen vaaditulle tasolle aiheuttaa taloudellisia vaikutuksia. Myös Poliisihallitus tuo esille, että Natosta saapuvien asiakirjojen jakelu tulee todennäköisesti laajenemaan ja poliisin pitää mukauttaa tietojen käsittelyä ja turvallisuustoimenpiteitään uusien määräysten mukaisiksi. Rajavartiolaitoksen esikunta katsoo Naton turvallisuussääntöjen toimeenpanon edellyttävän lisäksi mahdollisesti henkilöresursointitarpeita.

Liikenne- ja viestintävirasto toteaa, että sopimuksen ja turvallisuussääntöjen tietojärjestelmäturvallisuutta koskevat vaatimukset eivät eroa olennaisesti niistä vaatimuksista, joita Suomi on jo Naton kumppanimaana tehtyjen turvallisuusjärjestelyjen perusteella noudattanut. Merkittävimpänä erona aikaisempaan on se, että Liikenne- ja viestintävirasto voi jäsenyyden myötä arvioida ja hyväksyä kansallisia salaustuotteita turvallisuusluokiteltujen tietojen suojaamiseen NATO CONFIDENTIAL –tasolle asti.

Liikenne- ja viestintäministeriö sekä Liikenne- ja viestintävirasto pitävät molemmat tärkeänä, että korkean turvallisuusluokitellun tiedon kansallisen tietojenkäsittely-ympäristön suunnittelussa ja rakentamisessa otetaan huomioon kaikkien hallinnonalojen ja virastojen tarpeet Naton turvallisuusluokitellun tiedon sähköiselle käsittelylle. Rauhankumppanuuden aikana vakiintuneiden tietoturvallisuusprosessien sijasta valtioneuvoston kanslia korostaa, että Suomen kansallisen edun varmistamiseksi on olennaisen tärkeää, että erityissuojattavien aineistojen hallintaa ja myös tietoturvallisuuden menettelyjä kehitetään Nato-jäsenyyden tarpeiden mukaisesti.

Elinkeinoelämän keskusliitto EK:n lausunnossa pidetään tärkeänä, että suomalaisyritysten kilpailulliset edellytykset osallistua kansainvälisten tietoturvavelvoitteiden mukaisiin hankkeisiin, mukaan lukien Nato-liitännäiset hankkeet, ovat samalla tasolla kuin muissa jäsenmaissa. EK pitää välttämättömänä, että vaatimusten taso ja kansallinen tulkinta kansainvälisistä tietoturvallisuusvelvoitteista on samanlaista kuin muissa maissa.

Sopimuksen ja tietoturvallisuussääntöjen yksityiskohtaiset perustelut

Valtiovarainministeriö esittää täsmennystä sopimuksessa tarkoitetun asiakirjan määritelmän suhteesta julkisuussa laissa tarkoitettuun asiakirjan käsitteeseen. Valtiovarainministeriön lausunnossa ehdotetaan myös eräitä täsmennyksiä ja terminologisia muutoksia, jotka on mahdollisuuksien mukaan otettu huomioon.

Ahvenanmaa

Ahvenanmaan maakunnan hallitus toteaa lausunnossaan, että Suomen Nato-jäsenyys ei muuta lainsäädäntövallan jakautumista valtakunnan ja maakunnan välillä. Maakunnan hallitus toteaa, että Ahvenanmaan itsehallintolain 27 §:n 4 kohdan mukaan suhde ulkovaltoihin, ottaen huomioon itsehallintolain luvun 9 ja 9 a säännökset, kuuluu valtakunnan lainsäädäntövaltaan, samoin kuin puolustus- ja rajavartiolaitosta, järjestysvallan toimintaa valtion turvallisuuden varmistamiseksi, puolustustilaa ja valmiutta poikkeusolojen varalta koskevat asiat itsehallintolain 27 §:n 34 kohdan mukaan. Siviilikriisinhallinnan puitteissa hoidetaan osittain asioita, jotka Ahvenanmaan itsehallintolain mukaan kuuluvat maakunnan lainsäädäntötoimivaltaan, esimerkiksi terveyden- ja sairaanhoito (Ahvenanmaan itsehallintolain 18 §:n 12 kohta) ja palo- ja pelastustoimi (Ahvenanmaan itsehallintolain 18 §:n 6 kohta).

Sääntelyä asiakirjojen julkisuudesta maakunnan ja kunnallisessa hallinnossa ei mainita nimenomaisesti itsehallintolain lainsäädäntövallan jakautumista koskevissa säännöksissä. Maakunnan hallitus toteaa, että Ahvenanmaan nykyinen julkisuuslaki (ÅFS 2021:79) tuli voimaan 1.1.2022. Valtakunnan julkisuuslainsäädäntöä voidaan lausunnon mukaan soveltaa tietyissä rajoitetuissa tilanteissa maakunnan ja kuntahallinnon viranomaisissa. Itsehallintolain 60 a §:n mukaan salassapitovelvollisuuteen ja asiakirjojen julkisuuteen sovelletaan valtakunnan lainsäädäntöä itsehallintolain 9 ja 9 a luvuissa tarkoitetuissa asioissa (kansainvälisten velvoitteiden neuvottelut ja Euroopan unionin asiat). Sen lisäksi valtakunnan julkisuuslainsäädäntöä voidaan maakunnan hallituksen mukaan soveltaa maakunnan ja kuntahallinnon viranomaisissa vain silloin, kun ne hoitavat valtakunnan toimivaltaan kuuluvia hallintotehtäviä.

Pohjois-Atlantin sopimuksen osapuolten välisen tietoturvallisuussopimuksen kannalta merkityksellisten tietojen ja asiakirjojen osalta maakunnan hallitus toteaa, että niitä ei yleensä käytännössä lähetetä Ahvenanmaalle, koska tiedot koskevat pääasiassa turvallisuus- ja puolustuspolitiikkaa. Tämä ei lausunnon mukaan kuitenkaan tarkoita, että olisi poissuljettua, että Pohjois-Atlantin sopimuksen osapuolten välisen tietoturvallisuussopimuksen kannalta merkityksellisiä tietoja ja asiakirjoja voisi jatkossa joutua lähettämään Ahvenanmaalle, esim. siviilikriisinhallintaan liittyvät asiakirjat, jotka kuuluvat osittain maakunnan lainsäädäntövaltaan.

Siinä tapauksessa, että sopimuksessa tarkoitettuja tietoja tai asiakirjoja annetaan maakunnan viranomaisille, sovelletaan maakunnan hallituksen mukaan Ahvenanmaan julkisuuslakia. Sen 22 §:n mukaan Ahvenanmaan viranomaisen vastaanottamat kansalliset asiakirjat tai niissä olevat tiedot ovat turvallisuusluokiteltuja, jos asiakirjat tai tiedot on kansallisessa lainsäädännössä luokiteltu. Ahvenanmaan julkisuuslainsäädäntö ei sisällä eri tasoja salassa pidettävälle tiedolle eikä virkamiesten turvallisuusselvityksiä koskevia säännöksiä. Maakunnan hallitus katsoo, että Pohjois-Atlantin osapuolten välinen tietoturvasopimus sisältää maakunnan toimivaltaan kuuluvia määräyksiä, jotka edellyttävät Ahvenanmaan itsehallintolain 59 §:n mukaan siten maakuntapäivien hyväksymistä, jotta sopimus tulisi kokonaisuudessaan voimaan Ahvenanmaalla.

Viittaus Ahvenanmaan maakunnan hallituksen lausuntoon sekä perustuslakivaliokunnan lausuntoon (PeVL 80/2022 vp) on lisätty jaksoon 12.

8 Tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdyn sopimuksen määräykset ja niiden suhde Suomen lainsäädäntöön

8.1 Sopimus Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta

Johdanto. Sopimuksen johdannossa vahvistetaan se, että tehokas poliittinen neuvottelu, yhteistyö ja suunnittelu puolustusasioissa Pohjois-Atlantin sopimuksen tavoitteiden saavuttamiseksi edellyttävät turvallisuusluokitellun tiedon vaihtamista osapuolten välillä. Johdannossa tunnistetaan myös se, että tiedonvaihto Pohjois-Atlantin sopimuksen osapuolten välillä edellyttää määräyksiä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja turvaamisesta. Tällaisille turvallisuusvaatimuksille ja menettelyille tarvitaan yleiset puitteet, joista sopimuksessa sovitaan.

1 artikla. Sopimuksen 1 artiklan i kohdan mukaan osapuolet sitoutuvat suojaamaan ja turvaamaan sopimuksen I liitteessä tarkemmin määritellyn turvallisuusluokitellun tiedon, jonka alkuperäinen luovuttaja on Nato tai jonka jäsenvaltio toimittaa Natolle sekä jäsenvaltioiden turvallisuusluokitelluksi merkityn turvallisuusluokitellun tiedon, joka toimitetaan toiselle jäsenvaltiolle Naton ohjelman, hankkeen tai sopimuksen tueksi.

Sopimus soveltuu siten Suomen ja Naton välillä vaihdettavan turvallisuusluokitellun tiedon lisäksi jäsenvaltioiden välillä vaihdettavaan turvallisuusluokiteltuun tietoon, joka toimitetaan Naton ohjelman, hankkeen tai sopimuksen tueksi. Sopimuksen soveltaminen jäsenvaltioiden välillä ei siten edellytä muodollista Naton yhteistyötä vaan sitä sovelletaan myös jäsenvaltioiden väliseen kansainväliseen yhteistoimintaan, jolla tuetaan Naton toimintaa. Pohjois-Atlantin sopimuksen 3 artiklan mukaisesti osapuolet ylläpitävät ja kehittävät yhdessä ja erikseen, jatkuvan ja tehokkaan oman valmistautumisen ja keskinäisen avun pohjalta, kansallista ja yhteistä kykyään puolustautua aseellisia hyökkäyksiä vastaan. Artiklan mukaista yhteistoimintaa voidaan toteuttaa jäsenvaltioiden välillä ilman Naton muodollista yhteistoiminnan muotoa tai Naton toimielinten osallistumista. Naton tietoturvallisuussopimusta sovelletaan myös tällaisessa kahden-

tai monenvälisessä yhteistoiminnassa vaihdettavaan jäsenvaltioiden kansalliseen turvallisuusluokiteltuun tietoon. Usein myös tällaista yhteistoimintaa määrittävissä kansainvälisissä sopimusasiakirjoissa viitataan Naton tietoturvallisuutta koskeviin vaatimuksiin tai niiden suojaamisen tasoon. Sopimus voi edesauttaa lisäksi kansallisen turvallisuusluokitellun tiedon vaihtoa Naton jäsenvaltioiden kesken muissakin tilanteissa, jos kahdenvälistä tietoturvallisuutta koskevaa valtiosopimusta ei ole olemassa ja jos molemmat osapuolet katsovat sen siihen soveltuvan.

Artiklan ii kohdan mukaan osapuolet säilyttävät i kohdassa tarkoitetun tiedon turvallisuusluokituksen ja pyrkivät kaikin keinoin turvaamaan tiedon sen mukaisesti. Artiklan iii kohdan mukaan turvallisuusluokiteltua tietoa ei käytetä muihin kuin Pohjois-Atlantin sopimuksessa ja siihen liittyvissä päätöksissä ja päätöslauselmissa määrättyihin tarkoituksiin. Määräys sisältää kansainvälisiin tietoturvallisuussopimuksiin tyypillisesti kuuluvan käyttötarkoitussidonnaisuusperiaatteen. Artiklan iv kohdan mukaan sopimuksen osapuolet eivät ilmaise tällaista tietoa Natoon kuulumattomille osapuolille ilman tiedon alkuperäisen luovuttajan suostumusta.

Sopimukseen sovellettaisiin sopimuksen voimaan saattamisen jälkeen kansainvälisistä tietoturvallisuusvelvoitteista annettua lakia, jonka 3 luvun määräykset tietoturvallisuustoimenpiteistä sisältävät 1 artiklan määräysten täytäntöön panemiseksi tarvittavat säännökset.

2 artikla. Artiklan mukaan osapuolet varmistavat kansallisen turvallisuusviranomaisen perustamisen Naton toimintaa varten toteuttamaan suojaavia turvatoimia. Osapuolet laativat ja panevat täytäntöön turvallisuusvaatimuksia, joilla varmistetaan turvallisuusluokitellun tiedon yhteinen suojauksen taso. Näitä turvallisuusvaatimuksia selostetaan tarkemmin jäljempänä jaksossa 8.2.

Turvallisuusluokitellun tiedon käsittelylle asetetuista vaatimuksista säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa, julkisen hallinnon tiedonhallinnasta annetussa laissa ja turvallisuusluokitteluasetuksessa. Turvallisuusluokitteluasetusta sovelletaan Naton turvallisuusluokiteltavien asiakirjojen käsittelyyn, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu.

Kansainvälisitä tietoturvallisuusvelvoitteista annetun lain 3 luvun säännökset sisältävät keskeiset laintasoiset tietoturvallisuustoimenpiteet: salassapito ja tietojen käyttö (6 §), vaitiolovelvollisuus ja hyväksikäyttökielto (7 §), turvallisuusluokan merkitseminen (8 §), turvallisuusluokkaa vastaavat käsittelyvaatimukset (9 §) ja tiloihin liittyvät turvallisuusvaatimukset (10 §).

Turvallisuusluokitteluasetuksen 6–15 §:ssä säädetään turvallisuusluokiteltujen asiakirjojen käsittelyssä toteutettavista tietoturvallisuustoimenpiteistä, jotka liittyvät kansainvälisiä tietoturvallisuusvelvoitteita ja asiakirjan elinkaarta mukaillen asiakirjan antamisen edellytyksiin (6 §), monitasoiseen suojaukseen (7 §), käsittelyoikeuden antamiseen ja niiden luettelointiin (8 §), turvallisuusalueisiin eli toimitilaturvallisuuteen (9 §), asiakirjan käsittelyn ja tietojärjestelmien suojaamiseen turvallisuusalueiden avulla (10 §), tietojärjestelmiä ja tietoliikennejärjestelyjä koskeviin vaatimuksiin (11 §), asiakirjan siirtämiseen tietoverkon kautta (12 §), asiakirjan kuljettamiseen (13 §), asiakirjan käsittelyn seuraamiseen (14 §) ja asiakirjan tuhoamiseen (15 §).

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaan ulkoministeriö toimii kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa Suomen kansallisena turvallisuusviranomaisena. Puolustusministeriö, Pääesikunta, Suojelupoliisi ja Liikenne- ja viestintävirasto toimivat määrättyinä turvallisuusviranomaisina. Kansallisen turvallisuusviranomaisen tehtävänä on erityisesti ohjata ja valvoa, että tässä laissa tarkoitetut erityissuojattavat tietoaineistot suojataan ja niitä käsitellään asianmukaisesti.

Määrätyt turvallisuusviranomaiset huolehtivat niille kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetyistä ja muista niille kansainvälisistä tietoturvallisuusvelvoitteista johtuvista tehtävistä. Puolustusministeriö, Pääesikunta ja Suojelupoliisi toimivat kansallisen turvallisuusviranomaisen asiantuntijoina henkilöstö-, yritys- ja toimitilaturvallisuutta koskevissa asioissa sekä Liikenne- ja viestintävirasto tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa.

Kansallinen turvallisuusviranomainen on julkaissut Katakri-työkalun, johon on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset. Katakri on viranomaisten tietoturvallisuuden auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata kansallista tai kansainvälistä turvallisuusluokiteltua tietoa. Katakri itsessään ei aseta tietoturvallisuudelle ehdottomia vaatimuksia, vaan siihen kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin. Vaatimukset on kuvattu siten, että ne mahdollistavat erilaisia toteutustapoja. Lisätietokenttiin on tulkinnan tueksi koottu toteutusesimerkkejä, joissa kuvatuilla menettelyillä voidaan useimmissa ympäristöissä saavuttaa hyväksyttävä suojauksen vähimmäistaso. Toteutusesimerkit eivät ole sitovia ja ne ovat korvattavissa myös muilla vastaavan tasoisilla suojauksilla.

Kansallinen turvallisuusviranomainen yhteistyössä määrättyjen turvallisuusviranomaisten kanssa on julkaisemassa Katakria täydentävän Nato-liitteen tukemaan niitä julkishallinnon ja elinkeinoelämän organisaatioita, jotka tulevat käsittelemään Naton turvallisuusluokiteltua tietoa. Liite perustuu Suomelle vuoden 2022 aikana luovutettuihin Naton tarkentaviin turvallisuussääntöihin ja -ohjeisiin, joista on tehty vertailuanalyysi Katakriin. Liite ei tuo merkittäviä muutoksia Katakrin sisältöön tai sen soveltamiseen, vaan pyrkii esittämään ainoastaan huomionarvoiset eroavaisuudet kansallisten ja Naton turvallisuusvaatimusten välillä.

Voimassaolevan turvallisuusluokitteluasetuksen mukaisessa turvallisuusaluejaossa ja asiakirjojen käsittelysäännöissä (9-10 §) on otettu huomioon Euroopan unionin neuvoston turvallisuussäännöt, joiden mukaan turvallisuusluokiteltuja tietoja, jotka kuuluvat CONFIDENTIAL- (turvallisuusluokka III) tai SECRET- (turvallisuusluokka II) turvallisuusluokkaan, voidaan käsitellä hallinnollisella alueella, jos pääsy tietoihin on suojattu sivullisilta. Naton turvallisuussäännöstö mahdollistaa kuitenkin enintään NATO RESTRICTED- (turvallisuusluokka IV) turvallisuusluokan tiedon käsittelyn hallinnollisella alueella. Tämä käsittelysääntöjen ero ja tarvittavat rinnastukset on esitetty Katakrin Nato-liitteessä. Turvallisuusluokitteluasetusta sovelletaan Suomessa niin kansallisen kuin kansainvälisenkin turvallisuusluokitellun tiedon käsittelyyn, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu. Naton turvallisuussäännöstössä kuvatut vähimmäisvaatimukset ovat tällainen Suomea sitova kansainvälinen velvoite, jonka määräykset tulevat sovellettavaksi Natolta peräisin olevan tiedon käsittelyssä.

3 artikla. Artiklan 1 kohdan mukaan osapuolet sitoutuvat varmistamaan, että kaikista niiden kansalaisista, jotka virallisia tehtäviään hoitaessaan tarvitsevat tai saattavat saada pääsyn turvallisuusluokkaan CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon, tehdään asianmukaisesti turvallisuusselvitys ennen kuin he ottavat tehtävänsä vastaan. Naton turvallisuussääntöjen mukaan poikkeuksen PSC-vaatimuksesta muodostavat valtion ylimpien tehtävien haltijat (valtion- ja hallitusten päämiehet, ministerit, kansanedustajat sekä oikeuslaitoksen jäsenet), joiden osalta pääsy Naton turvallisuusluokiteltuun tietoon perustuu kansallisiin säädöksiin ja määräyksiin. Viimeksi mainittuja henkilöitä on kuitenkin ohjeistettava tiedon käsittelyyn liittyvistä turvallisuusvelvoitteista ja heillä tulee olla tiedon käsittelyyn tiedonsaantitarve.

Artiklan 2 kohta sisältää turvallisuusselvitysmenettelyitä koskevan vaatimuksen. Niillä on pystyttävä selvittämään, voiko henkilö hänen lojaliteettinsa ja luotettavuutensa huomioon ottaen saada pääsyn turvallisuusluokiteltuun tietoon ilman, että siitä aiheutuu turvallisuusriski, jota ei voida hyväksyä.

Artiklan 3 kohta edellyttää, että osapuolet tekevät pyydettäessä yhteistyötä muiden osapuolten kanssa niiden turvallisuusselvitysmenettelyjä suoritettaessa.

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n mukaan kansainvälisessä tietoturvallisuusvelvoitteessa edellytetty henkilöturvallisuusselvitys laaditaan siten kuin turvallisuusselvityslaissa säädetään. Henkilöturvallisuusselvitystodistuksen antaa kuitenkin kansallinen turvallisuusviranomainen, jollei eritvisistä svistä muuta johdu. Turvallisuusselvityslain 26 §:ssä säädetään tiedon hankkimisesta ulkomaan viranomaisen rekistereistä. Kansainvälisistä turvallisuusvelvoitteista annetun lain 17 §:ssä säädetään kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi välttämättömien asiakirjojen ja tietojen luovuttamisesta tietoturvallisuussopimuksen osapuolelle.

4 artikla. Artiklan mukaan Naton pääsihteerin tulee varmistaa, että vastaavasti Nato soveltaa sopimuksen turvallisuusluokitellun tiedon suojaamista koskevia määräyksiä. Asiaa koskeva tarkennus sisältyy sopimuksen III liitteeseen.

Natossa on hyväksytty tässä artiklassa tarkoitettuja yksityiskohtaisia määräyksiä, joita sovelletaan sekä jäsenvaltioiden että Naton toimintaan. Naton puolella Naton turvallisuustoimisto (Nato Office of Security, NOS) koordinoi, valvoo ja panee täytäntöön Naton turvallisuussäännöstön (Nato Security Policy).

5 artikla. Artiklan mukaan sopimus ei millään tavoin estä osapuolia tekemästä muita sopimuksia, jotka liittyvät niiden luovuttaman turvallisuusluokitellun tiedon vaihtamiseen eivätkä vaikuta tämän sopimuksen soveltamisalaan.

Suomella on tällä hetkellä kahdenvälisiä tietoturvallisuussopimuksia 20 valtion kanssa sekä Pohjoismaiden, Euroopan unionin jäsenvaltioiden, Euroopan avaruusjärjestön, Euroopan puolustusmateriaalijärjestö OCCARin sekä Pohjois-Atlantin liiton kanssa. Naton kanssa tehty aiempi sopimus ja hallinnollinen järjestely korvautuvat nyt hyväksyttävällä sopimuksella.

6 artikla. Sopimus on ollut avoinna allekirjoittamista varten Naton silloisille jäsenvaltioille, joiden ratifioimis- tai hyväksymiskirjat on tullut tallettaa Amerikan yhdysvaltojen hallituksen huostaan. Artiklan b kohdan mukaan sopimus on tullut voimaan kolmenkymmenen päivän kuluttua päivästä, jona kaksi allekirjoittajavaltiota on tallettanut ratifioimis- tai hyväksymiskirjansa. Sopimus on tullut määräyksen mukaisesti kansainvälisesti voimaan 16.8.1998. Sen jälkeen sopimus on tullut voimaan kunkin muun allekirjoittajavaltion osalta kolmenkymmenen päivän kuluttua kunkin valtion ratifioimis- tai hyväksymiskirjan tallettamisesta.

Artiklan c kohdan mukaan sopimus on korvannut Pohjois-Atlantin neuvoston 1952 hyväksymän asiakirjan D.C.2/7 liitteessä olevan lisäyksen liitteessä A (1 kohta) 19 päivänä huhtikuuta 1952 ja joka myöhemmin sisällytettiin Pohjois-Atlantin neuvoston 2 päivänä maaliskuuta 1955 hyväksymän asiakirjan C-M (55) 15 (final) liitteeseen A.

7 artikla. Artikla sisältää Suomeen soveltuvan määräyksen tietoturvallisuussopimukseen liittymisestä. Sopimus on avoinna liittymistä varten Pohjois-Atlantin sopimuksen uudelle osapuolelle sen valtiosäännön mukaisten menettelyjen mukaisesti. Liittymiskirja talletetaan Amerikan

yhdysvaltojen hallituksen huostaan. Sopimus tulee voimaan kunkin liittyvän valtion osalta kolmenkymmenen päivän kuluttua sen liittymiskirjan tallettamispäivästä. Suomi on liittymisneuvotteluissa sitoutunut liittymään tietoturvallisuussopimukseen 12 kuukauden kuluessa siitä, kun Suomi on tallettanut Pohjois-Atlantin sopimusta koskevan liittymiskirjansa

8 artikla. Amerikan yhdysvaltojen hallitus ilmoittaa muiden osapuolten hallituksille kunkin ratifioimis-, hyväksymis- tai liittymiskirjan tallettamisesta.

9 artikla. Artikla sisältää sopimuksen irtisanomista koskevat määräykset. Osapuoli voi irtisanoa sopimuksen antamalla kirjallisen irtisanomisilmoituksen tallettajalle, joka ilmoittaa irtisanomisilmoituksesta kaikille muille osapuolille. Irtisanominen tulee voimaan vuoden kuluttua siitä, kun tallettaja on vastaanottanut ilmoituksen, mutta ei vaikuta niihin velvoitteisiin, oikeuksiin tai valtaoikeuksiin, joita osapuolet ovat aiemmin sopineet tai saaneet tämän sopimuksen määräysten perusteella.

Todistusvoimaiset tekstit. Sopimuksen todistusvoimaiset kielet ovat englanti ja ranska. Sopimuksen tallettajana toimii Amerikan yhdysvaltojen hallitus.

Liite I. Sopimuksen liitteet muodostavat sopimuksen erottamattoman osan. Liitteessä I määritellään Naton turvallisuusluokiteltu tieto. Liitteen a kohdan mukaan "tieto" tarkoittaa missä tahansa muodossa välitettävää tietoa. Sen b kohdan mukaan turvallisuusluokiteltu tieto tarkoittaa tietoa tai aineistoa, jonka katsotaan edellyttävän suojaamista luvattomalta paljastamiselta ja joka on turvallisuusluokituksella osoitettu sellaiseksi. Liitteen c kohdan mukaan ”aineisto” sisältää asiakirjat ja myös valmistetut ja valmisteilla olevat koneet, laitteet ja aseet. Liitteen d kohdan mukaan ”asiakirja” tarkoittaa mitä tahansa tallennettua tietoa riippumatta sen fyysisestä muodosta tai ominaisuuksista, mukaan lukien kirjalliset ja painotuotteet; tietojenkäsittelyssä käytettävät kortit ja nauhat; kartat, kaaviot, valokuvat, maalaukset, piirustukset, kaiverrukset, luonnokset, työmuistiinpanot ja –paperit, hiilipaperikopiot ja värinauhat; millä tahansa keinolla tai menettelyllä tehdyt jäljennökset; kaikenlaiset ääni-, puhe- ja magneettitallenteet sekä elektroniset, optiset ja videotallenteet; kannettavat atk-laitteet, joissa on kiinteät tallennusvälineet, ja irrotettavat tietokoneen tallennusvälineet, mutta ei rajoittuen näihin. Asiakirja ja viranomaisen asiakirja on määritelty kansallisessa lainsäädännössä julkisuuslain 5 §:ssä. Julkisuuslaissa säädetty asiakirjan määritelmä eroaa joiltakin osin liitteen d kohdan mukaisesta asiakirjan määritelmästä. Lähtökohtaisesti Suomen viranomaiselle toimitettu ja sen hallussa oleva Naton asiakirja on julkisuuslain 5 §:ssä tarkoitettu viranomaisen asiakirja, johon sovelletaan julkisuuslakia. Naton luokiteltujen asiakirjojen osalta julkisuuslaki soveltuu kuitenkin vain sikäli kuin kansainvälisistä turvallisuusvelvoitteista annetussa laissa ei toisin säädetä.

Liite II. Liitteessä määritellään, mitä Natolla tässä sopimuksessa tarkoitetaan. ”Nato” tarkoittaa Pohjois-Atlantin liittoa ja niitä elimiä, joihin sovelletaan joko Ottawassa 20 päivänä syyskuuta 1951 allekirjoitettua sopimusta Pohjois-Atlantin liiton, kansallisten edustajien ja kansainvälisen henkilöstön asemasta tai Pariisissa 28 päivänä elokuuta 1952 allekirjoitettua pöytäkirjaa Pohjois-Atlantin sopimuksen mukaisesti perustettujen kansainvälisten sotilasesikuntien asemasta.

Liite III. Liite sisältää sopimuksen 4 artiklaa täydentävän määräyksen, jonka mukaan sotilaskomentajien kanssa neuvotellaan heidän valtaoikeuksiensa kunnioittamiseksi. Sotilaskomitea vastaa kaikista Naton sotilasrakenteen turvallisuusasioista ja sen alaisuuteen perustettujen Naton sotilaselinten johtajat vastaavat kaikista organisaatioidensa turvallisuusasioita. Turvallisuussääntöjen mukaan turvallisuustoimiston tulee esimerkiksi tiedottaa sotilaskomitean puheenjohtajalle Naton turvallisuustilanteesta sekä edistymisestä turvallisuutta koskevien NAC:n päätösten täytäntöönpanossa.

8.2 Naton tietoturvallisuutta koskevat vaatimukset ja osa-alueet

Naton turvallisuustoiminta perustuu Naton sisäisesti hyväksyttyyn turvallisuussäännöstöön (Nato Security Policy) ja sen pohjalle rakentuviin jäsenvaltioiden turvallisuusmenettelyihin. Naton osalta tietoturvallisuussopimuksen 2 artiklassa tarkoitetun yhteisen suojauksen tason perusperiaatteet ja vähimmäisvaatimukset on vahvistettu Naton asiakirjassa C-M(2002)49-REV1, ”Security within the North Atlantic Treaty Organization” (jäljempänä Naton turvallisuussäännöt), sitä tukevissa direktiiveissä (*directives*), suuntaviivoissa (*guidelines)* sekä tulkintaohjeissa (*supporting documents*). Turvallisuussääntöjen mukaan jäsenvaltiot varmistavat säännöissä määrättyjen perusperiaatteiden ja vähimmäisvaatimusten soveltamisen, jotta Naton turvallisuusluokitellun tiedon luottamuksellisuuden, eheyden ja käytettävyyden säilyminen turvataan.

Turvallisuussäännöstö asettaa turvallisuuden perusperiaatteet ja vähimmäisvaatimukset, jotta Naton turvallisuusluokitellulle tiedolle annetaan todennetusti vaatimustenmukainen suoja jäsenmaissa ja Naton elimissä. Turvallisuussäännöstö muodostaa tietoturvallisuussopimuksen täytäntöönpanoa koskevan laajan ja yksityiskohtaisen kokonaisuuden, joka ei ole kuitenkaan osa sopimusta.

Osapuolet arvioivat ja päivittävät Naton turvallisuussäännöstöä eri kokoonpanoissa. Naton tietoturvallisuutta koskevia asioita käsitellään Naton turvallisuuskomitean turvallisuuspolitiikka-kokoonpanossa. Komitean sihteeristönä toimii Naton turvallisuustoimisto (NOS (*NATO Office of Security*), joka myös asettaa komitean puheenjohtajan. Komitean jäsenistö muodostuu jäsenvaltioiden kansallisista (NSA; National Security Authority) ja/tai määrätyistä turvallisuusviranomaisista (DSA; Designated Security Authority). Suomi on osallistunut komitean työhön vuodesta 2011 alkaen. Turvallisuuskomitealla on myös teknisen tietoturvallisuuden CISS-kokoonpano (NATO SC(CISS)). Naton sotilas- ja siviilielimet vastaavat toimialojensa turvallisuusasioista.

Naton turvallisuussäännöstön tietoturvallisuuden osa-alueet ovat henkilöstöturvallisuus, toimitilaturvallisuus, tietoaineistoturvallisuus, viestintä- ja tietojärjestelmien turvallisuus ja yritysturvallisuus. Toimenpiteet ulottuvat henkilöihin, järjestelmiin, tiloihin, infrastruktuuriin ja ympäristöön sekä tiedon käsittelyn kontrolleihin ja tiedonhallintaan. Näitä koskevat keskeiset turvallisuusvaatimukset sisältyvät Naton turvallisuussääntöjen C-M(2002)49-REV1 liitteisiin B-H, joiden sisältöä selostetaan alla.

Liite A - Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta tehty sopimus

Turvallisuussääntöjen liite A sisältää varsinaisen tietoturvallisuussopimuksen tekstin, jonka sisältöä on selostettu edellä jaksossa 8.1.

Liite B – Perusperiaatteet, vähimmäisvaatimukset ja vastuut

Turvallisuussääntöjen liitteessä B kuvataan Naton turvallisuussääntöjen soveltamiseen liittyvät perusperiaatteet, vähimmäisvaatimukset sekä vastuut, joita soveltamalla Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet varmistavat osapuolten kesken vaihdettavalle turvallisuusluokitellulle tiedolle yhteisen suojauksen tason.

Kuvatut perusperiaatteet ja vähimmäisvaatimukset liittyvät muun muassa turvallisuusluokitellun tiedon käsittelyoikeuksien rajaamiseen, sisäpiiriuhkien huomioimiseen osana turvallisuusmenettelyjä, turvallisuuskoulutuksen järjestämiseen, tietoturvaloukkauksia koskevaan ilmoitusvelvollisuuteen ja -menettelyyn sekä turvallisuusluokitellun tiedon alkuperäisen luovuttajan määräysvaltaan luovuttamansa tiedon osalta. Naton turvallisuusluokiteltua tietoa luovutetaan

vakiintuneiden luovutusmenettelyjen ja –perusteiden mukaisesti ja tieto tulee suojata vähintään samantasoisesti kuin Naton turvallisuussäännöissä ja sitä tukevissa ohjeissa edellytetään.

Naton turvallisuusluokiteltua tietoa koskevat vähimmäisvaatimukset on ulotettava koskemaan kaikkia henkilöitä, joilla on pääsy turvallisuusluokiteltuun tietoon sekä kaikkia tiloja ja tietovälineitä, joissa tällaista tietoa käsitellään. Tällaista tietoa voidaan jakaa ainoastaan viralliseen tehtävään liittyvän tiedonsaantitarpeen perusteella. Turvallisuusluokan NATO CONFIDENTIAL ja tätä korkeammin luokiteltujen tietoaineistojen osalta edellytetään lisäksi, että tietoa käsittelevät henkilöt ovat asianmukaisesti turvallisuusselvitetty ja heille on annettu tieto käsittelyssä sovellettavista turvallisuusmenettelyistä. Turvallisuusluokitellun tiedon käsittelyedellytyksiä tulee arvioida myös turvallisuusselvitystodistuksen myöntämisen jälkeen erilaisten seurantatoimien kautta, minkä tarkoituksena on mahdollistaa tiedon vaarantumiseen liittyvän sisäpiiriuhkan hallinta.

Naton jäsenvaltion kansallinen turvallisuusviranomainen vastaa Naton turvallisuusluokitellun tiedon turvallisuudesta ja toimii Naton turvallisuustoimiston ensisijaisena yhteystahona kaikissa Naton turvallisuuteen liittyvissä asioissa. Tarvittaessa se voi ohjata Naton turvallisuustoimiston kääntymään myös muun toimivaltaisen turvallisuusviranomaisen puoleen. Kansallisen turvallisuusviranomaisen vastuulla on varmistaa Naton turvallisuusluokitellun tiedon turvallisuus sekä sotilas- että siviilialan virastoissa ja yksiköissä niin kotimaassa kuin ulkomaillakin. Sen vastuulla on varmistaa, että kaikissa kansallisissa organisaatioissa tehdään määräajoin asianmukaiset tarkastukset sen arvioimiseksi, suojataanko Naton turvallisuusluokiteltua tietoa asianmukaisesti, ja että turvallisuusluokiteltua tietoa käsitteleville henkilöille on annettu henkilöturvallisuusselvitystodistus Naton turvallisuusperiaatteiden mukaisesti. Kansallinen turvallisuusviranomainen valtuuttaa (authorize) myös kansallisten COSMIC-keskusrekisterien perustamisen ja lakkauttamisen. Tällaiseen keskusrekisteriin kirjataan COSMIC TOP SECRET luokkaan luokiteltu tieto. Tällainen keskusrekisteri voi toimia myös tilivelvollisuuden alaisen muun tiedon rekisterinä. Määrättyjen turvallisuusviranomaisten vastuulla on tiedottaa yrityksille ja muille yhteisölle kansallisista periaatteista kaikissa Naton yritysturvallisuuden periaatteita koskevissa asioissa ja antaa apua niiden soveltamisessa.

Naton jäsenvaltioiden kansallisten turvallisuusviranomaisten tai määrättyjen turvallisuusviranomaisten ja Naton sotilas- tai siviilielinten välinen Naton turvallisuusasia, jota ei voida ratkaista, tai Naton turvallisuusperiaatteiden toteuttamista tai tulkintaa koskeva asia saatetaan Naton turvallisuustoimiston ratkaistavaksi. Ratkaisemattomat erimielisyydet Naton turvallisuustoimisto antaa Naton turvallisuuskomitean käsiteltäväksi.

Naton jäsenvaltioiden ja Naton sotilas- ja siviilielinten ehdotukset Naton turvallisuusperiaatteiden muuttamiseksi annetaan ensisijaisesti Naton turvallisuustoimiston käsiteltäväksi. Naton turvallisuustoimisto käsittelee ehdotukset ja esittää ne tarvittaessa Naton turvallisuuskomitealle asian jatkokäsittelyä varten. Jäsenvaltioiden kansalliset turvallisuusviranomaiset sekä määrätyt turvallisuusviranomaiset voivat tämän estämättä tehdä virallisen ehdotuksen turvallisuusperiaatteiden muuttamisesta Naton turvallisuuskomitealle, jos ne niin tahtovat.

Liite C – Henkilöstöturvallisuus

Turvallisuussääntöjen henkilöstöturvallisuutta koskevat periaatteet ja vähimmäisvaatimukset on kuvattu turvallisuussääntöjen liitteessä C, jossa kuvattuja yleisperiaatteita tukee yksityiskohtaisempi Naton henkilöstöturvallisuutta koskeva direktiivi AC/35-D/2000. Henkilöstöturvallisuutta koskevat vaatimukset määrittelevät sitä, millä edellytyksillä henkilöille voidaan antaa pääsy Naton turvallisuusluokiteltuun tietoon.

Jäsenvaltion henkilöstöturvallisuusmenettelyjen tulee olla riittävät sen selvittämiseksi, voidaanko henkilölle myöntää hänen lojaalisuutensa, rehellisyytensä ja luotettavuutensa huomioon ottaen pääsy Naton turvallisuusluokiteltuun tietoon ilman, että siitä aiheutuva turvallisuusriski ylittää hyväksyttävän tason. Kaikki siviili- ja sotilashenkilöt, joiden tehtävät edellyttävät pääsyä turvallisuusluokan CONFIDENTIAL tai sitä ylempien turvallisuusluokkien tietoihin, on turvallisuusselvitettävä asianmukaisesti ja heillä tulee olla henkilöturvallisuusselvitystodistus (PSC), mikäli on saavutettu riittävä luottamuksen taso heidän kelpoisuudestaan saada pääsy tällaiseen tietoon. Poikkeuksen PSC-vaatimuksesta muodostavat valtion ylimpien tehtävien haltijat (valtion- ja hallitusten päämiehet, ministerit, kansanedustajat sekä oikeuslaitoksen jäsenet), joiden osalta pääsy Naton turvallisuusluokiteltuun tietoon perustuu kansallisiin säädöksiin ja määräyksiin. Viimeksi mainittuja henkilöitä on kuitenkin ohjeistettava tiedon käsittelyyn liittyvistä turvallisuusvelvoitteista ja heillä tulee olla tiedon käsittelyyn tiedonsaantitarve.

Naton jäsenvaltioiden sekä Naton siviili- ja sotilaselinten henkilöillä on pääsy vain sellaiseen Naton turvallisuusluokiteltuun tietoon, joihin heillä on tiedonsaantitarve (need-to-know). Kenelläkään ei ole oikeutta päästä Naton turvallisuusluokiteltuun tietoon yksinomaan henkilön aseman, viran tai henkilöturvallisuusselvitystodistuksen perusteella.

Kaikille henkilöille, joilla on pääsy Naton turvallisuusluokiteltuun tietoon tai joille on tehty henkilöturvallisuusselvitys turvallisuusluokitellun tiedon käsittelyä varten, tulee varmistaa asianmukaisen turvallisuuskoulutuksen järjestäminen. Tällaista tietoa käsitteleville henkilöille on ohjeistettava tiedon käsittelyyn liittyvistä turvallisuusmenettelyistä ja heidän turvallisuusvelvoitteistaan sekä säännöllisin väliajoin muistutettava myös erilaisista turvallisuusuhkista, joita tiedon käsittelyyn liittyy. Kaikkien turvallisuusselvitettyjen henkilöiden on vakuutettava ymmärtävänsä täysin vastuunsa ja heihin mahdollisesti kohdistuvat seuraukset, mikäli Naton turvallisuusluokiteltua tietoa joutuu luvattomiin käsiin joko tahallisesti tai huolimattomuudesta.

Kansallisten turvallisuusviranomaisten ja määrättyjen turvallisuusviranomaisten tai muiden toimivaltaisten turvallisuusviranomaisten, Naton jäsenvaltioiden ja Naton siviili- tai sotilaselinten päälliköiden yksityiskohtaiset vastuut on määritelty henkilöstöturvallisuutta koskevassa direktiivissä (AC/35-D/2000).

Liite D – Toimitilaturvallisuus

Turvallisuussääntöjen liitteessä D kuvataan toimitilaturvallisuutta koskevat periaatteet ja vähimmäisvaatimukset Naton turvallisuusluokitellun tiedon suojaamiseksi. Lisätietoja toimitilaturvallisuuteen liittyvistä yksityiskohtaisista vaatimuksista löytyy Naton turvallisuusperiaatteita tukevasta toimitilaturvallisuutta koskevasta direktiivistä (AC/35-D/2001).

Naton jäsenvaltioiden on laadittava aktiivisia ja passiivisia turvallisuustoimia sisältävät toimitilaturvallisuuden ohjelmat, joilla saavutetaan yhteinen toimitilaturvallisuuden taso, joka vastaa arvioita suojattavan tiedon uhkista, haavoittuvuuksista, turvallisuusluokituksesta ja määrästä. Kaikki kohteet, rakennukset, tilat ja muut alueet, joissa Naton turvallisuusluokiteltua tietoa käsitellään tai siitä keskustellaan, on suojattava asianmukaisin fyysisin turvallisuustoimenpitein. Näiden turvallisuustoimenpiteiden tarkoituksena on estää tunkeutuminen, ehkäistä, estää ja havaita sisäpiiriuhkan toimet, mahdollistaa henkilöstön erottelu ja pääsy Naton turvallisuusluokiteltuun tietoon heidän henkilöturvallisuusselvitystodistuksen ja tiedonsaantitarpeen perusteella sekä mahdollistaa kaikkien tietoturvapoikkeamien havaitseminen ja niihin puuttuminen mahdollisimman nopeasti.

Toimitilaturvallisuuden ohjelmien on perustuttava monitasoisen suojaamisen periaatteeseen, jossa käytetään asianmukaista yhdistelmää toisiaan täydentäviä fyysisiä turvallisuustoimenpiteitä, jotka tarjoavat sellaisen suojan tason, joka täyttää organisaation ja sen tietojen kriittisyyteen ja haavoittuvuuteen liittyvät vaatimukset. Fyysisiä turvallisuustoimenpiteitä tukemassa on oltavat asianmukaiset henkilöstö-, tieto- sekä viestintä- ja tietojärjestelmäturvallisuuden toimenpiteet.

Pysyvät tai tilapäiset alueet, joissa NATO CONFIDENTIAL tason turvallisuusluokiteltua tietoa säilytetään, käsitellään tai joissa siitä keskustellaan, on järjestettävä ja muodostettava siten, että ne vastaavat Naton I–luokan tai Naton II-luokan turva-alueen vaatimuksia. Naton I- tai II-luokan turva-alueiden ympärille tai niille johtavalle alueelle on perustettava hallinnollinen vyöhyke. Hallinnollisilla vyöhykkeillä sallitaan vain turvallisuusluokan NATO RESTRICTED tiedon säilyttäminen, käsittely tai siitä keskusteleminen. Tällaisilla alueilla on oltava selkeästi määritetyt rajat, joilla on mahdollisuus tarkastaa henkilöt ja ajoneuvot.

Teknisesti suojatut turva-alueet ovat joko kiinteitä tai tilapäisiä alueita, jotka ovat nimenomaisesti tunnistettu teknisiltä hyökkäyksiltä ja salakuuntelulta suojattaviksi alueiksi. Tällaisilla alueilla on tehtävä säännöllisiä fyysisiä ja teknisiä tarkastuksia ja niihin pääsyä on valvottava tarkasti.

Turvallisuusluokkiin COSMIC TOP SECRET, NATO SECRET ja NATO CONFIDENTIAL kuuluvat tiedot on säilytettävä luokan I tai II turva-alueella noudattaen Naton turvallisuussäännöissä määriteltyjä tarkempia ehtoja. Turvallisuusluokkaan NATO RESTRICTED kuuluva tieto on säilytettävä lukitussa kaapissa tai toimistokalusteessa hallinnollisella alueella tai luokan I tai II turva-alueella.

Naton jäsenvaltioiden tulee käyttää vain sellaisia laitteita, jotka asianomainen turvallisuusviranomainen on hyväksynyt Naton turvallisuusluokitellun tiedon säilyttämiseen.

Liite E – Naton turvallisuusluokitellun tiedon turvallisuus

Turvallisuussääntöjen liitteessä E kuvataan Naton turvallisuusluokitellun tiedon turvallisuutta koskevat periaatteet ja vähimmäisvaatimukset. Tietoturvallisuus on yleisten suojaustoimenpiteiden ja –menettelyjen soveltamista turvallisuusluokitellun tiedon katoamisen tai vaarantumisen estämiseksi, havaitsemiseksi ja korjaamiseksi.

Luovuttaja vastaa turvallisuusluokitellun tiedon turvallisuusluokan määrittämisestä. Keskeisen periaatteen mukaan turvallisuusluokkaa ei saa vaihtaa, alentaa eikä poistaa ilman alkuperäisen luovuttajan suostumusta. Liitteessä E luetellaan Naton turvallisuusluokat, niistä käytettävät lyhenteet sekä määritellään merkitykset seuraavasti:

COSMIC TOP SECRET (CTS) - luvaton ilmitulo aiheuttaisi Natolle poikkeuksellisen vakavaa vahinkoa; NATO SECRET (NS) - luvaton ilmitulo aiheuttaisi Natolle vakavaa vahinkoa; NATO CONFIDENTIAL (NC) - luvaton ilmitulo aiheuttaisi Natolle vahinkoa; ja NATO RESTRICTED (NR) - luvaton ilmitulo haittaisi Naton etuja tai sen toiminnan tehokkuutta.

Liitteessä määritellään myös erityisluokkien ”ATOMAL”, ”SIOP”, ”CRYPTO” ja ”BOHEMIA” merkintöjen suojaamisessa sovellettavat sopimukset ja säännöstöt.

Luokkiin COSMIC TOP SECRET, NATO SECRET ja ATOMAL luokiteltu tieto on liitteen E mukaan tilivelvollisuuden alaista tietoa. Käytössä on oltava rekisterijärjestelmä, joka vastaa

tilivelvollisuuden alaisen tiedon vastaanottamisesta, kirjaamisesta, käsittelystä, jakelusta ja hävittämisestä. Turvallisuusluokkiin NATO CONFIDENTIAL ja NATO RESTRICTED luokiteltua tietoa ei tarvitse kirjata rekisterijärjestelmään, jolleivat kansalliset säädökset ja määräykset tätä edellytä. Niiden organisaatioiden, jotka käsittelevät turvallisuusluokkaan COSMIC TOP SECRET luokiteltua tietoa, on nimettävä COSMIC-tiedon valvoja.

Liitteessä määritellään tietoturvapoikkeama, tietoturvaloukkaus, tiedon vaarantuminen ja vähäinen tietoturvapoikkeama. Kaikista tosiasiallisista ja mahdollisista tietoturvaloukkauksista on ilmoitettava viipymättä toimivaltaiselle turvallisuusviranomaiselle. Kansallinen turvallisuusviranomainen tai määrätty turvallisuusviranomainen tai Naton sotilas- tai siviilielimen johtaja välittää ilmoitukset vahingon arvioinnista ja vähentämistoimista Naton turvallisuustoimistolle. NOS voi pyytää toimivaltaisia viranomaisia tutkimaan asiaa tarkemmin ja ilmoittamaan havainnoistaan Naton turvallisuustoimistolle. NOS voi ilmoittaa asiasta myös Naton turvallisuuskomitealle.

Liite F – Viestintä- ja tietojärjestelmien turvallisuus

Liitteessä F esitetään periaatteet ja vähimmäisvaatimukset, jotka koskevat Naton turvallisuusluokitellun tiedon sekä sitä tukevien järjestelmäpalvelujen ja resurssien suojaamista viestinnässä, tallennettaessa tätä tietoa tietojärjestelmiin ja muihin sähköisin järjestelmiin sekä käsiteltäessä ja siirrettäessä sitä näissä järjestelmissä (viestintä- ja tietojärjestelmien turvallisuus). Liitteessä kuvataan tiedon luottamuksellisuutta, eheyttä, käytettävyyttä, aitoutta ja kiistämättömyyttä koskevat turvallisuustavoitteet. Kun yritykset käsittelevät turvallisuusluokiteltua tietoa sopimusten perusteella, sovelletaan lisäksi erityisiä yritysturvallisuustoimia (ks. liite G).

Kaikkien Naton turvallisuusluokiteltua tietoa käsittelevien kansallisten viestintä- ja tietojärjestelmien on läpäistävä turvallisuusakkreditointi, jossa osoitetaan turvallisuustavoitteiden toteutuminen. Turvallisuusakkreditoinnilla todetaan, että asianmukainen suojauksen taso on saavutettu ja sitä ylläpidetään.

