



STEFNA FJARSKIPTASTOFU

um fyrirkomulag og framkvæmd eftirlits með net-
og upplýsingaöryggi

Apríl 2025



Efnisyfirlit

Stefna Fjarskiptastofu um framkvæmd eftirlits með net- og upplýsingaöryggi	2
1. Net- og upplýsingaöryggi	3
2. Fjarskiptalög	5
3. Netöryggislög	6
4. Markmið eftirlits	8
5. Áhættumiðað eftirlit Fjarskiptastofu	9
5.1 Hringrás eftirlits	9
5.2 Sjálfsmat aðila	9
5.3 Úttektir og prófanir	10
5.4 Eftirfylgni	14
6. Sérækt eftirlit	15
6.1 Áherslur í séræku eftirliti	15
6.2 Heildstætt áhættumat fjarskiptainnviða	15
6.3 Sérækt áhættumat	15
6.4 Sérækar skoðanir	16
6.5 Rannsókn alvarlegra öryggisatvika, atvika og áhættu	16
6.6 Öryggi útivistunar og birgjakeðju farneta	17



Stefna Fjarskiptastofu um framkvæmd eftirlits með net- og upplýsingaöryggi

Fjarskiptastofa hefur mótað eftirfarandi stefnu um fyrirkomulag og framkvæmd eftirlits með:

Fjarskiptafyrirtækjum

Rekstraraðilum
stafrænna grunnvirkja

Veitendum
stafrænnar þjónustu

Það er stefna Fjarskiptastofu:

1. Að við mat á stjórnunarkerfi netöryggis fjarskiptafyrirtækja, hafi stofnunin almannahagsmuni og þjóðaröryggi í fyrirrúmi og leggi áherslu á að þjónustan haldist órofin.
2. Að eftirlit stofnunarinnar stuðli að auknu öryggi og viðnámsþrótti fjarskipta, og upplýsinga- og netkerfa rekstraraðila stafrænna grunnvirkja og veitenda stafrænnar þjónustu
3. Að leiðbeina og fylgja því eftir að rekstraraðilar stafrænna grunnvirkja, veitendum stafrænnar þjónustu og fjarskiptafyrirtæki uppfylli kröfur um net- og upplýsingaöryggi sem kveðið er á um í lögum og afleiddum réttarheimildum.
4. Að hafa yfirsýn yfir stöðu net- og upplýsingaöryggis rekstraraðila stafrænna grunnvirkja, virkni og áhættustýringu almennrar fjarskiptaþjónustu og almennra fjarskiptaneta fjarskiptafyrirtækja.
5. Að eftirlit stofnunarinnar sé samræmt, skilvirkt og að aðilar njóti jafnræðis.
6. Að eftirliti Fjarskiptastofu sé forgangsraðað með tilliti til fyrirliggjandi áhættu.
7. Að framkvæma skoðun á öllum alvarlegum öryggisatvikum fjarskiptafyrirtækja, sem og atvikum og áhættu rekstraraðila stafrænna grunnvirkja og veitendum stafrænnar þjónustu.
8. Að leggja fyrir sjálfsmat hjá a.m.k. stærstu fjarskiptafyrirtækjunum og rekstraraðilum stafrænna grunnvirkja á þriggja ára fresti og í kjölfar verulegra breytinga.
9. Að á hverju þriggja ára tímabili verði framkvæmdar úttektir og prófanir til að ná heildstæðari mynd á fylgni a.m.k. stærstu fjarskiptafyrirtækja og rekstraraðila stafrænna grunnvirkja við viðkomandi lög og afleiddra réttarheimilda.
10. Að framkvæma áhættumat vegna fjarskiptainnvíða fyrir lok árs 2027.

Stefnan er rýnd og endurskoðuð eftir þörfum en að lágmarki á þriggja ára fresti og í kjölfar verulegra breytinga ásamt breytingum á tengdri löggjöf eða afleiddum réttarheimildum.



1. Net- og upplýsingaöryggi

Við lifum á tímum mikilla tækniframfara og er svo komið að íslenskt nútímasamfélag er orðið mjög háð fjarskiptum og stafrænni tækni við veitingu nauðsynlegrar þjónustu hér á landi. Hnökkur í rekstri net-og upplýsingakerfa hjá rekstraraðilum geta haft víðtækar og alvarlegar afleiðingar í för með sér fyrir íslenskt samfélag. Á sama tíma og spennandi tækifæri tæknipróunar eru til staðar ríkir umtalsverð spennu í alþjóðastjórnámálum og stríð ríkir í austurhluta Evrópu sem og fyrir botni Miðjarðarhafs.

