

Frumvarp til laga

um breytingu á lögum nr. 82/2008, um almannavarnir o.fl. (efling netöryggissveitarinnar)

(Lagt fyrir Alþingi á 145. löggjafarþingi 2015–2016.)

1. gr.

Netöryggissveit ríkislögreglustjóra.

Á eftir 14. gr. laganna kemur nýr kafli, er nefnist: V. kafli a. Netöryggissveit ríkislögreglustjóra. Á eftir 14. grein laganna koma tvær nýjar greinar, 14. gr. a, og 14. gr. b, sem orðast svo ásamt fyrirsögnum:

Netöryggissveit ríkislögreglustjóra.

Ríkislögreglustjóri starfrækir netöryggissveit, sem gegna skal hlutverki öryggis- og viðbragðshóps til verndar mikilvægum samfélagslegum innviðum gegn netárásum. Netöryggissveitin skal sinna sólarhrings viðbragðsvöktum og vinna að því að fyrirbyggja, draga úr og bregðast við hættu vegna netárása eða hliðstæðra öryggisatvika í net- og upplýsingakerfum mikilvægra samfélagslegra innviða sem falla undir starfssvið sveitarinnar samkvæmt reglugerð.

Upplýsingakerfi mikilvægra samfélagslegra innviða er sá tækja- og hugbúnaður sem nauðsynlegur er til reksturs og virkni kerfisins og þær upplýsingar sem þar eru hýstar eða um kerfið fara. Til mikilvægra samfélagslegra innviða teljast meðal annars mannvirki eða kerfi, sem tryggja eiga þjóðaröryggi, almannaheill og margs konar öflun aðfanga í þróuðu og tæknivæddu þjóðfélagi, eða hlutar þess, sem er þannig háttáð, að eyðing þeirra, skemmdir eða skert starfsemi mundi stefna í hættu nauðsynlegri samfélagslegri starfsemi, heilbrigði, öryggi, umhverfi og efnahagslegri eða félagslegri velferð borgaranna.

Rekstraraðilar mikilvægra samfélagslegra innviða eru fyrirtæki, ríkisstofnanir eða tiltekin stjórnvöld sem eiga eða bera ábyrgð á rekstri mikilvægra samfélagslegra innviða.

Ríkislögreglustjóri skilgreinir nánar mikilvæga samfélagslega innviði og upplýsingakerfi þeirra, sem og þann hóp rekstraraðila mikilvægra samfélagslegra innviða sem netöryggissveit ber að sinna.

Netöryggissveit ríkislögreglustjóra skal gegna hlutverki CERT-teymis fyrir Ísland og skal hún taka þátt í og gegna hlutverki tengiliðar íslenskra stjórnvalda í innlendu og alþjóðlegu samstarfi um viðbragðsvarnir og aðgerðir vegna net- og upplýsingaöryggis.

Ríkislögreglustjóri getur gefið fyrirmæli um lágmarks öryggisráðstafanir rekstraraðila samfélagslega mikilvægra innviða. Skulu þeir aðilar verða við fyrirmælum ríkislögreglustjóra án tafar. Vanræki viðkomandi aðili að framkvæma fyrirmæli um öryggisráðstafanir getur ríkislögreglustjóri látið vinna verkið á kostnað viðkomandi. Krafa um kostnað vegna þessa er aðfararhæf skv. 5. tölul. 1. mgr. 1. gr. laga nr. 90/1989, um aðför.

Netöryggissveitin skal leitast við að greina öryggisatvik á frumstigi og fyrirbyggja að þau breiðist út og valdi tjóni á mikilvægum samfélagslegum innviðum. Skal netöryggissveitin aðstoða við forvarnir, veita leiðbeiningar og styðja við skjót viðbrögð gegn aðsteðjandi hættu. Við útbreitt öryggisatvik samhæfir netöryggissveitin aðgerðir gegn aðsteðjandi hættu til að lágmarka tjón og reisa við óvirk kerfi. Netöryggissveitin veitir ráðgjöf um varnir og viðbúnað og kemur upplýsingum á framfæri við almenning ef þurfa þykir.

Netöryggissveitinni er heimilt að óska eftir nafnlausum rauntímagögnum frá fjarskiptafyrirtækjum um magn umferðar á Netinu, þ.m.t. í samtengipunktum milli fjarskiptafyrirtækjanna og í útlandagáttum. Ef grunur er um að stórfelld netárás sé yfirvofandi eða yfirstandandi er netöryggissveitinni heimilt að skima stýrigögn fjarskiptapakka sem tengjast mögulegum öryggisögnum með tilliti til nánari upplýsinga um uppruna, áfangastað og tæknilega eiginleika. Eingöngu má nota gögn sem þannig er aflað í þeim tilgangi að koma í veg fyrir eða draga úr tjóni vegna öryggisatvika. Óheimilt er að persónugreina upplýsingar sem aflað er samkvæmt þessari grein og skal þeim eytt eins fljótt og auðið er og eigi síðar en sex mánuðum frá því að þeirra var aflað.