Liitteessä F luetellaan asianmukaiset turvallisuustoimenpiteet, joita on sovellettava kaikkiin Naton turvallisuusluokiteltua tietoa käsitteleviin viestintä- ja tietojärjestelmiin, jotta saavutetaan tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien suojaamisen turvallisuutavoitteet. Naton tietoliikenne- ja tietojärjestelmien turvallisuusriskien hallinnalla varmistetaan järjestelmän haavoittuvuuksien ja turvallisuusvaatimusten mukaisuuden jatkuva arviointi.

Kun Naton turvallisuusluokiteltua tietoa siirretään sähköisesti, on toteutettava erityiset toimenpiteet turvallisuustavoitteiden saavuttamiseksi näissä siirroissa. Turvallisuusluokkaan NATO SECRET ja sitä ylempiin luokkiin luokitellun tiedon luottamuksellisuus on tietoa siirrettäessä suojattava Naton sotilaskomitean hyväksymillä salaustuotteilla ja –menetelmillä. Turvallisuusluokkaan NATO CONFIDENTIAL tai NATO RESTRICTED luokitellun tiedon luottamuksellisuus on tietoa siirrettäessä suojattava joko Naton sotilaskomitean tai Naton jäsenvaltion hyväksymillä salaustuotteilla tai –menetelmillä.

Liitteessä kuvataan kansallisen viestintä- ja tietojärjestelmien turvallisuusviranomaisen (NCSA), Naton salausaineiston hallinnasta vastaavan kansallisen jakeluviranomaisen sekä akkreditointiviranomaisten tehtävät.

Liite G – Turvallisuusluokiteltujen hankkeiden turvallisuus ja yritysturvallisuus

Liitteessä G kuvataan Naton turvallisuusluokitellun tiedon turvallisuutta yrityksissä koskevat periaatteet ja vähimmäisvaatimukset. Yritysturvallisuus on suojaustoimien ja –menettelyjen soveltamista sellaisen turvallisuusluokitellun tiedon katoamisen tai vaarantumisen estämiseksi, havaitsemiseksi ja korjaamiseksi, jota yritykset käsittelevät hankesopimusten perusteella. Yrityksille annettava ja yritysten kanssa tehtävien hankesopimusten perusteella tuotettava Naton turvallisuusluokiteltu tieto sekä yritysten kanssa tehtävät hankesopimukset on suojattava Naton turvallisuusperiaatteiden ja niitä tukevien ohjeiden mukaisesti. Hankeosapuolen ja alihankkijoiden edellytetään sitoutuvan kaikkiin kansallisten turvallisuusviranomaisten tai määrättyjen turvallisuusviranomaisten määräämiin toimiin hankeosapuolen tuottaman tai Naton turvallisuusluokitellun tiedon suojaamiseksi. Liite sisältää erilliset määräykset Naton ulkopuolisten valtioiden hankeosapuolten kanssa tehtävistä hankesopimuksista.

Kunkin Naton jäsenvaltion kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen vastuulla on varmistaa, että sen toimivaltaan kuuluvat yhteisöt, jotka tarvitsevat pääsyn turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin luokkiin luokiteltuun tietoon, ovat toteuttaneet tarvittavat suojaustoimet saadakseen todistuksen yritysturvallisuusselvityksestä (Facility Security Clearance, FSC). Yritysten työntekijöillä, jotka tarvitsevat pääsyn turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin luokiteltuun Naton tietoon, on oltava asianmukainen todistus henkilöturvallisuusselvityksestä.

Liite G sisältää myös kansainvälisiin vierailuihin liittyviä valvontamenettelyitä koskevat periaatteet sekä Naton hankkeeseen tai ohjelmaan lainattavaa henkilöstöä sekä Naton turvallisuusluokitellun aineiston kansainvälisiin siirtoihin ja kuljettamiseen sovellettavat turvallisuusperiaatteet.

Liite H – Turvallisuus suhteissa Naton ulkopuolisiin toimijoihin

Turvallisuusääntöjen liitteessä H kuvataan ne periaatteet ja vähimmäisvaatimukset, joita on noudatettava suojattaessa Naton ulkopuolisille valtioille ja muille Naton ulkopuolisille elimille (esim. kansainvälisille järjestöille) luovutettavaa tai näiden pääsyoikeuden piiriin kuuluvaa Naton turvallisuusluokiteltua tietoa. Lisätietoja ja vaatimuksia Naton ulkopuolisille toimijoille luovutettavan tai näiden pääsyoikeuden piiriin kuuluvan Naton turvallisuusluokitellun tiedon suojaamiseksi on Naton turvallisuusperiaatteita tukevassa ohjeessa turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin.

Naton turvallisuusluokitellun tiedon jakamisen Naton ulkopuolisten toimijoiden kanssa tulee lähtökohtaisesti tapahtua Pohjois-Atlantin neuvoston hyväksymän Naton yhteistyötoiminnan yhteydessä, mutta poikkeustapauksissa se voi tapahtua myös tällaisen toiminnan ulkopuolella.

Ennen Naton turvallisuusluokitellun tiedon jakamista Naton ulkopuolisen toimijan kanssa kyseisen toimijan ja Naton on tullut tehdä turvallisuussopimus. Turvallisuussopimuksen turvallisuusperiaatteita tuetaan asianmukaisella hallinnollisten järjestelyjen kokonaisuudella. Mikäli turvallisuussopimusta ei ole tehty, ja tietoa on kuitenkin välttämätöntä jakaa oikea-aikaisesti, on tullut antaa turvallisuusvakuutus.

Erityiset määräykset koskien Naton ulkopuolisille toimijoille luovutettavan tai näiden pääsyoikeuden piiriin kuuluvan Naton turvallisuusluokitellun tiedon suojaamisesta koskevat henkilöstöturvallisuutta, toimitilaturvallisuutta, tietoaineistoturvallisuutta, luovuttajaviranomaisia, luovutettua tietoa koskevaa kirjanpitoa sekä viestintä- ja tietojärjestelmien turvallisuutta. Liitteessä H esitetään myös tietoturvapoikkeamien käsittelyä koskevat vaatimukset.

Sanasto

Turvallisuussääntöjen liitteenä on myös sanasto, joka sisältää säännöissä käytettyjen keskeisten termien määritelmät.

Keskeisimmät muutokset nykytilaan

Suomi noudattaa jo tällä hetkellä Naton turvallisuussääntöjä C-M(2002)49-REV1 vuonna 2012 tehdyn hallinnollisen järjestelyn nojalla. Naton turvallisuussopimukseen sitoutuminen ei siten muuta nykytilannetta merkittävästi. Tällä hetkellä Suomen viranomaisten tulkinnan apuna on tulkintaohje AC/35-D/1038, "Supporting Document on the Security Protection of NATO Information Released to Non-NATO Nations and International Organisations", joka on tarkoitettu Natoon kuulumattomien maiden turvallisuusviranomaisten käyttöön. Naton turvallisuusluokitellun tiedon luovuttaminen Suomelle Natoon kuulumattomana maana on edellyttänyt aikanaan erityistä Naton turvallisuustoimiston turvallisuussopimuksen täytäntöönpanon sertifiointiprosessin kautta antamaa muodollista vakuutusta siitä, että tietoa suojataan Suomessa Naton turvallisuussäännöstön minimistandardien mukaisesti.

Rauhankumppanina Nato-asiakirjojen saaminen on perustunut aina tiedon alkuperäisen luovuttajan kirjalliseen suostumukseen tai NAC:in hyväksymään yhteistyöhön taikka Naton toimintaan, johon Suomi osallistuu NAC:n tuella. Erona nykytilanteeseen on myös se, että Naton jäsenenä Suomi voi saada korkeimman turvallisuusluokan COSMIC TOP SECRET –tason asiakirjoja, joita ei pääsääntöisesti luovuteta Natoon kuulumattomille maille. Joiltakin osin turvallisuusluokiteltujen tietojen käsittelyvaatimukset ovat Nato-jäsenten kohdalla joustavammat. Esimerkiksi NATO CONFIDENTIAL- ja NATO RESTRICTED –asiakirjojen rekisteröinti jätetään kansallisen lainsäädännön varaan. Nato-jäsenyyden myötä Naton turvallisuustoimisto tekee Suomeen määräajoin Naton turvallisuusluokitellun tiedon suojaamiseen tarkoitettujen turvallisuusjärjestelyjen *tarkastuksia*. Rauhankumppanuuden aikana Naton turvallisuustoimisto on tehnyt Suomeen niin sanottuja *tarkastusvierailuja*.

Naton turvallisuusluokitellun tiedon suojaamiseen tulee käyttää hyväksyttyjä salaustuotteita. Luokkien NATO SECRET ja COSMIC TOP SECRET tiedon suojaaminen edellyttää Naton sotilaskomitean (NAMILCOM, NATO Military Committee) hyväksymän salaustuotteen käyttöä. Luokkien NATO CONFIDENTIAL ja NATO RESTRICTED tiedon suojaamiseen voidaan käyttää myös jäsenmaan NCSA-viranomaisen hyväksymiä kansallisia salaustuotteita. Jäsenyyden myötä Liikenne- ja viestintävirasto voi arvioida ja hyväksyä kansallisia salaustuotteita NC- ja NR-luokkien tietojen suojaamiseen.

9 Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehty hallinnollinen järjestely ja Pohjois-Atlantin liiton kanssa tehty tietoturvallisuussopimus

Pohjois-Atlantin liiton kanssa vuonna 1994 tehdyllä sopimuksella Suomi sitoutui luokittelemaan ja suojaamaan rauhankumppanuusohjelman puitteissa Natolta saadun aineiston sekä laatimaan turvallisuusselvitykset niistä henkilöistä, joilla on pääsy suojattuun aineistoon. Sopimuksen liitteenä on selvitys Naton käyttämästä asiakirjojen turvallisuusluokittelusta sekä tiettyjen hallinnollisten kysymysten järjestämisestä sopimuksen toimeenpanemiseksi.

Vuonna 2012 Suomi teki Pohjois-Atlantin liiton kanssa sopimusta täydentävän hallinnollisen järjestelyn turvallisuusluokitellun tiedon suojaamiseksi. Järjestelyssä määrätään turvallisuusviranomaisista, sovellettavista määritelmistä, turvallisuusluokitellun tiedon merkitsemisestä, suojaamisesta ja käytöstä, pääsystä turvallisuusluokiteltuun tietoon, turvallisuusluokitellun tiedon

lähettämisestä, immateriaalioikeuksista, turvallisuusvaatimusten yksityiskohdista, järjestelyn noudattamisesta ja turvallisuustarkastuksista, vierailuista, tarkastusvierailuista, tiedon katoamisesta ja vaarantumisesta, kustannuksista, riitojen ratkaisusta sekä tavanomaisista loppumääräyksistä.

Suomen liittyessä Natoon sen tulee liittyä myös vuonna 1997 Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta tehtyyn sopimukseen, jonka määräykset korvaavat vuonna 1994 tehdyn sopimuksen ja vuonna 2012 tehdyn järjestelyn. Sopimus ja järjestely eivät sisällä määräystä niiden irtisanomisesta, mutta Naton kanssa on käyty keskusteluja sopimuksen ja järjestelyn päättämisestä valtiosopimusoikeutta koskevan Wienin yleissopimuksen (SopS 32 ja 33/1980) 54 artiklan b kohdan mukaisesti. Näin ollen sopimus ja järjestely on tarkoitus irtisanoa ja niiden voimaansaattamislaki on tarpeen kumota. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 15 §:n mukaan lain tietoturvallisuustoimenpiteitä koskevia säännöksiä sovelletaan niin kauan kuin se turvallisuusluokituksen perusteena olevan yleisen edun vuoksi on tarpeen silloinkin, kun sopimus tai säädös, johon säännösten soveltaminen perustuu, ei enää ole voimassa.

10 Lakiehdotusten säännöskohtaiset perustelut

10.1 Laki tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdystä sopimuksesta ja turvallisuussäännöistä

1 §. Pykälä sisältäisi tavanomaisen blankettilain säännöksen siitä, että sopimuksen ja sen nojalla annettujen turvallisuussääntöjen, sellaisina kuin ne ovat muutettuina 20.11.2020 annetussa asiakirjassa C-M(2002)49-REV-1, lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut. Sopimuksen ja turvallisuussääntöjen lainsäädännön alaan kuuluvia määräyksiä käsitellään tarkemmin eduskunnan suostumuksen tarpeellisuutta käsittelevässä jaksossa.

2 §. Pykälä sisältäisi tavanomaisen blankettilain säännöksen, joka koskee sopimuksen ja turvallisuussääntöjen muiden kuin lainsäädännön alaan kuuluvien määräysten voimaansaattamista valtioneuvoston asetuksella.

3 §. Pykälä sisältäisi tavanomaisen blankettilain säännöksen, jonka mukaan lain voimaantulosta säädetään valtioneuvoston asetuksella. Voimaantulosta säätäminen asetuksella on tarpeen, jotta lain voimaantulo tapahtuu samanaikaisesti, kun sopimuksen voimaantulo Suomen osalta.

10.2 Laki Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain kumoamisesta

1 §. Lakiehdotuksen 1 §:n nojalla Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annettu laki (945/2012) kumottaisiin.

2 §. Lain voimaantulosta säädettäisiin valtioneuvoston asetuksella. Laki on tarkoitus saattaa voimaan samanaikaisesti sopimusten irtisanomisen voimaantulon kanssa.

11 Voimaantulo

Tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehty sopimus tulee Suomen osalta voimaan kolmenkymmenen päivän kuluttua siitä päivästä, kun Suomi tallettaa tietoturvallisuussopimusta koskevan liittymiskirjansa Amerikan yhdysvaltojen hallituksen huostaan. Ehdotetaan, että esitykseen sisältyvä sopimuksen voimaansaattamislaki tulee voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samanaikaisesti, kun sopimus tulee Suomen osalta voimaan.

Tarkoituksena on, että Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen irtisanominen tulee voimaan samaan aikaan, kun Suomen liittyminen Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta tehtyyn sopimukseen tulee voimaan. Ehdotetaan, että esitykseen sisältyvä laki kyseisten sopimusten lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain kumoamisesta tulee voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samanaikaisesti, kun irtisanominen tulee voimaan.

12 Ahvenanmaan maakuntapäivien suostumus

Ahvenanmaan itsehallintolain (1144/1991) 59 §:n 1 momentin mukaan, jos valtiosopimus tai muu kansainvälinen velvoite, johon Suomi sitoutuu, sisältää määräyksen itsehallintolain mukaan maakunnan toimivaltaan kuuluvassa asiassa, maakuntapäivien on, jotta määräys tulisi voimaan maakunnassa, hyväksyttävä säädös, jolla määräys saatetaan voimaan.

Suomessa tällä hetkellä voimassa olevan 25 tietoturvallisuussopimuksen ei ole katsottu sisältävän määräyksiä, jotka kuuluisivat maakunnan toimivaltaan, eikä niiden voimaansaattamissäädöksille ole siten pyydetty maakuntapäivien hyväksymistä.

Hallituksen näkemyksen mukaan myöskään tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehty sopimus ei sisällä Ahvenanmaan maakunnan toimivaltaan kuuluvia määräyksiä, eikä siten edellytä maakunnan suostumusta Ahvenanmaan itsehallintolain 59 §:n mukaisesti. Maakunnan hallituksen kantaa selostetaan jaksossa 7.

Itsehallintolain perusteella maakuntapäivien hyväksyminen ei ole tarpeen sopimuksen irtisanomiselle tai sopimuksen voimaansaattamislain kumoamista koskevalle lailleen.

Todettakoon tässä yhteydessä, että Pohjois-Atlantin sopimusta koskevan hallituksen esityksen HE 315/2022 vp mukaan sopimus ei sisällä määräyksiä, jotka kuuluisivat Ahvenanmaan itsehallintolain nojalla Ahvenanmaan maakunnan toimivaltaan. Perustuslakivaliokunnalla ei ollut huomauttamista tähän lähtökohtaan. Perustuslakivaliokunta kiinnitti kuitenkin huomiota siihen, että Nato-sopimukselle olisi aikaisemman kansainvälisten sopimusten hyväksynnän saamista koskevan käytännön perusteella mahdollista pyytää myöhemmässä vaiheessa maakuntapäivien hyväksyntä, mikäli se osoittautuisi tarpeelliseksi (PeVL80/2022 vp, s. 10).

13 Suhde muihin esityksiin

Tämä hallituksen esitys liittyy 5.12.2022 annettuun hallituksen esitykseen eduskunnalle Pohjois-Atlantin sopimuksen sekä Pohjois-Atlantin liiton, kansallisten edustajien ja kansainvälisen henkilöstön asemasta tehdyn sopimuksen hyväksymiseksi ja voimaansaattamiseksi (HE 315/2022 vp – EV 327/2022 vp). Suomi on liittymisneuvotteluissa sitoutunut liittymään Naton tietoturvallisuussopimukseen 12 kuukauden kuluessa siitä, kun Suomi on tallettanut Pohjois-

Atlantin sopimusta koskevan liittymiskirjansa. Pohjois-Atlantin sopimusta koskeva Suomen liittymiskirja talletettiin 4.4.2023.

Tietoturvallisuutta koskevia määräyksiä sisältyy myös Naton sopimukseen puolustukseen liittyvien, patentoitavaksi haettujen keksintöjen salassapidon vastavuoroiseksi turvaamiseksi, Naton sopimukseen teknisten tietojen välittämisestä puolustustarkoituksiin sekä Pohjois-Atlantin sopimuksen osapuolten väliseen sopimukseen ydinpuolustustietoja koskevasta yhteistyöstä. Sopimusten hyväksymisestä annetaan erilliset hallituksen esitykset.

Erillinen hallituksen esitys annetaan myös Pohjois-Atlantin sopimuksen sopimuspuolten välillä niiden joukkojen asemasta tehdyn sopimuksen (Nato SOFA) sekä Pohjois-Atlantin sopimuksen mukaisesti perustettujen kansainvälisten sotilasesikuntien asemasta tehdyn pöytäkirjan (Pariisin pöytäkirja) hyväksymiseksi.

14 Eduskunnan suostumuksen tarpeellisuus ja käsittelyjärjestys

14.1 Eduskunnan suostumuksen tarpeellisuus

Sopimus tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä

Perustuslain 94 §:n 1 momentin mukaan eduskunta hyväksyy sellaiset valtiosopimukset ja muut kansainväliset velvoitteet, jotka sisältävät lainsäädännön alaan kuuluvia määräyksiä tai ovat muutoin merkitykseltään huomattavia taikka vaativat perustuslain mukaan muusta syystä eduskunnan hyväksymisen. Eduskunnan hyväksyminen vaaditaan myös tällaisen velvoitteen irtisanomiseen. 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 (PeVL 11/2000 vp ja PeVL 12/2000 vp).

Sopimuksen 1 artiklan i kohdassa yhdessä sopimuksen I ja II liitteen kanssa määritellään, mitä tarkoitetaan suojattavalla turvallisuusluokitellulla tiedolla. Koska määritelmä vaikuttaa joko suoraan tai välillisesti sopimuksen lainsäädännön alaan kuuluvien aineellisten määräysten tulkintaan ja soveltamiseen, 1 artiklan i kohta ja I ja II liite edellyttävät eduskunnan hyväksymistä (PeVL 6/2001 vp).

Sopimuksen 1 artiklan i ja ii kohdassa määrätään sopimuksen soveltamisalaan piiriin kuuluvan turvallisuusluokitellun tiedon suojaamiseksi tarvittavista toimenpiteistä, jotka rajoittavat turvallisuusluokitellun tiedon luovuttamista sekä sen käyttöä. Artiklassa on kyse sopimuksen keskeisestä määräyksestä, jonka perusteella Suomi voi suojata sopimuksessa tarkoitettua turvallisuusluokiteltua tietoa ilman julkisuuslaissa säädettyä vahinkoedellytysarviointia. Määräys kuuluu lainsäädännön alaan.

Sopimuksen 2 artiklan mukaan osapuolet varmistavat kansallisen turvallisuusviranomaisen perustamisen Naton toimintaa varten toteuttamaan suojaavia turvatoimia. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:ssä on säännökset Suomen kansallisesta turvallisuusviranomaisesta ja määrätyistä turvallisuusviranomaisista sekä heidän toimivaltuuksistaan. Artiklan velvoite kansallisesta turvallisuusviranomaisesta kuuluu lainsäädännön alaan.

Sopimuksen 2 artiklan mukaan osapuolet laativat ja panevat täytäntöön turvallisuusvaatimuksia, joilla varmistetaan turvallisuusluokitellun tiedon yhteinen suojauksen taso. Artikla sisältää oikeusperustan Naton turvallisuusluokitellun tiedon suojaamista koskeville säännöille ja direktiiveille, joita Suomi Natoon liityttyään sitoutuu noudattamaan. Artiklassa delegoidaan turvallisuusvaatimuksia koskevaa sopimuksentekotoimivaltaa Pohjois-Atlantin neuvostolle. Delegointia koskeva määräys kuuluu lainsäädännön alaan.

Sopimuksen 3 artiklassa määrätään osapuolten velvollisuudesta tehdä asianmukaisesti turvallisuusselvitys henkilöistä, jotka virallisia tehtäviään hoitaessaan tarvitsevat tai saattavat saada turvallisuusluokkaan CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa. Artikla sisältää turvallisuusselvitysmenettelyjen jäännösriskiä ja osapuolten yhteistyötä koskevat määräykset. Suomessa turvallisuusselvityksen kohteena olevista henkilöistä sekä selvityksessä sovellettavasta menettelystä säädetään turvallisuusselvityslaissa. Sopimuksen 3 artikla sisältää lainsäädännön alaan kuuluvia määräyksiä.

Naton turvallisuussäännöt

Naton turvallisuussäännöstön keskeisimmät turvallisuuden periaatteet ja vähimmäisvaatimukset sisältyvät Pohjois-Atlantin neuvoston (NAC) hyväksymiin Naton turvallisuussääntöihin C-M(2002)49-REV1. Kansainvälisten tietoturvallisuussopimusten nojalla hyväksyttyjä turvallisuussäännöstöjä ei ole tapana saattaa kansallisesti voimaan. Naton turvallisuussäännöt sisältävät kuitenkin seuraavassa lueteltuja lainsäädännön alaan kuuluvia määräyksiä, jotka eivät ilmene suoraan tietoturvallisuussopimuksen tekstistä. Sellaisille määräyksille katsotaan tarpeelliseksi pyytää eduskunnan hyväksyminen ja saattaa ne kansallisesti voimaan (PeVL 19/2010 vp, s. 5-6). Turvallisuussääntöjen teksti on hallituksen esityksen liitteenä.

Turvallisuussääntöjen liite A sisältää varsinaisen tietoturvallisuussopimuksen tekstin, jonka lainsäädännön alaan kuuluvia määräyksiä on selostettu edellä.

Turvallisuussääntöjen B liitteen 1(b) kohta sisältää perusperiaatteen tarpeesta tietoon (need-to-know). Asiasta säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 3 momentissa. Liitteen 3 kohdassa määritellään kansallisen turvallisuusviranomaisen tehtävät ja 5 kohdassa edellytetään, että Naton jäsenvaltiolla on määrätty turvallisuusviranomainen yhteisöturvallisuusmääräysten täytäntöön panemiseksi. Suomen turvallisuusviranomaisista ja niiden tehtävistä säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:ssä. Liitteen 9(f) kohdassa annetaan Naton turvallisuustoimiston tehtäväksi suorittaa myös jäsenvaltioissa säännöllisiä turvallisuustarkastuksia Naton turvallisuusluokitellun tiedon suojaamiseksi. Kansainvälisen toimielimen vierailuista turvallisuustarkastusten suorittamiseksi säädetään kansainvälisistä turvallisuusvelvoitteista annetun lain 18 §:ssä.

Turvallisuussääntöjen C liitteen 7 kohdassa määritellään korkeassa valtion tehtävässä olevat henkilöt, esimerkiksi valtion ja hallitusten päämiehet, ministerit sekä parlamentin ja tuomioistuinlaitoksen jäsenet, joiden osalta tarve henkilöturvallisuusselvitykseen määräytyy kansallisen lainsäädännön ja säännösten mukaisesti. Myös näillä henkilöryhmillä tulee olla tarve tietoon ja heille tulee selvittää turvallisuusvelvoitteet.

Turvallisuussääntöjen E liitteen 6 kohdassa määritellään Naton turvallisuusluokat ja niiden merkitseminen. Liitteen 32-39 kohdassa määritellään tietoturvapoikkeama, tietoturvaloukkaus, tiedon vaarantuminen ja vähäinen tietoturvapoikkeama ja niitä koskevat selvitys- ja raportointivelvollisuudet. Rikkomusten selvittämisestä ja niistä ilmoittamisesta säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ssä.

Turvallisuussääntöjen F liite sisältää tietoaineistoturvallisuutta koskevat määräykset. Turvallisuussääntöjen F liitteen 3 kohta koskee tietojärjestelmien akkreditointivelvoitetta. Tietojärjestelmien arvioinnista säädetään laissa viranomaisten tietojärjestelmien arvioinnista. Lain 8 §:n mukaan valtioneuvoston asetuksella voidaan säätää, että 8 §:ssä tarkoitettu todistus on hankittava sellaisen valtionhallinnon viranomaisen määräysvallassa olevasta tietojärjestelmästä tai tietoliikennejärjestelystä, jossa käsitellään turvallisuusluokkaan I tai II kuuluviksi luokiteltuja asiakirjoja. Liitteen 13.4 koskee NCSA:n tehtäviä. Suomen turvallisuusviranomaisista ja niiden tehtävistä säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:ssä, jonka mukaan Liikenne- ja viestintävirasto toimii NSA:n asiantuntijana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa.

Turvallisuussääntöjen G liitteen 4 kohta sisältää vaatimuksen yritysturvallisuusselvitystodistuksesta, kun yritys käsittelee turvallisuusluokkaan CONFIDENTIAL tai sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa. Liitteen 10 kohta sisältää yritykselle asetettavan sopimusvelvoitteen luokitellun tiedon suojaamisesta. Yritysturvallisuusselvityksistä säädetään turvallisuusselvityslain 5 luvussa ja kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 §:ssä.

14.2 Käsittelyjärjestys

Tietoturvallisuudesta Pohjois-Atlantin liiton osapuolten välillä tehdyssä sopimuksessa määritellään Naton tietoturvallisuutta koskevat säännöt, joiden mukaan Naton jäsenmaiden tulee käsitellä turvallisuusluokiteltua tietoa. Kyse olisi erityissääntelystä suhteessa kansallisten viranomaisten asiakirjojen julkisuutta koskevaan yleislainsäädäntöön. Perustuslain 12 §:n mukaan viranomaisen asiakirjat ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Tietoturvallisuussopimus sisältää tällaisia perustuslain 12 §:n tarkoittamia sääntöjä, joilla julkisuutta rajoitetaan välttämättömien syiden vuoksi.

Kansainväliset tietoturvallisuussopimukset ovat vakiintunut tapa säännellä turvaluokiteltujen tietojen vaihtoa Suomen ja jonkin toisen valtion tai kansainvälisen järjestön välillä. Suomella on tällä hetkellä voimassa yhteensä 26 tietoturvallisuussopimusta, jotka eduskunta on hyväksynyt yksinkertaisella äänten enemmistöllä ja käsitellyt niiden voimaansaattamislait tavallisen lain säätämisjärjestyksessä. Perustuslakivaliokunta on katsonut lausunnossaan PeVL 39/1997 vp käsitellessään Suomen ja Länsi-Euroopan unionin (WEU) välistä tietoturvallisuussopimusta (ei enää voimassa), että julkisuusperiaatteen rajoittamista sopimuksen ja voimaansaattamislain 2 §:n mukaisesti voitiin pitää välttämättömänä Suomen ja WEUn yhteistyön mahdollistamisen kannalta. Salassapitointressi vastasi myös niitä perusteita, jotka mainittiin tuolloin voimassa olleen yleisten asiakirjain julkisuudesta annetun lain (83/1951) 9 §:ssä. Sopimuksen voimaansaattamislaki voitiin käsitellä tavallisen lain säätämisjärjestyksessä. Sen jälkeen on säädetty niin ikään tavallisen lain säätämisjärjestyksessä laki kansainvälisistä tietoturvallisuusvelvoitteista, jossa säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi.

Suomen ja Naton välillä vuonna 2012 tehty hallinnollinen järjestely turvallisuusluokitellun tiedon suojaamisesta on hyväksytty yksinkertaisella äänten enemmistöllä ja sen voimaansaattamislaki on säädetty tavallisen lain säätämisjärjestyksessä. Samassa yhteydessä saatettiin voimaan tavallisen lain säätämisjärjestyksessä vuonna 1994 Suomen ja Naton välillä tehdyn sopimuksen lainsäädännön alaan kuuluvat määräykset. Hallituksen esityksen mukaan eduskunnan hyväksyttävänä olleen hallinnollisen järjestelyn 5 artiklan määräykset eivät laajentaneet salassapitovelvollisuutta siitä, mitä salassapidosta on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun 6 §:ssä (HE 139/2012 vp).

Nyt käsiteltävänä olevalla tietoturvallisuussopimuksella sitoudutaan noudattamaan vastaavia tietoturvallisuusvelvoitteita, joihin Suomi on jo vuonna 1994 tehdyllä tietoturvallisuussopimuksella ja 2012 tehdyllä hallinnollisella järjestelyllä sitoutunut. Tietoturvallisuussopimuksen velvoitteiden voidaan katsoa olevan välttämättömiä rajoituksia julkisuudesta Pohjois-Atlantin sopimuksessa tarkoitetun yhteistyön mahdollistamiseksi.

Nyt hyväksyttävänä olevan sopimuksen 2 artiklan mukaan osapuolet laativat ja panevat täytäntöön turvallisuusvaatimuksia, joilla varmistetaan turvallisuusluokitellun tiedon yhteinen suojauksen taso. Edellä jaksossa 8.2. kuvataan näitä tietoturvallisuussopimuksen täytäntöönpanoa koskevia määräyksiä. Turvallisuussäännöstössä on oikeudellisesti kyse tietoturvasopimuksen toteutumista turvaavista teknisistä määräyksistä.

Suomen perustuslakia on muutettu vuonna 2012 siten, että perustuslain 94 §:n 2 momentin ja 95 §:n 2 momentin säännösten mukaan Suomen täysivaltaisuuden kannalta *merkittävän* toimivallan siirrosta Euroopan unionille, kansainväliselle järjestölle tai kansainväliselle toimielimelle päätetään kahden kolmasosan enemmistöllä. Sen sijaan tavallisella ääntenenemmistöllä voidaan päättää muuta kuin merkittävää toimivallan siirtoa koskevien kansainvälisten velvoitteiden hyväksymisestä ja voimaansaattamisesta.

Perustuslain muuttamista koskevassa hallituksen esityksessä todetaan, että eduskunnan toimivallan siirroissa on tavanomaisesti kyse sellaisista kansainvälisistä sopimusjärjestelyistä, joissa siirretään vähäisessä määrin säädösvaltaa kansainväliselle toimielimelle varsin teknisluonteisessa sääntelyssä tai hyvin rajatuilla aloilla, ja että tällaisen toimivallan siirtämisestä voitaisiin vastaisuudessa päättää tavallisella enemmistöllä (HE 60/2010 vp, s.28).

Sopimuksen 2 artiklassa delegoidaan turvallisuusvaatimuksia koskevaa sopimuksentekotoimivaltaa Pohjois-Atlantin neuvostolle. Kyseessä ei olisi kuitenkaan perustuslain täysivaltaisuussääntelyn kannalta merkittävä sopimuksentekovallan delegointi vaan nykyaikaisessa kansainvälisessä yhteistoiminnassa tavanomainen sopimuksen täytäntöönpanon tarkempi sääntely, josta Pohjois-Atlantin sopimuksen osapuolet päättävät konsensuksella. Tietoturvallisuutta koskevia määräyksiä sovelletaan pääosin viranomaisissa. Yrityksille niillä on merkitystä silloin, jos ne osallistuvat turvallisuusluokiteltuun sopimukseen, joka sisältää Naton turvallisuusluokitellun tiedon käsittelyä. Yksityisille ihmisille sopimuksella ja tietoturvallisuussäännöstöllä on lähinnä välillistä merkitystä.

Perustuslakivaliokunta on katsonut, että lainsäädännön alaan kuuluvien teknisluonteisten täytäntöönpanomääräysten antaminen ei ole ollut ongelmallista, mutta siltä osin kuin ne ovat kuuluneet lainsäädännön alaan, on valiokunta edellyttänyt pääsääntöisesti niiden voimaan saattamista ja julkaisemista (PeVL 19/2010 vp, s. 5 ja 6). Asiakirjaan C-M(2002)49-REV1 sisältyvät Naton turvallisuussäännöt sisältävät joitakin, edellä jaksossa 14.1. kuvattuja lainsäädännön alaan kuuluvia määräyksiä, jotka eivät ilmene suoraan tietoturvallisuussopimuksen tekstistä. Sellaisille määräyksille pyydetään eduskunnan hyväksyminen, ne on sisällytetty sopimuksen voimaansaattamislakiin ja turvallisuussäännöt julkaistaan yhdessä Naton turvallisuussopimuksen kanssa Suomen säädöskokoelman sopimussarjassa. Jatkossa turvallisuussääntöjen muutoksista julkaistaisiin sopimussarjassa Suomen säädöskokoelmasta annetun lain (188/2000) 9 §:n 2 momentin mukainen ilmoitus.

Koska tietoturvallisuudesta Pohjois-Atlantin liiton osapuolten välillä tehty sopimus ja turvallisuussäännöt eivät sisällä määräyksiä, jotka koskisivat perustuslakia sen 94 §:n 2 momentissa tai 95 §:n 2 momentissa tarkoitetulla tavalla, sopimus ja turvallisuussäännöt voidaan hallituksen käsityksen mukaan hyväksyä äänten enemmistöllä ja ehdotus niiden voimaansaattamislaiksi tavallisen lain säätämisjärjestyksessä.

Perustuslakivaliokunnan ja ulkoasianvaliokunnan kannan mukaan kansainvälisen velvoitteen irtisanomista koskeva päätös voidaan tehdä yksinkertaisella äänten enemmistöllä (PeVM 10/1998 vp ja UaVL 6/1998 vp). Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen irtisanomisen hyväksymisestä voidaan päättää äänten enemmistöllä ja laki kyseisten sopimusten lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain kumoamisesta voidaan hyväksyä tavallisen lain säätämisjärjestyksessä.

1. ponsi

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

että eduskunta hyväksyisi tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä Brysselissä 6.3.1997 tehdyn sopimuksen ja sen nojalla annetut turvallisuussäännöt sellaisina kuin ne ovat muutettuina 20.11.2020 hyväksytyssä asiakirjassa C-M(2002)49-REV1 ja

että eduskunta hyväksyisi Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi Helsingissä 3.7.2012 tehdyn hallinnollisen järjestelyn sekä Pohjois-Atlantin liiton kanssa Brysselissä 22.9.1994 tehdyn tietoturvallisuussopimuksen (SopS 7 ja 8/2013) irtisanomisen.

2. ponsi

Koska sopimukset sisältävät määräyksiä, jotka kuuluvat lainsäädännön alaan, annetaan samalla eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

1.

Laki

tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdystä sopimuksesta ja turvallisuussäännöistä

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä Brysselissä 6 päivänä maaliskuuta 1997 tehdyn sopimuksen ja sen nojalla annettujen turvallisuussääntöjen, sellaisina kuin ne ovat muutettuina 20 päivänä marraskuuta 2020 hyväksytyssä asiakirjassa C-M(2002)49-REV1, lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

2 §

Sopimuksen ja turvallisuussääntöjen muiden kuin lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta säädetään valtioneuvoston asetuksella.

3 §

Tämän lain voimaantulosta säädetään valtioneuvoston asetuksella.

———

2.

Laki

Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain kumoamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tällä lailla kumotaan Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetu laki (945/2012).

2 §

Tämän lain voimaantulosta säädetään valtioneuvoston asetuksella.

———

Helsingissä 17.5.2023

Pääministeri

Sanna Marin

Ulkoministeri Pekka Haavisto

SOPIMUS POHJOIS-ATLANTIN SOPIMUKSEN OSAPUOLTEN VÄLILLÄ TIETOTURVALLISUUDESTA

Washingtonissa 4 päivänä huhtikuuta 1949 allekirjoitetun Pohjois-Atlantin sopimuksen osapuolet, jotka

vahvistavat, että tehokas poliittinen neuvottelu, yhteistyö ja suunnittelu puolustusasioissa sopimuksen tavoitteiden saavuttamiseksi edellyttävät turvallisuusluokitellun tiedon vaihtamista osapuolten välillä,

katsovat, että Pohjois-Atlantin sopimuksen osapuolten hallitusten välillä tarvitaan määräyksiä sellaisen turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja turvaamisesta, jota ne voivat vaihtaa keskenään,

ymmärtävät, että turvallisuusvaatimuksille ja menettelyille tarvitaan yleiset puitteet, ja

toimivat omasta puolestaan ja Pohjois-Atlantin liiton puolesta,

ovat sopineet seuraavasta:

1 artikla

Osapuolet

i. suojaavat ja turvaavat

a. turvallisuusluokitelluksi merkityn turvallisuusluokitellun tiedon (katso liite I), jonka alkuperäinen luovuttaja on Nato (katso liite II) tai jonka jäsenvaltio toimittaa Natolle,

b. jäsenvaltioiden turvallisuusluokitelluksi merkityn turvallisuusluokitellun tiedon, joka toimitetaan toiselle jäsenvaltiolle Naton ohjelman, hankkeen tai sopimuksen tueksi,

AGREEMENT BETWEEN THE PARTIES TO THE NORTH ATLANTIC TREATY FOR THE SECURITY OF INFORMATION

The Parties to the North Atlantic Treaty, signed at Washington on 4th April, 1949.

Reaffirming that effective political consultation, cooperation and planning for defence in achieving the objectives of the Treaty entail the exchange of classified information among the Parties.

Considering that provisions between the Governments of the Parties to the North Atlantic Treaty for the mutual protection and safeguarding of the classified information they may interchange are necessary.

Realising that a general framework for security standards and procedures is required.

Acting on their own behalf and on behalf of the North Atlantic Treaty Organization,

have agreed as follows:

Article 1

The Parties shall:

(i) protect and safeguard:

(a) classified information (see Annex I), marked as such, which is originated by NATO (see Annex II) or which is submitted to NATO by a member state;

(b) classified information, marked as such, of the member states submitted to another member state in support of a NATO programme, project, or contract,

ii. säilyttävät edellä i alakohdassa määritellyn tiedon turvallisuusluokituksen ja pyrkivät kaikin keinoin turvaamaan tiedon tämän mukaisesti;

(ii) maintain the security classification of information as defined under (i) above and make every effort to safeguard it accordingly;

iii. eivät käytä edellä i alakohdassa määriteltyä turvallisuusluokiteltua tietoa muihin kuin Pohjois-Atlantin sopimuksessa ja siihen liittyvissä päätöksissä ja päätöslauselmissa määrättyihin tarkoituksiin;

(iii) not use classified information as defined under (i) above for purposes other than those laid down in the North Atlantic Treaty and the decisions and resolutions pertaining to that Treaty;

iv. eivät ilmaise edellä i alakohdassa määriteltyä tietoa Natoon kuulumattomille osapuolille ilman tiedon alkuperäisen luovuttajan suostumusta.

(iv) not disclose such information as defined under (i) above to non-NATO Parties without the consent of the originator.

2 artikla

Article 2

Tämän sopimuksen 1 artiklan mukaisesti osapuolet varmistavat kansallisen turvallisuusviranomaisen perustamisen Naton toimintaa varten toteuttamaan suojaavia turvatoimia. Osapuolet laativat ja panevat täytäntöön turvallisuusvaatimuksia, joilla varmistetaan turvallisuusluokitellun tiedon yhteinen suojaustaso.

Pursuant to Article 1 of this Agreement, the Parties shall ensure the establishment of a National Security Authority for NATO activities which shall implement protective security measures. The Parties shall establish and implement security standards which shall ensure a common degree of protection for classified information.

3 artikla

Article 3

1. Osapuolet varmistavat, että kaikista niiden kansalaisista, jotka virallisia tehtäviään hoitaessaan tarvitsevat tai saattavat saada pääsyn turvallisuusluokkaan CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon, tehdään asianmukaisesti turvallisuusselvitys ennen kuin he ottavat tehtävänsä vastaan.

(1) The Parties shall ensure that all persons of their respective nationality who, in the conduct of their official duties, require or may have access to information classified CONFIDENTIAL and above are appropriately cleared before they take up their duties.

2. Turvallisuusselvitysmenettelyt suunnitellaan sellaisiksi, että niillä pystytään selvittämään, voiko henkilö hänen lojaliteettinsa ja luotettavuutensa huomioon ottaen saada pääsyn turvallisuusluokiteltuun tietoon ilman, että siitä aiheutuu turvallisuusriski, jota ei voida hyväksyä.

(2) Security clearance procedures shall be designed to determine whether an individual can, taking into account his or her loyalty and trustworthiness, have access to classified information without constituting an unacceptable risk to security.

3. Osapuolet tekevät pyydettäessä yhteistyötä muiden osapuolten kanssa niiden turvallisuusselvitysmenettelyjä suoritettaessa.

(3) Upon request, each of the Parties shall cooperate with the other Parties in carrying out their respective security clearance procedures.

4 artikla

Pääsihteeri varmistaa, että Nato soveltaa tämän sopimuksen kulloinkin sovellettavia määräyksiä (katso liite III).

Article 4

The Secretary General shall ensure that the relevant provisions of this Agreement are applied by NATO (see Annex III).

5 artikla

Tämä sopimus ei millään tavoin estä osapuolia tekemästä muita sopimuksia, jotka liittyvät niiden luovuttaman turvallisuusluokitellun tiedon vaihtamiseen eivätkä vaikuta tämän sopimuksen soveltamisalaan.

Article 5

The present Agreement in no way prevents the Parties from making other Agreements relating to the exchange of classified information originated by them and not affecting the scope of the present Agreement.

6 artikla

a. Tämä sopimus on avoinna allekirjoittamista varten Pohjois-Atlantin sopimuksen osapuolille, ja se ratifioidaan tai hyväksytään. Ratifioimis- tai hyväksymiskirjat talletetaan Amerikan yhdysvaltojen hallituksen huostaan.

Article 6

(a) This Agreement shall be open for signature by the Parties to the North Atlantic Treaty and shall be subject to ratification, acceptance or approval. The instruments of ratification, acceptance or approval shall be deposited with the Government of the United States of America;

b. Tämä sopimus tulee voimaan kolmenkymmenen päivän kuluttua päivästä, jona kaksi allekirjoittajavaltiota on tallettanut ratifioimis- tai hyväksymiskirjansa. Sopimus tulee voimaan kunkin muun allekirjoittajavaltion osalta kolmenkymmenen päivän kuluttua kunkin valtion ratifioimis- tai hyväksymiskirjan tallettamisesta.

(b) This Agreement shall enter into force thirty days after the date of deposit by two signatory States of their instruments of ratification, acceptance or approval. It shall enter into force for each other signatory State thirty days after the deposit of its instrument of ratification, acceptance or approval;

c. Niiden osapuolten suhteen, joiden osalta tämä sopimus on tullut voimaan, sopimus korvaa Pohjois-Atlantin liiton osapuolten turvallisuussopimuksen, jonka Pohjois-Atlantin neuvosto hyväksyi asiakirjan D.C.2/7 liitteessä olevan lisäyksen liitteessä A (1 kohta) 19 päivänä huhtikuuta 1952 ja joka myöhemmin sisällytettiin Pohjois-Atlantin neuvoston 2 päivänä maaliskuuta 1955 hyväksymän asiakirjan C-M (55) 15 (final) liitteeseen A (1 kohta).

(c) This Agreement shall with respect to the Parties for which it entered into force supersede the "Security Agreement by the Parties to the North Atlantic Treaty Organization" approved by the North Atlantic Council in Annex A (paragraph 1) to Appendix to Enclosure to D.C.2/7, on 19th April, 1952, and subsequently incorporated in Enclosure "A" (paragraph 1) to C-M(55)15(Final), approved by the North Atlantic Council on 2nd March, 1955.

7 artikla

Tämä sopimus on avoinna liittymistä varten Pohjois-Atlantin sopimuksen uudelle osapuolelle sen valtiosäännön mukaisten menettelyjen mukaisesti. Tämän osapuolen liit-

Article 7

This Agreement shall remain open for accession by any new Party to the North Atlantic Treaty, in accordance with its own constitutional procedures. Its instrument of

tymiskirja talletetaan Amerikan yhdysvaltojen hallituksen huostaan. Sopimus tulee voimaan kunkin liittyvän valtion osalta kolmenkymmenen päivän kuluttua sen liittymiskirjan tallettamispäivästä.

8 artikla

Amerikan yhdysvaltojen hallitus ilmoittaa muiden osapuolten hallituksille kunkin ratifioimis-, hyväksymis- tai liittymiskirjan tallettamisesta.

9 artikla

Osapuoli voi irtisanoa tämän sopimuksen antamalla kirjallisen irtisanomisilmoituksen tallettajalle, joka ilmoittaa irtisanomisilmoituksesta kaikille muille osapuolille. Irtisanominen tulee voimaan vuoden kuluttua siitä, kun tallettaja on vastaanottanut ilmoituksen, mutta ei vaikuta niihin velvoitteisiin, oikeuksiin tai valtaoikeuksiin, joita osapuolet ovat aiemmin sopineet tai saaneet tämän sopimuksen määräysten perusteella.

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

Tehty Brysselissä 6 päivänä maaliskuuta 1997 yhtenä englannin- ja ranskankielisenä kappaleena, jonka kaikki tekstit ovat yhtä todistusvoimaiset, joka talletetaan Amerikan yhdysvaltojen hallituksen arkistoon ja josta tämä hallitus toimittaa oikeaksi todistetut jäljennökset kaikille muille allekirjoittajille.

accession shall be deposited with the government of the United States of America. It shall enter into force in respect of each acceding State thirty days after the day of the deposit of its instrument of accession.

Article 8

The Government of the United States of America shall inform the Governments of the other Parties of the deposit of each instrument of ratification, acceptance, approval or accession.

Article 9

This Agreement may be denounced by written notice of denunciation by any Party given to the depository which shall inform all the other Parties of such notice. Such denunciation shall take effect one year after receipt of notification by the depository, but shall not affect obligations already contracted and the rights or prerogatives previously acquired by the Parties under the provisions of this Agreement.

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

Done in Brussels, this 6th day of March, 1997 in a single copy in the English and French languages, each text being equally authoritative, which shall be deposited in the archives of the Government of the United States of America and of which certified copies shall be transmitted by that Government to each of the other signatories.

Liite I

Tämä liite on sopimuksen erottamaton osa.

Naton turvallisuusluokiteltu tieto määritellään seuraavasti:

a. "tieto" tarkoittaa missä tahansa muodossa välitettävää tietoa;

Annex I

This Annex forms an integral part of the Agreement.

NATO classified information is defined as follows:

(a) information means knowledge that can be communicated in any form;

b. turvallisuusluokiteltu tieto tarkoittaa tietoa tai aineistoa, jonka katsotaan edellyttävän suojaamista luvattomalta paljastamiselta ja joka on turvallisuusluokituksella osoitettu sellaiseksi;

(b) classified information means information or material determined to require protection against unauthorized disclosure which has been so designated by security classification;

c) ”aineisto” sisältää asiakirjat ja myös valmistetut ja valmisteilla olevat koneet, laitteet ja aseet;

(c) the word "material" includes documents and also any item of machinery or equipment or weapons either manufactured or in the process of manufacture;

d) ”asiakirja” tarkoittaa mitä tahansa tallennettua tietoa riippumatta sen fyysisestä muodosta tai ominaisuuksista, mukaan lukien kirjalliset ja painotuotteet; tietojenkäsittelyssä käytettävät kortit ja nauhat; kartat, kaaviot, valokuvat, maalaukset, piirustukset, kaiverrukset, luonnokset, työmuistiinpanot ja –paperit, hiilipaperikopiot ja värinauhat; millä tahansa keinolla tai menettelyllä tehdyt jäljennökset; kaikenlaiset ääni-, puhe- ja magneettitallenteet sekä elektroniset, optiset ja videotallenteet; kannettavat atk-laitteet, joissa on kiinteät tallennusvälineet, ja irrotettavat tietokoneen tallennusvälineet, mutta ei rajoittuen näihin.

(d) the word "document" means any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions by an means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable ADP equipment with resident computer storage media, and removable computer storage media.

Liite II

Tämä liite on sopimuksen erottamaton osa.

Tässä sopimuksessa ”Nato” tarkoittaa Pohjois-Atlantin liittoa ja niitä elimiä, joihin sovelletaan joko Ottawassa 20 päivänä syyskuuta 1951 allekirjoitettua sopimusta Pohjois-Atlantin liiton, kansallisten edustajien ja kansainvälisen henkilöstön asemasta tai Pariisissa 28 päivänä elokuuta 1952 allekirjoitettua pöytäkirjaa Pohjois-Atlantin sopimuksen mukaisesti perustettujen kansainvälisten sotilasesikuntien asemasta.