Með virkum og vönduðum öryggisráðstöfum er hægt að lágmarka þá áhættu sem steðjað getur að öryggi net- og upplýsingakerfa, þ.m.t. vegna fátíðra atburða sem geta valdið alvarlegum rekstrartruflunum eins og langtíma þjónusturofi hjá fyrirtækjum. Í flóknu pólitísku alþjóðaumhverfi nútímans og með vaxandi netógnum verður fyrirbyggjandi netöryggi síst ofmetið. Formföst og virk umgjörð og stjórnskipulag á öryggi net- og upplýsingakerfa leika ekki einungis lykilhlutverk við að tryggja virkni þjónustu og vernda upplýsingar fyrirtækja, heldur er það fyrsta varnarlínan til að gæta þjóðarhagsmuna, tryggja efnahagslegan- og samfélagslegan stöðugleika og vernda borgarana.

Með því að bera stöðugt kennsl á og taka á áhættu og veikleikum, innleiða viðhlítandi öryggisráðstafanir og semja og prófa viðbúnaðaráætlanir, geta aðilar best verndað eigin rekstur og þeirra sem á hann treysta.

Fjarskiptastofa hefur það hlutverk að hafa eftirlit með net- og upplýsingaöryggi fjarskiptafyrirtækja, rekstraraðilum stafrænna grunnvirkja og veitendum stafrænnar þjónustu. Kröfur til fjarskiptafyrirtækja hafa verið í gildi í nokkurn tíma og í mars 2020 setti stofnunin fram stefnu um um öryggi og virkni fjarskiptainnviða. Þeim markmiðum sem þar voru sett fram hefur nú verið náð og er orðið tímabært að endurskoða þá stefnu stofnunarinnar. Þá hafa einnig tekið gildi ný lög um fjarskipti, nr. 70/2022, þar sem kveðið er á um þær lágmarkskröfur til fjarskiptafyrirtækja að tryggja öryggi og virkni almennra fjarskiptaneta og almenna fjarskiptaþjónustu.

Eftir gildistöku laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða þann 1. september 2020 hóf stofnunin innleiðingu á eftirliti á grundvelli laganna. Var sett stefna um eftirlit á síðari hluta árs 2021. Var stefna sett til tveggja ára og er því tímabært að endurskoða hana.