Rekstraraðilum mikilvægra samfélagslegra innviða er skylt, netöryggissveitinni að kostnaðarlausu, að hýsa og samtengjast vöktunarbúnaði netöryggissveitarinnar og afhenda umsvifalaust þau gögn sem sveitin krefst. Sé rökstuddur grunur um að einstakar sendingar innihaldi spillikóða er netöryggissveitinni heimilt, með samþykki rekstraraðila einstakra mikilvægra samfélagslegra innviða, að greina efni einstakra fjarskiptasendinga til og frá viðkomandi neti. Tilkynna skal sendanda og móttakanda sendingarinnar ef innihald sendingar skal skoðað og gefa þeim tækifæri á því að vera viðstaddir skoðunina verði því við komið. Framangreind heimild tekur þó ekki til skoðunar sendingar í almennum fjarskiptanetum fjarskiptafyrirtækja. Netöryggissveitin skal starfa í samræmi við skilyrði sem Persónuvernd kann að setja.

Samráðshópur netöryggissveitar

Ríkislögreglustjóri skipar *Samráðshóp netöryggissveitarinnar* í þeim tilgangi að efla tengsl og samstarf á milli rekstraraðila mikilvægra samfélagsinnviða og netöryggissveitarinnar. *Samráðshópur netöryggissveitar* skal vera vettvangur tæknilegs samráðs og upplýsingaskipta á sviði netöryggis, m.a. til greiningar ógna og samræmingar viðbragða. Um þær öryggisupplýsingar sem ræddar eru á fundum skal ríkja trúnaður.

Hópurinn er skipaður að fengnum tilnefningum þeirra hópa rekstraraðila mikilvægra samfélagslegra innviða sem tilgreindir eru í 32. gr. a og sem greiða netöryggisgjald í ríkissjóð, skv. 3. mgr. 32. gr. laganna, auk fulltrúa skipuðum af ríkislögreglustjóra án tilnefningar sem veitir hópnum forustu, fulltrúa tilnefndum af Póst- og fjarskiptastofnun og eftir atvikum fulltrúum tilnefndum af öðrum aðilum, enda telji ríkislögreglustjóri það nauðsynlegt svo markmiðum samráðsins verði náð.

2. gr.

Á eftir 32. gr. laganna kemur ný grein, 32. gr. a, ásamt fyrirsögn, svohljóðandi:

Álagning netöryggisgjalds.

Rekstraraðilar mikilvægra samfélagslegra innviða skulu greiða sérstakt gjald, netöryggisgjald, í ríkissjóð vegna starfsemi netöryggissveitar ríkislögreglustjóra, sbr. 14. gr. a.

Eftirtaldir aðilar eru gjaldskyldir samkvæmt lögum þessum og skulu greiða gjald sem hér segir:

- a. Skráð fjarskiptafyrirtæki sem hafa tilkynnt Póst- og fjarskiptastofnun að þau muni starfa á grundvelli almennrar heimildar skv. 3. mgr. 4. gr. laga nr. 81/2003, um fjarskipti, skulu greiða 0,05% af bókfærðri veltu vegna fjarskiptastarfsemi. Með bókfærðri veltu er átt við rekstrartekjur sem fjarskiptafyrirtæki hefur af umræddri starfsemi hér á landi.
- b. Raforkuver, hitaveitur, dreifiveitur, flutningsfyrirtæki, vatns- og fráveitur sem eru leyfisskyldar samkvæmt raforkulögum, nr. 65/2003, orkulögum, nr. 58/1967, lögum um vatnsveitur sveitarfélaga, nr. 32/2004, og lögum nr. 9/2009, um uppbyggingu og rekstur fráveitna, skulu greiða 0,05% af bókfærðri veltu raforku- og veitustarfsemi. Með bókfærðri veltu er átt við rekstrartekjur sem raforku- og veitustarfsemi hefur af umræddri starfsemi hér á landi.
- c. Þeir aðilar sem fengið hafa starfsleyfi sem
 1. fjármálafyrirtæki á grundvelli 4. gr., sbr. 6. gr. laga nr. 161/2002, um fjármálafyrirtæki,
 2. rafeyrisfyrirtæki á grundvelli 15. gr. laga nr. 17/2013, um rafeyrisfyrirtæki, og,
 3. greiðslustofnun á grundvelli 13. gr. laga nr. 120/2011, um greiðsluþjónustu, skulu greiða 0,2% af gjaldstofni skv. 4. og 5. gr. laga nr. 165/2011, um fjársýsluskatt. Þó skulu þeir aðilar sem falla undir fyrsta og annan lið einungis greiða netöryggisgjald ef heildareignir þeirra eru umfram 20 milljarða króna í lok tekjuárs.
- d. Félög og fyrirtæki sem starfa samkvæmt lögum nr. 110/2007, um kauphallir, skulu greiða 0,2% af gjaldstofni skv. 4. og 5. gr. laga nr. 165/2011, um fjársýsluskatt.
- e. Rekstraraðilar flugleiðsöguþjónustu sem hlotið hafa starfsleyfi, sbr. 57. gr. a loftferðalaga, nr. 60/1998, skulu greiða 0,05% af bókfærðri veltu flugleiðsöguþjónustu og rekstrarstjórnun flugumferðar. Með bókfærðri veltu er átt við rekstrartekjur sem flugleiðsöguþjónusta og rekstrarstjórnun flugumferðar hefur af umræddri starfsemi hér á landi.