Annex II

This Annex forms an integral part of the Agreement.

For the purposes of the present Agreement, the term "NATO" denotes the North Atlantic Treaty Organization and the bodies governed either by the Agreement on the status of the North Atlantic Treaty Orgnization, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952.

Liite III

Tämä liite on sopimuksen erottamaton osa.

Annex III

This Annex forms an integral part of the Agreement.

Sotilaskomentajien kanssa neuvotellaan heidän valtaoikeuksiensa kunnioittamiseksi.	Consultation takes place with military commanders in order to respect their prerogatives.

20. marraskuuta 2020 ASIAKIRJA C-M(2002)49-REV1

TURVALLISUUS POHJOIS-ATLANTIN LIITOSSA (NATO)

Pääsihteerin ilmoitus
Kesäkuun 17. päivänä 2002 päivätyn asiakirjan C-M(2002)49 ensimmäinen tarkistus

Viite: Asiakirja C-M(2002)49-COR1–COR12 (konsolidoitu toisinto), päivätty 17. kesäkuuta 2002

1. Tämä asiakirja perustuu Naton turvallisuussäännöstön ja sitä tukevien ohjeiden merkittävään ja kokonaisvaltaiseen tarkistukseen sellaisena kuin turvallisuuskomitea on sen hyväksynyt.

2. Asiakirjalla C-M(2002)49-REV1, joka korvaa viitteessä mainitun asiakirjan, tehdään viiteasiakirjaan sekä rakenteellisia että sisällöllisiä muutoksia.

3. Rakennetta on muutettu lisäämällä uusi liite H, jossa käsitellään erikseen turvallisuutta suhteissa Naton ulkopuolisiin toimijoihin. Samaa aihetta käsitellään lisää äskettäin laaditussa Naton direktiivissä turvallisuudesta suhteissa Naton ulkopuolisiin toimijoihin (asiakirja AC/35-D/2006) sekä tätä direktiiviä tukevassa Naton ulkopuolisille toimijoille tarkoitetussa tarkistetussa asiakirjassa, joka käsittelee turvallisuutta suhteissa Natoon (asiakirja AC/35-D/1038-REV3).

4. Sisällön osalta tarkistuksella on muutettu osiota "Perusperiaatteet, vähimmäisvaatimukset ja vastuut" (liite B) sekä määräyksiä osioissa "Henkilöstöturvallisuus", "Toimitilaturvallisuus", "Tietoaineistoturvallisuus" ja "Turvallisuus suhteissa Naton ulkopuolisiin toimijoihin" (liitteet B, C, D, E ja H). Tarkistuksella ei ole muutettu asiakirjan C-M(2002)49 liitteitä F ja G.

(Allekirjoitus) Jens Stoltenberg

20 November 2020 DOCUMENT C-M(2002)49-REV1

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION (NATO)

Note by the Secretary General
Revision 1 to C-M(2002)49 dated 17 June 2002

Reference: C-M(2002)49-COR1 to COR12 (consolidated version), dated 17 June 2002

1. This document is the result of a major and comprehensive review of the NATO Security Policy and its supporting directives, as approved by the Security Committee.

2. C-M(2002)49-REV1, which replaces the document at reference, introduces both structural and content changes.

3. The structure has changed with the addition of a new Enclosure H to address specifically security in relation to non-NATO entities. This topic is developed further into the newly developed Directive for NATO on Security in Relation to Non-NATO Entities (reference AC/35-D/2006) and the revised Supporting Document for Non-NATO Entities on Security in Relation to NATO (reference AC/35-D/1038-REV3).

4. In terms of content, this revision has addressed Basic Principles, Minimum Standards and Responsibilities (Enclosure B), as well as provisions of Personnel Security, Physical Security, Security of Information and Security in Relation to Non NATO Entities (Enclosures B, C, D, E and H). Enclosures F and G to C-M(2002)49 were not subject to this review.

(Signed) Jens Stoltenberg

Liite 1
Liitteen 1 liitteet A, B, C, D, E, F, G, H
Sanasto

1 Annex
Enclosures A,B,C,D,E,F,G,H
1 Glossary

Alkuperäinen: Englanti

Original: English

TURVALLISUUS POHJOIS-ATLANTIN LIITOSSA (NATO)

JOHDANTO

1. Tässä C-M-asiakirjassa, jonka otsikkona on "Turvallisuus Pohjois-Atlantin liitossa (Nato)", kuvataan ne turvallisuuden perusperiaatteet ja vähimmäisvaatimukset, joita Naton jäsenvaltioiden ja Naton sotilas- ja siviilielinten on sovellettava varmistaakseen turvallisuusluokitellun tiedon yhteisen suojaustason. Naton turvallisuusmenettelyt toimivat parhaaksi eduksi vain, jos ne perustuvat niitä tukevaan kansalliseen turvallisuusjärjestelmään, joka on ominaisuuksiltaan näissä periaatteissa määritettyjen ominaisuuksien mukainen tai niitä vastaava. Lisäksi näissä periaatteissa käsitellään Naton sisäisiä turvallisuusrooleja, -tehtäviä ja -vastuita.

2. Tämä periaateasiakirja koostuu liitteessä A olevasta turvallisuussopimuksesta, jonka nimi on "sopimus Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta", sekä seuraavista liitteistä:

(a) Liite A – Sopimus Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta

(b) Liite B – Perusperiaatteet, vähimmäisvaatimukset ja vastuut

(c) Liite C – Henkilöstöturvallisuus

(d) Liite D – Toimitilaturvallisuus

(e) Liite E – Naton turvallisuusluokitellun tiedon turvallisuus

(f) Liite F – Viestintä- ja tietojärjestelmien turvallisuus

(g) Liite G – Turvallisuusluokiteltujen hankkeiden turvallisuus ja yritysturvallisuus

(h) Liite H – Turvallisuus suhteissa Naton ulkopuolisiin toimijoihin.

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION (NATO)

INTRODUCTION

1. This C-M, entitled Security Within the North Atlantic Treaty Organization (NATO), establishes the basic principles and minimum standards of security to be applied by NATO Nations and NATO Civil and Military bodies in order to ensure a common degree of protection for classified information. NATO security procedures only operate to the best advantage when they are based upon and supported by a national security system having the characteristics equivalent/conformant to those set out in this policy. In addition, this policy also addresses the security roles, functions and responsibilities within NATO.

2. This policy document consists of the Security Agreement at Enclosure “A” entitled “Agreement between the Parties to the North Atlantic Treaty for the Security of Information” together with the following additional Enclosures:

(a) Enclosure A – Agreement between the parties to NATO for the Security of Information

(b) Enclosure B – Basic Principles, Minimum Standards and Responsibilities.

(c) Enclosure C – Personnel Security.

(d) Enclosure D – Physical Security.

(e) Enclosure E – Security of NATO Classified Information.

(f) Enclosure F – Communication and Information System Security.

(g) Enclosure G – Classified Project and Industrial Security.

(h) Enclosure H – Security in relation to non-NATO entities.

3. Tämä periaateasiakirja tukee Naton tiedonhallinnan periaatteita (C-M(2007)0118). Naton turvallisuusluokittelemattoman tiedon hallinnan periaatteita koskevassa asiakirjassa C-M(2002)60 käsitellään niitä perusperiaatteita ja vaatimuksia, joita Naton sotilas- ja siviilielimissä sekä Naton jäsenvaltioissa sovelletaan Naton turvallisuusluokittelemattoman tiedon (NATO UNCLASSIFIED ja julkinen tieto) suojaamiseksi.

3. This policy document supports the NATO Information Management Policy (C-M(2007)0118). The Policy on Management of Non-Classified NATO Information (C-M(2002)60) addresses the basic principles and standards to be applied within NATO Civil and Military bodies and NATO Nations for the protection of Non-Classified NATO information (NATO UNCLASSIFIED and Information releasable to the Public).

TAVOITTEET JA PÄÄMÄÄRÄT

4. Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet varmistavat tässä C-M-asiakirjassa kuvattujen perusperiaatteiden ja vähimmäisvaatimusten soveltamisen, jotta Naton turvallisuusluokitellun tiedon luottamuksellisuuden, eheyden ja käytettävyyden säilyminen turvataan.

AIMS AND OBJECTIVES

4. NATO Nations and NATO Civil and Military bodies shall ensure that the basic principles and minimum standards of security set forth in this C-M are applied to safeguard NATO Classified Information from loss of confidentiality, integrity and availability.

5. Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet laativat turvallisuusohjelmat, jotka täyttävät nämä perusperiaatteet ja vähimmäisvaatimukset, jotta Naton turvallisuusluokitellulle tiedolle varmistetaan yhteinen suojaustaso.

5. NATO Nations and NATO Civil and Military bodies shall establish security programmes that meet these basic principles and minimum standards to ensure a common degree of protection for NATO Classified Information.

SOVELTAMISALA

6. Näitä perusperiaatteita ja vähimmäisvaatimuksia sovelletaan seuraaviin:

(a) Natosta peräisin oleva turvallisuusluokiteltu tieto;

(b) Naton jäsenvaltiosta peräisin oleva turvallisuusluokiteltu tieto, joka annetaan Natolle tai toiselle Naton jäsenvaltiolle Naton ohjelman, hankkeen tai sopimuksen tueksi;

(c) Naton ja Naton ulkopuolisten toimijoiden[1] välillä vaihdettava turvallisuusluokiteltu tieto; ja

APPLICABILITY

6. These basic principles and minimum standards shall be applied to:

(a) classified information originated by NATO;

(b) classified information originated by a NATO Nation which is provided to NATO or provided to another NATO Nation in support of a NATO programme, project, or contract;

(c) classified information exchanged between NATO and non-NATO entities (NNE)[1]; and

[1] Naton ulkopuoliset valtiot ja muut Naton ulkopuoliset elimet (esim. kansainväliset järjestöt), mukaan lukien näitä valtioita ja elimiä edustavat luonnolliset henkilöt.

[1] Non-NATO nations, and other non-NATO bodies (e.g. International Organizations) including individuals representing such nations or bodies.

(d) hallituksen (tai Naton sotilas- tai siviilielimen) ulkopuolisille luonnollisille henkilöille ja organisaatioille, kuten konsulteille, yrityksille ja yliopistoille, annettava turvallisuusluokiteltu tieto.

7. ATOMAL-tietoon pääsyyn ja sen suojaamiseen sovelletaan sopimusta Pohjois-Atlantin sopimuksen osapuolten välillä ydinpuolustustietoja koskevasta yhteistyöstä (C-M(64)39). Jotta varmistetaan asianmukainen ATOMAL-tietoon pääsyn valvonta sekä tämän tiedon asianmukainen käsittely ja suojaaminen, sovelletaan hallinnollisia järjestelyjä ydinpuolustustietoja koskevasta yhteistyöstä tehdyn Pohjois-Atlantin sopimuksen osapuolten välisen sopimuksen täytäntöön panemiseksi (C-M(68)41).

8. Yhdysvaltojen yhteistä operaatiosuunnitelmaa (US-SIOP) koskevaan tietoon pääsyyn ja sen suojaamiseen sovelletaan määräyksiä, jotka on annettu asiakirjassa C-M(71)27 (uudistettu) erityismenettelyistä Yhdysvaltojen yhteistä operaatiosuunnitelmaa (US-SIOP) koskevan tiedon käsittelemiseksi Natossa.

9. Signaalitiedusteluun (SIGINT) liittyvien tietojen, toimintojen, lähteiden ja menetelmien arkaluonteisuuden vuoksi on sovellettava tiukkoja turvallisuusmääräyksiä ja -menettelyjä, jotka usein menevät tämän C-M-asiakirjan määräyksiä ja menettelyjä pidemmälle. Siksi SIGINT-tietoihin, -toimintoihin, -lähteisiin ja -menetelmiin pääsyyn ja niiden suojaamiseen sovelletaan kansallisia määräyksiä sekä asiakirjan MC 101 (Naton signaalitiedustelun periaatteet) ja siihen liittyvän liittokunnan yhteisen AJP-julkaisun sekä Naton signaalitiedustelun neuvoa-antavan komitean (NACSI) SIGINT-hallinnon ja -menettelyjen oppaan määräyksiä.

ASEMA

10. Pohjois-Atlantin neuvosto (NAC) on hyväksynyt tämän asiakirjan, jolla pannaan täytäntöön sopimus Pohjois-Atlantin sopi-

(d) classified information entrusted to individuals and organizations outside a government (or a NATO Civil or Military body), e.g. consultants, industry, universities.

7. Access to, and the protection of, ATOMAL information are subject to the Agreement between the Parties to the North Atlantic Treaty for Co-operation Regarding Atomic Information (C-M(64)39). The Administrative Arrangements to implement the Agreement between the Parties to the North Atlantic Treaty for Co-operation Regarding ATOMAL Information (C-M(68)41) shall be applied to ensure appropriate access control, handling and protection of such information.

8. Access to, and protection of, US-SIOP information are subject to the provisions of C-M(71)27(Revised), "Special Procedures for the Handling of United States Single Integrated Operational Plan (US-SIOP) Information within NATO".

9. The sensitive nature of Signals Intelligence (SIGINT) information, operations, sources and methods require the application of stringent security regulations and procedures often beyond those set forth in this C-M. Therefore, access to and protection of, SIGINT information, operations, sources and methods are subject to national regulations and the provisions laid down in MC 101 (NATO Signals Intelligence Policy) its companion Allied Joint Publication (AJP) and the NATO Advisory Committee on Signals Intelligence (NACSI) Guide to SIGINT Administration and Procedures.

AUTHORITY

10. The North Atlantic Council (NAC) has approved this document which implements the Agreement Between the Parties to the North Atlantic Treaty for the Security of Information (reproduced at Enclosure “A”),

muksen osapuolten välillä tietoturvallisuudesta (liitteenä A) ja siten vahvistetaan Naton turvallisuusperiaatteet.[2]

and thereby establishes NATO Security Policy.[2]

[2] Turvallisuuskomitean työjärjestyksen (C-M(2015)0002) mukaan Naton turvallisuusperiaatteet koostuvat asiakirjoista C-M(2002)49 ja C-M(2002)50.

[2] Per Terms of reference for the Security Committee (C-M(2015)0002) NATO Security Policy consists of C-M(2002)49 and C-M(2002)50.

LIITE ”B”
PERUSPERIAATTEET, VÄHIMMÄISVAATIMUKSET JA VASTUUT

PERUSPERIAATTEET

1. Sovelletaan seuraavia perusperiaatteita:

(a) Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet varmistavat tässä C-M-asiakirjassa sovittujen vähimmäisvaatimusten noudattamisen, jotta osapuolten kesken vaihdettavalle turvallisuusluokitellulle tiedolle varmistetaan yhteinen suojaustaso.

(b) Yhteisen vastuun tunnustaen turvallisuusluokiteltua tietoa jaetaan ainoastaan tiedonsaantitarpeen periaatteen[1] perusteella henkilöille, joille on selostettu sovellettavat turvallisuusmenettelyt.

(c) Ainoastaan asianmukaisesti turvallisuusselvitetyille henkilöille annetaan pääsy turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin luokiteltuun tietoon.

(d) Turvallisuusselvitystodistuksen antamista ei katsota viimeiseksi vaiheeksi arvioitaessa henkilön kelpoisuutta päästä turvallisuusluokiteltuun tietoon, vaan otetaan käyttöön jatkuvat turvallisuusmenettelyt seurantatoimina, jotta voidaan huomioida sisäpiiriuhan hallinta[2].

ENCLOSURE “B”
BASIC PRINCIPLES, MINIMUM STANDARDS AND RESPONSIBILITIES

BASIC PRINCIPLES

1. The following basic principles shall apply:

(a) NATO Nations and NATO Civil and Military bodies shall ensure that the agreed minimum standards set forth in this C-M are applied to ensure a common degree of protection for classified information exchanged among the parties.

(b) Acknowledging the responsibility to share, classified information shall only be disseminated on the basis of the principle of need-to-know[1] to individuals who have been briefed on the relevant security procedures.

(c) Only appropriately cleared individuals shall have access to information classified NATO CONFIDENTIAL and above.

(d) The granting of a clearance shall not be considered as a final step in assessing an individual’s eligibility for access to classified information but ongoing personnel security procedures, referred to as Aftercare, shall be established in order to address the management of the Insider Threat[2].

---

[1] Periaate, jonka mukaan tehdään myönteinen päätös, että tiedon mahdollisella vastaanottajalla on tarve päästä tietoon, saada tieto siitä tai saada se haltuunsa pystyäkseen suorittamaan virallisia tehtäviä tai palveluja.

[1] The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services.

[2] Sisäpiiriuhan aiheuttaa henkilöstö, jolla on erioikeuteen perustuva pääsy Naton turvallisuusluokiteltuun tietoon ja/tai Naton omaisuuteen organisaatiossa hoitamansa tehtävän perusteella ja joka voi myöhemmin käyttää väärin tätä pääsyä hävittääkseen, vahingoittaakseen, poistaakseen tai paljastaakseen Naton turvallisuusluokiteltua tietoa ja/tai Naton omaisuutta joko tahallisesti tai huolimattomuudesta.

[2] Insider Threat is represented by personnel who have privileged access to NATO Classified Information and/or NATO assets by virtue of their role within the organization and could subsequently abuse this access to destroy, damage, remove or disclose NATO Classified Information and/or NATO assets either by intention or negligence.

(e) Naton turvallisuustoimisto (NOS) koordinoi sisäpiiriuhan hallintaa yhdessä toimivaltaisten kansallisten viranomaisten sekä Naton sotilas- ja siviilielinten kanssa.

(f) Turvallisuusriskien hallintaa[3] suoritetaan pakollisena Naton sotilas- ja siviilielimissä Naton turvallisuusriskien hallintaprosessin (AC/35-D/1035) mukaisesti. Sen soveltaminen Naton jäsenvaltioissa on vapaaehtoista. Riskienhallintaa ei saa käyttää keinona kiertää turvallisuusperiaatteita.

(g) Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet käynnistävät organisaatioissaan turvallisuuskoulutus- ja -tietoisuusohjelmia, joissa käsitellään kaikkia turvallisuusnäkökohtia jäljempänä l kohdassa esitetyllä tavalla.

(h) Kaikista epäillyistä turvallisuusluokiteltuun tietoon kohdistuneista tietoturvaloukkauksista ja tällaisen tiedon vaarantumisista ilmoitetaan viipymättä toimivaltaiselle turvallisuusviranomaiselle.

(i) Alkuperäisten luovuttajien luovuttaessa turvallisuusluokiteltua tietoa Natolle ja Naton jäsenvaltioille Naton ohjelman, hankkeen tai sopimuksen tueksi oletuksena on, että tietoa hallitaan ja suojataan Naton tiedonhallinnan periaatteiden ja Naton turvallisuusperiaatteiden mukaisesti.

(j) Turvallisuusluokiteltuun tietoon sovelletaan alkuperäisen luovuttajan määräysvaltaa[4].

(e) The NATO Office of Security (NOS) shall coordinate the management of the Insider Threat in conjunction with the appropriate national authorities and NATO Civil and Military bodies.

(f) Security risk management[3] shall be mandatory within NATO Civil and Military bodies in accordance with the NATO Security Risk Management Process (AC/35-D/1035). Its application within NATO Nations is optional. Risk management shall not be used to circumvent security policy.

(g) NATO Nations and NATO Civil and Military bodies shall establish Security Education and Awareness Programmes within their organizations addressing all security aspects as described in paragraph (l) below.

(h) All suspected Security Breaches and compromise of classified information shall be reported immediately to the appropriate security authority.

(i) Originators release classified information to NATO and to NATO Nations in support of a NATO programme, project or contract on the understanding that it will be managed and protected in accordance with the NATO Information Management Policy (NIMP) and NATO Security Policy.

(j) Classified information shall be subject to Originator Control[4].

---

[3] Uhkien ja haavoittuvuuksien arviointiin perustuva järjestelmällinen lähestymistapa sen määrittämiseksi, mitä vastatoimia tarvitaan tiedon sekä sitä tukevien palvelujen ja resurssien turvallisuuden suojaamiseksi. Riskienhallintaan sisältyy resurssien suunnittelu, järjestäminen, ohjaaminen ja valvonta, joiden avulla varmistetaan, että riski pysyy hyväksyttävyyden rajoissa.

[3] A systematic approach to determining which security counter-measures are required to protect information and supporting services and resources, based upon an assessment of the threats and vulnerabilities. Risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds.

[4] Periaate, jonka mukaan valtio, Nato tai muu organisaatio, jonka alaisuudessa tieto on luotu, tuotettu tai tuotu Natoon, määrää tämän tiedon käyttöön sovellettavat säännöt ja vaatimukset ja on toimivaltainen tiedon koko elinkaaren aikaisten muutosten suhteen.

[4] The principle by which a nation, NATO, or other organization, under whose authority information has been created, produced, or introduced into NATO, establishes the rules and standards which apply to the use of this information and has authority over any changes throughout information life-cycle.

(k) Naton turvallisuusluokiteltu tieto luovutetaan vakiintuneiden luovutusmenettelyjen ja -perusteiden mukaisesti, ja kaikissa tapauksissa kaikki luovutettava Naton turvallisuusluokiteltu tieto tulee suojata vähintään samantasoisesti kuin tässä C-M-asiakirjassa ja sitä tukevissa ohjeissa määrätään.

(k) The release of NATO Classified Information shall be in accordance with the established procedures and criteria for the release, and in all cases, a degree of protection, no less stringent than that specified in this C-M and the supporting directives, shall be required for any NATO Classified Information released.

(l) Turvallisuusluokiteltu tieto turvataan tasapainoisella turvallisuustoimenpiteiden kokonaisuudella, jolla varmistetaan henkilöstöturvallisuus, toimitilaturvallisuus, tietoturvallisuus sekä viestintä- ja tietojärjestelmien turvallisuus (CIS). Myös silloin, kun turvallisuusluokiteltua tietoa annetaan hankeosapuolille ja luovutetaan Naton ulkopuolisille toimijoille (NNE), se turvataan noudattamalla näissä turvallisuusperiaatteissa kuvattuja menettelyjä. Nämä vaatimukset koskevat kaikkia henkilöitä, joilla on pääsy turvallisuusluokiteltuun tietoon, kaikkia turvallisuusluokiteltua tietoa sisältäviä tietovälineitä ja kaikkia tiloja, joissa on tällaista tietoa.

(l) Classified information shall be safeguarded by a balanced set of security measures addressing the following subjects: personnel security, physical security, security of information and security of Communication and Information Systems (CIS). When classified information is provided to contractors and released to non-NATO entities (NNE) it shall also be safeguarded by following the procedural measures set by these policies. These requirements shall extend to all individuals having access to classified information, all media carrying classified information, and to all premises containing such information.

(m) Organisaatiot, joilla on hallussaan Naton turvallisuusluokiteltua tietoa, kehittävät mekanismit ja menettelyt, joilla varmistetaan Naton turvallisuusperiaatteiden vaatimusten soveltaminen poikkeuksellisissa toimintaolosuhteissa, kuten häiriötilojen aikana. Nämä järjestelmät ja menettelyt voidaan esittää joko toiminnan jatkuvuussuunnitelmassa tai palautumissuunnitelmassa, tapahtuman luonteen mukaan.

(m) Establishments that hold NATO Classified Information shall develop mechanisms and processes to ensure application of NATO Security Policy requirements under adverse operational conditions, including disruptive incidents. Such mechanisms and processes may be reflected in either a Business Continuity Plan or Disaster Recovery Plan, depending on the nature of the incident.

KRIITTISIÄ KOHTEITA KOSKEVAN TIEDON SUOJAAMINEN

2. Tiedon julkaiseminen kriittisistä siviilikohteista (esim. puolustusmateriaalivarastoista, energiavarastoista), joilla on sotilaallista merkitystä jännitteiden tai sodan aikana, saattaa edistää kineettistä hyökkäystä tai sabotaasia, koska julkaistun tiedon avulla mahdolliset viholliset tai terroristit voivat pystyä kokoamaan luettelon kriittisistä kohteista ja käyttämään sitä haavoittuvien kohteiden tunnistamiseen hyökkäystä varten. Jotta pystytään estämään vihollisia käyttämästä tällaista tietoa vihamielisiin tarkoituksiin, on toteutettava asianmukaiset toimet,

PROTECTION OF INFORMATION ON KEY POINTS

2. The publication of information about critical civilian installations (e.g. defence supplies, energy supply) of military significance in times of tension or war may assist in the delivery of a kinetic attack or act of sabotage by allowing potential enemies or terrorists to compile a key points list, and to use this in order to identify points which may be vulnerable to attack. Appropriate steps shall be taken to ensure that such information is not freely available in the public domain in order to prevent its use in a hostile manner by enemies. Additionally, installations'

joilla varmistetaan, ettei tätä tietoa ole vapaasti saatavilla julkisesti. Lisäksi tällaisten kohteiden omistajien ja käyttäjien on oltava täysin tietoisia niihin kohdistuvan mainitunlaisen toiminnan vaarasta ja toteutettava tarvittavat toimet näitä kohteita koskevan tiedon suojaamiseksi.

owners and operators shall be fully aware of the risk of such activity against them and take such steps as necessary to protect this information.

TURVALLISUUDEN VASTUUALUEET

SECURITY RESPONSIBILITIES

Kansallinen turvallisuusviranomainen (NSA)

National Security Authority (NSA)

3. Kukin Naton jäsenvaltio perustaa kansallisen turvallisuusviranomaisen (NSA), joka vastaa Naton turvallisuusluokitellun tiedon turvallisuudesta. Kansallinen turvallisuusviranomainen toimii Naton turvallisuustoimiston ensisijaisena yhteystahona kaikissa Naton turvallisuuteen liittyvissä asioissa. Kansallinen turvallisuusviranomainen voi ohjata Naton turvallisuustoimiston kääntymään toimivaltaisen määrätyn turvallisuusviranomaisen tai muun toimivaltaisen turvallisuusviranomaisen puoleen.

3. Each NATO Nation shall establish a National Security Authority (NSA) responsible for the security of NATO Classified Information. The NSA serves as the main point of contact for the NOS for any matter relating to security within NATO. Thereafter, the NSA may direct the NOS to the appropriate Designated Security Authority (DSA) or other competent security authority.

4. Kansallisen turvallisuusviranomaisen vastuulla on

4. The NSA is responsible for:

(a) varmistaa Naton turvallisuusluokitellun tiedon turvallisuus sekä sotilas- että siviilialan kansallisissa virastoissa ja muissa organisaatioissa, sekä kotimaassa että ulkomailla;

(a) the security of NATO Classified Information in national agencies and elements, military or civil, at home or abroad;

(b) varmistaa, että kaikissa kansallisissa sekä sotilas- että siviilialan organisaatioissa kaikilla tasoilla tarkastetaan asianmukaisesti määräajoin Naton turvallisuusluokitellun tiedon suojaamiseksi tehdyt turvallisuusjärjestelyt, jotta voidaan todeta, suojataanko tätä tietoa asianmukaisesti. Sellaisissa organisaatioissa, joilla on hallussaan turvallisuusluokkaan COSMIC TOP SECRET luokiteltua tietoa tai ATOMAL-tietoa, tehdään turvallisuustarkastukset vähintään 24 kuukauden välein, jollei Naton turvallisuustoimisto tee näitä tarkastuksia kyseisenä ajanjaksona;

(b) ensuring that periodic and appropriate inspections of the security arrangements for the protection of NATO Classified Information are undertaken in all national organizations at all levels, both military and civil, to determine that NATO Classified Information is appropriately protected in accordance with current NATO security regulations. In the case of organizations holding CTS or ATOMAL information, security inspections shall be made at least every 24 months, unless, during that period, they are carried out by the NOS;

(c) varmistaa, että kaikille kansalaisille, jotka tarvitsevat pääsyn turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin luokiteltuun

(c) ensuring that a Personnel Security Clearance (PSC) has been granted to all nationals who are required to have access

tietoon, on myönnetty henkilöturvallisuusselvitystodistus (PSC) Naton turvallisuusperiaatteiden mukaisesti;

(d) varmistaa, että on laadittu turvallisuussuunnitelmat, joiden avulla estetään Naton turvallisuusluokiteltua tietoa joutumasta asiattomien tai vihamielisten tahojen haltuun poikkeusolojen aikana; ja

(e) auktorisoida kansallisten COSMIC-keskusrekisterien perustaminen tai lakkauttaminen. COSMIC-keskusrekisterien perustamisesta tai lakkauttamisesta on ilmoitettava Naton turvallisuustoimistolle.

to information classified NATO CONFIDENTIAL and above, in accordance with NATO Security Policy;

(d) ensuring that security plans have been prepared in order to prevent NATO Classified Information from falling into unauthorised or hostile hands in the event of an emergency; and

(e) authorising the establishment (or disestablishment) of national COSMIC Central Registries. The establishment (or disestablishment) of COSMIC Central Registries shall be notified to the NOS.

Määrätty turvallisuusviranomainen (DSA)

5. Viranomainen, jonka vastuulla on tiedottaa yrityksille ja muille yhteisöille kansallisista periaatteista kaikissa Naton yritysturvallisuuden periaatteita koskevissa asioissa sekä antaa ohjausta ja apua niiden soveltamisessa. Joissakin valtioissa määrätyn turvallisuusviranomaisen tehtävää voi hoitaa kansallinen turvallisuusviranomainen.

Designated Security Authority (DSA)

5. An authority responsible for communicating to industry the national policy in all matters of NATO industrial security policy and for providing direction and assistance in its implementation. In some nations, the function of a DSA may be carried out by the NSA.

Turvallisuuskomitea (SC)

6. Turvallisuuskomitean asettaa Pohjois-Atlantin neuvosto (NAC). Komiteassa on edustajat kunkin Naton jäsenvaltion kansallisesta turvallisuusviranomaisesta / määrätystä turvallisuusviranomaisesta, ja komiteaa tukee tarvittaessa muu Naton jäsenvaltioiden turvallisuushenkilöstö. Kansainvälisen sotilasesikunnan (IMS), strategisten esikuntien sekä tiedonvälityksen, johtamisen ja valvonnan (C3) ohjausryhmän edustajat ovat läsnä turvallisuuskomitean kokouksissa. Myös Naton sotilas- ja siviilielinten edustajia voi olla läsnä käsiteltäessä asioita, joissa näillä elimillä on intressi. Naton turvallisuustoimisto nimeää turvallisuuskomitean puheenjohtajat komitean pääedustajien kokoonpanoa, turvallisuusperiaatteita käsittelevää kokoonpanoa sekä viestintä- ja tietojärjestelmiä käsittelevää kokoonpanoa varten.

Security Committee (SC)

6. The SC is established by the North Atlantic Council (NAC) and is composed of representatives from each NATO Nation's NSAs/DSAs and supported, where required, by additional NATO Nation security staff. Representatives of the International Military Staff (IMS), Strategic Commands and Consultation Command and Control (C3) Board shall be present at the meetings of the SC. Representatives of NATO Civil and Military bodies may also be present when matters of interest to them are addressed. The Chairpersons for the SC at Principal's level, the SC in Security Policy Format (SC (SP)), and the SC in Communications and Information Systems (CIS) Security Format (SC (CISS)) are provided by the NOS.

7. Turvallisuuskomitea vastaa suoraan Pohjois-Atlantin neuvostolle seuraavista:

7. The SC is responsible directly to the NAC for:

(a) (asiakirjoissa C-M(2002)49 ja C-M(2002)50 kuvattujen) Naton turvallisuussääntöjen tarkistaminen ja niiden muuttamista tai hyväksymistä koskevien suositusten antaminen Pohjois-Atlantin neuvostolle;

(a) reviewing NATO Security Policy (as set forth in C-M(2002)49 and C-M(2002)50) and making recommendations for change or endorsement to the NAC;

(b) Naton turvallisuussääntöjä koskevien kysymysten käsittely;

(b) examining questions concerning NATO Security Policy;

(c) Naton turvallisuussääntöjen tukemiseksi julkaistavien direktiivien ja ohjausasiakirjojen tarkistaminen ja hyväksyminen[5]; ja

(c) reviewing and approving the supporting directives and guidance documents published in support of NATO Security Policy;[5] and

(d) sellaisten turvallisuusasioiden käsittely, jotka Pohjois-Atlantin neuvosto, Naton jäsenvaltio, pääsihteeri, sotilaskomitea, tiedonvälityksen, johtamisen ja valvonnan ohjausryhmä tai Naton jonkin sotilas- tai siviilielimen johtaja on saattanut turvallisuuskomitean käsiteltäväksi, sekä asianmukaisten suositusten laatiminen näistä asioista.

(d) considering security matters referred to it by the NAC, a NATO Nation, the Secretary General, the Military Committee (MC), the C3 Board or the heads of NATO Civil and Military bodies and preparing appropriate recommendations thereon.

Naton turvallisuustoimisto (NOS)

8. Naton turvallisuustoimisto on perustettu Naton kansainväliseen sihteeristöön osana yhteistä tiedustelu- ja turvallisuusjaostoa. Turvallisuustoimiston henkilöstö on kokenutta sekä sotilas- että siviilialan turvallisuusasioissa. Naton turvallisuustoimisto toimii läheisessä yhteydessä Naton jäsenvaltioiden kansallisten turvallisuusviranomaisten / määrättyjen turvallisuusviranomaisten sekä Naton sotilas- ja siviilielinten kanssa. Turvallisuustoimisto voi myös tarvittaessa pyytää Naton jäsenvaltioita ja Naton sotilas- ja siviilielimiä antamaan turvallisuustoimistolle lisää turvallisuusasiantuntijoita avustamaan sitä osa-aikaisesti, kun kokoaikaisen henkilöstön lisääminen turvallisuustoimistoon ei olisi perusteltua.

NATO Office of Security (NOS)

8. The NOS is established within the NATO International Staff as part of the Joint Intelligence and Security Division. It is composed of personnel experienced in security matters in both military and civil spheres. The NOS maintains close liaison with the NSAs/DSAs of NATO Nations, and with NATO Civil and Military bodies. The NOS may also, as required, request NATO Nations and NATO Civil and Military bodies to provide additional security experts to assist it for limited periods of time when full-time additions to the NOS would not be justified.

9. Naton turvallisuustoimiston vastuulla on

(a) käsitellä Naton turvallisuuteen vaikuttavia asioita;

9. The NOS is responsible for:

(a) examining any questions affecting NATO security;

[5] Naton jäsenvaltio voi pyytää, että myös Pohjois-Atlantin neuvosto hyväksyy turvallisuusperiaatteita tukevan ohjeen.

[5] A NATO Nation may request that a supporting directive also be approved by the NAC.

(b) määrittää keinot, joilla Naton turvallisuutta voitaisiin parantaa;

(b) identifying means whereby NATO security might be improved;

(c) koordinoida yleisesti turvallisuutta Natossa Naton jäsenvaltioiden ja Naton sotilas- ja siviilielinten kesken;

(c) the overall co-ordination of security for NATO among NATO Nations and NATO Civil and Military bodies;

(d) varmistaa Naton turvallisuussääntöjen toteuttaminen ja valvonta muun muassa antamalla neuvoja, joita Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet voivat pyytää joko soveltaessaan tässä liitteessä kuvattuja perusperiaatteita ja turvallisuusvaatimuksia tai täyttäessään yksittäisiä turvallisuusvaatimuksia;

(d) ensuring the implementation and oversight of NATO Security Policy, including the provision of such advice as may be requested by NATO Nations and NATO Civil and Military bodies either in their application of the basic principles and the standards of security described in this Enclosure, or in the implementation of the specific security requirements;

(e) tiedottaa kulloisenkin tilanteen mukaan turvallisuuskomitealle, pääsihteerille ja sotilaskomitean puheenjohtajalle Naton turvallisuustilanteesta sekä edistymisestä turvallisuutta koskevien Pohjois-Atlantin neuvoston päätösten täytäntöönpanossa;

(e) informing, as appropriate, the SC, the Secretary General and the Chair of the MC of the state of security within NATO, and the progress made in implementing NAC decisions regarding security;

(f) tehdä määräajoin Naton turvallisuusluokitellun tiedon suojaamiseen tarkoitettujen turvallisuusjärjestelmien tarkastuksia Naton jäsenvaltioissa, Naton siviilielimissä, Naton operaatioesikunnassa ja Naton transformaatioesikunnan komentajan johtoesikunnassa[6];

(f) carrying out periodic inspections of security systems for the protection of NATO Classified Information in NATO Nations, NATO Civil bodies, SHAPE and HQ SACT;[6]

(g) tehdä turvallisuutta koskevia selvityksiä sellaisissa Naton ulkopuolisissa toimijoissa, joiden kanssa Nato on tehnyt turvallisuussopimuksen, aluksi varmentamista varten ja sen jälkeen määräajoin Naton turvallisuusperiaatteiden jatkuvan noudattamisen varmistamiseksi;

(g) conducting security surveys in NNEs with whom NATO has a signed Security Agreement for the initial purpose of certification and periodically thereafter for ensuring ongoing compliance with NATO Security Policy;

(h) koordinoida kansallisten turvallisuusviranomaisten / määrättyjen turvallisuusviranomaisten ja Naton sotilas- ja siviilielinten kanssa epäiltyyn tai tosiasialliseen Naton turvallisuusluokitellun tiedon

(h) co-ordinating, with NSAs/DSAs and NATO Civil and Military bodies, the investigation of cases relating to the actual

---

[6] Naton jäsenvaltiot voivat Naton turvallisuustoimiston pyynnöstä osallistua sen Naton sotilas- ja siviilielimissä tekemiin tarkastuksiin joko tarkkailijoina tai tarkastusryhmän aktiivisina jäseninä. Tämä ei kuitenkaan ole mahdollista sellaisissa siviilielimissä, joiden perusrakenteissa kaikki Naton jäsenvaltiot eivät ole mukana.

[6] NATO Nations may, upon request of the NOS, participate in the NOS' inspections to NATO Civil and Military bodies either as observers or as active members of the inspection team. However, this is not possible for civil bodies where not all NATO Nations are part of the constituting framework.

katoamiseen tai vaarantumiseen liittyvien asioiden tutkintaa;

(i) tiedottaa tarvittaessa kansallisille turvallisuusviranomaisille / määrätyille turvallisuusviranomaisille saamastaan epäedullisesta tiedosta, joka koskee kyseisten valtioiden kansalaisia;

(j) suunnitella turvatoimia Brysselissä sijaitsevan Naton päämajan suojaamiseksi ja varmistaa niiden toteuttaminen oikealla tavalla; ja

(k) valvoa pääsihteerin johdolla ja puolesta ATOMAL-tietojen suojaamiseksi tarkoitetun Naton turvallisuusohjelman toteuttamista ATOMAL-sopimuksen (C-M(64)39) ja sitä tukevien hallinnollisten järjestelyjen (C-M(68)41) määräysten mukaisesti.

Sotilaskomitea ja Naton sotilaselimet

10. Naton korkeimpana sotilasviranomaisena sotilaskomitea vastaa sotilasasioiden hoitamisesta yleisesti. Sotilaskomitea vastaa siten kaikista Naton sotilasrakenteen turvallisuusasioista, mukaan lukien niiden toimenpiteiden keskitetty kokonaiskäsittely, joita tarvitaan Naton turvallisuusluokitellun tiedon siirtämiseen käytettävän salaustekniikan ja -aineiston asianmukaisuuden varmistamiseksi, sekä tämän C-M-asiakirjan liitteessä F määriteltyjen Naton rahoittamien salauslaitteistojen turvallisuushyväksyntä. Aiemmin sovittujen periaatteiden sekä edellä olevien 8 ja 9 kohdan mukaisesti Naton turvallisuustoimisto hoitaa turvallisuuteen liittyviä toimeenpanotehtäviä Naton sotilasrakenteessa ja tiedottaa tästä toiminnasta sotilaskomitean puheenjohtajalle.

11. Sotilaskomitean alaisuuteen perustettujen Naton sotilaselinten johtajat vastaavat kaikista organisaatioidensa turvallisuusasioista. Tähän sisältyy vastuu siitä, että varmistetaan turvallisuusorganisaation perustaminen, asianmukaisten turvallisuustoimenpiteiden ja -menettelyjen suunnittelu ja to-

or suspected loss or compromise of NATO Classified Information;

(i) informing NSAs/DSAs of any adverse information which comes to light concerning their nationals, where appropriate;

(j) devising security measures for the protection of the NATO Headquarters, Brussels and ensuring their correct implementation; and

(k) supervising, under the direction and on behalf of the Secretary General, the application of the NATO security programme for the protection of ATOMAL information under the provisions of the Agreement (C-M(64)39) and the supporting Administrative Arrangements (C-M(68)41).

Military Committee and NATO Military bodies

10. As the highest military authority in NATO, the MC is responsible for the overall conduct of military affairs. The MC is consequently responsible for all security matters within the NATO military structure including centralised overall cognisance of measures necessary to assure the adequacy of cryptographic techniques and materials used for transmitting NATO Classified Information, including the security approval of NATO funded cryptographic equipment as defined in Enclosure "F" to this C-M. In accordance with previously agreed policy and in compliance with paragraphs 8 and 9 above, the NOS carries out the executive functions for security within the NATO military structure and keeps the Chair of the MC informed.

11. The Heads of NATO Military bodies established under the auspices of the MC are responsible for all security matters within their establishments. This includes the responsibility for ensuring that a security organization is set up, that appropriate security measures and procedures are devised and executed in accordance with NATO Security

teutus Naton turvallisuussääntöjen mukaisesti sekä turvallisuustoimenpiteiden tarkastaminen määräajoin kaikilla komentotasoilla. Sellaisissa organisaatioissa, joilla on hallussaan turvallisuusluokkaan COSMIC TOP SECRET luokiteltua tietoa tai ATOMAL-tietoa, tehdään turvallisuustarkastukset vähintään 24 kuukauden välein, jollei Naton turvallisuustoimisto ole tehnyt tällaista tarkastusta kyseisenä ajanjaksona;

Policy and that the security measures are inspected periodically at each command level. In cases where organizations hold COSMIC TOP SECRET (CTS) or ATOMAL information, security inspections are to be made at least every 24 months, unless, during that period, an inspection has been carried out by the NOS.

Naton siviilielimet

12. Naton kansainvälinen sihteeristö ja Naton siviilivirastot vastaavat Pohjois-Atlantin neuvostolle turvallisuuden ylläpitämisestä organisaatioissaan. Tähän sisältyy vastuu siitä, että varmistetaan turvallisuusorganisaation perustaminen, turvallisuusohjelmien suunnittelu ja toteutus Naton turvallisuussääntöjen mukaisesti sekä turvallisuustoimenpiteiden tarkastaminen määräajoin kaikilla komentotasoilla. Sellaisissa organisaatioissa, joilla on hallussaan turvallisuusluokkaan COSMIC TOP SECRET luokiteltua tietoa tai ATOMAL-tietoa, tehdään turvallisuustarkastukset vähintään 24 kuukauden välein, jollei Naton turvallisuustoimisto ole tehnyt tällaista tarkastusta kyseisenä ajanjaksona.

NATO Civil bodies

12. The NATO International Staff and NATO civil agencies are responsible to the NAC for the maintenance of security within their establishment. This includes responsibility for ensuring that a security organization is set up, that security programmes are devised and executed in accordance with NATO Security Policy and that the security measures are inspected periodically at each command level. In cases of organizations holding CTS or ATOMAL information, security inspections are to be made at least every 24 months, unless, during that period, an inspection has been carried out by the NOS.

TURVALLISUUSVALVONTA OSAAMISKESKUSTEN[7] / YHTEISYMMÄRRYSPÖYTÄKIRJAAN PERUSTUVIEN ELINTEN OSALTA

13. Turvallisuusvalvonnalla tarkoitetaan valvontatehtävää, jolla varmistetaan, että Naton turvallisuusluokiteltua tietoa käsittelevä organisaatio soveltaa Naton turvallisuussääntöjä oikein suojatakseen tätä tietoa. Naton komentorakenteen (NCS) ulkopuolisten elinten turvallisuusvalvonta Naton turvallisuusluokitellun tiedon suojaamisen osalta tapahtuu seuraavasti:

SECURITY OVERSIGHT FOR CENTRE OF EXCELLENCE (COE)[7] / MEMORANDUM OF UNDERSTANDING (MOU) BODIES

13. Security oversight is defined as the supervisory function to ensure that any organization which handles NATO Classified Information is correctly applying NATO Security Policy for the protection of such information. Security oversight for bodies that lie outside the NATO Command Structure (NCS) in respect of protecting NATO Classified Information shall be delivered as follows:

[7] Osaamiskeskukset, jotka Pohjois-Atlantin neuvosto on hyväksynyt asiakirjan PO(2020)0038 (INV) mukaisesti.
[7] NAC-approved COEs in accordance with PO(2020)0038 (INV).

(a) Osallistuvat valtiot vastaavat turvallisuusasioiden hoitamisesta kyseisessä Naton sotilaselimessä (NMB) ja tekevät asianmukaiset järjestelyt sitä varten. Jollei näiden yksiköiden turvallisuusvalvonnan hoitamiseksi ole tehty erillisiä sopimuksia, se valtio, jossa kyseinen yksi tai useampi yksikkö sijaitsee, eli isäntävaltio, johtaa turvallisuusvalvontaa.

(a) Participating nations are responsible and shall make appropriate arrangements as to how to deal with security within their NATO Military Body (NMB). Unless there are specific agreements in place regarding how to deal with security oversight for these elements, the Nation in which the element(s) is/are situated, i.e. the Host Nation, shall take the lead for exercising security oversight.

(b) Osaamiskeskukset / yhteisymmärryspöytäkirjaan perustuvat elimet voivat olla Naton sotilaselimiä, jos Pohjois-Atlantin neuvosto on tehnyt aktivointipäätöksen asiassa. Tällaisissa tapauksissa sovelletaan Naton turvallisuussääntöjä ja osaamiskeskuksen / yhteisymmärryspöytäkirjaan perustuvan elimen johtaja vastaa kaikista organisaationsa turvallisuusasioista. Osallistuvat valtiot vastaavat turvallisuusvaatimusten käsittelystä osaamiskeskuksessa / yhteisymmärryspöytäkirjaan perustuvassa elimessä ja tekevät tarvittavat järjestelyt sitä varten. Isäntävaltio johtaa turvallisuusvalvontaa, jolleivät osallistuvat valtiot ole sopineet muista järjestelyistä tämän valvonnan suhteen.

(b) COE/MOU bodies can be NMB if there is a NAC activating decision. In such cases NATO Security Policy is applicable and the head of the COE/MOU body shall be responsible for all security matters within their establishment. Participating nations are responsible and shall make necessary arrangements to deal with security requirements within any COE/MOU body. The Host Nation shall take the lead for exercising security oversight unless participating nations have agreed to alternative arrangements for this oversight.

(c) Jos osaamiskeskusta / yhteisymmärryspöytäkirjaan perustuvaa elintä ei ole aktivoitu Naton sotilaselimeksi (eikä Pohjois-Atlantin neuvosto siten ole myöntänyt sille kansainvälistä asemaa), mutta se on akkreditoitu Naton osaamiskeskukseksi / yhteisymmärryspöytäkirjaan perustuvaksi elimeksi, sovelletaan Naton turvallisuussääntöjä. Vaikka osallistuvat valtiot vastaavat kaikista osaamiskeskuksen / yhteisymmärryspöytäkirjaan perustuvan elimen turvallisuusasioista, isäntävaltio johtaa turvallisuusvalvontaa, jolleivät osallistuvat valtiot ole sopineet muista järjestelyistä tämän valvonnan suhteen. Osaamiskeskuksen / yhteisymmärryspöytäkirjaan perustuvan elimen perustamista koskevassa yhteisymmärryspöytäkirjassa esitetään, miten tämä toteutetaan osaamiskeskuksessa / yhteisymmärryspöytäkirjaan perustuvassa elimessä.

(c) If a COE/MOU body is not activated as a NMB (and thus not granted international status by the NAC), but accredited as a NATO COE/MOU, NATO Security Policy applies. Although participating nations will be responsible for all security matters within the COE/MOU, the Host Nation shall take the lead for exercising security oversight unless participating nations have agreed to alternative arrangements for this oversight. Any founding MOU shall describe how this is implemented within the COE/MOU body.

(d) Jos jonkin Naton jäsenvaltion monikansallista yksikköä ei ole akkreditoitu osaamiskeskukseksi eikä aktivoitu Naton

(d) If a multi-national entity within one of the NATO Nations is not accredited as a COE, nor activated as a NMB but uses

sotilaselimeksi, mutta se käyttää Naton turvallisuusluokiteltua tietoa, sovelletaan Naton turvallisuussääntöjä ja osallistuvat valtiot vastaavat turvallisuusasioista. Jos osallistujina on Naton ulkopuolisia valtioita, näiden kanssa on tehtävä turvallisuussopimus ennen kuin turvallisuusluokiteltua tietoa voidaan vaihtaa. Tällaisissa tapauksissa isäntävaltio johtaa turvallisuusvalvontaa, jolleivät osallistuvat valtiot ole sopineet muista järjestelyistä tämän valvonnan suhteen. Monikansallisen yksikön perustamista koskevassa yhteisymmärryspöytäkirjassa esitetään, miten tämä toteutetaan monikansallisessa yksikössä.