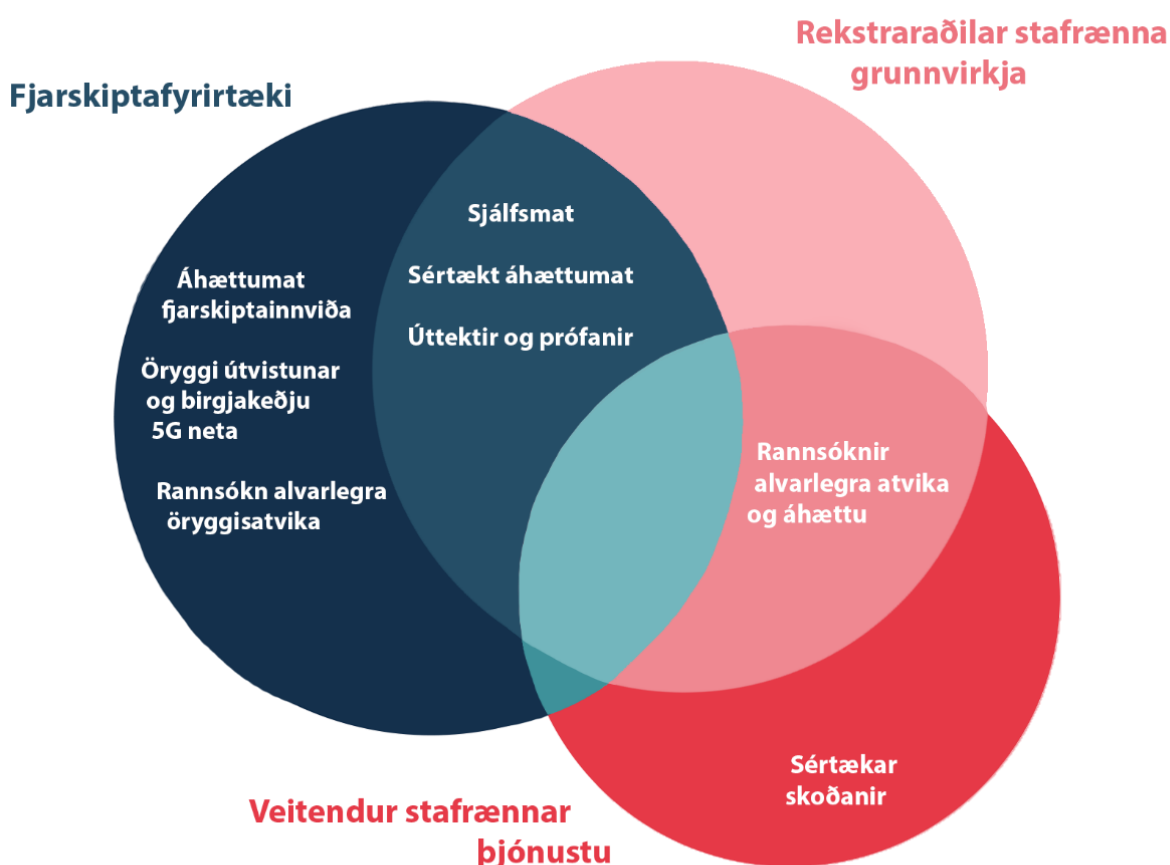
Fjarskiptastofa hefur með hliðsjón af leiðbeiningum Netöryggisstofnunar Evrópusambandsins (ENISA), samstarfshóps Evrópuríkja á sviði netöryggis (NIS Cooperation Group), og alþjóðlegum viðmiðum um framkvæmd eftirlits, byggt upp aðferðarfræði eftirlits. Nálgun stofnunarinnar er áhættumiðuð og áhersla er lögð á samvinnu við og leiðbeiningar til aðila á markaði um hvernig auka megi netöryggi. Lögð er áhersla á reglulegar úttektir hjá fleiri aðilum í stað viðamikilla stjórnsýslurannsókna hjá færri aðilum.

Þó kröfur til aðila á markaði og hlutverk stofnunarinnar komi fram í mismunandi lögum, er það stefna stofnunarinnar að aðferðafræði eftirlitsins sé sambærilegt og er því nú sett fram ein stefna um fyrirkomulag og framkvæmd eftirlits með fjarskiptafyrirtækjum og



rekstraraðilum stafrænum grunnvirkjum ásamt í fyrsta skipti er sett fram sýn stofnunar á eftirlit með veitendum stafrænar þjónustu.

Stefna þessi nær ekki til eftirlits með traustþjónustuveitendum þótt stofnunin viðhafi eftirlit með þeim á grundvelli laga nr. 55/2019, um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti. Stefna þessi afmarkast því við eftirlit með net- og upplýsingaöryggi fjarskiptafyrirtækja, rekstraraðilum stafrænna grunnvirkja og veitendum stafrænnar þjónustu. Skráð fjarskiptafyrirtæki¹ eru rúmlega 130 en um 15 fyrirtæki eru í virku fyrirbyggjandi (ex-ante) og eftirá (ex-post) eftirliti. Auk þess eru 10 rekstraraðilar stafrænna grunnvirkja² undir eftirliti stofnunarinnar en flest þeirra flokkast einnig sem fjarskiptafyrirtæki. Veitendur stafrænnar þjónustu teljast vera rekstraraðilar netmarkaða, leitarvéla á netinu og skýjavinnsluþjónustu. Eftirlit með veitendum stafrænnar þjónustu er eingöngu eftirá (ex-post), þ.e. ekki er farið í eftirlitsúrræði nema rökstuddur grunur sé að skortur á hlítu sé til staðar eða tilkynnt sé um alvarlegt atvik eða áhættu. Eftirlit stofnunar með fjarskiptafyrirtækjum og stafrænum grunnvirkjum er víðtækara og er því bæði fyrirbyggjandi (ex-ante) og eftirá (ex-post). Eftirlit með rekstraraðilum stafrænna grunnvirkja felst í rannsóknum alvarlegra atvika og áhættu sem og sjálfsmati aðila, sértæku áhættumati ásamt úttektum og prófunum. Eftirlit með fjarskiptafyrirtækjum nær til allra þeirra verkefna ásamt áhættumati fjarskiptainnviða og öryggi útvistunar og birgjakæðu.