Um álagningu og innheimtu netöryggisgjalds fer samkvæmt ákvæðum VIII.–XIV. kafla laga nr. 90/2003, um tekjuskatt, en varðandi viðurlög er sérstaklega vísað til XII. kafla þeirra laga.

3. gr.

Við 34. gr. laganna bætist ný málsgrein er verður 5. málsgrein og orðast svo:

Ráðherra setur, að fenginni umsögn frá ríkislögreglustjóra, Póst- og fjarskiptastofnun og Persónuvernd, nánari fyriræli um starfsemi netöryggissveitarinnar í reglugerð, sem skal m.a. fjalla um:

- a. hlutverk, skipulag, starfssvið og verkefni netöryggissveitarinnar,
- b. samræmingu á samstarfi þeirra rekstraraðila sem netöryggissveitin sinnir og miðlun upplýsinga á milli þeirra,
- c. skipun og hæfi starfsmanna netöryggissveitarinnar, þ.m.t. um öryggisvottun starfsmanna,
- d. miðlun upplýsinga til innlendra og erlendra samstarfsaðila og viðeigandi öryggisráðstafanir þar að lútandi,
- e. framkvæmd eftirlits um vélræna skimun fjarskiptaumferðar,
- f. verklag við skoðun efnis fjarskiptasendinga með samþykki ábyrgðaraðila,
- g. ráðstafanir til að tryggja öryggi og eyðingu gagna og aðrar ráðstafanir til að tryggja friðhelgi einkalífs,

- h. tilkynningarskyldu rekstraraðila mikilvægra samfélagslegra innviða og annarra hagsmunaaðila um öryggisatvik,
- i. prófanir og úttektir á net- og upplýsingaöryggi og viðnámsþrótti upplýsingakerfa sem netöryggissveitin getur ráðist í,
- j. skýrslugjöf um starfsemi netöryggissveitarinnar.

4. gr.

Lög þessi öðlast gildi 1. janúar 2016.

5. gr.

Við gildistöku laga þessara verða eftirfarandi breytingar á öðrum lögum:

1. *Lögreglulög nr. 90/1996*, með síðari breytingum: Við 2. mgr. 5. gr. laganna bætist nýr stafliður er orðast svo: að starfrækja netöryggissveit sem vinnur að því að fyrirbyggja, draga úr og bregðast við hættu vegna netárása eða hliðstæðra öryggisatvika í net- og upplýsingakerfum.
2. *Lög nr. 81/2003, um fjarskipti*, með síðari breytingum:
 - a. 23., 24., og 37. tölul. 3. gr. laganna falla brott.
 - b. 47. gr. a í lögnum fellur brott.
3. *Lög um Póst- og fjarskiptastofnun*, nr. 69/2003, með síðari breytingum:
 - a. Í stað „0,38%“ í 1. másl. 4. mgr. 14. gr. laganna kemur: 0,30%.

Ákvæði til bráðabirgða.

- I. Í kjölfar samþykktar laganna skal starfsmönnum netöryggissveitar Póst- og fjarskiptastofnunar boðið starf hjá ríkislögreglustjóra og skulu þeir þá njóta sambærilegra kjara og þeir njóta hjá Póst- og fjarskiptastofnun. Ákvæði 7. gr. laga nr. 70/1996 um réttindi og skyldur starfsmanna ríkisins gilda ekki um störf sem er ráðið í samkvæmt þessari málsgrein. Enn fremur skal sérhæfður hugbúnaður og tölvu- og tækjabúnaður flytjast með netöryggissveitinni til ríkislögreglustjóra.
- II. Þrátt fyrir gildistökuákvæði 4. gr. laganna leggur Póst- og fjarskiptastofnun á óbreytt rekstrargjald árið 2016 vegna rekstrarársins 2015 og netöryggisgjald samkvæmt 2. gr. laganna skal lagt á árið 2017 fyrir rekstrarárið 2016.

Athugasemdir við lagafrumvarp þetta.