NATO Classified Information, NATO Security Policy applies and the participating nations remain responsible for security matters. If there are non-NATO nations participating, a security agreement with those nations must be in place before classified information can be exchanged. In such circumstances the Host Nation shall take the lead for security oversight unless participating nations have agreed to alternative arrangements for this oversight. Any founding MOU shall describe how this is implemented within the multi-national entity.

TURVALLISUUSKOORDINOINTI

14. Naton jäsenvaltioiden kansallisten turvallisuusviranomaisten / määrättyjen turvallisuusviranomaisten ja Naton sotilas- tai siviilielinten välinen Naton turvallisuusasia, jota ei voida ratkaista, tai Naton turvallisuussääntöjen toteuttamista tai tulkintaa koskeva asia saatetaan Naton turvallisuustoimiston ratkaistavaksi. Jos asian saattavat turvallisuustoimiston ratkaistavaksi sotilasviranomaiset, tämä tehdään komentotietä pitkin. Ratkaisemattomat erimielisyydet Naton turvallisuustoimisto antaa turvallisuuskomitean käsiteltäväksi.

SECURITY CO-ORDINATION

14. Any NATO security issue between NSAs/DSAs of NATO Nations, and NATO Civil and Military bodies that cannot be resolved, or any issue with implementing or interpreting NATO Security Policy, shall be referred to the NOS. In cases where such reference is by military authorities, this shall be made through command channels. Any unresolved differences shall be submitted by the NOS to the SC for consideration.

TURVALLISUUSSÄÄNTÖJEN MUUTTAMINEN

15. Naton jäsenvaltioiden ja Naton sotilas- ja siviilielinten ehdotukset Naton turvallisuussääntöjen muuttamiseksi tulisi toimittaa ensisijaisesti Naton turvallisuustoimiston käsiteltäväksi. Sotilasviranomaisten tekemät ehdotukset välitetään komentotietä pitkin. Naton turvallisuustoimisto käsittelee ehdotukset, ja tarvittaessa ne esitetään turvallisuuskomitealle jatkokäsittelyä varten. Tämä kohta ei estä Naton jäsenvaltioiden kansallisia turvallisuusviranomaisia / määrättyjä turvallisuusviranomaisia tekemästä virallisesti ehdotuksia turvallisuuskomitealle, jos ne niin tahtovat

SECURITY POLICY MODIFICATIONS

15. Any proposals by NATO Nations and NATO Civil and Military bodies to modify NATO Security Policy should be referred in the first instance to the NOS. Any proposals made by the military authorities shall be transmitted through command channels. Proposals will be considered by the NOS and if necessary raised to the SC for further discussion. This paragraph does not preclude the NSAs/DSAs from NATO Nations formally making proposals to the SC if they wish.

LIITE C
HENKILÖSTÖTURVALLISUUS

JOHDANTO

1. Tässä liitteessä esitetään henkilöstöturvallisuutta koskevat periaatteet ja vähimmäisvaatimukset. Lisätietoja ja vaatimuksia löytyy Naton turvallisuussääntöjä tukevasta henkilöstöturvallisuusdirektiivistä (AC/35-D/2000).

2. Henkilöstöturvallisuusmenettelyt suunnitellaan sellaisiksi, että niillä pystytään selvittämään, voiko henkilölle hänen lojaalisuutensa, rehellisyytensä ja luotettavuutensa huomioon ottaen myöntää pääsyn turvallisuusluokiteltuun tietoon ilman, että siitä aiheutuu turvallisuusriski, jota ei voida hyväksyä. Tämä edellyttää, että kaikki siviili- ja sotilashenkilöt[1], joiden velvollisuudet tai tehtävät edellyttävät pääsyä turvallisuusluokkaan CONFIDENTIAL[2] ja sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon, on tutkittava asianmukaisesti, jotta saavutetaan riittävä luottamuksen taso heidän edellytyksistään päästä turvallisuusluokiteltuun tietoon, ja heillä on tämän johdosta oltava kansallinen henkilöturvallisuusselvitystodistus (PSC).[3]

3. Saadakseen pääsyn Naton turvallisuusluokkaan NATO CONFIDENTIAL (NC) ja sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon henkilöllä on oltava voimassa oleva

ENCLOSURE "C"
PERSONNEL SECURITY

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for Personnel Security. Additional details and requirements are found in the supporting Directive on Personnel Security (AC/35-D/2000).

2. Personnel security processes shall be designed to determine whether an individual can, taking into account their assessed loyalty, trustworthiness and reliability, be authorised to have access to classified information without constituting an unacceptable risk to security. To achieve this, all individuals[1], civilian and military, whose duties or functions require access to information classified CONFIDENTIAL[2] and above shall be appropriately investigated to give a satisfactory level of confidence as to their eligibility for access to such information and as such possess a national Personnel Security Clearance (PSC).[3]

3. In terms of access to NATO Classified Information NATO CONFIDENTIAL (NC) and above an individual will require a valid national PSC at the appropriate level along

---

[1] Poikkeuksena ne valtion ylimpien tehtävien haltijat, joihin viitataan tämän liitteen kohdassa 7.
[1] Aside from those Senior Government Officials, referred to in the paragraph 7 of this Enclosure.
[2] Jotkin Naton jäsenvaltiot edellyttävät kansallisten säädösten ja määräysten mukaisesti henkilöturvallisuusselvityksen turvallisuusluokkaan RESTRICTED tai vastaavaan kansalliseen turvallisuusluokkaan kuuluvaan tietoon pääsyä varten.
[2] Some NATO Nations, as mandated by their national laws and regulations, require a PSC for access to classified information at the level of RESTRICTED or national equivalent.
[3] Henkilöturvallisuusselvitys (PSC) on kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen tai muun toimivaltaisen turvallisuusviranomaisen myönteinen arvio, jolla tunnustetaan luonnollisen henkilön kelpoisuus päästä turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon ottaen huomion henkilön lojaalius, rehellisyys ja luotettavuus.
[3] A PSC is a positive determination by which an NSA/DSA or other competent security authority formally recognizes the individual's eligibility to have access to information classified NC and above taking into account their loyalty, trustworthiness and reliability.

asianmukaisen tason kansallinen henkilöturvallisuusselvitystodistus sekä asianmukaisen kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen tai muun toimivaltaisen turvallisuusviranomaisen vahvistus siitä, että kyseiselle henkilölle voidaan myöntää pääsy Naton turvallisuusluokiteltuun tietoon.

with the confirmation from the appropriate NSA/DSA or other competent security authority that the individual in question may be authorised to access NATO Classified Information.

TIEDONSAANTITARPEEN PERIAATTEEN SOVELTAMINEN

4. Naton jäsenvaltioiden ja Naton siviili- ja sotilaselinten henkilöillä on pääsy vain sellaiseen Naton turvallisuusluokiteltuun tietoon, johon heillä on tiedonsaantitarve. Kenelläkään ei ole yksinomaan aseman tai viran tai henkilöturvallisuusselvitystodistuksen perusteella pääsyä Naton turvallisuusluokiteltuun tietoon.

APPLICATION OF THE NEED-TO-KNOW PRINCIPLE

4. Individuals in NATO Nations and in NATO Civil and Military bodies shall only have access to NATO Classified Information for which they have a need-to-know. No individual is entitled solely by virtue of rank or appointment or PSC to have access to NATO Classified Information.

HENKILÖTURVALLISUUSSELVITYSTODISTUKSET (PSC)

5. Naton turvallisuussäännöt eivät edellytä henkilöturvallisuusselvitystodistusta turvallisuusluokkaan NATO RESTRICTED (NR) kuuluvaan tietoon pääsyyn.[4] Henkilöiden, jotka tarvitsevat pääsyn ainoastaan turvallisuusluokkaan NATO RESTRICTED kuuluvaan tietoon, on saatava ohjeistusta heidän turvallisuusvelvoitteistaan Naton turvallisuusluokitellun tiedon[5] suojaamisen osalta, heidän on annettava vakuutuksensa turvallisuutta koskevasta vastuustaan kirjallisesti tai vastaavalla kiistämättömyyden varmistavalla tavalla ja heillä on oltava myös tiedonsaantitarve.

PERSONNEL SECURITY CLEARANCES (PSCs)

5. A PSC is not required by NATO Security Policy for access to information classified NATO RESTRICTED (NR).[4] Individuals who only require access to information classified NR shall have been briefed on their security obligations in respect to the protection of NATO Classified Information[5], shall have acknowledged their security responsibilities in writing or an equivalent method which ensures non-repudiation and shall also have a need-to-know.

6. Asianmukainen henkilöturvallisuusselvitystodistus tarvitaan silloin, kun henkilöt tehtäviään suorittaessaan pääsevät tai saattavat päästä turvallisuusluokkaan NATO

6. An appropriate PSC is required when individuals access information classified NC

[4] Jotkin Naton jäsenvaltiot voivat kansallisten säädöstensä ja määräystensä mukaisesti vaatia henkilöturvallisuusselvitystä turvallisuusluokkaan NATO RESTRICTED kuuluvaan tietoon pääsyä varten.
[4] Some NATO Nations, in accordance with their national laws and regulations, may require a PSC for access to information classified NR.
[5] Jäsenvaltiot voivat käyttää joko Naton omaa ohjeistusta tai vastaavaa kansallista ohjeistusta, jos jälkimmäisessä korostetaan näiden kahden turvallisuuskehyksen vaatimusten eroja.
[5] Nations may use either NATO specific briefings or national equivalent if the latter highlights the differences between the requirements of the two security frameworks.

CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon. Lisäksi henkilöiltä edellytetään:

(a) tiedonsaantitarvetta;

(b) saatua ohjeistusta turvallisuusvelvoitteistaan Naton turvallisuusluokitellun tiedon suojaamisen osalta;

(c) vakuutuksen antamista turvallisuutta koskevasta vastuustaan joko kirjallisesti tai vastaavalla kiistämättömyyden varmistavalla tavalla.

and above or may have access to such information during the course of their duties. In addition, individuals are required to:

(a) have a need-to-know;

(b) have been briefed on their security obligations in respect to the protection of NATO Classified Information;

(c) have acknowledged their responsibilities either in writing or an equivalent method which ensures non-repudiation.

7. Edellä olevista 5 ja 6 kohdasta poiketen valtion ylimpien tehtävien haltijoiden (esimerkiksi valtion- ja hallitusten päämiehet, ministerit, kansanedustajat, oikeuslaitoksen jäsenet) pääsy Naton turvallisuusluokiteltuun tietoon perustuu kansallisiin säädöksiin ja määräyksiin; tällaisia henkilöitä on ohjeistettava heidän turvallisuusvelvoitteistaan, ja heillä on oltava tiedonsaantitarve.

7. As an exception to paragraphs 5 and 6 above, access to NATO Classified Information by Senior Government Officials (e.g. Heads of State and Government, Government Ministers, Members of Parliament, Members of the Judiciary) is determined by national laws and regulations; such officials shall be briefed on their security obligations and shall have a need-to-know.

8. Vaadittavan henkilöturvallisuusselvitystodistuksen taso ja siten tehtyjen turvallisuusselvitysmenettelyjen laajuus määräytyvät sen perusteella, mihin turvallisuusluokkaan kuuluvaan Naton turvallisuusluokiteltuun tietoon henkilön on saatava pääsy. Naton turvallisuusluokiteltuun tietoon pääsyn saaneiden henkilöiden tai virantoimituksessaan tai tehtävissään tietoon mahdollisesti pääsevien henkilöiden edellytyksistä on oltava sovittu luottamuksen taso.

8. The level of PSC required and, therefore, the extent of security clearance processes undertaken shall be determined by the level of classification of the NATO Classified Information to which the individual is to have access. There shall be an agreed standard of confidence regarding the eligibility of individuals granted access to, or whose duties or functions may afford access to, NATO Classified Information.

9. Henkilöturvallisuusselvitystodistuksen myöntämistä ei tule pitää henkilöstöturvallisuusmenettelyn viimeisenä vaiheena; vaatimuksena on varmistaa henkilön jatkuvat edellytykset päästä Naton turvallisuusluokiteltuun tietoon. Tämä saavutetaan, kun turvallisuusviranomaiset ja -johtajat osallistavat henkilöitä tehokkaasti ja arvioivat heitä säännöllisesti. Tähän sisältyy sellaisten henkilön olosuhteissa tai käyttäytymisessä tapahtuvien muutosten arviointi, joilla voi olla turvallisuusvaikutuksia. Lisäksi, turvallisuuskoulutus- ja tietoisuusohjelmien tehokkaalla käytöllä muistutetaan henkilöitä heidän turvallisuutta koskevasta vastuustaan ja

9. The granting of a PSC should not be considered as a final step in the personnel security process; there is a requirement to ensure an individual's continuing eligibility for access to NATO Classified Information. This is to be achieved through effective engagement and regular evaluation by security authorities and managers. This includes assessing any change in circumstance or behaviour with potential security implications. Additionally, the effective use of security education and awareness programme(s) shall be used in order to remind individuals of their security responsibilities and of the need to report, to their managers or security

heidän velvollisuudestaan ilmoittaa johtajilleen tai turvallisuushenkilöstölle tietoja, jotka voivat vaikuttaa heidän turvallisuusstatukseensa.

staff, information which may affect their security status.

Poikkeukselliset olosuhteet

10. Voi syntyä tilanteita, joissa joitain 6 kohdan vaatimuksista ei voida täyttää esimerkiksi kiireellisestä operaatiosta johtuen. Väliaikaisia nimityksiä sekä tilapäisesti tai kiireellisyyssyistä myönnettyä pääsyä koskevat käytännöt määritellään tarkemmin Naton turvallisuussääntöjä tukevassa henkilöstöturvallisuusdirektiivissä.

Exceptional Circumstances

10. Circumstances may arise when, for example for urgent mission purposes, some of the requirements in paragraph 6 above cannot be met. Details in respect to provisional appointments, temporary and emergency access, are set out in the supporting Directive on Personnel Security.

Vastuut

11. Henkilöturvallisuusselvitystodistuksen käsittely kuuluu sille Naton jäsenvaltioille, jonka kansalaista selvitys koskee. Tähän sisältyy vaatimus siitä, että jäsenvaltiot varmistavat, että niiden henkilöstöturvallisuusselvitystodistusta koskevat menettelyt täyttävät tutkinnalliset vähimmäisvaatimukset ja perusteet, joilla arvioidaan henkilön lojaaliutta, rehellisyyttä ja luotettavuutta henkilöturvallisuusselvitystodistuksen myöntämistä varten sekä henkilöturvallisuusselvitystodistuksen uusimisen vaatimukset, jotka määritellään henkilöstöturvallisuusdirektiivissä.

Responsibilities

11. It is the responsibility of the NATO Nation, of which the individual is a national, to process PSC applications. This includes the requirement to ensure that their PSC process meets the minimum investigative requirements and criteria for assessing the loyalty, trustworthiness and reliability of an individual in order to be granted a PSC as well as the requirements for renewal of PSC as set out in the Directive on Personnel Security.

12. Naton siviili- ja sotilaselimet vastaavat henkilöstönsä henkilöturvallisuusselvitystodistushakemusten ja uusimispyyntöjen jättämisestä asianomaiselle kansalliselle turvallisuusviranomaiselle tai määrätylle turvallisuusviranomaiselle tai muulle toimivaltaiselle turvallisuusviranomaiselle.

12. NATO Civil and Military bodies are responsible for submitting PSC applications and renewals for their staff to the relevant NSA/DSA or other competent security authority.

13. Kansallisten turvallisuusviranomaisten tai määrättyjen turvallisuusviranomaisten tai muiden toimivaltaisten turvallisuusviranomaisten, Naton jäsenvaltioiden ja Naton siviili- tai sotilaselinten päälliköiden yksityiskohtaiset vastuut on määritelty henkilöstöturvallisuusdirektiivissä.

13. The detailed responsibilities of NSAs/DSAs or other competent security authorities, NATO Nations and the Heads of a NATO Civil or Military bodies are set out in the Directive on Personnel Security.

TURVALLISUUSKOULUTUS JA -TIETOISUUS

SECURITY EDUCATION AND AWARENESS

14. Kaikkia henkilöitä, jotka työskentelevät tehtävissä, joissa heillä on pääsy turvalli-

14. All individuals employed in positions where they have access to information classified NR, or hold a PSC for access to NC or

suusluokkaan NATO RESTRICTED kuuluvaan tietoon tai joilla on henkilöturvallisuusselvitystodistus, joka antaa heille pääsyn turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon, on ohjeistettava turvallisuusmenettelyistä ja heidän turvallisuusvelvoitteistaan. Kaikkien turvallisuusselvitettyjen henkilöiden on vakuutettava ymmärtävänsä täysin vastuunsa ja heihin mahdollisesti kohdistuvat seuraukset siitä, että Naton turvallisuusluokiteltua tietoa joutuu luvattomiin käsiin joko tahallisesti tai huolimattomuudesta. Tiedon tästä vakuutuksesta säilyttää se Naton jäsenvaltio tai Naton siviili- tai sotilaselin, joka on myöntänyt pääsyn Naton turvallisuusluokiteltuun tietoon.

above, shall be briefed on security procedures and their security obligations. All cleared individuals shall acknowledge that they fully understand their responsibilities and the potential consequences to them when NATO Classified Information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement shall be maintained by the NATO Nation or NATO Civil or Military Body authorising access to NATO Classified Information.

15. Kaikille henkilöille, joille on myönnetty pääsy Naton turvallisuusluokiteltuun tietoon tai joiden edellytetään käsittelevän sitä, on aluksi tiedotettava ja säännöllisin väliajoin muistutettava niistä turvallisuusuhkista, joita voi aiheuttaa muun muassa:

(a) henkilöiden käyttäytyminen työpaikan ulkopuolella, mukaan lukien sosiaalisen median käyttö;

(b) varomattomat keskustelut sellaisten henkilöiden kanssa, joilla ei ole tiedonsaantitarvetta;

(c) työskentely työpaikan ulkopuolella ja matkustaessa;

(d) kyberuhkat;

(e) henkilöiden suhde tiedotusvälineisiin; ja

(f) Natoon ja Naton jäsenvaltioihin kohdistuvasta tiedustelutoiminnasta aiheutuva uhka.

15. All individuals who are authorised access to, or are required to handle NATO Classified Information, shall initially be made aware, and periodically reminded of the threats to security arising from but not limited to the following:

(a) personal conduct outside the office, including activity on social media;

(b) indiscreet conversations with individuals without the need-to-know;

(c) working outside the office and when travelling;

(d) cyber threats;

(e) their relationship with the media; and

(f) the threat presented by the activities of intelligence services which target NATO and its Nations.

16. Luonnollisten henkilöiden on välittömästi ilmoitettava asianomaisille turvallisuusviranomaisille epäilyttävinä tai epätavanomaisina pitämistään yhteydenotoista tai toimista.

16. Individuals shall report immediately to the appropriate security authorities any approach or manoeuvre which they consider suspicious or unusual.

LIITE D
TOIMITILATURVALLISUUS

JOHDANTO

1. Tässä liitteessä esitetään periaatteet ja vähimmäisvaatimukset, jotka koskevat fyysisiä turvallisuustoimenpiteitä Naton turvallisuusluokitellun tiedon suojaamiseksi. Lisätietoja ja vaatimuksia löytyy Naton turvallisuussääntöjä tukevasta toimitilaturvallisuutta koskevasta direktiivistä (AC/35-D/2001).

2. Toimitilaturvallisuudella tarkoitetaan fyysisten suojatoimenpiteiden toteuttamista kohteissa, rakennuksissa, tiloissa tai laitteistoissa, joissa on turvallisuusluokiteltua tietoa, jota on suojeltava katoamiselta tai vaarantumiselta.

3. Naton jäsenvaltioiden ja Naton siviili- ja sotilaselinten on laadittava aktiivisia ja passiivisia turvallisuustoimenpiteitä sisältävät toimitilaturvallisuuden ohjelmat, joilla saavutetaan yhteinen toimitilaturvallisuuden taso, joka vastaa suojattavan tiedon uhkista, haavoittuvuuksista, turvallisuusluokituksesta ja määrästä tehtyä arviota.

TURVALLISUUSVAATIMUKSET

4. Kaikki kohteet, rakennukset, tilat, toimistot, huoneet ja muut alueet, joissa Naton turvallisuusluokiteltua tietoa säilytetään ja/tai käsitellään ja/tai joissa siitä keskustellaan, on suojattava asianmukaisin fyysisin turvallisuustoimenpitein. Tarvittavasta toimitilaturvallisuuden suojauksen tasosta päätettäessä on otettava huomioon kaikki siihen vaikuttavat tekijät, kuten:

(a) turvallisuusluokituksen taso ja tietoluokka;

(b) säilytettävän ja/tai käsiteltävän turvallisuusluokitellun tiedon määrä ja muoto (paperi- ja/tai sähköinen muoto);

(c) kulunvalvonta ja tiedonsaantitarpeen periaatteen täytäntöönpano;

ENCLOSURE “D”
PHYSICAL SECURITY

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for physical security measures for the protection of NATO Classified Information. Additional details and requirements are found in the supporting Directive on Physical Security (AC/35-D/2001).

2. Physical security is the application of physical protective measures to sites, buildings, facilities or installations that contain classified information requiring protection against loss or compromise.

3. NATO Nations and NATO Civil and Military bodies shall establish physical security programmes, consisting of active and passive security measures, to provide a common degree of physical security consistent with the assessment of the threats, vulnerabilities, security classification and quantity of the information to be protected.

SECURITY REQUIREMENTS

4. All sites, buildings, facilities, offices, rooms, and other areas in which NATO Classified Information is stored, handled and/or discussed shall be protected by appropriate physical security measures. In deciding what degree of physical security protection is necessary, account shall be taken of all relevant factors, such as:

(a) the level of security classification and category of information;

(b) the quantity and form of the classified information (hard copy, and/or electronic) stored, and/or handled;

(c) access control and enforcement of the need-to-know principle;

(d) Natoon ja/tai Naton jäsenvaltioihin kohdistuvasta vihamielisestä tiedustelutoiminnasta aiheutuva uhka sekä paikallisesti arvioitu terrorismin, vakoilun, sabotaasin, kumouksellisen toiminnan ja (järjestäytyneen) rikollisuuden uhka; ja

(e) turvallisuusluokitellun tiedon tallennustavat (esimerkiksi paperiasiakirja tai sähköinen ja salattu).

(d) the threat from hostile intelligence services which target NATO and/or its member Nations, and the locally-assessed threat of terrorism, espionage, sabotage, subversion and (organized) crime; and

(e) how the classified information will be stored (e.g. hard copy or electronic and encrypted).

5. Fyysisten turvallisuustoimenpiteiden tarkoituksena on:

(a) estää tunkeutuminen salaa tai väkisin;

(b) ehkäistä, estää ja havaita sisäpiiriuhkan toimet;

(c) mahdollistaa Naton turvallisuusluokiteltuun tietoon pääsevän henkilöstön erottelu sen perusteella, minkä tasoinen henkilöturvallisuusselvitystodistus heillä on ja mikä heidän tiedonsaantitarpeensa on; ja

(d) havaita kaikki tietoturvapoikkeamat ja ryhtyä niiden osalta tarvittaviin toimenpiteisiin mahdollisimman nopeasti.

5. Physical security measures shall be designed to:

(a) deny surreptitious or forced entry by an intruder;

(b) deter, impede and detect actions from the insider threat;

(c) allow for segregation of personnel in their access to NATO Classified Information in accordance with their level of Personnel Security Clearance (PSC) and the need-to-know principle; and

(d) detect and act upon all security incidents as soon as possible.

TOIMITILATURVALLISUUTTA KOSKEVAT YLEISET VAATIMUKSET

6. Fyysiset toimenpiteet ovat vain osa suojaavaa turvallisuutta, ja niitä tukemassa on oltava vakaat henkilöstöturvallisuuden, tietoturvallisuuden ja viestintä- ja tietojärjestelmien turvallisuustoimenpiteet. Turvallisuusriskien järkevään hallintaan kuuluu, että luodaan oikeasuhteisimmat, tehokkaimmat ja kustannusvaikuttavimmat keinot torjua uhkia ja kompensoida haavoittuvuuksia näiden alojen suojatoimenpiteitä yhdistäen. Tehokkuus ja kustannusvaikuttavuus saavutetaan parhaiten määrittelemällä toimitilaturvallisuuden vaatimukset osana tilojen suunnittelua ja rakentamista, mikä vähentää kalliiden peruskorjausten tarvetta.

GENERAL PHYSICAL SECURITY REQUIREMENTS

6. Physical measures represent only one aspect of protective security and shall be supported by sound personnel security, security of information, and Communication and Information Systems (CIS) security measures. Sensible management of security risks will involve establishing the most proportionate, efficient and cost-effective methods of countering the threats and compensating for vulnerabilities by a combination of protective measures from these domains. Such efficiency and cost-effectiveness is best achieved by defining physical security requirements as part of the planning and design of facilities, thereby reducing the need for costly renovations.

7. Toimitilaturvallisuuden ohjelmien on perustuttava syvyyssuuntaisen turvallisuuden periaatteeseen, ja niissä on käytettävä asianmukaista yhdistelmää täydentäviä fyysisiä

7. Physical security programmes shall be based on the principle of “defence in depth”, using an appropriate combination of complementary physical security measures

turvallisuustoimenpiteitä, jotka tarjoavat sellaisen suojan tason, joka täyttää organisaation ja sen tietojen kriittisyyteen ja haavoittuvuuteen liittyvät vaatimukset.

8. Vaikka fyysiset turvallisuustoimenpiteet ovat kohdekohtaisia ja ne perustuvat useisiin tekijöihin, niiden tulee noudattaa seuraavia yleisiä periaatteita:

(a) ensin on tunnistettava suojattavat resurssit. Tämän jälkeen luodaan kerroksellisia turvallisuustoimenpiteitä, joilla rakennetaan syvyyssuuntainen turvallisuus ja viivyttävät tekijät;

(b) uloimmat fyysiset turvallisuustoimenpiteet rajaavat suojatun alueen ja estävät luvattoman pääsyn;

(c) seuraava toimenpiteiden taso havaitsee luvattoman pääsyn tai sen yrityksen ja varoittaa vartiointihenkilöstöä; ja

(d) sisin toimenpiteiden taso viivyttää tunkeilijoita niin kauan, että vartiointihenkilöstö voi heidät pidättää. Näin ollen vartijoiden vasteaika ja tunkeilijoiden viivyttämiseen suunnitellut fyysiset turvallisuustoimenpiteet liittyvät toisiinsa.

9. Fyysisen turvallisuuden laitteet (kuten kameravalvonta, tunkeutumisen ilmaisujärjestelmä, turvakaapit) on huollettava säännöllisesti tai erityisestä syystä sen varmistamiseksi, että ne toimivat parhaalla mahdollisella tavalla. Yksittäisten turvallisuustoimenpiteiden tehokkuutta sekä koko turvallisuusjärjestelmää on myös tarpeen arvioida määräajoin uudelleen. Tämä on erityisen tärkeää, jos kohteen käytössä tai erityisissä turvallisuusjärjestelmän osissa tapahtuu muutoksia. Tämä voidaan saavuttaa turvallisuussuunnitelmien säännöllisellä harjoittelulla.

Turva-alueet

10. Pysyvät tai tilapäiset alueet, joilla turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa säilytetään tai käsitellään tai joissa siitä keskustellaan, on järjestettävä ja jäsennettävä siten, että ne vastaavat jotakin seuraavista:

which provide a degree of protection meeting the requirements associated with the criticality and vulnerability of the organization and its information.

8. Although physical security measures are site-specific, and determined by a number of factors, the following general principles shall apply:

(a) it is first necessary to identify the assets that require protection. This is followed by the creation of layered security measures to provide “defence in depth” and delaying factors;

(b) the outermost physical security measures shall define the protected area and deter unauthorised access;

(c) the next layer of measures shall detect unauthorised or attempted access and alert the guard force; and

(d) the innermost layer of measures shall sufficiently delay intruders until they can be detained by the guard force. Consequently, there is an interrelationship between the reaction time of the guard force and the physical security measures designed to delay intruders.

9. Equipment that provides physical security (e.g. CCTV, IDS, secure cabinets) shall be maintained regularly or in response to a specific cause to ensure that it operates at optimum performance. It is also necessary to periodically re-evaluate the effectiveness of individual security measures as well as the complete security system. This is particularly important if there is a change in use of the site or specific elements of the security system. This can be achieved by regularly exercising security plans.

Security Areas

10. Areas**,** either fixed or temporary, in which information classified NATO CONFIDENTIAL (NC) and above is stored, handled and/or discussed shall be organised and structured so as to correspond to one of the following:

(a) **Naton luokan I turva-alue**: erityisen arkaluonteinen alue, jossa turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa säilytetään ja/tai käsitellään ja/tai siitä keskustellaan siten, että alueelle tulo merkitsee käytännössä Naton turvallisuusluokiteltuun tietoon pääsyä, jolloin luvaton tulo alueelle olisi tietoturvaloukkaus.

Tällaisia alueita voivat olla operaatiotilat, viestintäkeskukset tai arkistotilat, ja niissä täytyy olla:

(i) selkeästi määritetyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos;

(ii) kulunvalvontajärjestelmä, joka päästää alueelle vain henkilöt, joilla on asianmukainen turvallisuusselvitys ja erityinen lupa[1] tulla alueelle;

(iii) määrittely turvallisuusluokituksen tasosta ja alueella tavanomaisesti säilytettävän tiedon luokasta eli siitä tiedosta, johon alueelle tulo antaa pääsyn; ja

(iv) selkeä maininta siitä, että alueelle tulo vaatii paikallisen turvallisuusviranomaisen erityisen luvan. Tämä maininta voi sisältää tiedon turvallisuusluokituksen tasosta ja/tai alueen arkaluonteisuudesta.

(b) **Naton luokan II turva-alue**: alue, jolla turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa säilytetään ja/tai käsitellään ja/tai siitä keskustellaan siten, että ulkopuolisten henkilöiden pääsy tietoon voidaan estää sisäisesti perustetuin valvontajärjestelmin.

(a) **NATO Class I Security Area**: a particularly sensitive area in which information classified NC and above is stored, handled and/or discussed in such a way that entry into the area constitutes, for all practical purposes, access to NATO Classified Information and therefore unauthorised entry would constitute a Security Breach.

Such areas may include operations rooms, communications centres or archive facilities and require:

(i) a clearly defined and protected perimeter through which all entry and exit is controlled;

(ii) an entry control system which grants access only to those individuals appropriately cleared and specifically authorised[1] to enter the area;

(iii) a determination of the level of security classification and the category of the information normally held in the area, i.e. the information to which entry gives access; and

(iv) a clear indication that entrance into such areas requires specific authorization by the local security authority. This indication may include the level of security classification and/or the sensitivity of the area.

(b) **NATO Class II Security Area:** an area in which information classified NC and above is stored, handled and/or discussed in such a way that it can be protected from access by unauthorised individuals through utilizing controls established internally.

---

[1] Erityisen luvan haltijoilla tarkoitetaan henkilöstöä, joilla on muodollisesti tunnustettu tiedonsaantitarve ja pääsy tietoon työtehtäviensä luonteen perusteella ja jotka ovat kulunvalvontalistalla, sekä henkilöitä, jotka kyseessä olevan organisaation päällikkö on tapauskohtaisesti muodollisesti valtuuttanut suorittamaan tiettyä tehtävää.

[1] Specifically authorised refers to those personnel who have been formally recognised as having a need-to-know and access based on the nature of their employment responsibilities, and are included on an access control list, as well as individuals who have been formally authorised by the head of the organization in question on an ad hoc basis to perform a specific role or duty.

Tällaisia alueita voivat olla työskentelytilat tai neuvotteluhuoneet, joissa Naton turvallisuusluokiteltua tietoa säilytetään, ja/tai käsitellään ja/tai siitä keskustellaan. Näillä alueilla täytyy olla:

(i) selkeästi määritetyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos;

(ii) kulunvalvontajärjestelmä, joka päästää alueelle ilman saattajaa vain henkilöt, joilla on asianmukainen turvallisuusselvitys ja lupa tulla alueelle; ja

(iii) saattaja tai vastaava valvontamekanismi, jonka avulla järjestetään sellaisten henkilöiden kulku, jotka eivät täytä edellä b) ii) alakohdassa kuvattuja perusteita, jotta voidaan estää luvaton pääsy Naton turvallisuusluokiteltuun tietoon ja hallitsematon pääsy alueille, jotka on nimenomaisesti nimetty teknisiltä hyökkäyksiltä ja salakuuntelulta suojatuiksi alueiksi.

Such areas may include working offices or meeting rooms where NATO Classified Information is stored, handled and/or discussed. These areas require:

(i) a clearly defined and protected perimeter through which all entry and exit is controlled;

(ii) an entry control system which permits unescorted access only to those individuals who are security cleared and authorised to enter the area; and

(iii) an escort or equivalent control mechanism to deal with those individuals who do not meet the criteria described in sub-paragraph (b) (ii) above in order to prevent unauthorised access to NATO Classified Information and uncontrolled entry to areas which have been specifically designated as protected against technical attacks and eavesdropping.

Hallinnollinen vyöhyke

11. Naton luokan I tai II turva-alueiden ympärille tai niille johtavalle alueelle on perustettava hallinnollinen vyöhyke. Hallinnollisilla vyöhykkeillä sallitaan vain turvallisuusluokkaan NATO RESTRICTED kuuluvan tiedon säilyttäminen ja/tai käsittely ja/tai siitä keskusteleminen. Tällaisilla alueilla on oltava selkeästi määritetyt näkyvät rajat, joilla on mahdollisuus tarkastaa henkilöt ja ajoneuvot. Henkilöt eivät kuitenkaan tarvitse saattajaa.

Administrative Zone

11. An Administrative Zone shall be established around or leading to NATO Class I or Class II Security Areas. Only information classified NATO RESTRICTED (NR) may be stored, handled and/or discussed in Administrative Zones. Such areas require a visibly defined perimeter, within which the possibility exists for the control of individuals and vehicles. However, individuals are not required to be escorted.

Teknisesti suojatut turva-alueet

12. Teknisesti suojatut turva-alueet ovat joko pysyviä tai tilapäisiä alueita, jotka on nimenomaisesti tunnistettu teknisiltä hyökkäyksiltä ja salakuuntelulta suojattaviksi alueiksi. Tällaisilla alueilla on tehtävä säännöllisiä fyysisiä ja teknisiä tarkastuksia, ja niille kulkua on valvottava tarkasti. Teknisiltä hyökkäyksiltä ja salakuuntelulta on suojauduttava seuraavilla toimenpiteillä:

Technically Secure Areas

12. Technically Secure Areas, either fixed or temporary, are areas which have been specifically identified as requiring protection against technical attacks and eavesdropping. Such areas shall be subject to regular physical and technical inspections and entry to them shall be strictly controlled. The following measures shall be applied to protect against technical attacks and eavesdropping:

(a) Asianmukainen fyysisten ja teknisten turvallisuustoimenpiteiden taso kulunvalvonnan toteuttamiseksi riskiin perustuen. Riskin määrittämisen vastuun jakavat asianmukaiset tekniset asiantuntijat sekä turvallisuusviranomainen, joka neuvoo riskin omistajaa päätöksentekoon tai hyväksymiseen liittyen.

(b) Tällaiset alueet on lukittava ja/tai niitä on vartioitava silloin, kun niitä ei käytetä, ja kaikkia avaimia tulee käsitellä turva-avaimina. Alueella on tehtävä säännöllisiä fyysisiä ja/tai teknisiä tarkastuksia asianmukaisen turvallisuusviranomaisen vaatimusten mukaisesti. Tarkastuksia on tehtävä myös luvattoman alueelle tulon tai sen epäilyn jälkeen sekä ulkopuolisen henkilöstön (esimerkiksi huoltotöiden tai remontin vuoksi) alueelle tulon jälkeen.

(c) Näille alueille ei saa tuoda mitään esineitä, kalusteita tai laitteita ennen kuin koulutettu turvallisuushenkilöstö on tutkinut ne salakuuntelulaitteiden varalta. Kaikista alueelle tuoduista tai viedyistä esineistä, kalusteista ja laitteista on pidettävä asianmukaista luetteloa.

(d) Alueilla ei saa olla tallentavia ja/tai lähettäviä elektronisia järjestelmiä tai laitteita.

(e) Alueille ei yleensä saa asentaa puhelimia ja muita videoneuvottelulaitteita. Jos niiden asentaminen kuitenkin on välttämätöntä, ne tulee irrottaa verkosta, kun tilassa keskustellaan turvallisuusluokitelluista asioista. Tämä ei koske asianmukaisesti asennettuja ja hyväksyttyjä viestintävälineitä.

(a) Appropriate level of physical and technical security measures to enforce access control, based upon the risk. The responsibility for determining the risk is shared between the appropriate technical specialists and the security authority which provides advice to the risk owner for a decision/approval.

(b) Such areas shall be locked and/or guarded when not occupied and any keys shall be treated as security keys. Regular physical and/or technical inspections, in accordance with the requirements of the appropriate security authority, shall be undertaken. Such inspections shall also be conducted following any unauthorised entry or suspicion thereof, as well as following the entry by external personnel (e.g. for the purposes of maintenance work, redecoration).

(c) No item, furnishing or equipment shall be allowed into these areas until they have been thoroughly examined for eavesdropping devices by trained security staff. An appropriate record of items, furnishing and equipment moved into and out of these areas shall be maintained.

(d) The presence of any electronic systems or devices with recording and/or transmitting capabilities shall be prohibited.

(e) Telephones and other video conference devices shall normally not be installed in such areas. However, where their installation is unavoidable, they shall be physically disconnected when classified discussions take place. This does not apply to appropriately installed and approved communication devices.

ERITYISET FYYSISET TURVALLISUUSTOIMENPITEET

13. Erilaiset erityiset fyysiset ja tekniset turvallisuustoimenpiteet ja -menettelyt voivat edistää organisaation tai kohteen turvallisuuskehystä. Tällaisiin toimiin ja menettelyihin kuuluvat muun muassa: rajattu-alue, tunkeutumisen ilmaisujärjestelmä, kulunval-

SPECIFIC PHYSICAL SECURITY MEASURES

13. Various specific physical and technical security measures and procedures can contribute to the security framework of an organization or site. Such measures and procedures include but are not limited to: Perimeter, Intrusion Detection System (IDS), Ac-

vonta, kameravalvonta, turvavalaistus, turvakaapit ja toimistokalusteet, lukot, avainten ja numeroyhdistelmien valvonta, vierailijahallinta, sisään- ja ulostulotarkastukset. Tarkempia tietoja erityisistä fyysisistä ja teknisistä turvallisuustoimenpiteistä ja -menettelyistä on Naton turvallisuussääntöjä tukevassa toimitilaturvallisuutta koskevassa direktiivissä.

cess Control, Closed Circuit Television, Security Lighting, Secure Cabinets and Office Furniture, Locks, Control of Keys and Combinations, Visitor Control, Entry and Exit Searches. The supporting Directive on Physical Security provides detailed information on specific physical and technical security measures and procedures.

NATON TURVALLISUUSLUOKITELLUN TIEDON SÄILYTTÄMISEN VÄHIMMÄISVAATIMUKSET

14. Naton turvallisuusluokiteltua tietoa on säilytettävä alueilla, turvakaapeissa ja/tai toimistokalusteissa, jotka on suunniteltu estämään ja havaitsemaan luvattoman pääsyn tietoon.

MINIMUM STANDARDS FOR STORAGE OF NATO CLASSIFIED INFORMATION

14. NATO Classified Information shall be stored in areas, secure cabinets and/or office furniture designed to deter and detect unauthorised access to the information.

15. **COSMIC TOP SECRET (CTS)**. Turvallisuusluokkaan COSMIC TOP SECRET kuuluva tieto on säilytettävä luokan I tai II turva-alueella noudattaen jotain seuraavista ehdoista:

(a) hyväksytyssä turvakaapissa soveltaen ainakin yhtä seuraavista lisävalvontakeinoista:

(i) jatkuva suojaus turvallisuusselvitetyn vartiointihenkilöstön tai päivystyshenkilöstön toimesta;

(ii) turvakaapin tarkastus vähintään kahden tunnin välein satunnaisin väliajoin turvallisuusselvitetyn vartiointihenkilöstön tai päivystyshenkilöstön toimesta; tai

(iii) hyväksytty tunkeutumisen ilmaisujärjestelmä ja hälytyksiin vastaava turvallisuushenkilöstö, joka hälytyksen saatuaan saapuu paikalle siinä ajassa, jonka arvioidaan kuluvan turvakaapin poistamiseen tai murtamiseen tai käytössä olevien fyysisten turvallisuustoimenpiteiden nujertamiseen;

(b) toimitilaturvallisuutta koskevan direktiivin vaatimusten mukaisesti rakennetulla avoimella varastoalueella, jossa on tunkeutumisen ilmaisujärjestelmä sekä hälytyksiin vastaava turvallisuushenkilöstö, joka hälytyksen saatuaan saapuu paikalle

15. **COSMIC TOP SECRET (CTS).** Information classified CTS shall be stored within a Class I or Class II Security Area under one of the following conditions:

(a) in an approved secure cabinet with one of the following supplemental controls:

(i) continuous protection by cleared guard or duty personnel;

(ii) inspection of the secure cabinet not less than every two hours, at randomly timed intervals, by cleared guard or duty personnel; or

(iii) an approved IDS in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed to remove or break open the secure cabinet, or overcome the physical security measures in place;

(b) in an open storage area constructed in accordance with the requirements set out in the supporting Directive on Physical Security, which is equipped with an IDS in combination with a response force that will, after an alarm annunciation, arrive at the

siinä ajassa, jonka arvioidaan kuluvan alueelle väkisin tunkeutumiseen; tai

(c) tunkeutumisen ilmaisujärjestelmällä varustetussa kassaholvissa, jonka lisäksi on oltava hälytyksiin vastaava turvallisuushenkilöstö, joka hälytyksen saatuaan saapuu paikalle siinä ajassa, jonka arvioidaan kuluvan kassaholviin väkisin tunkeutumiseen.

location within the estimated timeframe needed for forced entry; or

(c) in an IDS-equipped vault in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed for forced entry.

16. **NATO SECRET (NS)**. Turvallisuusluokkaan NATO SECRET kuuluva tieto on säilytettävä luokan I tai II turva-alueella jollakin seuraavalla tavalla:

(a) siten kuin turvallisuusluokkaan COSMIC TOP SECRET kuuluvan tiedon säilyttämisestä on määrätty;

(b) hyväksytyssä turvakaapissa tai kassaholvissa ilman lisävalvontakeinoja; tai

(c) avoimella varastoalueella, jolloin edellytetään ainakin yhtä seuraavista lisävalvontakeinoista:

(i) avoimen varastoalueen sijoitustilaa suojaa jatkuvasti turvallisuusselvitetty vartiointihenkilöstö tai päivystyshenkilöstö;

(ii) turvallisuusselvitetty vartiointihenkilöstö tai päivystyshenkilöstö tarkastaa avoimen varastoalueen vähintään kerran neljän tunnin välein; tai

(iii) tunkeutumisen ilmaisujärjestelmä, jonka lisäksi on oltava hälytyksiin vastaava turvallisuushenkilöstö, joka hälytyksen saatuaan saapuu paikalle siinä ajassa, jonka arvioidaan kuluvan alueelle väkisin tunkeutumiseen.

16. **NATO SECRET (NS).** Information classified NS shall be stored within a Class I or Class II Security Area by one of the following methods:

(a) in the same manner as prescribed for information classified CTS;

(b) in an approved secure cabinet or vault without supplemental controls; or

(c) in an open storage area, in which case one of the following supplemental controls is required:

(i) the location that houses the open storage area shall be subject to continuous protection by cleared guard or duty personnel;

(ii) cleared guard or duty personnel shall inspect the open storage area not less than once every four hours; or

(iii) an IDS in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed for forced entry.

17. **NATO CONFIDENTIAL (NC)**. Turvallisuusluokkaan NATO CONFIDENTAL kuuluva tieto on säilytettävä luokan I tai II turva-alueella hyväksytyssä turvakaapissa.

17. **NATO CONFIDENTIAL (NC).** Information classified NC shall be stored in a Class I or Class II Security Area in an approved secure cabinet.

18. **NATO RESTRICTED (NR)**. Turvallisuusluokkaan NATO RESTRICTED kuuluva tieto on säilytettävä lukitussa kaapissa tai toimistokalusteessa (esimerkiksi toimistopöydän laatikossa) hallinnollisella vyöhykkeellä, luokan I turva-alueella tai luokan

18. **NATO RESTRICTED (NR).** Information classified NR shall be stored in a locked cabinet or office furniture (e.g. office desk drawer) within an Administrative

II turva-alueella. Turvallisuusluokkaan NATO RESTRICTED kuuluvaa tietoa voidaan säilyttää myös lukitussa kaapissa, kassaholvissa tai avoimella varastoalueella, joka on hyväksytty turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempään turvallisuusluokkaan kuuluvan tiedon säilyttämiseen.

Zone, Class I Security Area, or Class II Security Area. Information classified NR may also be stored in a locked cabinet, vault, or open storage area approved for information classified NC or higher.

19. Lisätietoja ja -vaatimuksia Naton turvallisuusluokitellun tiedon säilyttämisestä annetaan Naton turvallisuussääntöjä tukevassa toimitilaturvallisuutta koskevassa direktiivissä.

19. Additional details and requirements for the storage of NATO Classified Information are set out in the supporting Directive on Physical Security.

VIESTINTÄ- JA TIETOJÄRJESTELMIEN FYYSINEN SUOJAAMINEN

PHYSICAL PROTECTION OF COMMUNICATION AND INFORMATION SYSTEMS

20. Alueet, joilla Naton turvallisuusluokiteltua tietoa esitetään tai käsitellään tietotekniikkaa käyttäen, tai joilla on mahdollista päästä sellaiseen tietoon, on perustettava niin, että luottamuksellisuuden, eheyden ja käytettävyyden kokonaisvaatimus täyttyy.

20. Areas in which NATO Classified Information is presented or handled using information technology, or where potential access to such information is possible, shall be established in a way that the aggregate requirement for confidentiality, integrity and availability is met.

21. Alueet, joilla viestintä- ja tietojärjestelmiä käytetään turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempiin turvallisuusluokkiin kuuluvan tiedon näyttämiseen, tallentamiseen, käsittelyyn tai siirtämiseen tai joissa on mahdollista päästä sellaiseen tietoon, on perustettava Naton luokan I tai II turva-alueena tai vastaavan kansallisen tason alueena. Alueet, joilla viestintä- ja tietojärjestelmiä käytetään turvallisuusluokkaan NATO RESTRICTED kuuluvan tiedon näyttämiseen, tallentamiseen, käsittelyyn tai siirtämiseen tai joilla on mahdollista päästä sellaiseen tietoon, voidaan perustaa hallinnollisina vyöhykkeinä.

21. Areas in which CIS are used to display, store, process, or transmit information classified NC and above, or where potential access to such information is possible, shall be established as NATO Class I or Class II Security Areas or the national equivalent. Areas in which CIS are used to display, store, process or transmit information classified NR, or where potential access to such information is possible, may be established as Administrative Zones.

22. Pääsyä alueille, joilla säilytetään ja hallitaan kriittisiä viestintä- ja tietojärjestelmien osia, on nimenomaisesti valvottava, ja pääsy on rajoitettava koskemaan vain sellaista turvallisuuteen ja järjestelmä-/verkko-/salaushallintaan liittyvää henkilöstöä, jolla on lupa olla alueella.

22. Access to areas where critical CIS components are housed and managed shall be specifically controlled and limited to only authorised personnel associated with security and system/network/crypto administration.

SUOJAAMINEN TEKNISILTÄ HYÖKKÄYKSILTÄ

23. Työskentelytilat tai alueet, joissa säännöllisesti keskustellaan turvallisuusluokkaan NATO SECRET tai sitä ylempiin turvallisuusluokkiin kuuluvasta tiedosta, on suojattava passiivisia ja aktiivisia salakuuntelu-hyökkäyksiä vastaan luotettavilla fyysisillä turvallisuustoimenpiteillä ja kulunvalvonnalla, kun riski sitä edellyttää. Vastuu riskin määrittämisestä tulee koordinoida teknisten asiantuntijoiden kanssa, ja siitä päättää asianmukainen turvallisuusviranomainen. Lisätietoja passiiviselta ja aktiiviselta salakuuntelulta suojautumisesta on Naton turvallisuussääntöjä tukevassa toimitilaturvallisuutta koskevassa direktiivissä.

PROTECTION AGAINST TECHNICAL ATTACKS

23. Offices or areas in which information classified NS and above is regularly discussed shall be protected against passive and active eavesdropping attacks, by means of sound physical security measures and access control, where the risk warrants it. The responsibility for determining the risk shall be co-ordinated with technical specialists and decided by the appropriate security authority. The supporting Directive on Physical Security provides details on protection against passive and active eavesdropping.