I. Inngangur.

Frumvarp þetta til laga um breytingu á lögum um almannavarnir o.fl. (efling netöryggissveitar) er samið í innanríkisráðuneytinu í samráði við ríkislögreglustjóra og Póst- og fjarskiptastofnun. Megintilgangur frumvarpsins er að efla starfsemi netöryggissveitarinnar og getu hennar til samstarfs við rekstraraðila mikilvægra innviða samfélagsins. Eitt lykilatriði í því er flutningur starfsemi netöryggissveitar frá Póst- og fjarskiptastofnun til ríkislögreglustjóra. Við samningu frumvarpsins var m.a. byggt á skýrslu netöryggissveitar Póst- og fjarskiptastofnunar frá 27. mars 2014 um netárásina á Fjarskipti hf. (Vodafone) þann 30. nóvember 2013, þar sem m.a. kemur fram hvaða lærdóm megi draga af því atviki varðandi varnir og viðbrögð við netárásum. Jafnframt var byggt á minnisblaði Páls Ásgrímssonar hdl., til innanríkisráðuneytisins, dagsett 28. febrúar 2014. Minnisblaðið var tekið saman að ósk innanríkisráðherra í tilefni netárásarinnar og var tilgangur úttektar að greina heildstætt stöðu netöryggis á Íslandi og koma með tillögur til úrbóta.

Á 143. löggjafarþingi, 2013-2014, var lagt fram frumvarp sem einnig miðaði að því að flytja netöryggissveit frá Póst- og fjarskiptastofnun til almannavarnadeildar ríkislögreglustjóra (þingskjal nr. 881). Markmið með því var að það væri unnt strax að hefja undirbúning að flutningi sveitarinnar og að hann gæti komið til framkvæmda á haustmánuðum 2014. Frumvarpið náði ekki fram að ganga. Það frumvarp sem nú er lagt fram er að því leyti frábrugðið hinu fyrra að hér er miðað við varanlega breytingu á rekstrargrunni sveitarinnar, en ekki var unnt að útfæra slíka breytingu á miðju starfsári og jafnframt er hér ekki tiltekið hvar sveitin skuli staðsett innan embættis ríkislögreglustjóra.

II. Tilefni og nauðsyn lagasetningar.

Í *Stefnu í almannavarna- og öryggismálum ríkisins 2015 – 2017*, sem samþykkt var af almannavarna og öryggismálaráði, 24. júní 2015, er lögð áhersla á að stuðlað verði að vernd mikilvægra samfélagsinnviða með áhættumati, mótvægisáðgerðum og viðbragðsáætlunum, þar á meðal á sviði net- og upplýsingaöryggis og gegnir rekstur netöryggissveitar þar lykilhlutverki. Öflug netöryggissveit gegnir einnig lykilhlutverki í *Stefnu um net- og upplýsingaöryggi*, sem innanríkisráðherra kynnti í ríkisstjórn 28. apríl 2015 og síðar með skýrslu til Alþingis. Í áhættuskoðun almannavarnadeildar ríkislögreglustjóra frá árinu 2011, kemur fram að á undanförunum áratugum hafi verið lögð áhersla á uppbyggingu helstu innviða í gegnum flókin tölvukerfi. Við áhættuskoðunina var niðurstaða sú að heildstætt mat á landsvísu yrði að fara fram á mikilvægum innviðum, s.s. fjarskipta og raforku, þar sem um landskerfi er að ræða og kerfin hvort öðru háð.

Interpol og Europol hafa bent á ört vaxandi ógn vegna misnotkunar á net- og upplýsingatækni, ekki síst af hálfu þeirra sem stunda skipulagða glæpastarfsemi. Upplýsingum um veitur í kerfum er dreift ört og ganga jafnvel kaupum og solum. Árásartöl sem nýta þessa veikleika eru auðfánleg á svörtum markaði og glæpasamtök sem vinna þvert á lögsögu ríkja þurfa ekki lengur að búa sjálf yfir sérþekkingu á þessu sviði. Mjög brýnt er að gera ríkari kröfur um öryggisvarnir samfélagslegra mikilvægra stofnana og fyrirtækja og að mögulegt sé að grípa til skjótra og samhæfðra viðbragða. Gera verður mun ríkari kröfur um að slíkir aðilar uppfylli lágmarksskilyrði varðandi öryggisráðstafanir og að skilgreina

ábyrgð forstöðumanna á því að öryggismál séu fullnægjandi. Mikilvægt er að fram fari könnun á veikleikum og áfallaþoli mikilvægra samfélagslegra innviða samfélagsins þ.m.t. net- og upplýsingakerfa. Auðkennd verði þau net- og upplýsingakerfi er varða þjóðaröryggi. Þau verði greind með tilliti til áhættu og veikleika og öryggi þeirra samhæft. Þeir sem ábyrgð bera á hverju kerfi verði skyldaðir til þess að tryggja öryggi þess. Sérstaklega þarf að huga að því hvernig tryggja má öryggi á sviðum sem reiða sig mjög á fjarskipti. Má þar nefna æðstu stjórn ríkisins, öryggisstofnanir, fjármálafyrirtæki, orkufyrirtæki og ýmsa þætti stjórnáslu.

Netöryggissveitin (CERT-ÍS) hóf formlega störf á grunni reglugerðar nr. 475/2013 um málefni CERT-ÍS netöryggissveitar sem öðlaðist gildi þann 1. júní 2013 og hefur aðsetur innan Póst- og fjarskiptastofnunar sem vann ötullega að því að koma sveitinni á stofn og að uppbyggingu hennar. Upphaf starfsemi sveitarinnar má rekja til fyrri hluta árs 2011. Markmiðið með starfsemi netöryggissveitarinnar er að fyrirbyggja og draga úr hættu á netarásum og öðrum öryggisatvikum í mikilvægum samfélagslegum innviðum og sporna við og lágmarka tjón af þeim sökum. Þá greinir sveitin og metur öryggisatvik, leiðbeinir og/eða leiðir viðbrögð við öryggisatvikum og er samhæfingaraðili þegar um stærri atvik er að ræða. Sveitin er jafnframt tengiliður íslenskra stjórnvalda í alþjóðlegu samstarfi CERT-netöryggissveita um viðbrögð og varnir vegna net- og upplýsingaöryggis.

Á fundi með fjölda hagsmunaaðila, fyrirtækja og opinberra aðila þann 2. júní 2014 um stefnumótun varðandi net- og upplýsingaöryggi kom fram að auknar væntingar eru gerðar til starfsemi netöryggissveitarinnar. Flutningur sveitarinnar er fyrsta skrefið í áætluðum breytingum til að efla sveitina þannig að hún geti betur brugðist við þörfum og væntingum þjóðfélagsins og að starfsemin uppfylli alþjóðlegar kröfur, t.d. þær sem munu verða í væntanlegri tilskipun Evrópusambandsins um net- og upplýsingaöryggi. Á fundum með fulltrúum sveitarinnar og ríkislögreglustjóra hefur komið fram að koma þurfi upp viðvörunarnemum í netkerfum til að geta greint og brugðist við alvarlegum netarásum. Í tengslum við framangreinda stefnumótun er unnið að nánari greiningu á þörfum, skipulagningu og kostnaði vegna þessa og annarra þátta og mun tillaga um útfærslu verða lögð fram að greiningu lokinni. Útfærslan mun fela í sér kostnað vegna kaupa á sérstökum tækjabúnaði.

Innanríkisráðuneytið telur að út frá eðli starfsemi netöryggissveitar, sem aðallega er fólgið í því að veita ráðgjöf, leiðbeina og samræma aðgerðir í tengslum við öryggisatvik, geti verið óæskilegt að hún sé á hendi stofnunar sem jafnframt fer með eftirlits- og úrskurðarvald um hugsanleg brot á fjarskiptalögum um öryggi og heildstæði neta. Getur sú staða, að mati ráðuneytisins, valdið ákveðnum hagsmunaaðrekstri sem leitt getur til þess að rekstraraðilar mikilvægra samfélagslegra innviða, einkum fjarskiptafyrirtæki, geti verið tregari til nauðsynlegrar upplýsingagjafar um eðli og umfang öryggisatvika og um það fyrirkomulag öryggis og viðbúnaðar sem fyrir hendi var á þeim tíma. Með því að færa netöryggissveitina til ríkislögreglustjóra er verið að bregðast við þessu mögulega vandamáli. Að auki mun viðbragðsvöktun vegna netarása jafnframt eflast með því að tengjast sólarhringsvakt ríkislögreglustjóra auk þess að njóta góðs af þekkingu og reynslu embættisins við að semja og útfæra viðbragðsáætlanir og við að bregðast við alvarlegum áföllum í samfélaginu.

Markmið frumvarpsins er jafnframt að útvíkka starfsemi netöryggissveitarinnar þannig að hún nái til net- og upplýsingaöryggis stjórnvalda en slíkar sveitir eru oft nefndar „govCERT“ á alþjóðlegum vettvangi. Telur ráðuneytið að sú útvíkkun á starfsemi netöryggissveitarinnar fari ekki endilega vel saman við eftirlitshlutverk PFS við að framfylgja fjarskiptaregluverkinu. Starfræksla CERT-ÍS hjá ríkislögreglustjóra gefur betri

möguleika á að samhæfa skipulagningu viðbúnaðar og viðbragða vegna öryggisatvika sem snerta net- og upplýsingakerfi, atvika sem kunna að hafa áhrif langt utan þeirra kerfa sem sveitinni var upphaflega ætlað að fylgjast með. Þetta er sérstaklega mikilvægt hvað snertir mikilvæga samfélagslega innviði þjóðfélagsins, en þar geta mótvægisáðgerðir þurft að taka til fjölbreyttra þátta. Varnir mikilvægra samfélagslegra upplýsingainnviða voru ein af grunnástæðum þess að netöryggisveitin CERT-ÍS var stofnuð. Rétt er að taka fram að fyrirkomulag þetta fellur nær fyrirkomulagi þessara mála erlendis. Með breytingunni á starfsumhverfi CERT-ÍS er einnig ætlunin að skapa grunn sem nýta má til frekari þróunar og samþættingar starfsemi á sviði net- og upplýsingaöryggis og að gera sveitinni mögulegt að byggja upp varnir upplýsingakerfa mikilvægra samfélagslegra innviða samfélagsins.