HYVÄKSYTYT LAITTEET

24. Naton jäsenvaltioiden tulee käyttää vain sellaisia laitteita, jotka asianmukainen turvallisuusviranomainen on hyväksynyt Naton turvallisuusluokitellun tiedon suojaamiseen. Naton siviili- ja sotilaselinten on varmistettava, että hankitut laitteet on hyväksytty käyttöön vastaavissa olosuhteissa jossakin Naton jäsenvaltiossa. Naton siviili- ja sotilaselimet voivat myös hankkia asianmukaisen turvallisuusviranomaisen käyttöön hyväksymiä laitteita, kun hankinta perustuu tehtyyn riskinarviointiin, joka tukee tunnistetun riskin tai tunnistettujen riskien vähentämistä tai lieventämistä.

APPROVED EQUIPMENT

24. NATO Nations shall only use equipment which has been approved for the protection of NATO Classified Information by an appropriate security authority. NATO Civil and Military bodies shall ensure that any equipment purchased has been approved for use by one of the NATO Nations in similar conditions. NATO Civil and Military bodies may also purchase equipment approved for use by an appropriate security authority based on a completed risk assessment that supports the reduction or mitigation of the identified risk(s).

LIITE E
NATON TURVALLISUUSLUOKITELLUN TIEDON TURVALLISUUS

JOHDANTO

1. Tässä liitteessä esitetään Naton turvallisuusluokitellun tiedon turvallisuutta koskevat periaatteet ja vähimmäisvaatimukset. Lisätietoja ja -vaatimuksia on Naton turvallisuussääntöjä tukevassa direktiivissä Naton turvallisuusluokitellun tiedon turvallisuudesta (AC/35-D/2002).

2. Tietoturvallisuus on yleisten suojaustoimenpiteiden ja -menettelyjen soveltamista turvallisuusluokitellun tiedon katoamisen tai vaarantumisen estämiseksi, sekä katoamisen tai vaarantumisen havaitsemiseksi ja korjaamiseksi. Turvallisuusluokiteltua tietoa on suojattava koko sen elinkaaren ajan sen turvallisuusluokan mukaisella tasolla. Tietoa hallittaessa varmistetaan, että se on asianmukaisesti luokiteltu, selvästi määritetty turvallisuusluokitelluksi ja pysyy turvallisuusluokiteltuna ainoastaan niin kauan kuin tämä on tarpeen. Tietoturvallisuutta täydennetään henkilöstöturvallisuudella, toimitilaturvallisuudella sekä viestintä- ja tietojärjestelmien turvallisuudella, jotta varmistetaan tasapainoinen toimenpiteiden kokonaisuus Naton turvallisuusluokitellun tiedon suojaamiseksi.

NATON TURVALLISUUSLUOKAT, ERITYISET TUNNUKSET, MERKINNÄT JA YLEISET PERIAATTEET

3. Alkuperäinen luovuttaja vastaa turvallisuusluokitellun tiedon turvallisuusluokan määrittämisestä ja tiedon alustavasta jakelusta.

4. Turvallisuusluokkaa ei saa vaihtaa eikä alentaa eikä turvallisuusluokitusta saa poistaa ilman alkuperäisen luovuttajan suostumusta. Turvallisuusluokkaa määrittäessään alkuperäinen luovuttaja ilmoittaa mahdollisuuksien mukaan, voidaanko sitä alentaa tai

ENCLOSURE “E”
SECURITY OF NATO CLASSIFIED INFORMATION

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for the security of NATO Classified Information. Additional details and requirements are found in the supporting Directive on the Security of NATO Classified Information (AC/35-D/2002).

2. Security of information is the application of general protective measures and procedures to prevent, detect and recover from the loss or compromise of classified information. Classified information shall be protected throughout its life cycle to a level commensurate with its security classification. It shall be managed to ensure that it is appropriately classified, is clearly identified as classified and remains classified only as long as this is necessary. Security of information shall be complemented by Personnel, Physical and Communication and Information Systems (CIS) Security in order to ensure a balanced set of measures for the protection of NATO Classified Information.

NATO SECURITY CLASSIFICATIONS, SPECIAL DESIGNATORS, MARKINGS AND GENERAL PRINCIPLES

3. The originator is responsible for determining the security classification and initial dissemination of classified information.

4. The security classification shall not be changed, downgraded or declassified without the consent of the originator. At the time of its creation, the originator shall indicate,

voidaanko tiedon luokitus poistaa tiettynä ajankohtana tai tietyn tapahtuman jälkeen.

where possible, whether their classified information can be downgraded or declassified on a certain date or event.

5. Tiedolle annettu turvallisuusluokka määrää sen, minkälaisella toimitilaturvallisuudella ja viestintä- ja tietojärjestelmien turvallisuudella tietoa suojataan sitä säilytettäessä, siirrettäessä, välitettäessä, jaettaessa ja hävitettäessä sekä minkälaista henkilöturvallisuusselvitystodistusta pääsy kyseiseen tietoon edellyttää. Siksi tosiasiallisen turvallisuuden ja tehokkuuden vuoksi on vältettävä tiedon luokittelemista sekä liian korkeaan että liian alhaiseen turvallisuusluokkaan.

5. The security classification assigned determines the physical and CIS Security provided to the information in storage, transfer and transmission, its circulation, destruction and the Personnel Security Clearance (PSC) required for access. Therefore, both overclassification and underclassification shall be avoided in the interests of effective security as well as efficiency.

6. Turvallisuusluokat merkitään turvallisuusluokiteltuun tietoon osoittamaan sitä vahinkoa, joka Naton ja/tai sen jäsenvaltioiden turvallisuudelle voi aiheutua, jos tieto altistuu luvattomalle ilmitulolle. Turvallisuusluokitellun tiedon alkuperäisellä luovuttajalla on etuoikeus määrätä turvallisuusluokka tai muuttaa sitä. Naton turvallisuusluokat ja niiden merkitykset ovat seuraavat:

6. Security classifications shall be applied to classified Information in order to indicate the possible damage to the security of NATO and/or its member Nations if the information is subjected to unauthorised disclosure. It is the prerogative of the originator of the classified information to determine or modify the security classification. NATO security classifications and their significance are:

(a) COSMIC TOP SECRET (CTS)
luvaton ilmitulo aiheuttaisi Natolle poikkeuksellisen vakavaa vahinkoa;

(a) COSMIC TOP SECRET (CTS)
unauthorised disclosure would result in exceptionally grave damage to NATO;

(b) NATO SECRET (NS)
luvaton ilmitulo aiheuttaisi Natolle vakavaa vahinkoa;

(b) NATO SECRET (NS)
unauthorised disclosure would result in grave damage to NATO;

(c) NATO CONFIDENTIAL (NC)
luvaton ilmitulo aiheuttaisi Natolle vahinkoa; ja

(c) NATO CONFIDENTIAL (NC)
unauthorised disclosure would be damaging to NATO; and

(d) NATO RESTRICTED (NR)
luvaton ilmitulo haittaisi Naton etuja tai sen toiminnan tehokkuutta.

(d) NATO RESTRICTED (NR)
unauthorised disclosure would be detrimental to the interests or effectiveness of NATO.

7. Naton turvallisuusluokat osoittavat Naton turvallisuusluokitellun tiedon arkaluonteisuuden, ja niitä sovelletaan tarkoituksena kiinnittää vastaanottajien huomio tarpeeseen varmistaa tiedon suojaaminen sen vahingon vakavuuden mukaan, joka luvattomasta pääsystä tietoon tai sen luvattomasta ilmitulosta aiheutuisi.

7. NATO security classifications indicate the sensitivity of NATO Classified Information and are applied in order to alert recipients to the need to ensure protection in proportion to the degree of damage that would occur from unauthorised access or disclosure.

8. Ryhmään NATO UNCLASSIFIED kuuluvaa tietoa ja julkista tietoa suojataan ja käsitellään Naton tiedonhallinnan periaatteiden (C-M(2007)0118) ja Naton turvallisuusluokittelemattoman tiedon hallintaa koskevan asiakirjan (C-M(2002)60) mukaisesti.

8. NATO UNCLASSIFIED information and Information releasable to the Public shall be protected and handled in accordance with the NATO Information Management Policy (C-M(2007)0118) and The Management of Non-Classified NATO Information (C-M(2002)60).

9. Naton operaatioiden, koulutuksen, harjoitusten, transformaation ja yhteistyön (OTETC) suunnittelu, valmistelu, toteuttaminen ja tukeminen voi edellyttää myös tiettyjen muiden turvallisuusnäkökulmien huomioon ottamista; Naton turvallisuussääntöjä tukeva asiakirja tiedustelutiedon ja muun tiedon jakamisesta muiden kuin Natoon kuuluvien toimijoiden kanssa (AC/35-D/1040) sisältää näissä tilanteissa sovellettavat turvallisuusmääräykset ja -ohjeet.

9. The planning, preparation, execution and support relating to NATO Operations, Training, Exercises, Transformation and Co-operation (OTETC) may require specific additional security aspects to be addressed; the Supporting Document on Information and Intelligence Sharing with Non-NATO Entities (AC/35-D/1040) contains security provisions and guidance applicable in these circumstances.

10. Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet toteuttavat toimenpiteet, joilla varmistetaan, että Naton tuottamalle ja Natolle annettavalle turvallisuusluokitellulle tiedolle määritetään oikea turvallisuusluokka ja että tämä tieto suojataan Naton turvallisuussääntöjä tukevan Naton turvallisuusluokitellun tiedon turvallisuutta koskevan direktiivin vaatimusten mukaisesti.

10. NATO Nations and NATO Civil and Military bodies shall introduce measures to ensure that classified information created by, or provided to NATO is assigned the correct security classification, and is protected in accordance with the requirements of the supporting Directive on the Security of NATO Classified Information.

11. Kukin Naton sotilas- ja siviilielin ottaa käyttöön järjestelmän, jonka avulla varmistetaan, että sen luovuttamaa turvallisuusluokkaan COSMIC TOP SECRET luokiteltua tietoa arvioidaan uudelleen vähintään viiden vuoden välein ja luokkaan NATO SECRET luokiteltua tietoa vähintään 10 vuoden välein tarkoituksena tarkistaa, onko turvallisuusluokkia edelleen sovellettava. Tätä arviointia ei tarvita, jos alkuperäinen luovuttaja on määrännyt ennalta, että tietyn Naton turvallisuusluokitellun tiedon turvallisuusluokkaa alennetaan ilman eri toimenpiteitä ennalta määrätyn ajan jälkeen, ja jos tämä on merkitty kyseiseen tietoon.

11. Each NATO Civil or Military Body shall establish a system to ensure that CTS information which it has originated is reviewed no less frequently than every five years and NS information no less frequently than every 10 years in order to ascertain whether the security classification still applies. Such a review is not necessary in those instances where the originator has predetermined that specific NATO Classified Information shall be automatically downgraded after a predetermined period and the classified information has been so marked.

12. Koko asiakirjan turvallisuusluokan on oltava vähintään yhtä korkea kuin sen korkeimmalle turvallisuusluokitellun osan luokka. Kansiasiakirjoihin on merkittävä niihin liitettyyn tietoon kokonaisuutena so-

12. The overall security classification of a document shall be at least as high as that of its most highly classified component. Covering documents shall be marked with the overall NATO security classification of the

vellettava Naton turvallisuusluokka. Mahdollisuuksien mukaan alkuperäisen luovuttajan olisi asianmukaisesti merkittävä turvallisuusluokkaan NATO RESTRICTED ja sitä ylempiin turvallisuusluokkiin luokiteltujen asiakirjojen osat, kuten kappaleet, liitteet, lisäykset jne., helpottaakseen päätöksiä asiakirjojen jakelusta eteenpäin.

information to which they are attached. Where possible, component parts like paragraphs, enclosures, annexes, etc., of documents classified NR and above should be marked appropriately by the originator to facilitate decisions on further dissemination.

13. Kun suuri määrä Naton turvallisuusluokiteltua tietoa kootaan yhteen, sen alkuperäiset turvallisuusluokitusmerkinnät on säilytettävä ja on arvioitava, miten tämän tietokokonaisuuden katoaminen tai vaarantuminen vaikuttaisi järjestöön. Jos tämä kokonaisvaikutus arvioidaan suuremmaksi kuin kyseisten yksittäisten Naton turvallisuusluokkien mukainen vaikutus, olisi harkittava kyseisen tietokokonaisuuden käsittelemistä ja suojaamista sen turvallisuusluokan mukaisesti, joka vastaa sen katoamisen tai vaarantumisen arvioitua vaikutusta.

13. When a large amount of NATO Classified Information is collated together, the original security classification markings shall be retained and that information shall be assessed for the impact its collective loss or compromise would have upon the organization. If this overall impact is assessed as being higher than the impact of the actual individual NATO security classifications then consideration should be given to handling and protecting it at a level commensurate with the assessed impact of its loss or compromise.

Lisämerkinnät

14. COSMIC ja NATO ovat Natoon viittaavia merkintöjä, jotka Naton turvallisuusluokiteltuun tietoon tehtyinä osoittavat, että tietoa on suojattava Naton turvallisuusperiaatteiden mukaisesti.

Qualifying Markings

14. The terms COSMIC and NATO are qualifying markings which, when applied to NATO Classified Information, signify that the information shall be protected in accordance with NATO Security Policy.

Erityisluokkien tunnukset

15. "ATOMAL" on merkintä, joka tehdään erityisluokan tietoon osoittamaan, että tieto on suojattava Pohjois-Atlantin sopimuksen osapuolten välillä ydinpuolustustietoja koskevasta yhteistyöstä tehdyn sopimuksen (C-M(64)39) ja sitä tukevien hallinnollisten järjestelyjen (C-M(68)41) mukaisesti.

Special Category Designators

15. The term "ATOMAL" is a marking applied to special category information signifying that the information shall be protected in accordance with the Agreement between the Parties to the North Atlantic Treaty for Co-operation Regarding Atomic Information (C-M(64)39) and the supporting Administrative Arrangements (C-M(68)41).

16. "SIOP" on merkintä, joka tehdään erityisluokan tietoon osoittamaan, että tiedon suojaamisessa on noudatettava asiakirjaa C-M(71)27(Revised), joka koskee erityismenettelyjä Yhdysvaltojen yhteistä operaatiosuunnitelmaa (US-SIOP) koskevan tiedon käsittelemiseksi Natossa.

16. The term "SIOP" is a marking applied to special category information signifying that the information shall be protected in accordance with "Special Procedures for the Handling of United States Single Integrated Operational Plan (US-SIOP) Information Within NATO C-M(71)27(Revised)".

17. "CRYPTO" on merkintä ja erityisluokan tunnus, joka merkitään kaikkeen COMSEC-

17. The term “CRYPTO” is a marking and a special category designator identifying all COMSEC keying material used to protect or

avainmateriaaliin, jota käytetään suojaamaan tai todentamaan televiestintää, joka sisältää Naton salausten turvallisuuteen liittyvää tietoa ja joka osoittaa, että tieto on suojattava asianmukaisten salausturvallisuusperiaatteiden ja -ohjeiden mukaisesti.

18. "BOHEMIA" on merkintä, joka tehdään viestitiedustelusta saatuun tai siihen liittyvään erityisluokan tietoon. Kaikki merkinnällä COSMIC TOP SECRET – BOHEMIA merkitty tieto suojataan noudattaen tarkasti asiakirjaa MC 101 (Naton signaalitiedustelun periaatteet) ja siihen liittyvää liittokunnan yhteistä AJP-julkaisua, jossa käsitellään sovellettavia periaatteita, sekä Naton signaalitiedustelun neuvoa-antavan komitean SIGINT-hallinnon ja -menettelyjen oppaan määräyksiä.

Merkinnät jakelun rajoittamisesta

19. Tiedon alkuperäinen luovuttaja voi käyttää merkintää jakelun rajoittamisesta lisämerkintänä, jolla Naton turvallisuusluokitellun tiedon jakelua rajoitetaan tarkemmin.

VALVONTA JA KÄSITTELY

Tilivelvollisuuden tavoitteet

20. Tilivelvollisuuden ensisijaisena tavoitteena on saada käyttöön riittävät tiedot, joiden avulla pystytään tutkimaan tahallinen tai tahaton tilivelvollisuuden alaisen tiedon katoaminen tai vaarantuminen sekä arvioimaan katoamisesta tai vaarantumisesta aiheutunut vahinko. Tilivelvollisuuden vaatimuksen tarkoituksena on kurinalaisuus tilivelvollisuuden alaisen tiedon käsittelyssä ja siihen pääsyn valvonnassa.

21. Tilivelvollisuuden vaatimuksen toissijaisina tavoitteina on

(a) seurata pääsyä tilivelvollisuuden alaiseen tietoon: kenellä on tosiasiallisesti tai mahdollisesti ollut pääsy tällaiseen tietoon, ja kuka on yrittänyt päästä siihen;

(b) pysyä selvillä tilivelvollisuuden alaisen tiedon sijainnista;

authenticate telecommunications carrying NATO cryptographic security-related information; signifying that the information shall be protected in accordance with the appropriate cryptographic security policies and directives.

18. The term “BOHEMIA” is a marking applied to special category information derived from or pertaining to Communications Intelligence (COMINT). All information marked COSMIC TOP SECRET - BOHEMIA will be protected in strict accordance with MC 101 (NATO Signals Intelligence Policy) and its companion Allied Joint Publication (AJP) which covers doctrine and the NACSI Guide to SIGINT Administration and Procedures which addresses administration and procedures.

Dissemination Limitation Markings

19. As an additional marking to further limit the dissemination of NATO Classified Information, a Dissemination Limitation Marking may be applied by the originator.

CONTROL AND HANDLING

Objectives of Accountability

20. The primary objective of accountability is to provide sufficient information to be able to investigate a deliberate or accidental loss or compromise of accountable information and assess the damage arising from the loss or compromise. The requirement for accountability serves to impose a discipline on the handling of, and control of access to, accountable information.

21. Subordinate objectives are:

(a) to keep track of access to accountable information – who has, or potentially has, had access to accountable information; and who has attempted to access accountable information;

(b) to know the location of accountable information;

(c) seurata tilivelvollisuuden alaisen tiedon liikkeitä Natossa ja kansallisesti; ja

(d) pitää kirjaa Naton ulkopuolisille toimijoille luovutetusta tilivelvollisuuden alaisesta tiedosta.

22. Luokkiin COSMIC TOP SECRET, NATO SECRET ja ATOMAL luokiteltu tieto on tilivelvollisuuden alaista, ja sitä on valvottava ja käsiteltävä noudattaen tämän liitteen vaatimuksia sekä Naton turvallisuusluokitellun tiedon turvallisuutta koskevaa tätä liitettä tukevaa direktiiviä. Jos kansalliset säädökset ja määräykset sitä edellyttävät, sellainen tieto, johon on merkitty muu turvallisuusluokka tai erityisluokan merkintä, voidaan katsoa tilivelvollisuuden alaiseksi tiedoksi.

Rekisterijärjestelmä

23. Rekisterijärjestelmän turvallisuusmenettelyjä ja -vaatimuksia sovelletaan yhtäläisesti sekä fyysisessä että sähköisessä ympäristössä. Sähköistä ympäristöä koskevia lisätietoja ja -vaatimuksia on tämän C-M-asiakirjan liitteessä F ja tätä asiakirjaa tukevissa ohjeissa.

24. Käytössä on oltava rekisterijärjestelmä, joka vastaa tilivelvollisuuden alaisen tiedon vastaanottamisesta, kirjaamisesta, käsittelystä, jakelusta ja hävittämisestä. Tämä vastuu voidaan täyttää joko käyttämällä yhtä rekisterijärjestelmää, jolloin turvallisuusluokkaan COSMIC TOP SECRET ja muuhun erityisluokkaan luokiteltu tieto on kaikkina aikoina pidettävä tarkasti osastoituna, tai perustamalla erilliset rekisterit ja valvontapisteet.

25. Tapauksen mukaan kukin Naton jäsenvaltio ja Naton sotilas- ja siviilielin perustaa yhden tai useamman turvallisuusluokkaan COSMIC TOP SECRET luokitellun tiedon keskusrekisterin, joka toimii sen jäsenvaltion tai elimen vastaanottavana ja lähettävänä pääviranomaisena, johon rekisteri on perustettu. Tällainen keskusrekisteri voi toimia myös tilivelvollisuuden alaisen muun tiedon rekisterinä.

(c) to keep track of the movement of accountable information within the NATO and national domains; and

(d) register accountable information that has been released to NNEs.

22. Information classified CTS, NS and ATOMAL shall be accountable, controlled and handled in accordance with the requirements of this Enclosure and the supporting Directive on the Security of NATO Classified Information. Where required by national laws and regulations, information bearing other classification or special category markings may be considered as accountable information.

The Registry System

23. The security procedures and requirements of the registry system apply equally across both the physical and electronic domains. Additional details and requirements concerning the electronic domain can be found within Enclosure “F” to this C-M and its supporting directives.

24. There shall be a Registry System which is responsible for the receipt, accounting, handling, distribution and destruction of accountable information. Such a responsibility may be fulfilled either within a single Registry System, in which case strict compartmentalisation of information classified CTS and other special category information shall be maintained at all times, or by establishing separate registries and control points.

25. Each NATO Nation or NATO Civil or Military Body, as appropriate, shall establish a Central Registry(s) for information classified CTS, which acts as the main receiving and dispatching authority for the Nation or body within which it has been established. The Central Registry(s) may also act as a registry(s) for other accountable information.

26. Rekisterit ja valvontapisteet toimivat vastuuorganisaatioina turvallisuusluokkiin COSMIC TOP SECRET ja NATO SECRET luokitellun tiedon sisäisessä jakelussa sekä kaiken kyseisen rekisterin tai valvontapisteen vastuulla olevan tilivelvollisuuden alaisen tiedon kirjaamisessa; ne voidaan perustaa ministeriöiden, osastojen tai komento-osastojen tasolle. Turvallisuusluokkiin NATO CONFIDENTIAL ja NATO RESTRICTED luokiteltua tietoa ei tarvitse kirjata rekisterijärjestelmään, jolleivät kansalliset säädökset ja määräykset tätä edellytä.

26. Registries and control points shall act as the responsible organization for the internal distribution of information classified CTS and NS and for keeping records of all accountable information held on that registry's or control point's charge; they may be established at ministry, department, or command levels. NC and NR information is not required to be processed through the Registry System unless specified by national laws and regulations.

27. Rekisterien ja valvontapisteiden on kaikkina aikoina pystyttävä paikantamaan Naton tilivelvollisuuden alaisen tiedon sijainti. Harvoin sallittava ja tilapäinen pääsy tällaiseen tietoon ei välttämättä edellytä rekisterin tai valvontapisteen perustamista, jos käytössä on menettelyt, joilla varmistetaan, että tieto pysyy rekisterijärjestelmän valvonnassa.

27. With regard to NATO accountable information, registries and control points shall be able at all times to establish its location. Infrequent and temporary access to such information does not necessarily require the establishment of a registry or control point, provided that procedures are in place to ensure that the information remains under the control of the Registry System.

28. Turvallisuusluokkaan COSMIC TOP SECRET luokitellun tiedon jakelun on tapahduttava COSMIC-rekisterin välityksellä. Kunkin rekisterin on vähintään kerran vuodessa luetteloitava kaikki turvallisuusluokkaan COSMIC TOP SECRET luokiteltu tieto, josta rekisteri on tilivelvollinen, noudattaen Naton turvallisuusluokitellun tiedon turvallisuutta koskevan Naton turvallisuussääntöjä tukevan direktiivin vaatimuksia. Rekisteriorganisaation tyypistä riippumatta niiden organisaatioiden, jotka käsittelevät turvallisuusluokkaan COSMIC TOP SECRET luokiteltua tietoa, on nimettävä COSMIC-tiedon valvoja (CCO).

28. The dissemination of information classified CTS shall be through COSMIC registry channels. At least annually, each registry shall carry out an inventory of all information classified CTS for which it is accountable, in accordance with the requirements of the supporting Directive on the Security of NATO Classified Information. Regardless of the type of registry organization, those that handle information classified CTS shall appoint a "COSMIC Control Officer" (CCO).

29. Naton turvallisuussääntöjä tukevassa direktiivissä Naton turvallisuusluokitellun tiedon turvallisuudesta käsitellään muun muassa COSMIC-tiedon valvojan tehtäviä, turvallisuusluokkiin COSMIC TOP SECRET ja NATO SECRET luokitellun tiedon yksityiskohtaisia käsittelyprosesseja rekisterijärjestelmässä, Naton turvallisuusluokitellun tiedon jäljennöksiä, käännöksiä ja otteita koskevia menettelyjä, sen jakelua ja lähettä-

29. The supporting Directive on the Security of NATO Classified Information sets out, inter alia, the responsibilities of the CCO, the detailed registry system handling processes for information classified CTS and NS, the procedures for reproductions, translations and extracts, the requirements for the dissemination and transfer, and the requirements for the disposal and destruction of NATO Classified Information.

mistä koskevia vaatimuksia sekä sen hallussapitoa ja hävittämistä koskevia vaatimuksia.

30. Sotilaskomitea on perustanut erillisen järjestelmän salausaineistoa koskevan tilivelvollisuuden täyttämistä sekä salausaineiston valvontaa ja jakelua varten. Tämän järjestelmän kautta välitettävä aineisto ei edellytä tilivelvollisuuden täyttämistä rekisterijärjestelmässä.

30. The Military Committee (MC) has established a separate system for the accountability, control and distribution of cryptographic material. Material being transferred through this system does not require accountability in the Registry System.

VALMIUSSUUNNITTELU

31. Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet laativat valmiussuunnitelmat Naton turvallisuusluokitellun tiedon suojaamiseksi ja hävittämiseksi poikkeusolojen aikana estääkseen luvattoman pääsyn tähän tietoon sekä sen luvattoman ilmitulon ja sen käytettävyyden estymisen. Nämä suunnitelmat perustuvat määräajoin tarkistettaviin uhka-arvioihin, ja niissä asetetaan etusijalle arkaluonteisin sekä tehtävän tai ajan kannalta ratkaisevin tieto.

CONTINGENCY PLANNING

31. NATO Nations and NATO Civil and Military bodies shall prepare contingency plans for the protection or destruction, during emergency situations, of NATO Classified Information to prevent unauthorised access and disclosure and loss of availability. These plans will be based on periodically reviewed threat assessments and shall give highest priority to the most sensitive, and mission- or time-critical information.

TIETOTURVAPOIKKEAMAT

32. Tietoturvapoikkeama on tapahtuma tai muu tilanne, joka voi vaikuttaa haitallisesti Naton turvallisuusluokitellun tiedon turvallisuuteen ja joka edellyttää tarkempia tutkintatoimia, jotta voidaan todeta tarkasti, onko kyseessä tietoturvaloukkaus vai vähäinen tietoturvapoikkeama.

SECURITY INCIDENTS

32. A Security Incident is an event or other occurrence that may have an adverse effect upon the security of NATO Classified Information which requires further investigative actions in order to accurately determine whether or not it constitutes a Security Breach or Infraction.

Tietoturvaloukkaus

33. Tietoturvaloukkaus on tahallinen tai tahaton teko tai laiminlyönti, joka on näiden turvallisuussääntöjen vastainen ja voi johtaa Naton turvallisuusluokitellun tiedon tai sitä tukevien palvelujen ja resurssien tosiasialliseen tai mahdolliseen vaarantumiseen.

Security Breach

33. A Security Breach is an act or omission, deliberate or accidental, contrary to the security rules laid down in this policy that may result in the actual or possible compromise of NATO Classified Information or supporting services and resources.

Vaarantuminen

34. Vaarantuminen tarkoittaa tilannetta, jossa tietoturvaloukkauksen tai haitallisen toiminnan vuoksi Naton turvallisuusluokiteltu tieto on menettänyt luottamuksellisuutensa, eheytensä tai käytettävyytensä tai tätä

Compromise

34. Compromise denotes a situation when, due to a Security Breach or adverse activity, NATO Classified Information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability. This includes

tietoa tukevat palvelut ja resurssit ovat menettäneet eheytensä tai käytettävyytensä. Vaarantumiseen sisältyvät katoaminen, ilmitulo asiattomille, luvaton muuttaminen, hävittäminen luvattomalla tavalla ja palvelun estyminen.

loss, disclosure to unauthorized individuals, unauthorised modification, destruction in an unauthorised manner, or denial of service.

Vähäinen tietoturvapoikkeama

35. Vähäinen tietoturvapoikkeama on tahallinen tai tahaton teko tai laiminlyönti, joka on näiden turvallisuussääntöjen vastainen, mutta ei johda Naton turvallisuusluokitellun tiedon tosiasialliseen tai mahdolliseen vaarantumiseen.

Infraction

35. Infraction is an act or omission, deliberate or accidental, contrary to the security rules laid down in this policy, that does not result in the actual or possible compromise of NATO Classified Information.

36. Kaikista tosiasiallisista ja mahdollisista tietoturvaloukkauksista on ilmoitettava viipymättä toimivaltaiselle turvallisuusviranomaiselle. Kaikki ilmoitetut tietoturvaloukkaukset on tutkittava sellaisten henkilöiden toimesta, joilla on asiantuntemusta turvallisuuden, tutkinnan ja tarvittaessa vastatiedustelun alalla ja jotka ovat riippumattomia niistä henkilöistä, joita tietoturvaloukkaus välittömästi koskee. Naton turvallisuussääntöjä tukevassa direktiivissä Naton turvallisuusluokitellun tiedon turvallisuudesta selostetaan yksityiskohtaisesti toimia, jotka on toteutettava todettaessa tietoturvaloukkaus tai vähäinen tietoturvapoikkeama.

36. All Security Breaches or potential Security Breaches shall be reported immediately to the appropriate security authority. Each reported Security Breach shall be investigated by individuals who have security, investigative and, where appropriate, counter-intelligence experience, and who are independent of those individuals immediately concerned with the Security Breach. The supporting Directive on Security of NATO Classified Information provides details on actions to be taken upon discovery of a Security Breach or Infraction.

ILMOITTAMINEN

37. Naton turvallisuusluokiteltuun tietoon kohdistuneiden tietoturvaloukkausten ja vaarantumisten ilmoittamisella pyritään ensisijaisesti antamaan tiedon luovuttaneelle Naton organisaatiolle mahdollisuus arvioida Natolle aiheutunut vahinko ja ryhtyä tarpeellisiksi katsottaviin tai mahdollisiin toimenpiteisiin vahingon minimoimiseksi. Kansallinen turvallisuusviranomainen / määrätty turvallisuusviranomainen tai kyseisen Naton sotilas- tai siviilielimen johtaja välittää tiedot vahingon arvioinnista ja vahingon mimimoimiseksi tehdyistä toimenpiteistä Naton turvallisuustoimistolle.

REPORTING

37. The main purpose of reporting Security Breaches and compromises of NATO Classified Information is to enable the originating NATO component to assess the resulting damage to NATO and to take whatever action is desirable or practicable to minimize the damage. Reports of the damage assessment and minimising action taken shall be forwarded to the NOS by the NSA/DSA or Head of the NATO Civil or Military Body concerned.

38. Ilmoittavan viranomaisen olisi mahdollisuuksien mukaan ilmoitettava asiasta tiedon luovuttaneelle Naton organisaatiolle samaan aikaan kuin Naton turvallisuustoimistolle,

38. Where possible, the reporting authority should inform the originating NATO component at the same time as the NOS, but the latter may be requested to do this when the

mutta Naton turvallisuustoimistoa voidaan pyytää tekemään ilmoitus, jos alkuperäistä luovuttajaa on vaikea selvittää. Naton turvallisuustoimistolle tehtävien ilmoitusten ajoitus riippuu tiedon arkaluonteisuudesta ja olosuhteista.

originator is difficult to identify. The timing of submitting reports to the NOS depends on the sensitivity of the information and the circumstances.

39. Naton turvallisuustoimisto voi Naton pääsihteerin puolesta pyytää toimivaltaisia viranomaisia tutkimaan asiaa tarkemmin ja ilmoittamaan havainnoistaan Naton turvallisuustoimistolle. Olosuhteista ja vaarantumisen vakavuudesta riippuen Naton turvallisuustoimisto voi ilmoittaa asiasta turvallisuuskomitealle.

39. The NOS, on behalf of the Secretary General of NATO, may request the appropriate authorities to make further investigations and to report their findings back to the NOS. Depending upon the circumstances and severity of the compromise, the NOS may inform the Security Committee (SC).

40. Naton turvallisuussääntöjä tukevassa direktiivissä Naton turvallisuusluokitellun tiedon turvallisuudesta käsitellään tietoturvaloukkauksiin ja turvallisuuden vaarantumisiin liittyviä yksityiskohtaisia toimia, kirjauksia ja ilmoittamista koskevia vaatimuksia

40. The supporting Directive on the Security of NATO Classified Information sets out the detailed actions, records and reporting requirements for Security Breaches and compromises of security.

41. Sotilaskomitea on antanut Naton jäsenvaltioiden viestintäturvallisuusviranomaisille ja Naton sotilas- ja siviilielimille erilliset määräykset salausaineiston vaarantumisesta.

41. Separate provisions relating to the compromise of cryptographic material have been issued by the MC to communications security authorities of NATO Nations and NATO Civil and Military bodies.

LIITE F
VIESTINTÄ- JA TIETOJÄRJESTELMIEN TURVALLISUUS

1. JOHDANTO

1.1 Tässä liitteessä esitetään periaatteet ja vähimmäisvaatimukset, jotka koskevat Naton turvallisuusluokitellun tiedon sekä sitä tukevien järjestelmäpalvelujen ja resurssien[1] suojaamista viestinnässä, tallennettaessa tätä tietoa tietojärjestelmiin ja muihin sähköisiin järjestelmiin sekä käsiteltäessä ja siirrettäessä sitä näissä järjestelmissä.

1.2 Tämä liite tukee Naton tiedonhallinnan periaatteita ja täydentää Naton turvallisuusluokittelemattoman tiedon hallinnan periaatteita, joissa käsitellään niitä perusperiaatteita ja vaatimuksia, joita Naton sotilas- ja siviilielimissä sekä Naton jäsenvaltioissa sovelletaan Naton turvallisuusluokittelemattoman tiedon suojaamiseksi.

1.3 Viestintä- ja tietojärjestelmien turvallisuus (CIS Security) on yksi tietojen turvaamisen (kuva 1) osatekijöistä, ja sillä tarkoitetaan turvatoimien soveltamista tarkoituksena suojata viestinnän, tietojärjestelmien ja muiden sähköisten järjestelmien[2] sekä näihin järjestelmiin tallennettavan ja niissä käsiteltävän ja siirrettävän[3] tiedon luottamuksellisuutta, eheyttä, käytettävyyttä, aitoutta ja kiistämättömyyttä.

ENCLOSURE “F”
COMMUNICATION AND INFORMATION SYSTEM SECURITY

1. INTRODUCTION

1.1. This Enclosure sets out the policy and minimum standards for the protection of NATO classified information, and supporting system services and resources[1] in communication, information and other electronic systems storing, processing or transmitting NATO classified information.

1.2. This Enclosure supports the NATO Information Management Policy and complements the Policy on Management of Non-Classified NATO Information which addresses the basic principles and standards to be applied within NATO civil and military bodies and NATO member nations for the protection of non-classified NATO information.

1.3. Communication and Information System Security (CIS Security) is one of the elements of Information Assurance (Figure 1) and is defined as the application of security measures for the protection of communication, information and other electronic systems[2], and the information that is stored, processed or transmitted[3] in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

---

[1] Tietoa tukevilla järjestelmäpalveluilla ja resursseilla tarkoitetaan niitä palveluja ja resursseja, jotka tarvitaan varmistamaan, että viestintä- ja tietojärjestelmien turvallisuustavoitteet saavutetaan; näitä palveluja ja resursseja ovat esimerkiksi salaustuotteet ja -menetelmät, COMSEC-aineisto, luettelopalvelut sekä käyttöympäristön järjestelyt ja valvonta.

[1] Supporting System Services and Resources - those services and resources required to ensure that the security objectives of the CIS are achieved; to include, for example, cryptographic products and mechanisms, COMSEC materials, directory services, and environmental facilities and controls.

[2] Jäljempänä tässä liitteessä "CIS".

[2] Hereafter referred to within this Enclosure as CIS.

[3] Jäljempänä tässä liitteessä "käsiteltävä".

[3] Hereafter referred to within this Enclosure as handled.

1.4 Jotta saavutetaan näissä viestintä- ja tietojärjestelmissä käsiteltävän turvallisuusluokitellun tiedon luottamuksellisuuden, eheyden, käytettävyyden, aitouden ja kiistämättömyyden turvallisuustavoitteet[4], toteutetaan tasapainoinen toimitila-, henkilöstö- ja tietoturvallisuutta sekä viestintä- ja tietojärjestelmien turvallisuutta koskevien toimenpiteiden kokonaisuus turvallisen käyttöympäristön aikaansaamiseksi näille järjestelmille. Kun yritykset käsittelevät turvallisuusluokiteltua tietoa sopimusten perusteella, sovelletaan lisäksi erityisiä yritysturvallisuustoimia tämän C-M-asiakirjan liitteen G ja sitä tukevan yritysturvallisuusdirektiivin mukaisesti.

1.4. In order to achieve the security objectives of confidentiality, integrity, availability, authentication and non-repudiation[4] for classified information handled in these CIS, a balanced set of security measures (physical, personnel, information and CIS) shall be implemented to create a secure environment in which to operate a CIS. Where classified information is handled by industry in contracts, additional specific industrial security measures shall be applied in accordance with Enclosure G of this C-M and the supporting industrial security directive.

[*Kuva asiakirjan lopussa]

[*Figure at the end of the document]

Kuva 1 – Suhde tietojen turvaamisen ja viestintä- ja tietojärjestelmien turvallisuuden välillä

Figure 1 - Relationship between Information Assurance and CIS Security

1.5 Viestintä- ja tietojärjestelmien turvallisuuden päädirektiivissä, jonka turvallisuuskomitea (SC) ja tiedonvälityksen, johtamisen ja valvonnan ohjausryhmä (C3B) ovat julkaisseet näiden turvallisuussääntöjen tueksi, käsitellään näitä järjestelmiä koskevia turvallisuustoimia niiden elinkaaren aikana sekä komiteoiden ja Naton sotilas- ja siviilielinten vastuuta näiden järjestelmien turvallisuudesta. Viestintä- ja tietojärjestelmien turvallisuuden päädirektiiviä tukevat direktiivit, joissa käsitellään viestintä- ja tietojärjestelmien turvallisuuden hallintaa (kuten turvallisuusriskien hallintaa, turvallisuuden akkreditointia, turvallisuuteen liittyvää dokumentointia ja turvallisuuden uudelleenarviointia/tarkastamista) sekä viestintä- ja tietojärjestelmien turvallisuuden teknisiä ja toteuttamiseen liittyviä näkökohtia (kuten tietokoneiden ja lähiverkkojen turvallisuutta, yhteen liitettyjen verkkojen turvallisuutta,

1.5. The “Primary Directive on CIS Security”, which is published by the SC and the C3B in support of this policy, addresses the CIS Security activities in the CIS life-cycle, and the CIS Security responsibilities of committees, and NATO civil and military bodies. The “Primary Directive on CIS Security” is supported by directives addressing CIS Security management (including security risk management, security accreditation, security-related documentation, and security review / inspection) and CIS Security technical and implementation aspects (including computer and local area network (LAN) security, interconnection of networks security, cryptographic security, transmission security, and emission security).

[4] Jäljempänä tässä liitteessä "turvallisuustavoitteet".

[4] Hereafter referred to within this Enclosure as Security Objectives.

salaukseen perustuvaa turvallisuutta, tiedonsiirron turvallisuutta ja hajasäteilyn turvallisuutta).

2. TURVALLISUUSTAVOITTEET

2.1. Viestintä- ja tietojärjestelmissä käsiteltävän Naton turvallisuusluokitellun tiedon suojaamiseksi asianmukaisesti määritetään ja toteutetaan tasapainoinen toimitila- ja henkilöstöturvallisuuden, tietoturvallisuuden sekä viestintä- ja tietojärjestelmien turvallisuuden toimenpiteiden kokonaisuus turvallisen ympäristön luomiseksi näiden järjestelmien toiminnalle ja seuraavien turvallisuustavoitteiden saavuttamiseksi:

(a) varmistetaan Naton turvallisuusluokitellun tiedon luottamuksellisuus valvomalla tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien paljastamista ja pääsyä niihin;

(b) varmistetaan Naton turvallisuusluokitellun tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien eheys;

(c) varmistetaan Naton turvallisuusluokitellun tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien käytettävyys;

(d) varmistetaan niiden henkilöiden, laitteiden ja palvelujen luotettava määrittäminen ja tunnistaminen, jotka pääsevät Naton turvallisuusluokiteltua tietoa käsitteleviin viestintä- ja tietojärjestelmiin; ja

(e) varmistetaan tietoa käsitelleiden henkilöiden ja toimijoiden asianmukainen kiistämättömyys.

2.2. Naton turvallisuusluokiteltu tieto sekä sitä tukevat järjestelmäpalvelut ja resurssit suojataan vähintään toimenpidekokonaisuudella, jonka tarkoituksena on varmistaa yleinen suojaus yleisesti esiintyviltä (tahattomilta tai tahallisilta) ongelmilta, joiden tiedetään vaikuttavan kaikkiin järjestelmiin ja tietoa tukeviin järjestelmäpalveluihin ja resursseihin. Olosuhteiden mukaan ryhdytään muihin toimenpiteisiin, jos turvallisuusriskien arvioinnissa on todettu, että Naton turvallisuusluokiteltuun tietoon ja/tai sitä tukeviin järjestelmäpalveluihin ja resursseihin

2. SECURITY OBJECTIVES

2.1. To achieve adequate security protection of NATO classified information handled in CIS, a balanced set of security measures (physical, personnel, information and CIS) shall be identified and implemented to create a secure environment in which a CIS operates, and to meet the following security objectives:

(a) to ensure the confidentiality of information by controlling the disclosure of, and access to, NATO classified information, and supporting system services and resources;

(b) to ensure the integrity of NATO classified information, and supporting system services and resources;

(c) to ensure the availability of NATO classified information, and supporting system services and resources;

(d) to ensure the reliable identification and authentication of persons, devices and services accessing CIS handling NATO classified information; and

(e) to ensure appropriate non-repudiation for individuals and entities having processed the information.

2.2. NATO classified information and supporting system services and resources, shall be protected by a minimum set of measures aimed at ensuring general protection against commonly encountered problems (whether accidental or intentional) known to affect all systems and supporting system services and resources. Additional measures shall be taken, appropriate to the circumstances, where a security risk assessment has established that NATO classified information and/or supporting system sevices and resources are subject to increased risks from specific threats and vulnerabilities.

kohdistuu tiettyjen uhkien ja haavoittuvuuksien vuoksi aiempaa suurempia riskejä.

2.3. Käsiteltävän Naton tiedon turvallisuusluokasta riippumatta Naton turvallisuusviranomaiset arvioivat riskit ja sen vahingon tason, joka Natolle aiheutuu, jos toimenpiteet muiden turvallisuustavoitteiden kuin luottamuksellisuuden saavuttamiseksi laiminlyödään. Muun kuin luottamuksellisuuden varmistavia palveluja koskevien toimenpiteiden vähimmäiskokonaisuus määritetään näitä turvallisuussääntöjä tukevien direktiivien mukaisesti.

3. TURVALLISUUDEN AKKREDITOINTI

3.1. Se, missä määrin turvallisuustavoitteet on saavutettava ja missä määrin viestintä- ja tietojärjestelmiin kohdistuvia turvallisuustoimenpiteitä tarvitaan Naton turvallisuusluokitellun tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien suojaamiseksi, määritellään kyseistä turvallisuusvaatimusta laadittaessa. Turvallisuuden akkreditoinnilla todetaan, että riittävä suojauksen taso on saavutettu ja sitä ylläpidetään.

3.2. Kaikkien Naton turvallisuusluokiteltua tietoa käsittelevien kansallisten viestintä- ja tietojärjestelmien osalta suoritetaan turvallisuuden akkreditointi, jossa käsitellään turvallisuustavoitteita.

4. HENKILÖSTÖTURVALLISUUS

4.1. Henkilöt, joille sallitaan pääsy Naton turvallisuusluokiteltuun tietoon sen jossakin muodossa, on turvallisuusselvitettävä, ottaen tarvittaessa huomioon heidän kokonaisvastuunsa tietoa ja sitä tukevia järjestelmäpalveluja ja resursseja koskevien turvallisuustavoitteiden saavuttamisesta. Näitä henkilöitä ovat myös ne, joille sallitaan pääsy tietoa tukeviin järjestelmäpalveluihin ja resursseihin tai jotka vastaavat niiden suojauksesta, vaikkei heille sallittaisikaan pääsyä järjestelmässä käsiteltävään tietoon.

2.3. Independent of the security classification of the NATO information being handled, NATO security authorities shall assess the risks and the level of damage done to NATO if the measures to achieve the nonconfidentiality security objectives fail. The minimum set of measures for nonconfidentiality services shall be determined in accordance with directives supporting this policy.

3. SECURITY ACCREDITATION

3.1. The extent to which the security objectives are to be met, and the extent to which CIS Security measures are to be relied upon for the protection of NATO classified information and supporting system services and resources shall be determined during the process of establishing the security requirement. The security accreditation process shall determine that an adequate level of protection has been achieved, and is being maintained.

3.2 All CIS handling NATO classified information shall be subject to a security accreditation process, addressing the Security Objectives.

4. PERSONNEL SECURITY

4.1. Individuals authorised access to NATO classified information in any form shall be security cleared, where appropriate, taking account of their aggregate responsibility for achieving the Security Objectives of the information and the supporting system services and resources. This includes individuals who are authorised access to supporting system services and resources, or who are responsible for their protection, even if they are not authorised access to the information handled by the system.

5. PHYSICAL SECURITY

5. TOIMITILATURVALLISUUS

5.1. Alueet, joilla Naton turvallisuusluokiteltua tietoa esitetään tai käsitellään tietotekniikkaa käyttäen tai joilla on mahdollista päästä sellaiseen tietoon, on perustettava siten, että turvallisuustavoitteiden saavuttamisen kokonaisvaatimus täyttyy.

6. TIETOTURVALLISUUS

6.1. Kaikki turvallisuusluokitellut tietokoneiden tallennusvälineet on merkittävä, säilytettävä ja suojattava asianmukaisesti, tallennettavan tiedon korkeimman turvallisuusluokan mukaan.

6.2. Uudelleen käytettävälle tietokoneen tallennusvälineelle tallennetun Naton turvallisuusluokitellun tiedon saa poistaa tallennusvälineeltä ainoastaan toimivaltaisen turvallisuusviranomaisen hyväksymiä menettelyjä noudattaen.

6.3. Tietokoneen tallennusvälineelle tallennetun Naton turvallisuusluokitellun tiedon suojaamiseen voidaan soveltaa näitä turvallisuussääntöjä tukevien direktiivien mukaisesti toteutettavia hyväksyttyjä (luottamuksellisuutta ja muuta kuin luottamuksellisuutta koskevia) turvatoimia siten, että toimitilaturvallisuuden vaatimuksia lievennetään alempaa turvallisuusluokkaa vastaaviksi.

7. YRITYSTURVALLISUUS

7.1 Sopimusten toteuttamiseen käytettävä hankeosapuolen toimitila, jossa käsitellään Naton turvallisuusluokiteltua tietoa viestintä- ja tietojärjestelmissä, on perustettava siten, että se täyttää turvallisuustavoitteiden saavuttamisen kokonaisvaatimuksen.

7.2. Tapauksen mukaan sopimuksissa, turvallisuusnäkökohtia koskevissa kirjeissä (SAL) ja/tai ohjelman/hankkeen turvallisuusohjeissa (PSI) ja/tai palvelutasosopimuksissa (SLA) on selostettava johdonmukainen viestintä- ja tietojärjestelmiin kohdistuvien turvatoimien kokonaisuus, joka hankeosapuolten on toteutettava saavuttaakseen

5.1. Areas in which NATO classified information is presented or handled using information technology, or where potential access to such information is possible, shall be established such that the aggregate requirement for the Security Objectives is met.

6. SECURITY OF INFORMATION

6.1. All classified computer storage media shall be properly identified, stored and protected in a manner commensurate with the highest classification of the stored information.

6.2. NATO classified information recorded on re-usable computer storage media, shall only be erased in accordance with procedures approved by the appropriate security authority.

6.3. Approved security measures (confidentiality and non-confidentiality), implemented in accordance with directives supporting this policy, may be used to protect NATO classified information in computer storage media in such a manner as to reduce the physical security requirements commensurate with a lower classification level.

7. INDUSTRIAL SECURITY

7.1. A contractor facility used for contracts in which NATO classified information is handled on CIS shall be established to meet the aggregate requirement for the Security Objectives.

7.2. A consistent set of CIS security measures shall be described in contracts, Security Aspect Letters (SAL) and/or Project Security Instructions (PSI) and/or Service Level Agreements (SLA), as applicable, and be implemented by contractors to meet the NATO CIS security objectives and to protect NATO classified information and supporting services.

Naton viestintä- ja tietojärjestelmien turvallisuustavoitteet ja suojatakseen Naton turvallisuusluokitellun tiedon ja sitä tukevat palvelut.