III. Meginefni frumvarpsins.

Frumvarpið miðar að því að treysta net og upplýsingaöryggi hér á landi og styrkja og auka starfsemi netöryggisveitarinnar, CERT-ÍS. Sveitin verði flutt til ríkislögreglustjóra og starfsviðið víkkað þannig að það nái til helstu mikilvægra innviða samfélagsins. Jafnframt verði komið á formlegu samstarfi við rekstraraðila þessara samfélagsinnviða. Með frumvarpinu er þannig opnað fyrir að netöryggisveitin geti verið í daglegu og nánu samstarfi við aðra grunnþætti almannavarna landsins. Í frumvarpinu er ákvæði um að bjóða skuli starfsmönnum netöryggisveitar starf hjá ríkislögreglustjóra og þeir eigi þar að njóta sambærilegra kjara og þeir nutu fyrir hjá Póst- og fjarskiptastofnun.

IV. Samráð.

Í aðdraganda frumvarpsins var efni þess kynnt eftirfarandi aðilum: Embætti ríkislögreglustjóra, Póst- og fjarskiptastofnun og starfsmönnum netöryggisveitar Póst- og fjarskiptastofnunar. Jafnframt var haft samráð við framangreinda aðila við samningu frumvarpsins. Auk þess var tekið tillit til sjónarmiða sem fram komu á fundi innanríkisráðuneytisins með fjölda hagsmunaaðila í Safnahúsinu við Hverfisgötu þann 2. júní 2014 í tengslum við stefnumótun um net- og upplýsingaöryggi og þeirra umsagna sem bárust við fyrra frumvarp. Þá var haft samráð við fulltrúa úr þeim hópi rekstraraðila mikilvægra samfélagslegra innviða sem mun verða gert að greiða netöryggisgjald skv. 2. gr. frumvarpsins.

V. Mat á áhrifum.

Með flutningi netöryggisveitarinnar til embættis ríkislögreglustjóra fæst samlegð með verkferlum embættisins, þ.m.t. almannavarnadeildar, sem nýtist vel til að skipuleggja viðbragðsgetu allan sólarhringinn alla daga ársins ásamt því að nýtast þegar glímt er við hugsanlegar víðtækar afleiðingar alvarlegra netatvika. Jafnframt mun sveitin eiga mun auðveldara að nýta sér trúnaðarupplýsingar varðandi netógnir sem einungis er dreift á milli löggæsluadila. Með *Samráðshópi netöryggisveitar* verður hægt að byggja upp mun nánari samvinnu við rekstraraðila mikilvægra samfélagsinnviða en unnt hefur verið til þessa og með fyrirhuguðum tölvubúnaði verður unnt að greina netógnir mun fyrir en ella og gera aðilum mögulegt að grípa til fyrirbyggjandi ráðstafana.

Athugasemdir við einstakar greinar frumvarpsins.

Um 1. gr.

Greinin er að mestu efnislega samhljóða 47. gr. a. laga nr. 81/2003 um fjarskipti, sbr. 8. gr. laga nr. 62/2012, að öðru leyti en því að starfsemi sveitarinnar er flutt frá Póst- og fjarskiptastofnun til ríkislögreglustjóra, umfangi starfseminnar er breytt frá því að snúa einkum að upplýsingakerfum fjarskiptafyrirtækja til þess að ná einnig til mikilvægra samfélagslegra innviða og sérstakur samráðshópur netöryggisveitar verður stofnaður.

Mikilvægir samfélagslegir innviðir eru t.d. *mannvirki, kerfi eða hlutar þess sem er þannig háttáð, að eyðing þeirra, skemmdir eða skert starfsemi myndi stefna í hættu lífsnauðsynlegri samfélagslegri starfsemi, heilbrigði, öryggi, umhverfi, efnahagslegri eða félagslegri velferð borgaranna*. Markmið með starfsemi netöryggissveitarinnar er skilgreint með sambærilegum hætti og í gildandi lögum, nema hvað hér er fjallað um netárásir og *hliðstæð öryggisatvik* í stað þess að vísa í *önnur öryggisatvik* eins og gert er í gildandi lögum. Við upphaf netöryggisatviks þarf ekki að vera ljóst hvort rótin sé árás, tæknileg bilun eða eitthvað annað. Það er því mikilvægt að umboð til viðbragða sé ekki bundið við að sú greining liggi fyrir að um árás sé að ræða. Aðgerðir sveitarinnar til að fyrirbyggja, draga úr og bregðast við hættu vegna netárása nýtast einnig vegna atvika sem geta haft aðrar rætur en svipaðar afleiðingar. Hins vegar þótti rétt að þrengja tilvísun og vísa því í *hliðstæð öryggisatvik* í stað þess að vísa í *önnur öryggisatvik*. Með þessu er verið að gera ljóst að ekki sé átt við öryggisatvik almennt heldur þau sem geta haft svipaðar afleiðingar og netárás og krafist svipaðra viðbragða og forvarna.