8. TURVATOIMET

8.1. Kaikkiin Naton turvallisuusluokiteltua tietoa käsitteleviin viestintä- ja tietojärjestelmiin on sovellettava johdonmukaista turvallisuustoimenpiteiden kokonaisuutta, jotta saavutetaan tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien suojaamisen turvallisuustavoitteet. Näitä turvallisuustoimenpiteitä ovat tapauksen mukaan seuraavat:

(a) keinot, joiden avulla saadaan riittävät tiedot, jotta pystytään tutkimaan mahdollisesti aiheutuvan vahingon edellyttämällä tavalla tahallinen tai tahaton turvallisuusluokiteltua tietoa ja sitä tukevia järjestelmäpalveluja ja resursseja koskevien turvallisuustavoitteiden vaarantuminen tai vaarantamisen yritys;

(b) keinot, joiden avulla määritetään ja tunnistetaan luotettavasti henkilöt, laitteet ja palvelut, joille sallitaan pääsy tietoon, järjestelmäpalveluihin ja resursseihin. Tietoa ja aineistoa, jonka avulla säädellään pääsyä viestintä- tai tietojärjestelmään, on valvottava ja se on suojattava sitä tietoa vastaavien järjestelyjen mukaisesti, johon tieto tai aineisto voi mahdollistaa pääsyn. Naton viestintä- ja tietojärjestelmissä on sovellettava henkilöiden vahvan tunnistamisen menetelmää;

(c) keinot, joiden avulla valvotaan tiedonsaantitarpeen periaatteen perusteella Naton turvallisuusluokitellun tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien paljastamista ja pääsyä niihin;

(d) keinot, joiden avulla todennetaan Naton turvallisuusluokitellun tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien eheys ja alkuperä;

(e) keinot, joiden avulla ylläpidetään Naton turvallisuusluokitellun tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien eheyttä;

8. SECURITY MEASURES

8.1. For all CIS handling NATO classified information, a consistent set of security measures shall be applied to meet the Security Objectives to protect information and supporting system services and resources. The security measures shall include, where appropriate, the following:

(a) a means to provide sufficient information to be able to investigate a deliberate, accidental or attempted compromise of the security objectives of classified information and supporting system services and resources, commensurate with the damage that would be caused;

(b) a means to reliably identify and authenticate persons, devices and services authorised access. Information and material which controls access to a CIS shall be controlled and protected under arrangements commensurate with the information to which it may give access. On NATO CIS strong authentication mechanisms for persons shall be implemented;

(c) a means to control disclosure of, and access to, NATO classified information and supporting system services and resources, based upon the need-to-know principle;

(d) a means to verify the integrity and origin of NATO classified information, and supporting system services and resources;

(e) a means to maintain the integrity of NATO classified information and supporting system services and resources;

(f) keinot, joiden avulla ylläpidetään Naton turvallisuusluokitellun tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien käytettävyyttä;

(f) a means to maintain the availability of NATO classified information and supporting system services and resources;

(g) keinot, joiden avulla valvotaan Naton turvallisuusluokiteltua tietoa käsittelevien viestintä- ja tietojärjestelmien yhteyttä;

(g) a means to control the connection of CIS handling NATO classified information;

(h) viestintä- ja tietojärjestelmien suojausmenetelmien luotettavuuden toteaminen;

(h) a determination of the confidence to be placed in the protection mechanisms of CIS Security;

(i) keinot, joiden avulla arvioidaan ja todennetaan viestintä- ja tietojärjestelmien turvallisuuden suojausmenetelmien asianmukainen toimivuus näiden järjestelmien elinkaaren ajan;

(i) a means to assess and verify the proper functioning of the protection mechanisms of CIS Security over the life-cycle of the CIS;

(j) keinot, joiden avulla tutkitaan käyttäjien ja viestintä- ja tietojärjestelmien toimintaa;

(j) a means to investigate user and CIS activity;

(k) keinot, joiden avulla annetaan takeet kiistämättömyydestä siten, että tiedon lähettäjälle todistetaan, että tieto on lähetetty, ja tiedon vastaanottajalle todistetaan lähettäjän identiteetti; ja

(k) a means to provide non-repudiation assurances that the sender of information is provided with proof of delivery and the recipient is provided proof of the sender's identity; and

(l) keinot, joiden avulla suojataan säilytettävä Naton turvallisuusluokiteltu tieto, jos fyysiset turvallisuustoimenpiteet eivät täytä vähimmäisvaatimuksia.

(l) a means to protect stored NATO classified information where the physical security measures do not meet the minimum standards.

8.2. Käytössä on oltava turvallisuuden hallintajärjestelmät ja -menettelyt, joiden avulla estetään, torjutaan, havaitaan ja kestetään Naton turvallisuusluokiteltua tietoa ja sitä tukevia järjestelmäpalveluja ja resursseja koskeviin turvallisuustavoitteisiin vaikuttavien tapahtumien vaikutukset ja korjataan ne, mukaan lukien tietoturvapoikkeamista ilmoittaminen.

8.2. Security management mechanisms and procedures shall be in place to deter, prevent, detect, withstand, and recover from, the impacts of incidents affecting the Security Objectives of NATO classified information and supporting system services and resources, including the reporting of security incidents.

8.3. Turvallisuustoimenpiteitä hallitaan ja ne toteutetaan näitä turvallisuusääntöjä tukevien direktiivien mukaisesti.

8.3. The security measures shall be managed and implemented in accordance with directives supporting this policy.

9. TURVALLISUUSRISKIEN HALLINTA

9. SECURITY RISK MANAGEMENT

9.1. Naton sotilas- ja siviilielimissä käytettäviin Naton turvallisuusluokiteltua tietoa käsitteleviin viestintä- ja tietojärjestelmiin so-

9.1. CIS handling NATO classified information, in NATO civil and military bodies,

velletaan turvallisuusriskien hallintaa, mukaan lukien turvallisuusriskien arviointi, näitä turvallisuussääntöjä tukevien direktiivien vaatimusten mukaisesti.

9.2. Naton viestintä- ja tietojärjestelmien turvallisuusriskien hallinnalla varmistetaan järjestelmän haavoittuvuuksien ja turvallisuusvaatimustenmukaisuuden jatkuva arviointi, ja siinä on pyrittävä dynaamiseen riskienhallintaan, jotta voidaan reagoida tehokkaasti nykyisten monimutkaisten toimintaskenaarioiden ja monitahoisten uhkaympäristöjen asettamiin haasteisiin.

10. NATON TURVALLISUUSLUOKITELLUN TIEDON SÄHKÖMAGNEETTINEN SIIRTÄMINEN[5]

10.1. Kun Naton turvallisuusluokiteltua tietoa siirretään sähkömagneettisesti, on toteutettava erityiset toimenpiteet turvallisuustavoitteiden saavuttamiseksi näissä siirroissa. Naton viranomaiset määräävät vaatimukset, joita sovelletaan siirrettävän tiedon suojaamiseksi ilmitulolta, sieppaamiselta tai hyväksikäytöltä.

11. SALAUKSEEN PERUSTUVA TURVALLISUUS

11.1. Kun luottamuksellisuuden ja muun kuin luottamuksellisuuden suojaamiseksi tarvitaan salaustuotteita tai -menetelmiä tiedon siirtämisen, käsittelyn tai säilyttämisen (data at rest) aikana, nämä tuotteet tai menetelmät on erikseen hyväksytettävä tätä tarkoitusta varten ja fyysisten, menettelyllisten ja teknisten toimenpiteiden on täytettävä erityiset salausta koskevat vaatimukset, jotta vaadittavat turvallisuustavoitteet saavutetaan.

11.2. Säilytettävä tieto on suojattava vaadittavien turvallisuustavoitteiden edellyttämää tasoa vastaavasti, ja käytettäessä salaustuotteita tai -menetelmiä on salausta koskevien

shall be subject to security risk management, including security risk assessment, in accordance with the requirements of directives supporting this policy.

9.2. Security risk management of NATO CIS shall ensure continuous assessment of system vulnerabilities and security compliance and shall move towards dynamic risk management to be able to face effectively the challenges posed by today's complex operational scenarios and multifaceted threat environments.

10. ELECTROMAGNETIC TRANSMISSION[5] of NATO CLASSIFIED INFORMATION

10.1. When NATO classified information is transmitted electromagnetically, special measures shall be implemented to achieve the Security Objectives of such transmissions. NATO authorities shall determine the requirements for protecting transmissions from detection, interception or exploitation.

11. CRYPTOGRAPHIC SECURITY

11.1. When cryptographic products or mechanisms are required to provide confidentiality and non-confidentiality protection, whether during information transmission, processing or storage (data at rest), such products or mechanisms shall be specifically approved for the purpose and specific cryptographic requirements for physical, procedural and technical measures shall be implemented to achieve the required Security Objectives.

11.2. Data at rest shall be protected to a level adequate to the required Security Objectives, and, where cryptographic products and mechanisms are used, the requirements

[5] "Sähkömagneettinen siirtäminen" tarkoittaa siirtämistä, joka on luonteeltaan tai ominaisuuksiltaan sekä sähköistä että magneettista, ja se sisältää muun muassa näkyvän valon, radioaallot, mikroaallot ja infrapunasäteilyn.
[5] The term "electromagnetic transmission" covers transmission having both an electrical and magnetic character or properties, and includes, inter alia, visible light, radio waves, microwave, and infrared radiation

turvallisuusvaatimusten oltava sovellettavien Naton teknisten ja täytäntöönpanoa koskevien direktiivien mukaiset.

for cryptographic security shall be in accordance with the relevant NATO Technical and Implementation Directives.

11.3. Turvallisuusluokkaan NATO SECRET ja sitä ylempiin luokkiin luokitellun tiedon luottamuksellisuus on tietoa siirrettäessä suojattava Naton sotilaskomitean (NAVMILCOM) hyväksymillä salaustuotteilla tai -menetelmillä.

11.3. During transmission, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

11.4. Turvallisuusluokkaan NATO CONFIDENTIAL tai NATO RESTRICTED luokitellun tiedon luottamuksellisuus on tietoa siirrettäessä suojattava joko Naton sotilaskomitean tai Naton jäsenvaltion hyväksymillä salaustuotteilla tai -menetelmillä.

11.4. During transmission, the confidentiality of information classified NC or NR shall be protected by cryptographic products or mechanisms approved by either the NAMILCOM or a NATO member nation.

11.5. Tietoa siirrettäessä on muuta kuin luottamuksellisuutta koskevien vaatimusten täyttäminen varmistettava viestintäjärjestelmää koskevan käyttövaatimuksen mukaisesti. Salaustekniikkaan perustuvien muuta kuin luottamuksellisuutta koskevien menetelmien arviointia koskevat vaatimukset ja näiden menetelmien hyväksyntäviranomainen on yksilöitävä ja hyväksyttävä teknisissä direktiiveissä hyväksytyllä tavalla käyttövaatimukseen sisältyvien näitä menetelmiä koskevien vaatimusten yhteydessä.

11.5. During transmission, the non-confidentiality requirements shall be assured in accordance with the communications system's operational requirement. The evaluation requirements and approval authority, for non-confidentiality mechanisms based on cryptography, shall be identified and agreed in conjunction with the specification of such mechanisms in the operational requirement, as agreed in technical directives.

11.6. Poikkeuksellisissa toimintaolosuhteissa turvallisuusluokkiin NATO CONFIDENTIAL ja NATO SECRET luokiteltu tieto voidaan siirtää selväkielisenä, jos kukin tällainen siirto raportoidaan asianmukaisesti ylemmille viranomaisille. Poikkeuksellisia olosuhteita ovat seuraavat:

11.6. Under exceptional operational circumstances, information classified NC and NS may be transmitted in clear text provided each occasion is properly reported to the higher authorities. The exceptional circumstances are as follows:

(a) kriisin uhka tai toteutuminen, selkkaus tai sotatila; ja

(a) during impending or actual crisis, conflict, or war situations; and

(b) tilanteet, joissa lähetyksen nopeus on ensiarvoisen tärkeää, salauskeinoja ei ole käytettävissä ja arvioidaan, ettei siirrettävää tietoa ehditä käyttää ajoissa toiminnan haittaamiseen.

(b) when speed of delivery is of paramount importance, means of encryption are not available and it is assessed that the transmitted information cannot be exploited in time to adversely influence operations.

11.7. Poikkeuksellisissa toimintaolosuhteissa, joissa nopeus on ensiarvoisen tär-

11.7. Under exceptional operational circumstances, when speed is of paramount im-

keää, salauskeinoja ei ole käytettävissä ja arvioidaan, ettei siirrettävää tietoa ehditä käyttää ajoissa toiminnan haittaamiseen, turvallisuusluokkaan NATO RESTRICTED luokiteltu tieto voidaan siirtää selväkielisenä.

portance, means of encryption are not available and it is assessed that the transmitted information cannot be exploited in time to adversely influence operations, information classified NR may be transmitted in clear text.

11.8. Kun turvallisuusluokkaan NATO SECRET ja sitä ylempiin luokkiin luokiteltua tietoa siirretään Naton ja Naton ulkopuolisen valtion tai kansainvälisen järjestön (NNN/IO) viestintä- ja tietojärjestelmien välillä, tiedon luottamuksellisuus on siirron aikana suojattava Naton sotilaskomitean hyväksymillä salaustuotteilla tai -menetelmillä.

11.8. During transmission between NATO and non-NATO nations / International Organisations (NNN/IO) CIS, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

11.9. Kun turvallisuusluokkaan NATO SECRET ja sitä ylempiin luokkiin luokiteltua tietoa siirretään Naton ulkopuolisen valtion tai kansainvälisen järjestön viestintä- ja tietojärjestelmissä, tiedon luottamuksellisuus on siirron aikana suojattava Naton sotilaskomitean (NAVMILCOM) hyväksymillä salaustuotteilla tai -menetelmillä.

11.9. During transmission within NNN/IO CIS, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

11.10. Jos 11.8 ja 11.9 kohdan vaatimuksia ei voida täyttää, Nato ja kansainvälinen järjestö voivat sopia, että ne hyväksyvät vastavuoroisesti toistensa arviointi- valinta- ja hyväksymismenettelyt, joita sovelletaan niihin salaustuotteisiin tai -menetelmiin, joiden käyttö sallitaan turvallisuusluokkaan NATO SECRET tai kansainvälisen järjestön vastaavaan turvallisuusluokkaan luokitellun tiedon suojaamiseksi sitä siirrettäessä. Tämän hyväksynnän ehdot on esitetty jäljempänä kohdassa 11.12.

11.10. Where the requirements of paragraphs 11.8 and 11.9 above cannot be met, NATO and an IO may reach agreement on the mutual acceptance of each others' evaluation, selection and approval processes for cryptographic products or mechanisms authorised for the protection in transmission of NS information or IO information of the equivalent classification level. The conditions for such acceptance are set out in paragraph 11.12 below.

11.11. Poikkeuksellisissa olosuhteissa, jos 11.8 ja 11.9 kohdan vaatimuksia ei voida täyttää, Nato voi tiettyjen käyttövaatimusten täyttämistä tukeakseen hyväksyä Naton ulkopuolisen valtion arviointi- valinta- ja hyväksymismenettelyt, joita sovelletaan niihin salaustuotteisiin tai -menetelmiin, joiden käyttö sallitaan turvallisuusluokkaan NATO SECRET tai Naton ulkopuolisen valtion vastaavaan turvallisuusluokkaan luokitellun tiedon suojaamiseksi sitä siirrettäessä. Tämän hyväksynnän ehdot on esitetty jäljempänä kohdassa 11.12.

11.11. In exceptional circumstances, in order to support specific operational requirements, and where the requirements of paragraphs 11.8 and 11.9 above cannot be met, NATO may agree the NNN's evaluation, selection and approval processes for cryptographic products or mechanisms authorised for the protection in transmission of NS information or NNN information of the equivalent classification level. The conditions for such agreement are set out in paragraph 11.12 below.

11.12. Edellä 11.10 ja 11.11 kohdassa esitettyihin tilanteisiin sovelletaan seuraavia ehtoja:

(a) Naton ulkopuolisella valtiolla tai kansainvälisellä järjestöllä on oltava voimassa Naton kanssa tehty turvallisuussopimus ja Naton turvallisuustoimiston todistus siitä, että ne pystyvät asianmukaisesti suojaamaan luovutettavaa Naton turvallisuusluokiteltua tietoa;

(b) kutakin Naton ulkopuolista valtiota tai kansainvälistä järjestöä kohdellaan tapauskohtaisesti, ja kunkin hyväksynnän perusta määrätään Naton ja Naton ulkopuolisen valtion tai kansainvälisen järjestön välistä turvallisuussopimusta tukevissa turvallisuusjärjestelyissä;

(c) hyväksynnän ehdot on hyväksytettävä Naton sotilaskomitealla Naton turvallisuustoimiston tekemän puolueettoman arvion pohjalta; tämä arvio koskee Naton ulkopuolisen valtion tai kansainvälisen järjestön valmiutta tehdä salausta koskevia arvioita, jotka täyttävät vastaavat vaatimukset kuin Naton vaatimukset turvallisuusluokkaan NATO SECRET luokitellun tiedon suojaamiselle salauksen avulla; arvion tekee Naton turvallisuustoimisto yhdessä sotilaskomitean viestintä- ja tietojärjestelmien turvallisuus- ja arviointiviraston (SECAN), tiedonvälityksen, johtamisen ja valvonnan ohjausryhmän tietojen turvaamista ja kyberpuolustusvalmiutta käsittelevän paneelin sekä Naton päämajan tiedonvälityksen, johtamisen ja valvonnan esikunnan kanssa; ja

(d) Naton turvallisuustoimiston, SECANin ja Naton päämajan tiedonvälityksen, johtamisen ja valvonnan esikunnan on yhdessä vakuututtava todentamisen ja määräajoin tapahtuvan uudelleen todentamisen avulla siitä, että Naton ulkopuolisella valtiolla tai kansainvälisellä järjestöllä on käytössään asianmukaiset rakenteet, säännöt ja menettelyt salaustuotteiden ja -menetelmien arviointia, valintaa, hyväksyntää ja valvontaa varten ja että näitä rakenteita, sääntöjä ja menettelyjä sovelletaan käytännössä tehokkaasti ja turvallisesti.

11.12. The following conditions are applicable in respect to the scenarios described at paragraphs 11.10 and 11.11 above:

(a) the NNN/IO shall have a Security Agreement with NATO and be certified by the NATO Office of Security (NOS) that they can appropriately protect released NATO classified information;

(b) each NNN/IO shall be treated on a case-by-case basis; and the basis of any acceptance / agreement shall be set out in the security arrangements supporting the Security Agreement between NATO and the NNN/IO;

(c) the terms of any such acceptance / agreement shall be approved by the NAMILCOM on the basis of an objective assessment carried out by the NOS, working in conjunction with the NAMILCOM Communications and Information Systems Security and Evaluation Agency (SECAN), the C3B Information Assurance and Cyber Defence Capability Panel and the NATO HQ C3 Staff, of the capability of the NNN/IO to perform cryptographic evaluations that meet requirements equivalent to those used within NATO for the cryptographic protection of NS information; and

(d) the NOS, in conjunction with SECAN and the NATO HQ C3 Staff, shall satisfy themselves, through verification and periodic re-verification, that the NNN/IO has in place appropriate structures, rules and procedures for the evaluation, selection, approval and control of cryptographic products and mechanisms, and that those structures, rules and procedures are being effectively and securely applied in practice.

11.13. Kun hyväksyntä tapahtuu 11.12 kohdan ehtojen mukaisesti, turvallisuusluokkaan NATO SECRET luokitellun tiedon luottamuksellisuus voidaan suojata joko Naton sotilaskomitean hyväksymillä salaustuotteilla tai -menetelmillä tai sellaisilla salaustuotteilla tai -menetelmillä, jotka Naton ulkopuolisen valtion tai kansainvälisen järjestön kansallinen viestintä- ja tietojärjestelmien turvallisuusviranomainen (tai vastaava viranomainen) on hyväksynyt vastaavan turvallisuusluokan tiedon suojaamiseen.

11.13. Where acceptance / agreement is reached in accordance with the conditions set out in paragraph 11.12 above, the confidentiality of information classified NS may be protected by either cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM) or cryptographic products or mechanisms approved by the NCSA (or equivalent authority) of the NNN/IO for the protection of the equivalent classification level.

11.14. Kun turvallisuusluokkaan NATO CONFIDENTIAL tai NATO RESTRICTED luokiteltua tietoa siirretään Naton ja Naton ulkopuolisen valtion tai kansainvälisen järjestön viestintä- ja tietojärjestelmien välillä ja Naton ulkopuolisen valtion tai kansainvälisen järjestön viestintä- ja tietojärjestelmissä, tiedon luottamuksellisuus on siirron aikana suojattava toimivaltaisen viranomaisen hyväksymillä salaustuotteilla tai -menetelmillä. Toimivaltainen viranomainen voi olla Naton sotilaskomitea, Naton jäsenvaltion kansallinen viestintä- ja tietojärjestelmien turvallisuusviranomainen tai Naton ulkopuolisen valtion tai kansainvälisen järjestön vastaava viranomainen, jos tällä valtiolla tai järjestöllä on käytössään asianmukaiset rakenteet, säännöt ja menettelyt kyseisten tuotteiden ja menetelmien arviointia, valintaa, hyväksyntää ja valvontaa varten ja jos näitä rakenteita, sääntöjä ja menettelyjä sovelletaan käytännössä tehokkaasti ja turvallisesti. Näistä rakenteista, säännöistä ja menettelyistä sovitaan Naton sotilaskomitean ja kyseisen Naton ulkopuolisen valtion tai kansainvälisen järjestön välillä.

11.14. During transmission between NATO and NNN/IO CIS and within NNN/IO CIS, the confidentiality of information classified NC or NR shall be protected by cryptographic products or mechanisms evaluated and approved by an appropriate authority. The appropriate authority may be the NAMILCOM, the NCSA of a NATO member nation or the equivalent authority of the NNN/IO, provided that the NNN/IO has appropriate structures, rules and procedures in place for the evaluation, selection, approval and control of such products or mechanisms, and that those structures, rules and procedures are being effectively and securely applied in practice. The structures, rules and procedures shall be agreed between the NAMILCOM and the NNN/IO.

11.15. Naton turvallisuusluokitellun tiedon suojaamiseen käytettävän salausaineiston arkaluonteisuus edellyttää erityisten turvatoimien soveltamista niiden toimien lisäksi, jotka vaaditaan Naton muun turvallisuusluokitellun tiedon suojaamiseksi.

11.15. The sensitive nature of the cryptomaterial used to protect NATO classified information necessitates the application of special security precautions beyond those required for the protection of other NATO classified information.

11.16. Salausaineiston suojauksen on vastattava sitä vahinkoa, joka voi aiheutua, jos suojaus laiminlyödään. Käytössä on oltava positiiviset keinot, joilla arvioidaan ja todennetaan salaustuotteiden ja -menetelmien

11.16. The protection which shall be afforded to cryptomaterial shall be commensurate with the damage that may be caused should that protection fail. There shall be

suojaaminen ja asianmukainen toiminta sekä salaustiedon (esim. toteuttamisen yksityiskohtien ja niihin liittyvän dokumentoinnin) suojaaminen ja hallinta.

positive means to assess and verify the protection and proper functioning of the cryptographic products and mechanisms, and the protection and control of cryptographic information (e.g. implementation details and associated documentation).

11.17. Salaustiedon erityisen arkaluonteisuuden vuoksi Natossa ja kaikissa jäsenvaltioissa on oltava käytössä erityismääräykset ja -elimet, jotka säätelevät Naton salaustiedon vastaanottamista ja hallintaa sekä sen jakelua erikseen hyväksytyille henkilöille.

11.17. In recognition of the particular sensitivity of cryptographic information, special regulations and bodies shall exist within NATO and within each member nation to govern the receipt, control and dissemination of NATO cryptographic information to specially certified persons.

11.18. On myös noudatettava erityisiä menettelyjä, joilla säädellään teknisen tiedon jakamista sekä salaustuotteiden ja -menetelmien valintaa, tuottamista ja hankintaa.

11.18. Special procedures shall also be followed which regulate the sharing of technical information, and which regulate the selection, production and procurement of cryptographic products and mechanisms.

12. HAJASÄTEILYTURVALLISUUS

12.1. On toteutettava turvatoimet, joilla suojataan turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin luokiteltu tieto vaarantumiselta, joka johtuu tahattomasta sähkömagneettisesta hajasäteilystä. Toimenpiteiden on oltava hyväksikäytön riskin ja tiedon arkaluonteisuuden mukaiset.

12. EMISSION SECURITY

12.1. Security measures shall be implemented to protect against the compromise of information classified NC and above through unintentional electromagnetic emissions. The measures shall be commensurate with the risk of exploitation and the sensitivity of the information.

13. VIESTINTÄ- JA TIETOJÄRJESTELMIÄ KOSKEVAT ERITYISET VASTUUT

13.1. **Naton sotilaskomitea (NAVMILCOM)**

13.1.1. Naton sotilaskomitean vastuulla viestintä- ja tietojärjestelmien turvallisuuden osalta on salauslaitteiden turvallisuuden hyväksyminen ja niiden luovuttaminen sekä osallistuminen salaustuotteiden ja -menetelmien arviointiin ja valintaan Naton tavanomaista käyttöä varten. Sotilaskomitean neljä virastoa (SECAN, DACAN, EUSEC ja EUDAC), joissa on kansallinen henkilöstö, neuvovat ja tukevat viestintä- ja tietojärjestelmien turvallisuusasioissa sotilaskomiteaa, turvallisuuskomiteaa, tiedonvälityksen, johtamisen ja valvonnan ohjausryhmää sekä

13. SPECIFIC CIS SECURITY RESPONSIBILITIES

13.1 **NATO Military Committee (NAMILCOM)**

13.1.1. The NAMILCOM's responsibilities on CIS Security include the security approval and release of cryptographic equipment and participating in the evaluation and selection of cryptographic products and mechanisms for standard NATO use. The four nationally manned agencies of the Military Committee (SECAN, DACAN, EUSEC and EUDAC) provide advice and support on CIS Security to the NAMILCOM, to the SC, to the C3B and, as appropriate, to their substructures, to member nations and to other NATO organisations.

tarvittaessa näiden alaisia yksiköitä, jäsenvaltioita ja muita Naton organisaatioita.

13.2. **C3-ohjausryhmä (C3B)**

13.2.1. Liittokunnan ylimpänä alansa komiteana tiedonvälityksen, johtamisen ja valvonnan (C3) ohjausryhmä (C3B) tukee Naton sotilaskomiteaa ja Naton poliittisia viranomaisia niiden C3-toiminnan valmiuksien ja hankkeiden arviointiprosessissa arvioimalla C3-toimintaa koskevia operatiivisia vaatimuksia. Ohjausryhmä vastaa turvallisten ja yhteentoimivien Naton laajuisten C3-järjestelmien saattamisesta käyttöön. Naton päämajan C3-esikunta (NHQC3S) antaa henkilöstöä C3-ohjausryhmän tueksi.

13.3. **Naton kyberpuolustuksen ohjausryhmä (CDMB)**

13.3.1. Kyberpuolustuksen ohjausryhmä on kyberpuolustusta koordinoiva elin, joka vastaa kyberpuolustuksen periaatteiden toteuttamisen strategisesta suunnittelusta ja ohjauksesta sekä Naton jäsenvaltioiden kanssa tehtävän yhteistyön edistämisestä. Kyberpuolustuksen ohjausryhmä raportoi Pohjois-Atlantin neuvostolle ja saa siltä poliittista ohjausta puolustuspolitiikan ja -suunnittelun komitean vahvistetun kokoonpanon (DPPC(R)) välityksellä. Jäsenvaltiot valvovat kyberpuolustuksen ohjausryhmää kyberpuolustuksen periaatteita ja C3-periaatteiden toteuttamista koskevissa asioissa C3-ohjausryhmän välityksellä. Kyberpuolustuksen ohjausryhmä neuvottelee yksittäisistä asioista toimivaltaisten Naton komiteoiden välityksellä.

13.4. **Kansallinen viestintä- ja tietojärjestelmien turvallisuusviranomainen (NCSA)**

13.4.1. Kukin Naton jäsenvaltio ja tapauksen mukaan Naton ulkopuolinen valtio määrää kansallisen viestintä- ja tietojärjestelmien turvallisuusviranomaisen, joka voidaan perustaa virastoksi kansalliseen turvallisuusinfrastruktuuriin. Kansallisen viestintä- ja tietojärjestelmien turvallisuusviranomaisen vastuulla on

13.2. **C3 Board (C3B)**

13.2.1. As the senior Consultation, Command and Control (C3) policy committee within the Alliance, the C3B supports the NAMILCOM and the NATO political authorities in their validation process for C3 capabilities and projects by reviewing operational C3 requirements. The C3B is responsible for the provision of secure and interoperable NATO-wide C3 systems. Staff support to the C3B is provided by the NATO HQ C3 Staff (NHQC3S).

13.3. **NATO Cyber Defence Management Board (CDMB)**

13.3.1 The CDMB is the cyber defence coordination body providing strategic planning and direction for the implementation of the Cyber Defence Policy and facilitating cooperation with Allies. The CDMB reports to and receive political guidance from the NAC through the Defence Policy and Planning Committee in reinforced format (DPPC(R)). The CDMB is supervised by Allies through the C3B on C3 policy and implementation aspects of cyber defence. CDMB consults on specific subject matters through the appropriate NATO committees.

13.4. **National CIS Security Authority (NCSA)**

13.4.1. Each NATO and non-NATO nation, where applicable to the latter, shall identify an NCSA, which may be established as an agency in the national security infrastructure. The NCSA is responsible for:

(a) valvoa teknistä salaustietoa, joka liittyy Naton tiedon suojaamiseen kyseisessä valtiossa;

(b) varmistaa, että Naton tiedon suojaamiseen käytettävät salausjärjestelmät, -tuotteet ja -menetelmät valitaan asianmukaisesti ja niitä käytetään ja ylläpidetään asianmukaisesti;

(c) varmistaa, että Naton tiedon suojaamiseen käytettävät viestintä- ja tietojärjestelmien turvallisuustuotteet valitaan asianmukaisesti ja niitä käytetään ja ylläpidetään asianmukaisesti kyseisessä valtiossa;

(d) olla yhteydessä toimivaltaisiin Naton elimiin ja kansallisiin elimiin viestintä- ja tietojärjestelmien turvallisuuteen liittyvissä Naton viestintäturvallisuutta ja tekniikkaa koskevissa asioissa sekä sotilas- että siviilialalla; ja

(e) kansallisen TEMPEST-viranomaisen yksilöiminen tarvittaessa.

13.4.2. Kansallisten viestintä- ja tietojärjestelmien turvallisuusviranomaisten toiminta koordinoidaan kansallisten turvallisuusviranomaisten toiminnan kanssa.

13.5. **Kansallinen jakeluviranomainen (NDA)**

13.5.1. Kukin Naton jäsenvaltio ja tapauksen mukaan Naton ulkopuolinen valtio yksilöi kansallisen jakeluviranomaisen, joka voidaan perustaa virastoksi kansalliseen turvallisuusinfrastruktuuriin ja joka vastaa Naton salausaineiston hallinnasta kyseisessä valtiossa ja varmistaa, että kaiken salausaineiston kattavaa kirjaamista, turvallista käsittelyä, säilyttämistä, jakelua ja hävittämistä varten toteutetaan asianmukaiset menettelyt ja perustetaan tarvittavat kanavat.

13.5.2. Kansallisten jakeluviranomaisten toiminta koordinoidaan kansallisten turvallisuusviranomaisten toiminnan kanssa.

13.6. **Turvallisuuden akkreditointiviranomainen/viranomaiset**

(a) controlling cryptographic technical information related to the protection of NATO information within their nation;

(b) ensuring that cryptographic systems, products and mechanisms for protecting NATO information are appropriately selected, operated and maintained;

(c) ensuring that CIS security products for protecting NATO information are appropriately selected, operated and maintained within their nation;

(d) communicating on NATO communications security and technical matters on CIS Security, both civil and military, with appropriate NATO and national bodies; and

(e) identifying a National TEMPEST Authority, as appropriate.

13.4.2. NCSAs work in co-ordination with their NSA(s).

13.5. **National Distribution Authority (NDA)**

13.5.1 Each NATO and non-NATO nation, where applicable to the latter, shall identify an NDA, which may be established as an agency in the national security infrastructure, which is responsible for the management of NATO cryptomaterial within their nation and shall ensure that appropriate procedures are enforced and channels established for the comprehensive accounting, secure handling, storage, distribution and destruction of all cryptomaterial.

13.5.2. NDAs work in co-ordination with their NSA(s).

13.6. **Security Accreditation Authority(s)**

13.6.1. Kukin Naton jäsenvaltio ja tapauksen mukaan Naton ulkopuolinen valtio määrää yhden tai useamman turvallisuuden akkreditointiviranomaisen, joka vastaa seuraavien turvallisuuden akkreditoinnista:

(a) Naton turvallisuusluokiteltua tietoa käsittelevät kansalliset viestintä- ja tietojärjestelmät; ja

(b) kansallisissa elimissä/organisaatioissa käytettävät Naton viestintä- ja tietojärjestelmät, tapauksen mukaan Naton ulkopuolisissa valtioissa.

13.6.2. Jos Naton jäsenvaltioon perustetaan Naton sotilas- tai siviilielin, Naton viestintä- ja tietojärjestelmien turvallisuuden akkreditoi Naton turvallisuuden akkreditointiviranomainen (SAA). Tällöin turvallisuuden akkreditointi voidaan koordinoida toimivaltaisen kansallisen turvallisuuden akkreditointiviranomaisen kanssa.

13.7. **Naton turvallisuuden akkreditointiviranomainen (SAA)**

13.7.1. Naton turvallisuusluokiteltua tietoa käsittelevien Naton viestintä- ja tietojärjestelmien turvallisuuden akkreditoinnista vastaa kolme Naton turvallisuuden akkreditointiviranomaista. Turvallisuuden akkreditointiviranomaiset ovat Naton turvallisuustoimiston johtaja ja strategiset komentajat tai heidän valtuutetut/nimetyt edustajansa, akkreditoitavan viestintä- tai tietojärjestelmän mukaan.

13.7.2. Naton viestintä- ja tietojärjestelmien turvallisuusjärjestelyjen hyväksyntälautakunta, joka koostuu edellisessä kohdassa tarkoitetuista Naton turvallisuuden akkreditointiviranomaisista, valvoo turvallisuuden akkreditointia kaikkien Naton turvallisuusluokiteltua tietoa käsittelevien Naton viestintä- ja tietojärjestelmien osalta varmistaakseen yhteisen ja johdonmukaisen lähestymistavan näiden järjestelmien turvallisuuteen. Hyväksyntälautakunnan työjärjestys hyväksytetään turvallisuuskomitealla.

13.8. **Naton ulkopuolisen valtion turvallisuusviranomainen**

13.6.1. Each NATO and non-NATO nation, where applicable to the latter, shall identify a security accreditation authority(s) which is responsible for the security accreditation of the following:

(a) national CIS handling NATO classified information; and

(b) NATO CIS operating within national bodies / organisations, as appropriate for non-NATO Nations.

13.6.2. Where a NATO civil or military body is established within a NATO nation, the NATO CIS shall be subject to security accreditation by a NATO SAA. In this case, the security accreditation may be co-ordinated with the appropriate national security accreditation authority.

13.7. **NATO Security Accreditation Authority (SAA)**

13.7.1. There are three NATO SAAs which are responsible for the security accreditation of NATO CIS handling NATO classified information. The SAA shall be the Director, NATO Office of Security and the Strategic Commanders, or their delegated / nominated representative(s), dependent upon the CIS to be accredited.

13.7.2. The NATO CIS Security Accreditation Board, composed of the NATO SAAs as identified in the paragraph above, shall have security accreditation oversight for all NATO CIS handling NATO classified information to ensure a corporate and consistent approach to security of NATO CIS. The NSAB Terms of Reference shall be subject to approval by the Security Committee.

13.8. **Security Authority for NNN**

13.8.1. Naton ulkopuolinen valtio nimeää turvallisuusviranomaisen vastaamaan tämän liitteen turvallisuusmääräysten noudattamisesta sekä valvonnasta, joka kohdistuu sellaisiin Naton ulkopuolisen valtion viranomaisiin, joilla on erityisiä turvallisuusvastuita Naton turvallisuusluokiteltua tietoa käsittelevistä kansallisista viestintä- ja tietojärjestelmistä (mukaan lukien kansallinen viestintä- ja tietojärjestelmien turvallisuusviranomainen, kansallinen jakeluviranomainen ja turvallisuuden akkreditointiviranomaiset).

13.8.1. The NNN shall appoint a security authority to be responsible for the security provisions of the present Enclosure and the oversight of the NNN Authorities with specific CIS Security responsibilities for national CIS handling NATO classified information (including NCSA, NDA and SAAs).

LIITE G
TURVALLISUUSLUOKITELTUJEN HANKKEIDEN TURVALLISUUS JA YRITYSTURVALLISUUS

JOHDANTO

1. Tässä liitteessä esitetään Naton turvallisuusluokitellun tiedon turvallisuutta yrityksissä koskevat periaatteet ja vähimmäisvaatimukset. Lisätietoja ja -vaatimuksia on Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

2. Yritysturvallisuus on suojaustoimien ja -menettelyjen soveltamista sellaisen turvallisuusluokitellun tiedon katoamisen tai vaarantumisen estämiseksi, havaitsemiseksi ja korjaamiseksi, jota yritykset käsittelevät hankesopimusten perusteella. Yrityksille annettava ja yritysten kanssa tehtävien hankesopimusten perusteella tuotettava Naton turvallisuusluokiteltu tieto sekä yritysten kanssa tehtävät turvallisuusluokitellut hankesopimukset on suojattava Naton turvallisuussääntöjen ja niitä tukevien direktiivien mukaisesti.

3. Kansallisten turvallisuusviranomaisten / määrättyjen turvallisuusviranomaisten on varmistettava, että niillä on keinot määrätä yritysturvallisuutta koskevat vaatimuksensa yrityksiä sitoviksi sekä oikeus tarkastaa ja hyväksyä yritysten toimet turvallisuusluokitellun tiedon suojaamiseksi.

YRITYSTURVALLISUUTTA KOSKEVAT VAATIMUKSET

4. Kaikilla hankeosapuolilla / alihankkijoilla, jotka tekevät sellaisia hankesopimuksia, joihin liittyy Naton turvallisuusluokiteltua tietoa ja jotka edellyttävät pääsyä turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempään luokkaan luokiteltuun tietoon tai tällaisen tiedon tuottamista, on oltava asianmukaisen tason yritysturvallisuusselvityksestä annettu todistus (FSC), jonka on antanut sen valtion toimivaltainen kansallinen

ENCLOSURE “G”
CLASSIFIED PROJECT AND INDUSTRIAL SECURITY

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for the security of NATO Classified Information within industry. Additional details and requirements are found in the supporting Directive on Classified Project and Industrial Security.

2. Industrial security is the application of protective measures and procedures to prevent, detect and recover from the loss or compromise of classified information handled by industry in contracts. NATO Classified Information disseminated to industry, generated as a result of a contract with industry, and classified contracts with industry shall be protected in accordance with NATO Security Policy and supporting directives.

3. NSAs/DSAs shall ensure that they have the means to make their industrial security requirements binding upon industry and that they have the right to inspect and approve the measures taken in industry for the protection of classified information.

FACILITY SECURITY REQUIREMENTS

4. All Contractors/Sub-contractors undertaking a contract involving NATO Classified Information requiring access to, or generation of information classified NATO CONFIDENTIAL (NC) or above shall hold a Facility Security Clearance (FSC) at the appropriate level issued by the responsible NSA/DSA of the country that has jurisdiction over the Contractor/Sub-contractor’s facility.

turvallisuusviranomainen / määrätty turvallisuusviranomainen, jonka toimivaltaan hankeosapuolen / alihankkijan yksikkö kuuluu.

5. Turvallisuusluokkaan NATO RESTRICTED luokiteltuun tietoon pääsemiseksi tai tällaisen tiedon tuottamiseksi ei vaadita todistusta yritysturvallisuusselvityksestä.

TARJOUSKILPAILUT, NEUVOTTELUT JA PÄÄTÖKSET SOPIMUKSISTA, JOIHIN LIITTYY NATON TURVALLISUUSLUOKITELTUA TIETOA

6. Naton ohjelman/hankkeen pääsopimuksen neuvottelee ja tekee Naton ohjelman/hankkeen johtokunta/toimisto. Todistus yritysturvallisuusselvityksestä vaaditaan kaikilta sellaisilta hankeosapuolilta, joilta hankesopimukset edellyttävät, että yksikkö hallitsee tai tuottaa turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa tai pääsee tähän tietoon. Turvallisuusluokkaan NATO RESTRICTED luokiteltujen hankesopimusten osalta ei vaadita todistusta yritysturvallisuusselvityksestä.

7. Naton ohjelman/hankkeen johtokunta/toimisto tai muu sopimusviranomainen, joka panee sopimuksenteon vireille, varmistaa, että hankeosapuolen yksiköillä on asianmukaiset todistukset yritysturvallisuusselvityksestä kyseistä sopimuksenteon vaihetta varten. Sopimusviranomainen tarkistaa, että hankeosapuolen henkilöstöllä, joka pääsee turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempään luokkaan luokiteltuun tietoon sopimusviranomaisen toimitiloissa, on asianmukainen todistus henkilöturvallisuusselvityksestä.

8. Kun pääsopimus on tehty, ensisijainen hankeosapuoli voi neuvotella alihankintasopimuksia muiden hankeosapuolten eli alihankkijoiden kanssa. Nämä alihankkijat voivat myös neuvotella alihankintasopimuksia muiden alihankkijoiden kanssa. Jos nämä alihankintasopimukset edellyttävät pääsyä turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin luokkiin luokiteltuun

5. A FSC is not required for access to, or generation of information classified NATO RESTRICTED (NR).

TENDERING, NEGOTIATION AND LETTING OF CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION

6. The prime contract for a NATO programme/project shall be negotiated and awarded by a NATO Programme/Project Agency/Office (NPA/NPO). An FSC shall be required for all Contractors involved in contracts that require the Contractor's facility to manage, generate or have access to information classified NATO CONFIDENTIAL (NC) and above. For contracts classified NATO RESTRICTED (NR), an FSC is not required.

7. The NPA/NPO or other contracting authority which initiates the contract shall ensure that Contractor's facilities hold an appropriate FSC for the specific phase of the contract. The contracting authority shall verify that Contractor's personnel accessing information classified NC or above at the premises of the contracting authority hold the appropriate PSC.

8. After the prime contract has been let, a prime Contractor may negotiate sub-contracts with other Contractors, i.e., Sub-contractors. These Sub-contractors may also negotiate sub-contracts with other Sub-contractors. If these sub-contracts require access to information classified NC and above, the facility and personnel security requirements identified in the "Industrial Security Clearances for NATO Contracts" section of this

tietoon, sovelletaan niitä yritys- ja henkilöstöturvallisuutta koskevia vaatimuksia, jotka on asetettu tämän liitteen osassa "Naton hankesopimuksiin liittyvät yritysturvallisuusselvitykset" sekä direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta. Jos mahdollinen alihankkija kuuluu Naton ulkopuolisen valtion toimivaltaan[1], Naton ohjelman/hankkeen johtokunnalta/toimistolta tai muulta sopimusviranomaiselta on saatava etukäteen lupa neuvotella alihankintasopimus. Jos Naton ohjelman/hankkeen johtokunta/toimisto on rajoittanut sopimusten tekemistä sellaisten Naton jäsenvaltioiden toimivaltaan kuuluvien hankeosapuolten kanssa, jotka eivät osallistu ohjelmaan/hankkeeseen, johtokuntaa/toimistoa pyydetään harkitsemaan luvan antamista ja antamaan luvan ennen sopimusneuvotteluja kyseisten valtioiden hankeosapuolten kanssa.

Enclosure and in the Directive on Classified Project and Industrial Security shall apply. If a potential Sub-contractor is under the jurisdiction[1] of a non-NATO nation prior permission to negotiate a sub-contract shall be obtained from the NPA/NPO or other contracting authority respectively. If the NPA/NPO has placed restrictions on the award of contracts to NATO Nations that are not participants in a programme/project, the NPA/NPO shall be requested to consider and give permission prior to contract discussion with contractors from those Nations.

9. Tehtyään hankesopimuksen Naton ohjelman/hankkeen johtokunta/toimisto tai muu sopimusviranomainen ilmoittaa asiasta hankeosapuolen valtion kansalliselle turvallisuusviranomaiselle / määrätylle turvallisuusviranomaiselle ja varmistaa, että ensisijaiselle hankeosapuolelle annetaan hankesopimuksen mukana tapauksen mukaan turvallisuusnäkökohtia koskeva kirje (SAL) ja/tai ohjelman/hankkeen turvallisuusohjeet (PSI).

9. Upon letting the contract, the NPA/NPO or other contracting authority shall notify the NSA/DSA of the Contractor, and ensure that the Security Aspect Letter (SAL) and/or the Project Security Instruction (PSI), as applicable, is provided to the prime Contractor, with the contract.

TURVALLISUUSVAATIMUKSET HANKESOPIMUKSILLE, JOIHIN LIITTYY NATON TURVALLISUUSLUOKITELTUA TIETOA

SECURITY REQUIREMENTS FOR CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION

10. Ensisijaisen hankeosapuolen ja alihankkijoiden on sopimuksella edellytettävä toteuttavan niiden sopimuksen irtisanomisen uhalla kaikki kansallisten turvallisuusviranomaisten / määrättyjen turvallisuusviranomaisten määräämät toimet hankeosapuolen tuottaman tai sille annetun tai hankeosapuolen valmistamiin esineisiin sisältyvän Naton turvallisuusluokitellun tiedon suojaamiseksi.

10. The prime Contractor and Sub-contractors shall be contractually required, under penalty of termination of their contract, to take all measures prescribed by the NSAs/DSAs for protecting all NATO Classified Information generated by or entrusted to the Contractor, or embodied in articles manufactured by the Contractor:

(a) Contracts for major programme/projects involving NATO Classified Information shall contain a PSI as an annex; a

[1] Oikeus käyttää valtaa tietyssä asiassa tai tietyllä maantieteellisellä alueella.
[1] Power to exercise authority over a subject matter or a territory/geographic area.

(a) Merkittäviä ohjelmia/hankkeita koskeviin hankesopimuksiin, joihin liittyy Naton turvallisuusluokiteltua tietoa, on liitettävä ohjelman/hankkeen turvallisuusohjeet; turvallisuusohjeiden osana on oltava ohjelman/hankkeen turvallisuusluokitusopas. Kaikkiin muihin hankesopimuksiin, joihin liittyy Naton turvallisuusluokiteltua tietoa, on sisällytettävä vähintään turvallisuusnäkökohtia koskeva kirje, jona voivat toimia soveltamisalaltaan rajoitetut ohjelman/hankkeen turvallisuusohjeet. Viimeksi mainitussa tapauksessa ohjelman/hankkeen turvallisuusluokitusoppaaseen voidaan viitata "turvallisuusluokituksen tarkistuslistana". Ohjelman/hankkeen turvallisuusohjeet täydentävät Naton turvallisuussääntöjä ja -vaatimuksia, ja näissä ohjeissa määrätään kyseiseen Naton ohjelmaan/hankkeeseen liittyvät erityiset turvallisuusmenettelyt sekä vastuut turvallisuusluokiteltua tietoa koskevien turvatoimien toteuttamisesta.

(b) Hankesopimuksista, joihin liittyy ainoastaan turvallisuusluokkaan NATO RESTRICTED luokiteltua tietoa, on erityiset määräykset direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta, etenkin sen liitteessä 4 sellaisten tarjousten ja hankesopimusten turvallisuuslausekkeesta, joihin liittyy turvallisuusluokkaan NATO RESTRICTED luokiteltua tietoa.

11. Ohjelman/hankkeen mahdollisiin alihankintasopimuksiin liittyvän tiedon turvallisuusluokituksen on perustuttava ohjelman/hankkeen turvallisuusluokitusoppaaseen.

NATON ULKOPUOLISTEN VALTIOIDEN HANKEOSAPUOLTEN KANSSA TEHTÄVÄT HANKESOPIMUKSET, JOIHIN LIITTYY NATON TURVALLISUUSLUOKITELTUA TIETOA

12. Kun Naton ulkopuolisten valtioiden hankeosapuolten kanssa tehdään hankesopimuksia, joihin liittyy Naton turvallisuusluokiteltua tietoa, tämä on tiedon luovuttamista, ja siinä on noudatettava tämän C-M-

"Project Security Classification Guide" shall be a part of the PSI. All other contracts involving NATO Classified Information shall include, as a minimum, a SAL, which may be a PSI that is reduced in scope. In the latter case, the Programme/Project Security Classification Guide may be referred to as a "Security Classification Checklist". The PSI supplements the NATO security policies and requirements, establishes specific security procedures associated with the NATO programme/project concerned and assigns responsibilities for the implementation of security measures concerning classified information.

(b) For contracts involving only information classified NR specific regulations have been established in the Directive on Classified Project and Industrial Security, in particular in its Appendix 4 "Contract Security Clause for Tenders and Contracts involving NATO RESTRICTED Information".

11. The security classification for programme/project elements of information associated with possible sub-contracts shall be based on the Programme/Project Security Classification Guide.

CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION WITH CONTRACTORS IN NON-NATO NATIONS

12. The letting of contracts involving NATO Classified Information with Contractors in non-NATO nations constitutes release of information and shall be in accordance with Enclosure "E" to this C-M, the Directive on the Security of NATO Classified Information and the Directive on Classified Project and Industrial Security. The release shall always be with the consent of the

asiakirjan liitettä E, direktiiviä Naton turvallisuusluokitellun tiedon turvallisuudesta sekä direktiiviä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta. Tiedon luovuttamiseen on aina oltava sen alkuperäisen yhden tai useamman luovuttajan suostumus.

13. Naton ulkopuolisten valtioiden hankeosapuolten kanssa tehtävät hankesopimukset, joihin liittyy Naton turvallisuusluokiteltua tietoa, edellyttävät kahdenvälisen turvallisuussopimuksen / järjestelyn olemassaoloa Naton tai sopimuksen tekevän / takaajana toimivan Naton jäsenvaltion ja kyseisen Naton ulkopuolisen valtion välillä. Jos hankesopimukseen sovelletaan kahdenvälistä turvallisuussopimusta / järjestelyä sopimuksen tekevän / takaajana toimivan Naton jäsenvaltion ja Naton ulkopuolisen valtion välillä, Naton jäsenvaltion on annettava Natolle kirjallinen turvallisuusvakuutus, jossa vahvistetaan, että luovutettavaan Naton turvallisuusluokiteltuun tietoon sovelletaan kyseistä turvallisuussopimusta / järjestelyä. Jäljennös vakuutuksesta on annettava Naton turvallisuustoimistolle ja kyseiselle Naton ohjelman/hankkeen toimistolle/johtokunnalle.

14. Tehtäessä hankesopimusta Naton ulkopuolisen valtion hankeosapuolen kanssa on noudatettava menettelyjä, jotka kuvataan direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

15. Naton ulkopuolisiin valtioihin on nimettävä yksi tai useampi toimivaltainen turvallisuusviranomainen, joka hoitaa Naton jäsenvaltion kansallisen turvallisuusviranomaisen / määrätyn turvallisuusviranomaisen tehtäviä vastaavia tehtäviä.

NATON HANKESOPIMUKSIIN LIITTYVÄT YRITYSTURVALLISUUSSELVITYKSET

Yleistä

16. Hankesopimuksiin ja alihankintasopimuksiin sovelletaan yksiköitä ja henkilöitä

relevant originator(s).

13. Contracts involving NATO Classified Information with Contractors in non-NATO nations require the existence of a bilateral Security Agreement/Arrangement between NATO or a contracting/sponsoring NATO Nation and the non-NATO nation. If the contract is governed by a bilateral Security Agreement/Arrangement between a contracting/sponsoring NATO Nation and a non-NATO nation, the NATO Nation shall provide a written Security Assurance to NATO confirming that the NATO Classified Information provided is governed under the scope of that Security Agreement/Arrangement. A copy of the assurance shall be provided to the NOS and the relevant NPO/NPA.

14. Placing a contract to a Contractor of a non-NATO nation shall follow the procedures as established in the Directive on Classified Project and Industrial Security.

15. For non-NATO nations, an appropriate security authority(s) shall be identified that fulfils the equivalent functions of a NATO Nation's NSA/DSA.

INDUSTRIAL SECURITY CLEARANCES FOR NATO CONTRACTS

General

16. The policy described in subsequent paragraphs for facilities and individuals apply to contracts and sub-contracts.

koskevia periaatteita, jotka esitetään seuraavissa kohdissa.

Yritysturvallisuusselvitystodistukset (FSC)

17. Kunkin Naton jäsenvaltion kansallisen turvallisuusviranomaisen / määrätyn turvallisuusviranomaisen vastuulla on varmistaa, että sen toimivaltaan kuuluvat yksiköt, jotka tarvitsevat pääsyn turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin luokkiin luokiteltuun tietoon, ovat toteuttaneet tarvittavat suojaustoimet saadakseen todistuksen yritysturvallisuusselvityksestä. Antaessaan todistuksen yritysturvallisuusselvityksestä kansallisen turvallisuusviranomaisen / määrätyn turvallisuusviranomaisen on varmistettava, että sillä on keinot saada tieto seikoista, jotka voivat vaikuttaa todistuksen antamiseen.

18. Arvioinnissa, joka tehdään ennen yritysturvallisuusselvitystä koskevan todistuksen antamista, on noudatettava sovellettavia kansallisia säädöksiä ja määräyksiä sekä niitä vaatimuksia ja perusteita, jotka on kuvattu direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta. Arvioinnin tulee kohdistua ainakin hankeosapuolen/alihankkijan rehellisyyteen ja nuhteettomuuteen, sen henkilöstön ja muiden sellaisten henkilöiden turvallisuusprofiiliin, jotka saattavat yhteyksiensä vuoksi tarvita pääsyä Naton turvallisuusluokiteltuun tietoon, sekä ulkomaiseen omistukseen, määräysvaltaan ja vaikutusvaltaan.

19. Tarjoajaa, jolla ei ole mahdollisen hankesopimuksen/alihankintasopimuksen edellyttämää asianmukaista todistusta yritysturvallisuusselvityksestä, ei saa automaattisesti sulkea pois kilpailusta. Sopimusviranomaisen olisi pyrittävä kaikin keinoin rajoittamaan tarjoajille annettava tieto mahdollisimman alhaisen turvallisuusluokan tietoon, joka kuitenkin edelleen mahdollistaa tietoon perustuvan ja kilpailukelpoisen vastauksen tarjouspyyntöön. Tarjouspyyntöasiakirjassa on kuitenkin ilmoitettava, että ennen hanke-

Facility Security Clearances (FSC)

17. The NSA/DSA of each NATO Nation is responsible for ensuring that any facility under its jurisdiction which will require access to information classified NC and above has adopted the protective security measures necessary to qualify for an FSC. In granting an FSC, the NSA/DSA shall ensure that they have the means to be advised of any circumstances that could have a bearing upon the viability of the clearance granted.

18. The assessment to be made prior to issuing an FSC shall be in accordance with the requirements and criteria set out in the supporting Directive on Classified Project and Industrial Security in addition to any applicable national laws and regulations. As a minimum the assessment shall cover aspects of the integrity and probity of the Contractor/Sub-Contractor, security status of its personnel and of other individuals who may, by virtue of their association be required to have access to NATO Classified Information, and aspects of the foreign ownership, control and influence.

19. A bidder, not holding an appropriate FSC as required by the potential contract/ subcontract shall not be automatically excluded from the competition. The contracting authority should make all efforts in restricting the security classification level of the information required to be provided to bidders to the lowest possible level still permitting an informed and qualified response to the invitation to tender. However, the tender document shall advise on the requirement for an appropriate FSC prior to the award of the contract/subcontract.

sopimuksen/alihankintasopimuksen tekemistä vaaditaan asianmukainen todistus yritysturvallisuusselvityksestä.

20. Yritysturvallisuusselvityksiä koskevien vaatimusten soveltamistilanteita esitetään Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

21. Todistusta yritys- tai henkilöturvallisuusselvityksestä ei vaadita sellaisia hankesopimuksia varten, joihin liittyy turvallisuusluokkaan NATO RESTRICTED luokiteltua tietoa, eikä tällaiseen tietoon pääsyä varten. Valtio, jonka kansalliset turvallisuussäädökset ja -määräykset edellyttävät todistusta yritysturvallisuusselvityksestä turvallisuusluokkaan NATO RESTRICTED luokitellun hankesopimuksen tai alihankintasopimuksen tekemiseksi, ei saa syrjiä tällaista todistusta vaatimattoman valtion hankeosapuolta, vaan sen on varmistettava, että hankeosapuolelle on tiedotettu sen velvollisuuksista tiedon suojaamisen suhteen ja että hankeosapuoli vahvistaa valtiolle hyväksyvänsä nämä velvollisuudet.

Yksiköiden työntekijöiden henkilöturvallisuusselvitykset

22. Yksikön työntekijöillä, jotka tarvitsevat pääsyn turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin luokiteltuun Naton turvallisuusluokiteltuun tietoon, on oltava asianmukainen todistus henkilöturvallisuusselvityksestä. Todistukset henkilöturvallisuusselvityksestä on annettava noudattaen tämän C-M-asiakirjan liitettä C, direktiiviä henkilöstöturvallisuudesta sekä direktiiviä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

23. Hankeosapuolen työntekijöiden turvallisuusselvityksiä haetaan siltä kansalliselta turvallisuusviranomaiselta / määrätyltä turvallisuusviranomaiselta, jonka vastuulle kyseinen yksikkö kuuluu.

24. Jos yksikkö tahtoo palkata Naton ulkopuolisen valtion kansalaisen tehtävään, joka

20. Scenarios identifying FSC requirements are provided in the supporting Directive on Classified Project and Industrial Security.

21. An FSC or PSC is not required for contracts or access to information classified NR. A nation which, under its national security laws and regulations, requires an FSC for a contract or sub-contract classified NR shall not discriminate against a Contractor from a nation not requiring an FSC, but shall ensure that the Contractor has been informed of its responsibilities in respect to the protection of the information, and obtains an acknowledgement of those responsibilities.

Personnel Security Clearances for Facility Employees

22. The facility's employees who require access to NATO Classified Information NC and above shall hold an appropriate PSC. The issuing of PSCs shall be in accordance with Enclosure "C" to this C-M, the Directive on Personnel Security and the Directive on Classified Project and Industrial Security.

23. Applications for the security clearance for Contractor employees shall be made to the NSA/DSA which is responsible for the facility.

24. If a facility wishes to employ a citizen of a non-NATO nation in a position that requires access to NATO Classified Information, it is the responsibility of the NSA/DSA of the Nation which has jurisdiction

edellyttää pääsyä Naton turvallisuusluokiteltuun tietoon, palkkaajayksikön suhteen toimivaltaisen valtion kansallisen turvallisuusviranomaisen / määrätyn turvallisuusviranomaisen on tehtävä tässä määrätty turvallisuusselvitys ja päätettävä, voidaanko henkilölle sallia pääsy tietoon noudattaen tämän C-M-asiakirjan liitteen C vaatimuksia, direktiiviä henkilöstöturvallisuudesta sekä direktiiviä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

NATON TURVALLISUUSLUOKITELLUN TIEDON LUOVUTTAMINEN HANKESOPIMUKSIA TEHTÄESSÄ

25. Hankesopimuksia tehtäessä Naton turvallisuusluokiteltua tietoa voidaan luovuttaa joko Naton ulkopuolisille valtioille ja kansainvälisille järjestöille tai Naton valtioiden toimijoille, jotka eivät osallistu ohjelmiin/hankkeisiin. Luovuttamiseen on saatava tapauksen mukaan kyseisen ohjelman/hankkeen johtokunnan/toimiston ja/tai tiedon alkuperäisen luovuttajan suostumus, ja siinä on noudatettava muita sovellettavia Naton turvallisuussääntöjen liitteitä, direktiiviä Naton turvallisuusluokitellun tiedon turvallisuudesta sekä direktiiviä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

TURVALLISUUSLUOKITELLUN TIEDON KÄSITTELY VIESTINTÄ- JA TIETOJÄRJESTELMISSÄ

26. Naton turvallisuusluokitellun tiedon säilyttämiseen, käsittelyyn ja siirtämiseen (jäljempänä "käsittely") saa käyttää ainoastaan asianmukaisesti akkreditoituja viestintä- ja tietojärjestelmiä. Tämän C-M-asiakirjan liitteessä F, päädirektiivissä viestintä- ja tietojärjestelmien turvallisuudesta (AC/35-D/2004), viestintä- ja tietojärjestelmien turvallisuuden hallintaa koskevassa direktiivissä (AC/35-D/2005) sekä kaikissa sovellettavissa viestintä- ja tietojärjestelmien turvallisuuden teknisissä ja toimeenpanodirektiiveissä (AC/322-asiakirjat) esitetään lisää periaatteita ja ohjeita Naton turvallisuusluokiteltua tietoa käsittelevien viestintä- ja

over the hiring facility, to carry out the security clearance procedure prescribed herein, and determine that the individual can be granted access in accordance with the requirements of Enclosure “C” to this C-M, the Directive on Personnel Security and the Directive on Classified Project and Industrial Security.

RELEASE OF NATO CLASSIFIED INFORMATION IN CONTRACTING

25. The release of NATO Classified Information in contracting can constitute either release to non-NATO nations and International Organizations or release to non-Programme/Project participants from NATO Nations. The release shall be with the consent of the relevant NPA/NPO and/or originator, as applicable, and in accordance with other relevant enclosures to the NATO Security Policy, the Directive on the Security of NATO Classified Information as well as the Directive on Classified Project and Industrial Security.

THE HANDLING OF CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

26. Only appropriately security accredited CIS shall be used for the storing, processing or transmitting (called hereafter “handling") of NATO Classified Information. Enclosure “F” to this C-M, the “Primary Directive on CIS Security” (AC/35-D/2004), the “Management Directive on CIS security” (AC/35-D/2005) and all relevant Technical and Implementation Directives on CIS Security (AC/322 documents) provide further policy and directions for the conformant implementation of CIS handling NATO Classified Information.

tietojärjestelmien vaatimustenmukaisesta toteuttamisesta.

27. Turvallisuusluokkaan NATO RESTRICTED luokiteltua tietoa käsittelevien viestintä- ja tietojärjestelmien akkreditointi voidaan kansallisten turvallisuussäädösten ja -määräysten perusteella siirtää hankeosapuolten tehtäväksi. Jos tehtävä siirretään hankeosapuolille, toimivaltaisten kansallisten turvallisuusviranomaisten / määrättyjen turvallisuusviranomaisten / akkreditointiviranomaisten on vastattava hankeosapuolen käsittelemän turvallisuusluokkaan NATO RESTRICTED luokitellun tiedon suojaamisesta, ja niillä on oikeus tarkastaa hankeosapuolten toteuttamat turvatoimet.

27. The security accreditation of CIS handling information classified NR may be delegated to Contractors according to national security laws and regulations. Where this delegation is exercised, the relevant NSAs/ DSAs/SAAs shall retain the responsibility for the protection of NR information handled by the Contractor and the right to inspect the security measures taken by the Contractors.

KANSAINVÄLISIIN VIERAILUIHIN LIITTYVÄT VALVONTAMENETTELYT

28. Naton jäsenvaltioiden, Naton sotilas- ja siviilielinten, hankeosapuolten ja alihankkijoiden edustajien kansainvälisiin vierailuihin, joihin liittyy Naton turvallisuusluokiteltua tietoa, sovelletaan kansainvälisiin vierailuihin liittyviä valvontamenettelyjä. Niitä sovelletaan myös Naton ulkopuolisen valtion edustajiin, sen hankeosapuolet/alihankkijat mukaan lukien, jos tämä valtio on ottanut kansainvälisiin vierailuihin liittyvät valvontamenettelyt käyttöön.

INTERNATIONAL VISIT CONTROL PROCEDURES (IVCP)

28. IVCP apply to international visits by representatives of NATO Nations, NATO Civil and Military bodies, Contractors and Sub-Contractors involving NATO Classified Information. They also apply to representatives of a non-NATO nation including Contractors/Sub-Contractors of such Nation if the Nation has adopted the IVCP.

29. Vierailut, joihin liittyy pääsy turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin luokkiin luokiteltuun tietoon tai pääsy turvallisuusalueille ilman saattajaa, on hyväksytettävä kansallisella turvallisuusviranomaisella / määrätyllä turvallisuusviranomaisella. Vierailut, joihin liittyy pääsy ryhmään NATO UNCLASSIFIED[2] kuuluvaan tai turvallisuusluokkaan NATO RESTRICTED luokiteltuun tietoon, voidaan järjestää suoraan lähettävän ja vastaanottavan yksikön välillä ilman muodollisia vaatimuksia.

29. Visits involving access to information classified NC and above or unescorted access to security areas shall be approved by the NSA/DSA. Visits involving access to NU[2] or information classified NR may be arranged directly between the sending and receiving facility without formal requirements.

30. Detailed arrangements for the conduct of International Visits are laid down in the Directive on Classified Project and Industrial Security.

[2] NATO UNCLASSIFIED ei ole Naton turvallisuusluokka.
[2] NU is not a NATO security classification.

30. Yksityiskohtaisia järjestelyitä kansainvälisten vierailujen toteuttamiseksi on kuvattu direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

NATON HANKKEESEEN/OHJELMAAN LAINATTAVA HENKILÖSTÖ

31. Jos henkilö, josta on tehty turvallisuusselvitys Naton turvallisuusluokiteltuun tietoon pääsyä varten, on määrä lainata yksiköstä toiseen samassa Naton ohjemassa/hankkeessa, mutta toisessa Naton jäsenvaltiossa, henkilön oman yksikön on pyydettävä valtionsa kansallista turvallisuusviranomaista / määrättyä turvallisuusviranomaista antamaan vahvistus tämän henkilön henkilöturvallisuusselvityksestä sen yksikön valtion kansalliselle turvallisuusviranomaiselle / määrätylle turvallisuusviranomaiselle, johon hänet on määrä lainata.

NATON TURVALLISUUSLUOKITELLUN AINEISTON SIIRTÄMINEN JA KULJETTAMINEN KANSAINVÄLISESTI

Kaikkiin kuljetusmuotoihin sovellettavat turvallisuusperiaatteet

32. Tarkasteltaessa turvallisuusjärjestelyjä, joita aiotaan noudattaa turvallisuusluokiteltua aineistoa sisältävien lähetysten kansainvälisissä kuljetuksissa, on noudatettava seuraavia periaatteita:

(a) turvallisuus on varmistettava kaikissa kuljetuksen vaiheissa ja olosuhteissa alkuperäisestä lähtöpaikasta lopulliseen kohteeseen;

(b) lähetyksen suojauksen taso on määritettävä sen sisältämän aineiston ylimmän turvallisuusluokan mukaan;

(c) kuljetuksen hoitaville yrityksille on tarvittaessa hankittava todistus yritysturvallisuusselvityksestä. Näissä tapauksissa lähetystä käsittelevälle henkilöstölle on annettava todistus henkilöturvallisuusselvityksestä tämän liitteen määräysten mukaisesti;

PERSONNEL ON LOAN WITHIN A NATO PROJECT/ PROGRAMME

31. When an individual who has been cleared for access to NATO Classified Information is to be loaned from one facility to another in the same NATO programme/ project, but in a different NATO Nation, the individual's parent facility shall request its NSA/DSA to provide a Personnel Security Clearance Confirmation for the individual to the NSA/DSA of the facility to which they are to be loaned.

INTERNATIONAL TRANSMISSION AND TRANSPORTATION OF NATO CLASSIFIED MATERIAL

Security Principles Applicable to all Forms of Transportation

32. The following principles shall be enforced when examining proposed security arrangements for the international transportation of consignments of classified material:

(a) security shall be assured at all stages during the transportation and under all circumstances, from the point of origin to the ultimate destination;

(b) the degree of protection accorded to a consignment shall be determined by the highest security classification level of material contained within it;

(c) an FSC shall be obtained, where required, for companies providing transportation. In such cases, personnel handling the consignment shall be issued a PSC in compliance with the provisions of this Enclosure;

(d) journeys shall be point-to-point to the extent possible, and shall be completed as quickly as circumstances permit; and

(d) kuljetusten on mahdollisuuksien mukaan tapahduttava suoraan pisteestä pisteeseen, ja ne on tehtävä niin pian kuin olosuhteet sallivat; ja

(e) kuljetusreitit on huolellisesti järjestettävä kulkemaan ainoastaan Naton jäsenvaltioiden kautta. Naton ulkopuolisten valtioiden kautta kulkevia reittejä olisi käytettävä vain, jos lähettäjän suhteen toimivaltainen kansallinen turvallisuusviranomainen / määrätty turvallisuusviranomainen sallii tämän, ja tällöin on noudatettava Naton turvallisuussääntöjä tukevaa direktiiviä Naton turvallisuusluokitellun tiedon turvallisuudesta.

33. Järjestelyistä turvallisuusluokitellun aineiston lähettämiseksi määrätään erikseen kunkin ohjelman/hankkeen yhteydessä. Näitä järjestelyjä on kuitenkin noudatettava, jotta minimoidaan todennäköisyys luvattomaan pääsyyn tähän aineistoon.

34. Naton turvallisuusluokitellun tiedon kansainvälistä välittämistä koskevat turvallisuusvaatimukset esitetään Naton turvallisuussääntöjä tukevassa direktiivissä Naton turvallisuusluokitellun tiedon turvallisuudesta. Yksityiskohtaiset vaatimukset Naton turvallisuusluokitellun aineiston kuljettamiselle mukana ja kaupallisten kuriiriyritysten, turvallisuusvartijoiden ja saattajien välityksellä sekä räjähteiden, ajoaineiden ja muiden vaarallisten aineiden kuljettamiselle esitetään kuitenkin Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

(e) care shall be exercised to arrange routes only through NATO Nations. Routes through non-NATO nations should only be undertaken when authorised by the NSA/ DSA having jurisdiction over the consignor and in accordance with the supporting Directive on the Security of NATO Classified Information.

33. Arrangements for consignments of classified material shall be stipulated for each programme/project. However, such arrangements shall be in force in order to minimize the likelihood of unauthorised access to classified material.

34. The security standards for the international transfer of NATO Classified Information can be found in the supporting Directive on the Security of NATO Classified Information. However, the detailed requirements for the hand carriage of NATO classified material, carriage of classified material by commercial courier companies, security guards and escorts, and the transportation of explosives, propellants or other dangerous substances are set out in the supporting Directive on Classified Project and Industrial Security.

LIITE H
TURVALLISUUS SUHTEISSA NATON ULKOPUOLISIIN TOIMIJOIHIN

JOHDANTO

1. Tässä liitteessä esitetään ne periaatteet ja vähimmäisvaatimukset, joita noudatetaan suojattaessa Naton ulkopuolisille valtioille ja muille Naton ulkopuolisille elimille (esim. kansainvälisille järjestöille) (jäljempänä "Naton ulkopuoliset toimijat" (NNE)) luovutettavaa tai näiden pääsyoikeuden piiriin kuuluvaa Naton turvallisuusluokiteltua tietoa, mukaan lukien näitä valtioita tai elimiä edustavat henkilöt.

2. Naton turvallisuusluokitellun tiedon jakamisen Naton ulkopuolisten toimijoiden kanssa tulee tapahtua Pohjois-Atlantin neuvoston (NAC) hyväksymän Naton yhteistyötoiminnan yhteydessä. Pohjois-Atlantin neuvosto tai asianomainen valtuutettu viranomainen käsittelee ja hyväksyy tapauskohtaisesti pyynnöt Naton turvallisuusluokitellun tiedon jakamisesta Naton ulkopuolisten toimijoiden kanssa tällaisen yhteistyötoiminnan ulkopuolella. Lisätietoja ja vaatimuksia Naton ulkopuolisille toimijoille luovutettavan tai näiden pääsyoikeuden piiriin kuuluvan Naton turvallisuusluokitellun tiedon suojaamiseksi on Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin.

3. "7 Naton ulkopuolista valtiota", (7NNN), tarkoittaa yksinomaan seuraavia valtioita ja niiden kansalaisia: Australia, Irlanti, Itävalta, Ruotsi, Suomi, Sveitsi ja Uusi-Seelanti.[1]

4. Kukin Naton ulkopuolinen toimija perustaa asianmukaisen turvallisuusviranomaisen, joka vastaa Naton turvallisuusluokitellun tiedon turvallisuudesta. Naton turvallisuus-

ENCLOSURE “H”
SECURITY IN RELATION TO NON-NATO ENTITIES

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for the protection of NATO Classified Information to be released to or accessed by non-NATO nations and other non-NATO bodies (e.g. International Organizations) including individuals representing such nations or bodies (hereinafter referred to as non-NATO entities (NNEs)).

2. The sharing of NATO Classified Information with NNEs shall take place in the context of NATO cooperative activities approved by the North Atlantic Council (NAC). Any request to share NATO Classified Information with NNEs outside such cooperative activities shall be considered and approved by the NAC or the appropriate delegated authority on a case-by-case basis. Additional details and requirements for the protection of NATO Classified Information to be released or accessed by NNEs are found in the supporting Directive for NATO on Security in Relation to NNEs.

3. The term 7 Non-NATO Nations (7NNN) refers solely to the following countries and their citizens: Australia, Austria, Finland, Ireland, New Zealand, Sweden and Switzerland.[1]

4. NNEs shall establish an appropriate security authority responsible for the security of NATO Classified Information. The Supporting Document for Non-NATO Entities on

[1] Kansalliset turvallisuusviranomaiset / määrätyt turvallisuusviranomaiset voivat ehdottaa muutoksia valtioiden luetteloon turvallisuuskomitean hyväksyttäväksi.
[1] NSAs/DSAs may propose changes to the list of countries, for approval by the Security Committee.

sääntöjä tukevassa asiakirjassa turvallisuudesta Naton ulkopuolisten toimijoiden suhteissa Natoon annetaan näille toimijoille yleiskuva niistä turvallisuuden perusperiaatteista ja vähimmäisvaatimuksista, joita on sovellettava suojattaessa ja käsiteltäessä Naton turvallisuusluokiteltua tietoa ja vastaavaa kansallista tietoa, kun sitä vaihdetaan Pohjois-Atlantin neuvoston hyväksymän Naton yhteistyötoiminnan yhteydessä.

YLEISET VAATIMUKSET

5. Naton turvallisuusluokiteltua tietoa voidaan vaihtaa Naton ulkopuolisten toimijoiden kanssa seuraavissa yhteyksissä:

(a) Pohjois-Atlantin neuvoston hyväksymä yhteistyötoiminta, johon Pohjois-Atlantin neuvosto on hyväksynyt Naton ulkopuolisen toimijan osallistumaan;

(b) Naton toiminta (esim. ohjelma, hanke, operaatio, tehtävä), jossa Naton ulkopuolisen toimijan osallistumisen ja sen mukanaolon toiminnassa joltakin osin katsotaan hyödyttävän Natoa; tai

(c) Naton jäsenvaltion ja Naton ulkopuolisen toimijan väliset kahdenväliset sitoumukset, joiden osalta Naton turvallisuusluokitellun tiedon jakamisen Naton ulkopuolisen toimijan kanssa katsotaan hyödyttävän Natoa.

6. Ennen Naton turvallisuusluokitellun tiedon jakamista Naton ulkopuolisen toimijan kanssa kyseisen toimijan ja Naton on tullut tehdä turvallisuussopimus, jonka toteuttaminen Naton turvallisuustoimiston (NOS) on vahvistettava. Jos turvallisuussopimusta ei ole tehty, on tullut antaa turvallisuusvakuutus, jos on poliittisesti tai operatiivisesti välttämätöntä jakaa Naton turvallisuusluokiteltua tietoa oikea-aikaisesti Pohjois-Atlantin neuvoston hyväksymän yhteistyötoiminnan tukemiseksi tai poikkeustapauksissa tällaisen toiminnan ulkopuolella. Turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin kuvataan yksityiskohtaiset määräykset, joita sovelletaan Naton turvallisuus-

Security in Relation to NATO provides the NNEs with an overview of the basic principles and minimum standards of security to be applied to the protection and handling of NATO Classified Information, and national equivalents exchanged in the context of NATO cooperative activities approved by the NAC.

GENERAL REQUIREMENTS

5. The sharing of NATO Classified Information with NNEs may take place in the contexts of:

(a) NAC-approved cooperative activities where the NNE's participation has been approved by the North Atlantic Council (NAC);

(b) NATO activities (e.g. programme, project, operation, task) where the NNE's participation and the nature of its engagement in a specific aspect of an activity is deemed beneficial to NATO; or

(c) bilateral engagements between a NATO Nation and an NNE, where sharing of NATO Classified Information with an NNE has been determined to be beneficial to NATO.

6. Prior to sharing NATO Classified Information with an NNE, the NNE and NATO shall have entered into a Security Agreement, the implementation of which shall be certified by the NATO Office of Security (NOS). In the absence of a Security Agreement, a Security Assurance shall be in place where there is a political or operational imperative to share NATO Classified Information in a timely manner in support of a NAC-approved cooperative activity or, in exceptional cases, outside such an activity. The supporting Directive for NATO on Security in Relation to NNEs describes detailed provisions applicable to sharing NATO Classified Information with NNEs in the contexts specified in paragraph 5.

luokitellun tiedon jakamiseen Naton ulkopuolisten toimijoiden kanssa 5. kohdassa mainituissa yhteyksissä.

TURVALLISUUSSOPIMUKSET JA HALLINNOLLISET JÄRJESTELYT

7. Turvallisuussopimus on järjestelmä, jonka avulla mahdollistetaan turvallisuusluokitellun tiedon vaihtaminen tietyn Naton ulkopuolisen toimijan kanssa. Turvallisuussopimuksessa määrätään Naton ja Naton ulkopuolisen toimijan välillä sovitut korkean tason strategiset periaatteet, jotka toimivat perustana asianmukaisten turvatoimien toteuttamiselle tarkoituksena suojata tarvittaessa sekä Naton että Naton ulkopuolisen toimijan turvallisuusluokiteltua tietoa. Ennen Naton turvallisuusluokitellun tiedon luovuttamista Naton ulkopuoliselle toimijalle Naton turvallisuustoimiston on vahvistettava, että tämä toimija noudattaa turvallisuussopimusta.

8. Turvallisuussopimuksen turvallisuusperiaatteita tuetaan asianmukaisella hallinnollisten järjestelyjen kokonaisuudella. Hallinnolliset järjestelyt tukevat turvallisuussopimuksen toteuttamista ja koostuvat määräyksistä, joissa asetetaan turvallisuuden perusvaatimukset vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi asianmukaisella ja keskinäisesti hyväksyttävällä tavalla. Kun hallinnollisista järjestelyistä on sovittu, Naton turvallisuustoimisto vahvistaa niiden soveltamisen turvallisuustarkastuksen avulla.

9. Naton turvallisuustoimisto tekee Naton ulkopuolisten toimijoiden asianomaisille elimille määräajoin, vähintään kahden vuoden välein, riskinhallinnan lähestymistapaan perustuvia turvallisuustarkastuksia varmistaakseen turvallisuussopimuksen ja hallinnollisten järjestelyjen jatkuvan noudattamisen.

TURVALLISUUSVAKUUTUKSET

10. Turvallisuusvakuutusta käytetään, jos Naton ja Naton ulkopuolisen toimijan välillä ei ole voimassa vahvistettua turvallisuusso-

SECURITY AGREEMENTS AND ADMINISTRATIVE ARRANGEMENTS

7. A Security Agreement is a mechanism used to enable the exchange of classified information with an identified NNE. It sets out high level strategic principles agreed between NATO and the NNE, providing the basis for the implementation of appropriate security measures to protect NATO Classified Information as well as the NNE's classified information, when required. The implementation of the Security Agreement by the NNE shall be certified by the NOS before any NATO Classified Information is released to an NNE.

8. The security principles identified in the Security Agreement shall be supported by an appropriate set of Administrative Arrangements. The Administrative Arrangements act in support of the implementation of a Security Agreement and are a set of provisions which outline the basic security requirements for the appropriate and mutually acceptable protection of the exchanged classified information. Once the Administrative Arrangements have been concluded their application shall be confirmed by the NOS through the conduct of a security survey.

9. The NOS shall carry out periodic security surveys, at least once every two years, based on a risk management approach, of the relevant bodies within the NNE to ensure continued compliance with the Security Agreement and the Administrative Arrangements.

SECURITY ASSURANCES

10. A Security Assurance is utilized in the absence of a certified Security Agreement between NATO and an NNE where there is a political or operational imperative that necessitates the sharing of NATO Classified

pimusta ja jos on poliittisesti tai operatiivisesti välttämätöntä jakaa Naton turvallisuusluokiteltua tietoa oikea-aikaisesti Pohjois-Atlantin neuvoston hyväksymän yhteistyötoiminnan tukemiseksi tai poikkeustapauksissa tällaisen toiminnan ulkopuolella. Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin määrätään yksityiskohtaisista edellytyksistä, jotka on täytettävä käytettäessä turvallisuusvakuutusta.

11. Turvallisuusvakuutus virallistaa Naton ulkopuolisen toimijan sitoumuksen suojata vastaanottamansa Naton turvallisuusluokiteltu tieto asianmukaista tasoa noudattaen. Turvallisuusvakuutus rajoitetaan koskemaan tiettyä toimintaa tietyn ajan.

12. Naton ulkopuolisen toimijan antama turvallisuusvakuutus, jonka tämän toimijan asianmukaisesti valtuuttama edustaja on allekirjoittanut, annetaan Naton turvallisuustoimistolle, kun turvallisuusvakuutusta käytetään tarkoituksena mahdollistaa Naton turvallisuusluokitellun tiedon jakaminen seuraavien tukemiseksi:

(a) Pohjois-Atlantin neuvoston hyväksymä yhteistyötoiminta tai

(b) tapauskohtaisesti Naton toiminta, johon Pohjois-Atlantin neuvosto tai asianomainen valtuutettu viranomainen on hyväksynyt Naton ulkopuolisen toimijan osallistumaan.

Naton jäsenvaltion toimiminen takaajana

13. Naton turvallisuusluokitellun tiedon jakaminen muun kuin 12.a tai 12.b kohdassa määritellyn toiminnan yhteydessä Naton jäsenvaltion erityisestä pyynnöstä edellyttää takaajaa. Takaajana toimiminen tarkoittaa tietynlaista Naton jäsenvaltion tukea Naton ulkopuoliselle toimijalle tarkoituksena mahdollistaa Naton turvallisuusluokitellun tiedon jakaminen tämän toimijan kanssa, jos Naton ja tämän toimijan välillä ei ole voimassa vahvistettua turvallisuussopimusta.

Information in a timely manner in support of a NAC-approved cooperative activity, or in exceptional cases outside such an activity. The supporting Directive for NATO on Security in Relation to NNEs provides detailed criteria to be fulfilled in cases when a Security Assurance is used.

11. A Security Assurance formalises the NNE's commitment to provide an appropriate degree of protection to any NATO Classified Information received. A Security Assurance is limited to the specific activity, for a specific period of time.

12. A Security Assurance from an NNE, signed by a representative duly mandated by the NNE, shall be provided to the NOS in cases where a Security Assurance is utilized for the purposes of enabling sharing of NATO Classified Information in support of a:

(a) NAC-approved cooperative activity, or

(b) NATO activity, where the NNE's participation has been approved by the NAC or the appropriate delegated authority, on a case-by-case basis.

Sponsorship by a NATO Nation

13. Sharing of NATO Classified Information outside activities defined in 12 (a) or (b), further to a special request by a NATO Nation, requires sponsorship. A sponsorship means a form of support provided by a NATO Nation to an NNE in order to enable sharing of NATO Classified Information with an NNE in case of absence of a certified Security Agreement between NATO and the NNE.

14. In order for a NATO Nation to be able to act as a Sponsor there shall be an appropriate security framework (e.g. security

14. Jotta Naton jäsenvaltio voi toimia takaajana, takaajan ja Naton ulkopuolisen toimijan välillä on oltava olemassa asianmukainen turvallisuusjärjestely (esim. turvallisuussopimus tai muu sovellettava järjestely). Takaajan on toimitettava Naton turvallisuustoimistolle kirjallinen turvallisuusvakuutus, jonka on allekirjoittanut Naton ulkopuolisen toimijan asianmukaisesti valtuuttama edustaja. Turvallisuusvakuutuksessa asetetaan ne vähimmäisvaatimukset, joita Naton ulkopuolisen toimijan on sovellettava Naton turvallisuusluokitellun tiedon suojaamiseksi.

15. Takaajana toimiminen rajoitetaan koskemaan tiettyä toimintaa tietyn ajan.

ERITYISET TURVALLISUUSMÄÄRÄYKSET

16. Jaettaessa Naton turvallisuusluokiteltua tietoa Naton ulkopuolisten toimijoiden kanssa voidaan pääsy Naton turvallisuusluokiteltuun tietoon tai toimitilaan sallia näille toimijoille kolmella tavalla: pääsy Naton toimitiloihin, pääsy Naton turvallisuusluokiteltuun tietoon ja Naton turvallisuusluokitellun tiedon luovuttaminen. Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin määrätään kussakin tilanteessa sovellettavista yksityiskohtaisista edellytyksistä sekä erityistoimista ja menettelyistä.

Henkilöstöturvallisuus

17. Ennen kuin Naton ulkopuolista toimijaa edustavalle henkilölle annetaan pääsy turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempään luokkaan luokiteltuun tietoon, hänen on tullut läpäistä vähintään samantasoinen PSC-menettely kuin se, joka Naton turvallisuusperiaatteiden ja niitä tukevien ohjeiden mukaan vaaditaan Naton jäsenvaltion kansalaiselta.

18. Turvallisuusluokkaan NATO RESTRICTED luokiteltuun tietoon pääsemiseksi ei vaadita todistusta henkilöturvallisuusselvityksestä. Kyseisellä Naton ulkopuolista toi-

agreement or other applicable arrangement) in place between the Sponsor and the NNE. The Sponsor shall provide a written Security Assurance, signed by a representative duly mandated by the NNE, to the NOS. The Security Assurance stipulates the minimum standards that the NNE shall apply for the protection of NATO Classified Information.

15. A sponsorship is limited to a specific activity, for a specific period of time.

SPECIFIC SECURITY PROVISIONS

16. When sharing NATO Classified Information with NNEs there are three circumstances in which access to NATO Classified Information or premises can be provided to NNEs: access to NATO premises, access to NATO Classified Information, and release of NATO Classified Information. The supporting Directive for NATO on Security in Relation to NNEs provides detailed criteria and the related specific measures and procedures applicable for each scenario.

Personnel Security

17. Before an NNE individual is granted access to information classified NC or above, the individual shall have successfully completed a PSC procedure no less rigorous than that required for a NATO national in accordance with NATO Security Policy and its supporting directives.

18. A PSC is not required for access to information classified NATO RESTRICTED (NR). However, the NNE individual shall have a need-to-know, shall be briefed on their security obligations in respect to the protection of NATO Classified Information and shall have acknowledged their security

mijaa edustavalla henkilöllä on kuitenkin oltava tiedonsaantitarve, hänelle on selostettava hänen turvallisuusvelvoitteensa Naton turvallisuusluokitellun tiedon suojaamisen suhteen, ja hänen on tullut kirjallisesti tai vastaavalla kiistämättömyyden varmistavalla menetelmällä ilmoittaa ymmärtäneensä turvallisuusvelvoitteensa.

19. Todistusta henkilöturvallisuusselvityksestä voidaan vaatia edellytyksenä pääsylle Naton toimitiloihin sellaisten erityisten edellytysten perusteella, joista määrätään Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin ja sovellettavissa paikallisissa turvallisuusmääräyksissä.

Toimitilaturvallisuus

20. Naton ulkopuolisia toimijoita edustaville henkilöille, joiden on toimeksiantonsa ja virallisten tehtäviensä vuoksi tavattava säännöllisesti Naton henkilöstöä, voidaan sallia pääsy tietyille alueille, joilla säilytetään tai käsitellään turvallisuusluokkaan NATO RESTRICTED ja sitä ylempiin luokkiin luokiteltua tietoa ja/tai siitä keskustellaan. Näille henkilöille voidaan myös antaa työskentelytilaa tietyiltä alueilta. Pääsyn salliminen ilman saattajaa ja/tai työskentelytilan antaminen käsitellään tapauskohtaisesti.

21. Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin on yksityiskohtaista tietoa edellytyksistä, joilla Naton ulkopuolisia toimijoita edustaville henkilöille voidaan sallia pääsy Naton luokan I tai II turva-alueelle tai hallinnolliselle vyöhykkeelle, sekä tällöin noudatettavasta menettelystä ja toimivaltaisista hyväksyntäviranomaisista.

Tietoaineistoturvallisuus

22. Naton ulkopuolisten toimijoiden kanssa tehtävässä yhteistyössä voidaan pääsy Naton turvallisuusluokiteltuun tietoon sallia näille toimijoille kolmella tavalla:

responsibilities in writing or an equivalent method which ensures non-repudiation.

19. A PSC may be required to access NATO premises based on specific criteria stipulated in the supporting Directive for NATO on Security in Relation to NNEs, and the relevant local security regulations.

Physical Security

20. Individuals from NNEs who, because of their assignment and official duties, need regular interface with NATO staff may be granted access to specific areas in which information classified NR and above is stored, handled and/or discussed. Such individuals may also be assigned office space within specific areas. The granting of unescorted access and/or the assignment of office space shall be handled on a case-by-case basis.

21. The supporting Directive for NATO on Security in Relation to NNEs provides detailed information on the procedure, approval authorities and the criteria to be fulfilled for individuals from NNEs to be granted access to a NATO Class I or Class II Security Area, or to an Administrative Zone.

Security of Information

22. In the context of cooperation with NNEs there are three circumstances in which access to NATO Classified Information or premises can be provided to NNEs:

(a) **Access to NATO premises**. A circumstance when an individual representing an NNE is authorised to physically access a specific NATO site, facility or

(a) **pääsy Naton toimitiloihin.** Naton ulkopuolista toimijaa edustavalle henkilölle sallitaan fyysinen pääsy tiettyyn Naton tilaan tai yksikköön tai tietylle alueelle yksikön sisällä. Fyysinen pääsy ei automaattisesti sisällä pääsyä Naton turvallisuusluokiteltuun tietoon;

(b) **pääsy Naton turvallisuusluokiteltuun tietoon.** Naton ulkopuolista toimijaa edustavalle henkilölle sallitaan pääsy Naton turvallisuusluokiteltuun tietoon, jotta hän voi hoitaa toimeksiantonsa ja viralliset tehtävänsä, kun pääsy hyödyttää Natoa. Pääsy sallitaan vain kyseiselle henkilölle, eikä hän saa jakaa Naton turvallisuusluokiteltua tietoa eteenpäin edustamalleen Naton ulkopuoliselle toimijalle, ellei kyseistä tietoa ole luovutettu vakiintuneiden menettelyjen mukaisesti;

(c) **Naton turvallisuusluokitellun tiedon luovuttaminen.** Naton turvallisuusluokiteltua tietoa sallitaan luovutettavan Naton ulkopuoliselle toimijalle.

23. Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin määrätään yksityiskohtaisista edellytyksistä, jotka on täytettävä tietyissä tilanteissa, kun Naton sotilas- tai siviilielinten tai Naton jäsenvaltioiden on määrä sallia pääsy Naton turvallisuusluokiteltuun tietoon tai luovuttaa sitä.

24. Naton turvallisuusluokitellun tiedon luovuttaminen Naton ulkopuoliselle toimijalle edellyttää aina alkuperäisen yhden tai useamman luovuttajan kirjallista ennakkosuostumusta.

25. Naton turvallisuusluokiteltua tietoa voidaan luovuttaa Pohjois-Atlantin neuvoston hyväksymän yhteistyötoiminnan yhteydessä tai Naton toiminnan yhteydessä, jos Pohjois-Atlantin neuvosto tai asianomainen valtuutettu viranomainen on hyväksynyt tähän toimintaan osallistuvat Naton ulkopuoliset toimijat. Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhspecific area located within a facility. Physical access does not automatically include access to NATO Classified Information.

(b) **Access to NATO Classified Information.** A circumstance when an individual representing an NNE is authorised to access NATO Classified Information in order to fulfil their assignments and official duties when access is for NATO's benefit. Access is limited to the individual in question and they are not permitted to disseminate NATO Classified Information further to their NNE unless that information has been released in accordance with the established procedures.

(c) **Release of NATO Classified Information.** A circumstance when NATO Classified Information is authorised to be released to an NNE.

23. The supporting Directive for NATO on Security in Relation to NNEs provides detailed criteria that needs to be fulfilled in specific circumstances when access to or release of NATO Classified Information is to be provided by NATO Civil or Military bodies, or by NATO Nations.

24. Release of NATO Classified Information to an NNE is always subject to receiving prior written consent of the originator(s).

25. NATO Classified Information may be released in the context of NAC-approved cooperative activity or in the context of NATO activities, where the NNE participants to that activity have been endorsed by the NAC or the appropriate delegated authority. The supporting Directive for NATO on Security in Relation to NNEs provides additional criteria to be applied prior to release.

teissa Naton ulkopuolisiin toimijoihin määrätään lisäedellytyksistä, joita on sovellettava ennen tiedon luovuttamista.

26. Direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin määritetään myös lisäedellytykset, joita on sovellettava ennen Naton turvallisuusluokitellun tiedon luovuttamista, kun sitä luovutetaan Naton jäsenvaltion (takaajan) erityisestä pyynnöstä Naton ulkopuoliselle toimijalle, joka ei osallistu Pohjois-Atlantin neuvoston hyväksymään yhteistyötoimintaan tai Naton toimintaan, ja kun Pohjois-Atlantin neuvosto tai asianomainen valtuutettu viranomainen on hyväksynyt kyseiseen toimintaan osallistuvat Naton ulkopuoliset toimijat.

27. Jos kansainvälisen järjestön kanssa on voimassa turvallisuussopimus tai turvallisuusvakuutus, on luovutettaessa Naton turvallisuusluokiteltua tietoa Naton ulkopuolisille järjestön jäsenille noudatettava sovellettavia turvallisuussopimuksen määräyksiä sekä muita vakiintuneita sääntöjä niiden osallistumisesta Naton toimintaan. Jollei turvallisuussopimusta ole voimassa, ja jos kansainvälisen järjestön kanssa on voimassa turvallisuusvakuutus, on luovutettaessa Naton turvallisuusluokiteltua tietoa Naton ulkopuolisille järjestön jäsenille noudatettava Naton turvallisuussääntöjä tukevan direktiivin sovellettavia määräyksiä ja turvallisuusvakuutusta.

28. Mihinkään turvallisuusluokkaan luokiteltuun ATOMAL-tietoon ei saa sallia pääsyä eikä sitä saa luovuttaa Naton ulkopuoliselle toimijalle, joka ei ole osapuolena voimassa olevassa sopimuksessa Pohjois-Atlantin sopimuksen osapuolten välillä ydinpuolustustietoja koskevasta yhteistyöstä (C-M(64)39).

Luovuttajaviranomainen

29. Pohjois-Atlantin neuvostolla on ylin toimivalta luovutettaessa Naton turvallisuusluokiteltua tietoa Naton ulkopuolisille toimi-

26. For NATO Classified Information to be released on a special request from a NATO Nation (the Sponsor) to an NNE outside NAC-approved cooperative activities or NATO activities, where the NNE participants in that activity have been endorsed by the NAC or the appropriate delegated authority, the supporting Directive for NATO on Security in Relation to NNEs provides additional criteria to be applied prior to release.

27. Where a Security Agreement or Security Assurance is in force with an international organization, the release of NATO Classified Information to its non-NATO members shall be in accordance with the relevant provisions of the Security Agreement, as well as other established rules concerning their participation in NATO activities. In the absence of a Security Agreement, where a Security Assurance is in place with an international organization, the release of NATO Classified Information to its non-NATO members shall be in accordance with the relevant provisions of the supporting Directive and the Security Assurance.

28. ATOMAL information of any security classification shall not be accessed by or released to any NNE which is not a party to the current Agreement Between the Parties to the North Atlantic Treaty for Co-operation Regarding Atomic Information C-M(64)39.

Release Authority

29. The NAC is the ultimate authority for the release of NATO Classified Information to NNEs. This authority respects the principle of originator consent and is delegated to:

joille. Tätä toimivaltaa käytettäessä noudatetaan alkuperäisen luovuttajan suostumuksen periaatetta, ja toimivaltaa siirretään

(a) asianomaiselle aihekohtaiselle komitealle sellaisen turvallisuusluokkaan NATO SECRET ja sitä alempiin luokkiin luokitellun tiedon osalta, joka on peräisin kyseiseltä komitealta ja/tai sen alaisilta elimiltä. Turvallisuusluokkaan NATO RESTRICTED luokitellun tiedon osalta asianomainen aihekohtainen komitea voi siirtää toimivaltaa edelleen käytettäväksi selvästi määritellyssä henkilöstön tukitoiminnossa tai kyseisen komitean tukihenkilöstön tietyssä yhdessä tai useammassa tehtävässä;

(b) sotilaskomitealle sellaisen turvallisuusluokkaan NATO SECRET ja sitä alempiin luokkiin luokitellun tiedon osalta, joka on peräisin sotilaskomitealta ja/tai sen alaisilta elimiltä. Turvallisuusluokkaan NATO RESTRICTED luokitellun tiedon osalta sotilaskomitea voi siirtää toimivaltaa edelleen käytettäväksi selvästi määritellyssä henkilöstön tukitoiminnossa tai sotilaskomitean tukihenkilöstön tietyssä yhdessä tai useammassa tehtävässä;

(c) Naton Euroopan joukkojen komentajalle tai varakomentajalle sellaisen turvallisuusluokkaan NATO SECRET ja sitä alempiin luokkiin luokitellun tiedon osalta, joka katsotaan voitavan luovuttaa kulloisellekin operaatiolle (XFOR) tai joka on luokiteltu turvallisuusluokkaan NATO/XFOR SECRET (mission SECRET), tietyin edellytyksin, joista määrätään yksityiskohtaisesti Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin.