Í greininni er tekið fram að rekstraraðilum mikilvægra samfélagslegra innviða er skylt, netöryggissveitinni að kostnaðarlausu, að hýsa og samtengjast vöktunarbúnaði netöryggissveitarinnar og afhenda umsvifalaust þau gögn sem sveitin krefst. Þetta er hliðstætt ákvæði í 47. gr. a. laga nr. 81/2003 þar sem tiltekið er að fjarskiptafyrirtækjum er skylt að hýsa og samtengjast eftirlitsbúnaði netöryggissveitarinnar endurgjaldslaut. Í þingskjali 438 á 140. lögjafarþingi 2011 – 2012 kemur fram í skýringum við 8. gr. að *ekki er fyrir séð að fjöldi eftirlitsbúnaðar verði mikill eða hann fyrirferðarmikill. Þar sem starfræksla búnaðarins er í þágu þess að efla öryggi og heildstæði ómissandi upplýsingainnviða þykja ekki vera forsendur til þess að fjarskiptafyrirtækin eða aðrir í notendahópi CERT-IS innheimti kostnað eða gjöld fyrir að hýsa og samtengjast búnaðinum*.

Í 6. mgr. greinarinnar er lagt til að ríkislögreglustjóra verði veitt heimild til þess að gefa fyrirmæli um lágmarks öryggisráðstafanir rekstraraðila samfélagslegra mikilvægra innviða. Skulu þeir aðilar verða við fyrirmælum ríkislögreglustjóra án tafar. Ekki er gert ráð fyrir því að um reglubundið eftirlit og tilmæli sé að ræða heldur er gert ráð fyrir því að ríkislögreglustjóri geti gripið inn í þegar upp koma eða hætta er talin á að öryggisatvikum. Eins er gert ráð fyrir því að ríkislögreglustjóri geti gefið fyrirmæli ef viðkomandi rekstraraðilar/stofnanir eru að mati ríkislögreglustjóra ekki að gera fullnægjandi öryggisráðstafanir og hann telur að hætta kunni að skapast ef ekkert verður að gert, þó hætta sé ekki talin yfirvofandi. Ákvæði um viðbrögð við vanrækslu er hliðstætt ákvæði í 64. gr. laga nr. 81/2003 um fjarskipti þegar vanrækt er að bregðast við fyrirmælum Póst- og fjarskiptastofnunar vegna skaðlegrar truflunar á rekstri fjarskiptavirkis.

Í greininni kemur fram að ríkislögreglustjóri skipi, í kjölfar tilnefninga rekstraraðila mikilvægra samfélagsinnviða, samráðshóp netöryggisveitar. Þar segir jafnframt að hópurinn skuli vera vettvangur tæknilegs samráðs og upplýsingaskipta á sviði netöryggis, m.a. til greiningar ógna og samhæfingar viðbragða. Markmið með starfi þessa samráðshóps er að

efla tengsl og samstarf á milli rekstraraðila mikilvægra samfélagsinnviða og netöryggisveitarinnar. Getur hvoru tveggja verið um að ræða reglubundna fundi eða upplýsingaskipti vegna einstakra öryggisatvika. Upplýsingaskipti á grundvelli þessarar greinar teljast ekki til samráðs sem fellur undir ólögmett samráð samkvæmt samkeppnislöggjöf, enda er hér eingöngu um að ræða upplýsingaskipti sem felur í sér tæknilegt samráð sem er ætlað að byggja upp forvarnir á sviði netöryggis með almannahagsmuni að leiðarljósi. Ekki er um samstarf að ræða sem felur í sér höft eða röskun á samkeppni og er því ekki til þess fallið að draga úr virkri samkeppni. Þvert á móti er um sérstakar ráðstafanir að ræða í þágu netöryggis sem beinast fyrst og fremst að samfélagslega mikilvægum innviðum.

Í grein þessari er byggt á orðskýringum 3. gr. laga nr. 81/2003 um fjarskipti og eftirtöldum orðskýringum sem eru efnislega samhljóða framangreindri grein, sbr. 2. gr. laga nr. 62/2012.

- a. Öryggisatburður: Það að upp kemur staða kerfis, þjónustu eða nets sem gefur til kynna hugsanlegt brot gegn öryggisstefnu eða bilun í öryggisráðstöfun eða áður óþekkt staða sem getur skipt máli fyrir öryggi.
- b. Öryggisatvik: Atvik sem er gefið til kynna með einum eða fleiri óæskilegum eða óvæntum öryggisatburðum sem talsverðar líkur eru á að stofni rekstrarþáttum í hættu og ógni upplýsingaöryggi.
- c. Nafnlaus rauntímagögn: Tölulegar upplýsingar og kóðar sem bjóða upp á rekjanleika fjarskiptaumferðar í IP-fjarskiptanetum.

Um 2. gr.