(d) Naton transformaatioesikunnan komentajalle tai varakomentajalle turvallisuusluokkaan NATO SECRET ja sitä alempiin luokkiin luokitellun tiedon osalta tietyin edellytyksin, joista määrätään yksityiskohtaisesti Naton turvallisuussääntöjä tukevassa ohjeessa turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin;

(a) the appropriate subject-matter committee for information classified up to and including NS which has been originated by that committee and/or bodies subordinate to it. For information classified NR, the appropriate subject-matter committee may further delegate authority to a clearly identified staff support function or a specific role(s) within the support staff to that committee;

(b) the MC for information classified up to and including NS which has been originated by the MC and/or bodies subordinate to it. For information classified NR, the MC may further delegate authority to a clearly identified staff support function or a specific role(s) within the support staff to the MC;

(c) SACEUR or D/SACEUR for information classified up to and including NS which is identified as being releasable to the mission (XFOR), or is classified NATO/ XFOR SECRET (mission SECRET), under specific conditions, which are in detail described in the supporting Directive for NATO on Security in Relation to NNEs;

(d) SACT or D/SACT for information classified up to and including NS information, under specific conditions, which are in detail described in the supporting Directive for NATO on Security in Relation to NNEs;

(e) the mission commander for an operation involving Non-NATO Troop Contributing Nations (NNTCN), as endorsed by the NAC, for information classified up to and including NS that has already been

(e) operaation komentajalle Pohjois-Atlantin neuvoston hyväksymässä operaatiossa, johon osallistuu joukkoja luovuttavia Naton ulkopuolisia valtioita (NNTCN), sellaisen turvallisuusluokkaan NATO SECRET ja sitä alempiin luokkiin luokitellun tiedon osalta, joka on jo katsottu voitavan luovuttaa operaatiolle (XFOR), tietyin edellytyksin, joista määrätään yksityiskohtaisesti Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin;

(f) Naton tuotanto- ja logistiikkaorganisaatiolle (NPLO), organisaatioon osallistuvien valtioiden kanssa koordinoiden, sellaisen Naton turvallisuusluokitellun tiedon osalta, joka on peräisin yhdeltä tai useammalta organisaatioon osallistuvalta valtiolta ja kuuluu tälle.

30. Lukuun ottamatta 29.a ja 29.b kohdassa mainittuja poikkeuksia, jotka koskevat turvallisuusluokkaan NATO RESTRICTED luokiteltua tietoa, valtuutetut luovuttajaviranomaiset eivät saa siirtää valtuuksiaan eteenpäin.

31. Toimivaltaa luovuttamiseen saa siirtää asianomaiselle aihekohtaiselle komitealle vain, jos tiedon alkuperäinen yksi tai useampi luovuttaja on edustettuna komiteassa. Jos alkuperäistä yhtä tai useampaa luovuttajaa ei voida selvittää, asianomainen aihekohtainen komitea ottaa alkuperäisen luovuttajan vastuun.

32. Täytäntöönpano-ohjeissa tiedustelutiedon jakamiseksi Naton ja Naton ulkopuolisten toimijoiden välillä (DSG(2015)0307-REV1) sekä Naton turvallisuussääntöjä tukevassa asiakirjassa tiedon ja tiedustelutiedon jakamisesta Naton ulkopuolisten toimijoiden kanssa (AC/35-D/1040) määritellään luovuttajaviranomainen operaatioiden, koulutuksen, harjoitusten, transformaation ja yhteistyön yhteydessä.

determined as releasable to the mission (XFOR), under specific conditions, which are in detail described in the supporting Directive for NATO on Security in Relation to NNEs;

(f) the NATO Production and Logistics Organization (NPLO), in coordination with the participating nations, for NATO Classified Information originated by and belonging to one or more of the nations participating in the NPLO.

30. With the exceptions applying to information classified NR stated in paragraphs 29 (a) and (b) above, delegated release authorities cannot further delegate their powers.

31. Authority for release shall only be delegated to an appropriate subject-matter committee on which the originator(s) is/are represented. If the originator(s) cannot be established, the appropriate subject-matter committee shall assume the responsibility of the originator.

32. The Implementing Instructions on Intelligence Sharing Between NATO and NNEs (DSG(2015)0307-REV1) and the Supporting Document on Information and Intelligence Sharing with Non-NATO Entities (AC/35-D/1040) define the Release Authority in the environments of Operations, Training, Exercises, Transformation or Cooperation.

Records of Released Information

33. NATO Civil and Military bodies shall keep records of decisions of all information classified NC and above which they have released to an NNE and shall, at least every

Luovutettua tietoa koskeva kirjanpito

33. Naton sotilas- ja siviilielinten on pidettävä kirjaa kaikista päätöksistä, jotka koskevat niiden Naton ulkopuoliselle toimijalle luovuttamaa turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin luokkiin luokiteltua tietoa, sekä ilmoitettava yksityiskohtaisesti päätösten viitenumerot, otsikot ja antamispäivät vähintään kuuden kuukauden välein Naton keskusrekisterille Brysseliin, jollei toimivaltainen turvallisuusviranomainen toisin määrää.

Viestintä- ja tietojärjestelmien turvallisuus

34. Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin asetetaan erityiset vaatimukset, jotka on täytettävä, jotta Naton ulkopuolista toimijaa edustavalle henkilölle voidaan sallia pääsy Naton viestintä- ja tietojärjestelmiin.

35. Naton viestintä- ja tietojärjestelmien yhteenkytkentä Naton ulkopuolisen toimijan viestintä- ja tietojärjestelmien kanssa on akkreditoitava Naton turvallisuussääntöjen ja niitä tukevien direktiivien mukaisesti.

TIETOTURVAPOIKKEAMAT

36. Sellaisten tietoturvapoikkeamien käsittelyssä, joihin liittyy Naton hallussa olevaa Naton ulkopuolisen toimijan turvallisuusluokiteltua tietoa, on noudatettava direktiiviä Naton turvallisuusluokitellun tiedon turvallisuudesta (AC/35-D/2002) ja mahdollisia muita määräyksiä, jotka on annettu turvallisuussopimuksessa ja täytäntöönpanoa koskevissa hallinnollisissa järjestelyissä tai Naton ulkopuolisen toimijan kanssa sovellettavassa turvallisuusvakuutuksessa.

37. Tietoturvapoikkeamista, joihin liittyy Naton ulkopuolisen toimijan turvallisuusluokiteltua tietoa, on viipymättä ilmoitettava Naton turvallisuustoimistolle. Naton turvallisuustoimiston vastuulla on ilmoittaa viipymättä asianomaisen Naton ulkopuolisen toisix months, report details of the reference number, title and release date to the NATO Central Registry, Brussels, unless otherwise directed by an appropriate Security Authority.

Communication and Information Systems Security

34. The supporting Directive for NATO on Security in Relation to NNEs outlines specific requirements that shall be met in order for an NNE individual to be provided access to NATO Communication and Information System (CIS).

35. Interconnection of NATO CIS with an NNE's CIS shall be security accredited in accordance with the NATO Security Policy and its supporting directives.

SECURITY INCIDENTS

36. Security incidents involving an NNE's classified information in NATO's possession shall follow the provisions of the Directive on the Security of NATO Classified Information (AC/35-D/2002) and any additional provisions specified in the Security Agreement and the implementing Administrative Arrangements, or Security Assurance with the NNE.

37. Security incidents involving an NNE's classified information shall be immediately reported to the NOS. The NOS is responsible for promptly informing the relevant NNE's Security Authority on security incidents involving an NNE's classified information in accordance with the Security Agreement and the implementing Administrative Arrangements, or Security Assurance.

mijan turvallisuusviranomaiselle tietoturvapoikkeamista, joihin liittyy Naton ulkopuolisen toimijan turvallisuusluokiteltua tietoa, noudattaen turvallisuussopimusta ja täytäntöönpanoa koskevia hallinnollisia järjestelyjä tai turvallisuusvakuutusta.

SANASTO		**GLOSSARY**	
Pääsy tietoon	Luvan antaminen yhdelle tai useammalle henkilölle mahdollisuuteen saada tiettyä tietoa vaadittavien turvallisuusrajoitusten mukaisesti, jotta henkilö voi suorittaa selvästi määritellyt tehtävänsä, joihin hänellä on asianmukaiset valtuudet. Pääsy tietoon tällaisissa olosuhteissa on kyseisen henkilön erioikeus, johon ei sisälly oikeuksia tiedon levittämiseen laajemmalti.	Access to information	The granting of permission for an individual or individuals to be exposed to specific information in line with the required security parameters for the execution of their clearly defined and appropriately authorized duties. Access in such circumstances is the privilege of the individual in question where rights of further dissemination are not permitted.
Pääsy toimitiloihin	Luvan antaminen fyysiseen pääsyyn tiettyyn paikkaan, jossa nimetty yksi tai useampi henkilö saa oleskella joko nimetyn saattajan kanssa tai ilman tätä, sen mukaan, mitä kulloisetkin turvallisuusvaatimukset edellyttävät ja kulloisetkin turvallisuusselvitykset mahdollistavat.	Access to premises	The granting of permissions for the physical access to a defined location where a nominated individual or individuals will be allowed to be present either with or without a designated escort dependent upon specific security requirements and clearances.
Tilivelvollisuuden alainen tieto	Kaikki tieto, joka on luokiteltu turvallisuusluokkiin COSMIC TOP SECRET (CTS) ja NATO SECRET (NS) sekä kaikki erityisluokan (kuten ATOMAL) tieto.	Accountable Information	All information classified CTS and NS and all Special Category Information. (such as ATOMAL)
Hallinnollinen vyöhyke	Selvästi määritelty suojattu alue, jolla henkilöillä ei tarvitse olla saattajaa ja jolle pääsy on luvanvarainen.	Administrative Zone	A clearly defined protected area in which individuals are not required to be escorted and to which access is subject to authorization.

Kasautumisperiaate	Kun suuri määrä Naton turvallisuusluokiteltua tietoa kootaan yhteen, sen alkuperäiset turvallisuusluokitusmerkinnät on säilytettävä, ja on arvioitava, miten tämän tietokokonaisuuden katoaminen tai vaarantuminen vaikuttaisi järjestöön. Jos tämä kokonaisvaikutus arvioidaan suuremmaksi kuin kyseisten yksittäisten Naton turvallisuusluokkien mukainen vaikutus, olisi harkittava kyseisen tietokokonaisuuden käsittelemistä ja suojaamista sen turvallisuusluokan mukaisesti, joka vastaa tietokokonaisuuden katoamisen tai vaarantumisen arvioitua vaikutusta.	Aggregation Principle	When a large amount of NATO Classified Information is collated together, the original security classification markings must be retained and that information shall be assessed for the impact its collective loss or compromise would have upon the organization. If this overall impact is assessed as being higher than the impact of the actual individual NATO security classifications then consideration should be given to handling and protecting it at a level commensurate with the assessed impact of its loss or compromise.
Tunnistaminen	Tunnistaminen on toimi, jolla varmistetaan tietyn toimijan väitetty identiteetti.	Authentication	Authentication is the act of verifying the claimed identity of an entity.
Käytettävyys	Tiedon ja aineiston saavutettavuus ja käyttökelpoisuus valtuutetun henkilön tai yksikön pyytäessä sitä.	Availability	The property of information and material being accessible and usable upon demand by an authorised individual or entity.
Turvallisuusluokiteltu tieto	Sellainen tieto (jota voidaan välittää missä tahansa muodossa) tai aineisto, jonka katsotaan edellyttävän suojaamista luvattomalta ilmitulolta ja joka on turvallisuusluokituksella osoitettu sellaiseksi.	Classified Information	Any information (namely, knowledge that can be communicated in any form) or material determined to require protection against unauthorised disclosure and which has been so designated by a security classification.
Viestintä- ja tietojärjestelmien turvallisuus (CIS Security)	Turvallisuustoimenpiteiden soveltaminen viestintä- ja tietojärjestelmien ja muiden sähköisten järjestelmien sekä näihin järjestelmiin tal-	Communication and Information System Security (CIS Security)	The application of security measures for the protection of communication, information and other electronic systems, and the information that is stored, processed or

	lennettavien ja niissä käsiteltävien tai siirrettävien tietojen luottamuksellisuuden, eheyden, käytettävyyden, aitouden ja kiistämättömyyden suojaamiseksi.		transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.
Toimivaltainen turvallisuusviranomainen (CSA)	Kansallisen turvallisuusviranomaisen nimeämä viranomainen, jolla on toimivalta hoitaa tiettyjä turvallisuustehtäviä, jotka liittyvät muun muassa henkilöturvallisuusselvityksiin, jotta kyseisen valtion kansalaisille voidaan sallia pääsy Naton turvallisuusluokiteltuun tietoon.	Competent Security Authority (CSA)	An authority identified by the NSA which is authorised to carry out specific security roles including those relating to personnel security clearances in order to give their nationals access to NATO Classified Information.
Vaarantuminen	Vaarantuminen tarkoittaa tilannetta, jossa tietoturvaloukkauksen tai haitallisen toiminnan (kuten vakoilun, terroriteon, sabotaasin tai varkauden) vuoksi Naton turvallisuusluokiteltu tieto on menettänyt luottamuksellisuutensa, eheytensä tai käytettävyytensä tai tätä tietoa tukevat palvelut ja resurssit ovat menettäneet eheytensä tai käytettävyytensä. Vaarantumiseen sisältyvät katoaminen, paljastuminen asiattomille (esim. joukkoviestimille tai vakoilun vuoksi), luvaton muuttaminen, hävittäminen luvattomalla tavalla tai palvelun estyminen.	Compromise	Compromise denotes a situation when - due to a Security Breach or adverse activity (such as espionage, acts of terrorism, sabotage or theft) - NATO Classified Information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability. This includes loss, disclosure to unauthorized individuals (e.g. through espionage or to the media) unauthorized modification, destruction in an unauthorised manner, or denial of service.
Viestintäkeskus	Organisaatio, joka vastaa viestintäliikenteen käsittelystä ja valvonnasta ja johon tavallisesti kuuluu sanomakeskus ja salauskeskus sekä lähetys- ja vastaanottokeskukset.	Communications Centre	An organization responsible for handling and controlling communications traffic, normally comprising a message centre, a cryptographic centre, and transmitting and receiving stations.

Luottamuksellisuus	Se, ettei tietoa saateta asiattomien henkilöiden tai muiden toimijoiden saataville eikä paljasteta näille.	Confidentiality	The property that information is not made available or disclosed to unauthorised individuals or entities.
Vastaanottaja	Hankeosapuoli, yksikkö tai muu organisaatio, joka vastaanottaa aineistoa lähettäjältä.	Consignee	The contractor, facility or other organization receiving material from the consignor.
Lähettäjä	Hankeosapuoli, yksikkö tai muu organisaatio, joka vastaa aineiston järjestämisestä ja lähettämisestä.	Consignor	The contractor, facility or other organization responsible for organizing and dispatching material.
Hankesopimus	Oikeudellisesti täytäntöönpanokelpoinen sopimus tavaroiden tai palvelujen toimittamisesta.	Contract	A legally enforceable agreement to provide goods or services.
Hankeosapuoli	Teollinen, kaupallinen tai muu toimija, joka tekee sopimuksen tavaroiden tai palvelujen toimittamisesta.	Contractor	An industrial, commercial or other entity that agrees to provide goods or services.
Kuriiri	Henkilö, joka on virallisesti määrätty kuljettamaan aineistoa mukanaan.	Courier	A person officially assigned to hand-carry material.
Kuriiripalvelu	Palvelu, joka välittää henkilöitä, jotka on virallisesti määrätty kuljettamaan aineistoa mukanaan.	Courier Service	A service that provides personnel officially assigned to hand-carry material.
Salausaineisto	Salausalgoritmit, salauslaitteistot ja -ohjelmistomoduulit sekä tuotteet, joihin sisältyy täytäntöönpanoa koskevia yksityiskohtia sekä niihin liittyviä asiakirjoja ja avainnusaineistoa (sekä symmetrisiä että epäsymmetrisiä salausmenetelmiä varten).	Cryptomaterial	Includes cryptographic algorithms and cryptographic hardware – and software- modules and products including implementation details and associated documentation and keying material (for both, symmetric and asymmetric cryptographic mechanisms).
Määrätty turvallisuusviranomainen (DSA)	Viranomainen, jonka vastuulla on tiedottaa yrityksille ja muille yhteisöille kansallisista periaatteista kaikissa Naton	Designated Security Authority (DSA)	An authority responsible for communicating to industry the national policy in all matters of NATO industrial security policy

	yhteisöturvallisuuden periaatteita koskevissa asioissa sekä antaa ohjausta ja apua niiden soveltamisessa. Joissakin maissa määrätyn turvallisuusviranomaisen tehtävää voi hoitaa kansallinen turvallisuusviranomainen.		and for providing direction and assistance in its implementation. In some countries, the function of a DSA may be carried out by the NSA.
Asiakirja	Mikä tahansa tallennettu tieto riippumatta sen fyysisestä muodosta tai ominaisuuksista, mukaan lukien rajoituksetta kirjalliset ja painotuotteet; tietojenkäsittelyssä käytettävät kortit ja nauhat; kartat, kaaviot, valokuvat, maalaukset, piirustukset, kaiverrukset, luonnokset, työmuistiinpanot ja -paperit, hiilipaperikopiot ja värinauhat; millä tahansa menetelmällä tai menettelyllä tehdyt jäljennökset; kaikenlaiset ääni-, puhe- ja magneettitallenteet sekä elektroniset, optiset ja videotallenteet; kannettavat tietotekniset laitteet, joissa on kiinteät tallennusvälineet, ja irrotettavat tietokoneen tallennusvälineet.	Document	Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies or ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable IT equipment with resident computer storage media, and removable computer storage media.
Dynaaminen riskienhallinta	Kyky harjoittaa riskienhallintaa siten, että viestintä- ja tietojärjestelmien käytön riskiä arvioidaan jatkuvasti, että kaikki viestintä- ja tietojärjestelmien toiminnan yhteyteen liittyvät muutokset kuvastuvat dynaamisesti riskien tunnisteissa ja että kussakin tilanteessa sovelletaan oikea-aikaisesti tarkoituk-	Dynamic Risk Management	The ability to perform risk management in a way that the risk of using a CIS is continuously assessed, any change in the context in which the CIS operates is reflected in the risk signature dynamically and the security countermeasures, most appropriate to the situation, are applied timely.

	senmukaisimpia vastatoimia turvallisuuden ylläpitämiseksi.		
Saattajat	Aseistetut tai aseistamattomat kansalliset poliisit tai sotilashenkilöt tai muu valtion henkilöstö. Saattajien tehtävänä on helpottaa aineiston siirtämistä turvallisesti, mutta he eivät ole välittömästi vastuussa aineiston varsinaiseen suojaamiseen liittyvistä asioista.	Escorts	Armed or unarmed national police, military, or other government personnel. Their function is to facilitate the secure movement of the material, but they do not have direct responsibility in matters of the protection of the material itself.
Yksikkö	Laitos, tehdas, laboratorio, toimisto, yliopisto tai muu oppilaitos tai kaupallinen yritys, mukaan lukien näihin liittyvät varastot, säilytysalueet, aputilat ja osat, jotka tehtävänsä ja sijaintinsa suhteen muodostavat toimivan kokonaisuuden.	Facility	An installation, plant, factory, laboratory, office, university or other educational Institution, or commercial undertaking, including any associated warehouses, storage areas, utilities and components which, when related by function and location, form an operating entity.
Yritysturvallisuusselvitystodistus (FSC)	Kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen hallinnollinen päätös siitä, että turvallisuuden näkökulmasta yksikkö pystyy suojaamaan asianmukaisesti tiettyyn tai sitä alempaan turvallisuusluokkaan kuuluvan Naton turvallisuusluokitellun tiedon ja että yksikön henkilöstöstä, joka tarvitsee pääsyn Naton turvallisuusluokiteltuun tietoon, on tehty asianmukaisesti turvallisuusselvitys ja sille on selostettu ne Naton turvallisuusvaatimukset, joita on noudatettava Naton turvallisuusluokiteltuja sopimuksia toteutettaessa.	Facility Security Clearance (FSC)	An administrative determination by a NSA/DSA that, from a security viewpoint, a facility can afford adequate security protection to NATO Classified Information of a specified security classification or below, and its personnel who require access to NATO Classified Information have been properly cleared and briefed on NATO security requirements necessary to perform on the NATO Classified Contracts.
Vartijat	Sotilashenkilöstö tai (valtion tai osallistuvan	Guards	Civilian (government or participating contractor

	hankeosapuolen työntekijöistä koostuva) siviilihenkilöstö, joka voi olla aseistettu tai aseistamaton. Vartijat voidaan määrätä joko pelkästään turvallisuusvartiointiin tai sekä turvallisuusvartiointiin että muihin tehtäviin.		employees) or military personnel who may be armed or unarmed. They may be assigned for security guard duties only or may combine security guard duties with other duties.
Henkilökohtainen kuljettaminen	Tiedon siirtäminen siten, että henkilö kuljettaa sen mukanaan.	Hand Carriage	The transmission of information by an individual carrying that information on their person.
Isäntävaltio	Yleisesti: Valtio, johon Naton sotilas- tai siviilielin on sijoitettu. Yritysturvallisuuden yhteydessä: Valtio, jonka Naton virallinen elin on nimennyt siksi valtion virastoksi, joka tekee sopimuksen Naton pääsopimuksen toteuttamiseksi. Valtioita, joissa toteutetaan alihankintasopimuksia, ei sanota isäntävaltioiksi.	Host Nation	General: The nation in which a NATO Civil or Military body is located. Industrial security: The nation designated by an official body of NATO to act as the governmental agency to contract for the performance of a NATO prime contract. Nations in which sub-contracts are performed are not referred to as host nations.
Tieto	Missä tahansa muodossa välitettävä tieto.	Information	Knowledge that can be communicated in any form.
Tietojen turvaaminen	Tieto on suojattava soveltamalla tietojen turvaamisen periaatetta, jolla tarkoitetaan niiden toimenpiteiden kokonaisuutta, joilla pyritään saavuttamaan tietty luottamuksen taso viestintä- ja tietojärjestelmien, muiden sähköisten järjestelmien ja muiden kuin sähköisten järjestelmien sekä näihin järjestelmiin tallennettavien ja niissä käsiteltävien tai siirrettävien tietojen luottamuksellisuuden, eheyden,	Information Assurance	Information shall be protected by applying the principle of Information Assurance, which is described as the set of measures to achieve a given level of confidence in the protection of communication, information and other electronic systems, non-electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability,

	käytettävyyden, kiistämättömyyden ja aitouden suojaamisessa.		nonrepudiation and authentication.
Vähäinen tietoturvapoikkeama	Vähäinen tietoturvapoikkeama on tahallinen tai tahaton teko tai laiminlyönti, joka on Naton turvallisuussääntöjen ja niitä tukevien direktiivien vastainen mutta ei johda Naton turvallisuusluokitellun tiedon tosiasialliseen tai mahdolliseen vaarantumiseen (esimerkkejä: Naton turvallisuusluokiteltua tietoa jätetään suojaamattomana suojattuihin toimitiloihin, joissa toimivista henkilöistä on kaikista tehty asianmukaisesti turvallisuusselvitys; Naton turvallisuusluokiteltu tieto jätetään sulkematta kaksinkertaiseen suojakuoreen).	Infraction	A security infraction is an act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives that does not result in the actual or possible compromise of NATO Classified Information (e.g. NATO Classified Information left unsecured inside a secure facility where all individuals are appropriately cleared, failure to double wrap NATO Classified Information, etc.).
Eheys	Se, ettei tietoa (myöskään dataa, kuten salatekstiä) ole muutettu eikä hävitetty luvattomalla tavalla.	Integrity	The property that information (including data, such as cipher text) has not been altered or destroyed in an unauthorised manner.
Kansainväliset vierailut	Vierailut, joita kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen toimivaltaan tai Naton elimeen kuuluva henkilöstö tekee toisen kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen tai Naton toimivaltaan kuuluviin yksiköihin tai elimiin ja jotka edellyttävät pääsyä Naton turvallisuusluokiteltuun tietoon tai joihin voi liittyä pääsy siihen tai jotka kyseisen tiedon turvallisuusluo-	International Visits	Visits made by individuals subject to one NSA/DSA or belonging to a NATO body, to facilities or bodies subject to another NSA/DSA or to NATO, which will require, or may give rise to access to NATO Classified Information or where, regardless of the level of classification involved, national legislation governing the establishment or body to be visited in support of NATO approved related activities requires that

	kasta riippumatta edellyttävät toimivaltaisen kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen hyväksyntää sen kansallisen lainsäädännön mukaan, joka koskee tällaisen Naton hyväksymää toimintaa tukevan vierailun kohteena olevaa yksikköä tai elintä. Kaikki Naton sotilas- ja siviilielimet kuuluvat turvallisuusasioissa Naton toimivaltaan.		such visits shall be approved by the relevant NSA/DSA. All NATO Civil and Military bodies fall within the security jurisdiction of NATO.
Elinkaari	Tiedon elinkaari käsittää tiedon suunnittelun, keräämisen, luomisen tai tuottamisen; sen järjestämisen, haun, käytön, saavutettavuuden ja siirtämisen; sen säilyttämisen ja suojaamisen; sekä lopulta sen käytöstä poistamisen arkistoimalla tai hävittämällä.	Life-cycle	Life cycle of information encompasses the stages of planning, collection, creation or generation of information; its organization, retrieval, use, accessibility and transmission; its storage and protection; and, finally, its disposition through transfer to archives or destruction.
Koneellisesti luettava tietoväline	Tietoväline, joka voi välittää tietoja tiettyyn lukulaitteeseen.	Machine Readable Medium	A medium that can convey data to a given sensing device.
Merkittävä ohjelma/hanke	Suurimerkityksinen ohjelma tai hanke, johon tavallisesti liittyy enemmän kuin kaksi valtiota sekä sellaisia turvatoimia, jotka ylittävät tavanomaiset Naton turvallisuusperiaatteissa määritellyt perusvaatimukset.	Major Programme/Project	A programme or project of major significance, normally involving more than two nations and security measures that extend beyond the normal basic requirements described in NATO Security Policy.
Aineisto	Aineisto sisältää asiakirjat ja myös valmistetut ja valmisteilla olevat koneet, laitteet/komponentit, aseet ja työvälineet.	Material	Material includes documents and also any items of machinery, equipment/components, weapons or tools, either manufactured or in the process of manufacture.
Sotilaskomitea (MC)	Naton korkein sotilasviranomainen; sotilaskomitea vastaa sotilasasioiden hoitamisesta yleisesti.	Military Committee (MC)	The highest military authority in NATO; the MC is responsible for the

	Sotilaskomitea vastaa operatiivisesti niiden käyttäjien vaatimusten hyväksymisestä, joita strategiset komentajat välittävät, sekä näiden vaatimusten asettamisesta etusijajärjestykseen.		overall conduct of military affairs. The MC is responsible for endorsing and prioritising from an operational point of view the users' requirements submitted by Strategic Commanders.
Kansalaiset	Kansalaisia ovat eri valtioiden kansalaiset ja Kanadan pysyvät asukkaat. Kanadan pysyvät asukkaat ovat henkilöitä, jotka ovat läpäisseet asuinpaikkaa ja rikosrekisteriä koskevat tarkastukset sekä turvallisuustarkastukset sisältävän kansallisen arviointimenettelyn ja saavat laillisen luvan pysyvään oleskeluun Kanadassa.	Nationals	Nationals includes “nationals of a Kingdom”, “citizens of a State”, and “Permanent Residents in Canada”. “Permanent Residents in Canada” are individuals who have gone through a national screening process including residency checks, criminal records and security checks, and who are going to obtain lawful permission to establish permanent residence in the nation.
Kansallinen turvallisuusviranomainen (NSA)	Viranomainen, joka vastaa Naton turvallisuusluokiteltujen tietojen turvallisuudesta kansallisissa virastoissa ja yksiköissä, sekä sotilas- että siviilialalla, kotimaassa ja ulkomailla.	National Security Authority (NSA)	An authority which is responsible for the security of NATO Classified Information in national agencies and elements, military or civil, at home or abroad.
Nato	”Nato” tarkoittaa Pohjois-Atlantin liittoa ja niitä elimiä, joihin sovelletaan joko Ottawassa 20. syyskuuta 1951 allekirjoitettua sopimusta Pohjois-Atlantin liiton, kansallisten edustajien ja kansainvälisen henkilöstön asemasta tai Pariisissa 28. elokuuta 1952 allekirjoitettua pöytäkirjaa Pohjois-Atlantin sopimuksen mukaisesti perustettujen kansainvälisten sotilasesikuntien asemasta.	NATO	“NATO” denotes the North Atlantic Treaty Organization and the bodies governed either by the Agreement on the status of the North Atlantic Treaty Organization, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952.

Naton turvallisuus-luokiteltu sopimus	Naton sotilas- tai siviilielimen tai Naton jäsenvaltion tekemä sopimus, jolla tuetaan Naton rahoittamaa tai hallinnoimaa ohjelmaa tai hanketta, joka edellyttää pääsyä Naton turvallisuusluokiteltuun tietoon tai tällaisen tiedon tuottamista.	NATO Classified Contract	Any contract issued by a NATO Civil or Military Body or a NATO Nation in support of a NATO funded or administered programme/project that will require access to or generate NATO Classified Information.
Naton turvallisuus-luokiteltu tieto	a) Tieto tarkoittaa missä tahansa muodossa välitettävää tietoa; b) turvallisuusluokiteltu tieto tarkoittaa tietoa tai aineistoa, jonka katsotaan edellyttävän suojaamista luvattomalta ilmitulolta ja joka on turvallisuusluokituksella osoitettu sellaiseksi; c) "aineisto" sisältää asiakirjat ja myös valmistetut ja valmisteilla olevat koneet, laitteet ja aseet; d) "asiakirja" tarkoittaa mitä tahansa muodossa tallennettua tietoa riippumatta sen fyysisestä muodosta tai ominaisuuksista, mukaan lukien rajoituksetta kirjalliset ja painotuotteet; tietojenkäsittelyssä käytettävät kortit ja nauhat; kartat, kaaviot, valokuvat, maalaukset, piirustukset, kaiverrukset, luonnokset, työmuistiinpanot ja -paperit, hiilipaperikopiot ja värinauhat; millä tahansa menetelmällä tai menettelyllä tehdyt jäljennökset; kaikenlaiset ääni-,	NATO Classified Information	(a) Information means knowledge that can be communicated in any form; (b) Classified information means information or material determined to require protection against unauthorised disclosure which has been so designated by a security classification; (c) The word “material” includes documents and also any items of machinery or equipment or weapons either manufactured or in the process of manufacture; (d) The word “document” means any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies or ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable

	puhe- ja magneettitallenteet sekä elektroniset, optiset ja videotallenteet; kannettavat tietotekniset laitteet, joissa on kiinteät tallennusvälineet, ja irrotettavat tietokoneen tallennusvälineet.		IT equipment with resident computer storage media, and removable computer storage media.
Naton tieto	Naton tietoa on kaikki turvallisuusluokiteltu ja turvallisuusluokittelematon tieto, jota jaetaan Natossa, riippumatta siitä, onko tieto peräisin Naton sotilas- tai siviilielimiltä vai onko se saatu Naton jäsenvaltioilta tai muista lähteistä kuin Natosta.	NATO Information	NATO information embraces all information, classified and unclassified, circulated within NATO, whether such information originates in NATO Civil or Military bodies or is received from member nations or from non-NATO sources.
Naton tuotanto- ja logistiikkaorganisaatio (NPLO)	Apuelin, joka on perustettu Natoon suorittamaan Pohjois-Atlantin sopimuksesta johtuvia tehtäviä ja jolle Pohjois-Atlantin neuvosto antaa selvästi määritellyn organisatorisen, hallinnollisen ja taloudellisen riippumattomuuden. NPLO:ssa on johtokunta ja toimeenpaneva elin, joka koostuu pääjohtajasta ja henkilöstöstä.	NATO Production and Logistics Organization (NPLO)	A subsidiary body, created within the framework of NATO for the implementation of tasks arising from that Treaty, to which North Atlantic Council grants clearly defined organizational, administrative and financial independence. It shall be comprised of a board of directors; and an executive body, composed of a General Manager and staff.
Naton ohjelma	Neuvoston hyväksymä ohjelma, jota hallinnoi Naton määräämä johtokunta/toimisto Naton sääntöjen mukaisesti.	NATO Programme	A Council approved programme that is administered by a NATO management/office under NATO regulations.
Naton hanke	Neuvoston hyväksymä hanke, jota hallinnoi Naton määräämä johtokunta/toimisto Naton sääntöjen mukaisesti.	NATO Project	A Council approved project that is administered by a NATO management agency/office under NATO regulations.
Naton tuotanto- ja logistiikkaorganisaation johtokunta	NPLO:n toimeenpaneva elin.	NATO Project Management Agency	The executive body of a NPLO.

Tiedonsaantitarve	Periaate, jonka mukaan tiedon mahdollisella vastaanottajalla katsotaan olevan tarve päästä tietoon, saada tieto siitä tai saada se haltuunsa pystyäkseen suorittamaan virallisia tehtäviä tai palveluja.	Need-to-know	The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services.
Neuvottelut	Ilmaus käsittää kaikki hankinta- tai alihankintasopimuksen tekemisen näkökohdat alkuvaiheen tarjouspyyntöjä koskevasta aieilmoituksesta lopulliseen päätökseen tehdä hankinta- tai alihankintasopimus.	Negotiations	The term encompasses all aspects of awarding a contract or subcontract from the initial "notification of intention to call for bids" to the final decision to let a contract or sub-contract.
Muun kuin luottamuksellisuuden varmistavat palvelut	Viestintä- ja tietojärjestelmien turvallisuuden varmistavat palvelut, joilla varmistetaan muiden turvallisuustavoitteiden kuin luottamuksellisuuden saavuttaminen, eli käytettävyys, eheys, todentaminen ja kiistämättömyys.	Non-confidentiality services	Services for CIS Security assuring security objectives other than for Confidentiality, namely Availability, Integrity, Authentication, and Non-repudiation.
Kiistämättömyys	Toimenpide, jolla varmistetaan vastaanottajalle, että tiedon on lähettänyt tietty henkilö tai organisaatio, ja lähettäjälle, että aiotut vastaanottajat ovat vastaanottaneet tiedon.	Non-repudiation	The measure of assurance to the recipient that shows that information was sent by a particular person or organization and to the sender that shows that information has been received by the intended recipients.
Avoin säilytysalue	Alue, joka on rakennettu turvallisuusluokitellun tiedon avointa säilyttämistä varten turvallisuusvaatimusten mukaisesti ja jonka sotilas- tai siviilielimen johtaja on hyväksynyt tähän tarkoitukseen.	Open Storage Area	An area, constructed in accordance with security requirements and authorised by the head of the civil or military body for open storage of Classified Information.

Alkuperäinen luovuttaja	Valtio tai kansainvälinen järjestö, jonka alaisuudessa tieto on tuotettu tai tuotu Natoon.	Originator	The nation or international organization under whose authority information has been produced or introduced into NATO.
Alkuperäisen luovuttajan määräysvalta	Periaate, jonka mukaan valtio, Nato tai muu organisaatio, jonka alaisuudessa tieto on luotu, tuotettu tai tuotu Natoon, määrää tämän tiedon käyttöön sovellettavat säännöt ja vaatimukset ja on toimivaltainen tiedon koko elinkaaren aikaisten muutosten suhteen.	Originator Control	The principle by which the nation, NATO, or other organization, under whose authority information has been created, produced, or introduced into NATO, establishes the rules and standards which apply to the use of this information and has authority over any changes throughout information life-cycle.
Kansalaisuusvaltio	Se maa, jonka kansalainen henkilö on.	Parent Nation	The Nation of which an individual is a national.
Henkilöturvallisuusselvitystodistus (PSC)	Henkilöturvallisuusselvitystodistus (PSC) on kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen myönteinen arvio, jolla virallisesti tunnustetaan luonnollisen henkilön kelpoisuus päästä turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon, ottaen huomion henkilön lojaliteetti ja luotettavuus.	Personnel Security Clearance (PSC)	A PSC is a positive determination by which a NSA/DSA formally recognizes the individual's eligibility to have access to information classified NC and above taking into account their loyalty, trustworthiness and reliability.
Ohjelman/hankkeen pääsopimus	Alkuperäinen hankesopimus, jonka toteuttamista johtaa ohjelmaa/hanketta varten määrätty Naton hankkeen johtokunta/toimisto.	Prime Contract	The initial contract led by a NATO Project Management/Agency/Office for a Programme/project.
Ensisijainen hankeosapuoli	Jäsenvaltion teollinen, kaupallinen tai muu toimija, joka on tehnyt Naton hankkeen johtokunnan/toimiston kanssa sopimuksen palvelun suorittamisesta tai tuotteen	Prime Contractor	An industrial, commercial or other entity of a member nation which has contracted with a NATO Project Management Agency/Office to perform a service, or

	valmistamisesta Naton hankkeen yhteydessä ja joka voi puolestaan tehdä alihankintasopimuksia mahdollisten alihankkijoiden kanssa, jos tämä hyväksytään.		manufacture a product, in the framework of a NATO project, and which, in turn, may subcontract with potential subcontractors as approved.
Ohjelman tai hankkeen turvallisuusluokitusopas	Ohjelman (hankkeen) turvallisuusohjeiden osa, jossa määritellään ohjelman turvallisuusluokitellut osat ja ilmoitetaan kyseiset turvallisuusluokat. Turvallisuusluokitusopasta voidaan laajentaa ohjelman koko elinkaaren ajan, ja tietoa sisältäviä osia voidaan turvallisuusluokitella uudelleen tai niiden luokitusta voidaan alentaa.	Programme/Project Security Classification Guide	Part of the program (project) security instructions (PSI) which identifies the elements of the program that are classified, specifying the security classification levels. The security classification guide may be expanded throughout the program life cycle, and the elements of information may be re-classified or downgraded.
Ohjelman tai hankkeen turvallisuusohjeet (PSI)	Turvallisuusmääräysten/-menettelyjen kokoelma, joka perustuu niihin Naton turvallisuussääntöihin ja näitä tukeviin direktiiveihin, joita sovelletaan tiettyyn hankkeeseen/ohjelmaan turvallisuusmenettelyjen vakioimiseksi. Turvallisuusohjeet ovat myös yksi pääsopimuksen liitteistä ja niitä voidaan tarkistaa ohjelman koko elinkaaren ajan. Ohjelmassa tehtävien alihankintasopimusten turvallisuutta koskeva lisälauseke perustuu turvallisuusohjeisiin.	Programme/Project Security Instruction (PSI)	A compilation of security regulations/procedures, based upon NATO Security Policy and supporting directives, which are applied to a specific project/programme in order to standardise security procedures. The PSI also constitutes an Annex to the main contract, and may be revised throughout the programme lifecycle. For subcontracts let within the program, the PSI constitutes the basis for the SAL.
Kirjattu postilähetys	Postin palvelu, jonka avulla lähetyksen kulkua lähettäjältä vastaanottajalle voidaan seurata ja lähettäjälle todistetaan, että lähetys on toimitettu.	Registered Mail	A mail service that enables the possibility to track the shipment from the sender to the recipient and allows the sender a proof of the delivery.

Tiedon luovuttaminen	Tiedon vastaanottamisen salliminen vastaanottajana olevalle toimijalle siten, että tiedon katsotaan olevan koko toimijan käytettävissä. Luovuttamista voidaan edistää kyseistä toimijaa edustavan henkilön välityksellä.	Release of information	The act of authorizing a recipient entity to receive information with the understanding that this information will be available to the entire entity. The release may be facilitated through an individual representing the entity in question.
Riski	Todennäköisyys siihen, että uhka toteutuu haavoittuvuuden vuoksi, jolloin luottamuksellisuus, eheys ja/tai käytettävyys vaarantuvat ja syntyy vahinkoa.	Risk	The likelihood of a vulnerability being successfully exploited by a threat, leading to a compromise of confidentiality, integrity and/or availability and damage being sustained.
Riskienhallinta	Uhkien ja haavoittuvuuksien arviointiin perustuva järjestelmällinen lähestymistapa sen määrittämiseksi, mitä vastatoimia tarvitaan tietojen sekä niitä tukevien palvelujen ja resurssien turvallisuuden suojaamiseksi. Riskienhallintaan sisältyy niiden resurssien suunnittelu, järjestäminen, ohjaaminen ja valvonta, joiden avulla varmistetaan, että riski pysyy hyväksyttävyyden rajoissa.	Risk Management	A systematic approach to determining which security countermeasures are required to protect information and supporting services and resources, based upon an assessment of the threats and vulnerabilities. Risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds.
Riskin omistaja	Henkilö tai elin, jonka vastuulla on arvioida tiettyyn riskiin liittyvät uhat, haavoittuvuudet ja vaikutukset tarkoituksena määrittää asianmukainen riskinottohalu riskiä vähentävien tekijöiden toteutumisen perusteella.	Risk Owner	The individual or body that is charged with the responsibility of assessing the threats, vulnerabilities and impacts of any given risk with a view to establishing an appropriate risk appetite based upon the implementation of mitigating factors.

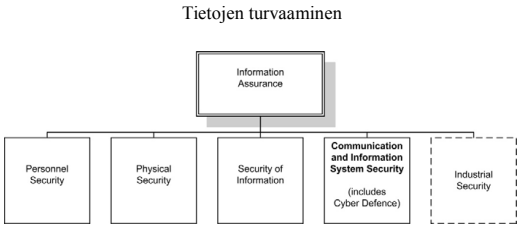
Turvallisuusnäkökohtia koskeva kirje (SAL)	Asiakirja, jonka toimivaltainen viranomainen antaa osana muuta Naton turvallisuusluokiteltua sopimusta tai alihankintasopimusta kuin merkittäviä ohjelmia/hankkeita koskevia sopimuksia ja jossa yksilöidään sovellettavat turvallisuusvaatimukset tai tietoturvallisuuden suojaamista edellyttävät sopimuksen osat.	Security Aspects Letter (SAL)	A document, issued by the appropriate authority, as part of any NATO classified contract or sub-contract, other than Major Programmes/Projects, identifying the security requirements or those elements thereof requiring security protection.
Turvallisuusvakuutus	Takeet, jotka annetaan Natolle joko suoraan tai Naton jäsenvaltion tai tietoa luovutettaessa takaajana toimivan Naton sotilas- tai siviilielimen välityksellä ja joiden mukaan muu kuin Natoon kuuluva Naton turvallisuusluokitellun tiedon vastaanottaja antaa tiedolle samantasoisen suojan kuin se suoja, jota Naton turvallisuusperiaatteet edellyttävät.	Security Assurance	A guarantee provided to NATO either directly or through a NATO Nation or NATO Civil or Military body sponsoring release, that a non- NATO recipient of NATO Classified Information will provide the same degree of protection to it as required by NATO Security Policy.
Tietoturvaloukkaus	Tahallinen tai tahaton teko tai laiminlyönti, joka on Naton turvallisuussääntöjen ja niitä tukevien direktiivien vastainen ja johtaa Naton turvallisuusluokitellun tiedon tai sitä tukevien palvelujen ja resurssien tosiasialliseen tai mahdolliseen vaarantumiseen (esimerkkejä: turvallisuusluokiteltu tieto katoaa kuljetuksen aikana; turvallisuusluokiteltua tietoa jätetään suojaamattomalle alueelle, jolle	Security Breach	An act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives, that results in the actual or possible compromise of NATO Classified Information or supporting services and resources (including, for example, classified information lost while being transported; classified information left in an unsecured area where uncleared individuals have

	turvallisuusselvittämättömillä henkilöillä on pääsy ilman saattajaa; tilivelvollisuuden alaista asiakirjaa ei löydetä; turvallisuusluokiteltua tietoa on muutettu ilman lupaa tai hävitetty luvattomalla tavalla; tai viestintä- tai tietojärjestelmien palvelu estyy).		unescorted access; an accountable document cannot be found; classified information has been subjected to unauthorised modification; destroyed in an unauthorised manner or, for CIS, there is a denial of service).
Turvallisuusluokituksen tarkistuslista	Turvallisuusnäkökohtia koskevan kirjeen (SAL) osa, jossa määritellään sopimuksen turvallisuusluokitellut osat ja ilmoitetaan kyseiset turvallisuusluokat. Ohjelmassa/hankkeessa tehtyjen sopimusten osien turvallisuusluokittelu perustuu kyseisen ohjelman/hankkeen turvallisuusohjeisiin.	Security Classification Check List	Part of a security aspect letter (SAL) which describes the elements of a contract that are classified, specifying the security classification levels. In case of contracts let within a program/project, such elements of information derive from the programme (project) security instructions issued for that programme.
Turva-avaimet	Turva-avaimet ovat avaimia, joita käytetään seuraavien lukoissa: turvallisuusluokitellun aineiston säilyttämiseen tarkoitetut turvakaapit; turvahuoneiden tai -vyöhykkeiden ovet; teknisesti turvallisuustarkastettujen turvahuoneiden tai -vyöhykkeiden ovet; ja turvallisuusluokiteltujen asiakirjojen jakeluun tarkoitetut turvakaapit.	Security Keys	Security keys are those which operate the locks fitted to: secure cabinets provided for the storage of classified material; doors of secure rooms or areas; doors of secure rooms or areas which have been subject to technical security inspections; and secure cabinets used for the circulation of classified documents.
Tietoturvapoikkeama	Tapahtuma tai muu tilanne, joka voi vaikuttaa haitallisesti Naton turvallisuusluokitellun tiedon turvallisuuteen ja edellyttää tutkintatoimia, jotta	Security Incident	An event or other occurrence that may have an adverse effect upon the security of NATO Classified Information which

	voidaan todeta tarkasti, onko kyseessä tietoturvaloukkaus vai vähäinen tietoturvapoikkeama.		requires further investigative actions in order to accurately determine whether or not it constitutes a Security Breach or Infraction.
Erityisluokan tieto	Tieto, johon sovelletaan ylimääräisiä käsittely-/suojaamismenettelyjä, kuten ATOMAL, yhteinen operaatiosuunnitelma (SIOP), BOHEMIA tai CRYPTO.	Special Category Information	Information such as ATOMAL, Single Integrated Operational Plan (SIOP), BOHEMIA or CRYPTO to which additional handling/protection procedures are applied.
Takaaja	Naton jäsenvaltio tai Naton sotilas- tai siviilielin, joka toimii takeiden antajana vakuuttamalla tarvittavalla tavalla, että Naton turvallisuusluokiteltua tietoa vastaanottava Naton ulkopuolinen toimija antaa tälle tiedolle tarvittavan suojan Naton turvallisuusperiaatteissa ja niitä tukevissa ohjeissa määriteltyjen perusperiaatteiden ja vaatimusten mukaisesti.	Sponsor	A NATO Nation or a NATO Civil or Military body acting as a guarantor in providing the necessary assurance that a NNE in receipt of NATO Classified Information will afford that information the necessary protection in line with the basic principles and requirements as set out in NATO Security Policy and supporting directives.
Alihankintasopimus	Sopimus, jonka ensisijainen hankeosapuoli tekee toisen hankeosapuolen (alihankkijan) kanssa tavaroiden tai palvelujen toimittamisesta.	Sub-contract	A contract entered into by a prime contractor with another contractor (i.e., the sub-contractor) for the furnishing of goods or services.
Alihankkija	Hankeosapuoli, jonka kanssa ensisijainen hankeosapuoli tekee alihankintasopimuksen.	Sub-contractor	A contractor to whom a prime contractor lets a sub-contract.
Uhka	Naton turvallisuusluokitellun tiedon tai sitä tukevien palvelujen ja resurssien vaarantumisen, ka-	Threat	The potential for compromise, loss or theft of NATO Classified Information or supporting services and resources. A

	toamisen tai varastamisen mahdollisuus. Uhka voidaan määritellä sen lähteen, motiivin tai tuloksen mukaan ja se voi olla tahallinen tai tahaton, väkivaltainen tai huomaamaton, ulkoinen tai sisäinen.		threat may be defined by its source, motivation or result, it may be deliberate or accidental, violent or surreptitious, external or internal.
Haavoittuvuus	Heikkous, ominaisuus tai valvonnan puute, joka mahdollistaisi Naton turvallisuusluokiteltuun tietoon tai sitä tukeviin palveluihin ja resursseihin kohdistuvan uhan toteutumisen tai helpottaisi sitä.	Vulnerability	A weakness, an attribute, or lack of control that would allow or facilitate a threat actuation against NATO Classified Information or supporting services and resources.

*Liite F, Kuva 1



Henkilöstöturvallisuus
Toimitilaturvallisuus
Tietoturvallisuus
Viestintä- ja tietojärjestelmien turvallisuus (ml. kyberpuolustus)
Yritysturvallisuus

Kuva 1 – Suhde tietojen turvaamisen ja viestintä- ja tietojärjestelmien turvallisuuden välillä

*Enclosure F, Picture 1

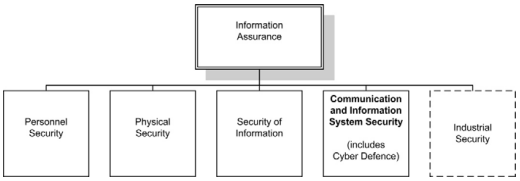


Figure 1 - Relationship between Information Assurance and CIS Security