Í greininni er fjallað um svokallað netöryggisgjald. Fjáröflun sú sem frumvarp þetta gerir ráð fyrir felst í álagningu netöryggisgjalds, sem samsvarar áætluðum kostnaði ríkissjóðs af starfsemi og uppbyggingu netöryggisveitar ríkislögreglustjóra. Með hliðsjón af auknu hlutverki sveitarinnar er gert ráð fyrir því að netöryggisgjaldið verði lagt á rekstraraðila mikilvægra samfélagslegra innviða. Áætlað er að netöryggisgjaldið geti skilað samtals um 180 milljónum króna árlega. Gera má ráð fyrir að útvíkkað starfssvið, sólarhrings viðbragðsviðbúnaður vegna net- og upplýsingaöryggis, ásamt nýjum nauðsynlegum tækjakosti og viðeigandi sérfræðipjálfunar starfsmanna, m.a. með þátttöku í erlendu samstarfi, feli í sér mun meiri kostnað en nú er. Við breikkun gjaldstofns var tekið mið af fyrirhugaðri útvíkkun starfssviðs netöryggisveitarinnar og að tilgreindir rekstraraðilar mikilvægra samfélagslegra innviða, þ.m.t. fjarskiptafyrirtæki, raforkuver, hitaveitur og dreifiveitur, fjármálafyrirtæki og rekstraraðilar flugleiðsöguþjónustu greiði netöryggisgjald sem renni í ríkissjóð. Gjald til þess að mæta þessum kostnaði dreifist, samkvæmt frumvarpi þessu, á fleiri rekstraraðila mikilvægra samfélagslegra innviða en eingöngu fjarskiptafyrirtæki. Núverandi starfsemi netöryggisveitarinnar er fjármögnuð með mörkuðum tekjustofnum Póst- og fjarskiptastofnunar, sbr. 14. gr. laga nr. 69/2003 um Póst- og fjarskiptastofnun, sbr. lög nr. 62/2012 til breytingar á þeim. Umrædd gjöld samkvæmt þessu frumvarpi fela ekki í sér markaðar tekjur, heldur er um að ræða skatt sem rennur í ríkissjóð. Þetta er veltutengdur skattur sem leggst á bókfærða veltu þessara aðila á liðnu ári og hvað fjármálafyrirtæki snertir er hér um skatt sambærilegan fjársýsluskatti að ræða og á sama skattstofn.

Samkvæmt ákvæði til bráðabirgða í þessu frumvarpi kemur álagning samkvæmt 2. grein fyrst til framkvæmda árið 2017 vegna rekstrarársins 2016. Áætlað er að gjald í ríkissjóð miðað við rekstrarárið 2014 hefði numið um 180 milljónum króna, miðað við þá

álagningarleið sem lögð er til í frumvarpinu. Í frumvarpi þessu er miðað við að fjárframlag til reksturs netöryggissveitarinnar hækki, sbr. athugasemd að framan um mat á áhrifum og athugasemd við 3. gr.

Um 3. gr.

Í þessu ákvæði er að finna reglugerðarheimild fyrir ráðherra sem fer með málefni almannavarna að gefa út reglugerð um starfsemi netöryggissveitar ríkislögreglustjóra. Efnistöðum reglugerðarinnar, sbr. þá töluliði sem taldir eru upp í ákvæðinu, er ætlað að skapa skýrari ramma um starfsemi netöryggissveitarinnar og útfæra nánar einstök verkefni hennar. Þetta ákvæði er tekið nær óbreytt upp úr 6. mgr. 47. gr. a. laga nr. 81/2003 um fjarskipti, sbr. 8. gr. laga nr. 62/2012, en hefur verið aðlagð með tilliti til þess að verið er að flytja starfsemi netöryggissveitarinnar til ríkislögreglustjóra og víkka út starfssvið hennar.

Um 4. gr.

Ákvæði þetta þarfnast ekki skýringa.

Um 5. gr.

Ákvæði þetta þarfnast ekki skýringa.

Um ákvæði til bráðabirgða I.

Í fyrra bráðabirgðaákvæðinu er það lagt til grundvallar að sem minnst röskun verði á yfirstandandi starfsemi netöryggissveitarinnar við flutninginn til ríkislögreglustjóra. Þannig er miðað við að starfsmönnum netöryggissveitarinnar verði gefinn kostur á að flytjast til embættis ríkislögreglustjóra við gildistöku laganna. Þá er gert ráð fyrir að sérhæfður hugbúnaður og tölvu- og tækjabúnaður flytjist með netöryggissveitinni til embættis ríkislögreglustjóra.

Um ákvæði til bráðabirgða II.

Í síðara bráðabirgðaákvæðinu er mælt fyrir um tiltekin lagaskil vegna framkvæmdar á álagningu gjalda sem á sér stað eftir að lög, samkvæmt frumvarpi þessu, hafa öðlast gildi þann 1. janúar 2016. Þykir þetta vera nauðsynlegt þar sem að rekstrargjaldið sem Póst- og fjarskiptastofnun leggur á samkvæmt 14. gr. laga nr. 69/2003 og hið nýja netöryggisgjald, samkvæmt 6. gr. frumvarpsins, eru veltutengd gjöld sem leggjast á gjaldstofna liðins árs. Tilgangur bráðabirgðaákvæðisins er þannig að tryggja samfellu í framkvæmd gjaldtökkunar.