¹ <https://www.fjarskiptastofa.is/fjarskiptastofa/fjarskiptainnvidir/skrad-fjarskiptafyrirtaeki/>

² stjornartidindi.is/Advert.aspx?RecordID=8f219edf-99a8-4c4a-b620-f5daf32b1f4a



2. Fjarskiptalög

Árið 2007 voru fyrst sett ákvæði um öryggi fjarskipta í lög hér á landi. Á grundvelli þeirra hefur Fjarskiptastofa sett reglur sem kveða á um kröfur til fjarskiptafyrirtækja. Um er að ræða reglur nr. 1221/2007, um vernd upplýsinga á almennum fjarskiptanetum og reglur nr. 1222/2007, um virkni almennra fjarskiptaneta. Framangreind öryggisákvæði byggðu ekki með beinum hætti á samevrópsku regluverki á sviði fjarskipta en sambærileg ákvæði komu inn í fjarskiptarétt Evrópusambandsins árið 2009. Íslensk ákvæði voru ekki uppfærð m.t.t. þeirra þar sem að evrópuregluverkið var ekki tekið inn í EES-samninginn. Með setningu nýrra fjarskiptalaga 2022, sem byggja á Kóðanum (EECC tilskipun Evrópusambandsins nr. 2018/1972), voru innleidd samevrópsk ákvæði sem fjalla um öryggi fjarskipta.

Um fjarskipti, fjarskiptaþjónustu og fjarskiptanet gilda fjarskiptalög nr. 70/2022, hér eftir nefnd fjarskiptalög. Markmið laganna er m.a. að tryggja aðgengileg, greið, hagkvæm, skilvirk og örugg fjarskipti hér á landi. Til að styðja við það markmið eru m.a. gerðar kröfur til fjarskiptafyrirtækja um lágmarks áhættustýringu og viðbúnað. Þá hafa verið birt í samráðsgátt stjórnvalda drög að nýrri reglugerð um öryggi fjarskipta þar sem ítarlega er kveðið á um þær lágmarkskröfur sem ákvæði 78. gr. kveður á um.

Fjarskiptastofa hefur eftirlit með framkvæmd fjarskiptalaga og er það hlutverk stofnunarinnar að taka út og framkvæma prófanir á því hvort fjarskiptafyrirtæki uppfylli kröfur laganna er varða net- og upplýsingaöryggi, virkni og áhættustýringu almennrar fjarskiptaþjónustu og almennra fjarskiptaneta. Enn fremur hvílir sú skylda á Fjarskiptastofu, við mat á öryggisskipulagi, ráðstöfunum og áhættustýringu fjarskiptafyrirtækis, að horfa til þess að fjarskiptaþjónusta haldist órofin, til almannahagsmuna og vegna þjóðaröryggis³.

Þá hefur stofnunin heimild til að afla allra upplýsinga og gagna um skipulag net- og upplýsingaöryggis frá fjarskiptafyrirtækjum sem stofnunin telur nauðsynleg vegna framkvæmdar eftirlitsins.

Fjarskiptastofa getur farið fram á að fjarskiptafyrirtæki framkvæmi sértækt áhættumat á einstökum hlutum rekstrar- og kerfisþáttum fjarskiptaneta eða fjarskiptaþjónustu eða á sérstökum ógnum sem geta steðjað að upplýsingum, fjarskiptanetum og fjarskiptaþjónustu. Fjarskiptastofu er enn fremur heimilt að framkvæma mat á heildstæði, öryggi og virkni almennra fjarskiptaneta og fjarskiptaþjónustu með tilliti til áhættu, í heild eða að hluta.

³ Sbr. 9. mgr. 78. gr. laga um fjarskipti nr. 70/2022.



3. Netöryggislög

Árið 2016 kom út tilskipun Evrópuþingsins og ráðsins varðandi ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum í öllu Evrópusambandinu (NIS1). Tilskipunin var innleidd á Íslandi með setningu laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða (almennt vísað til sem NIS1 eða netöryggislög). Á grundvelli laganna hafa verið settar tvær reglugerðir er kveða á um kröfur til net- og upplýsingaöryggis, þ.e. reglugerð nr. 866/2020, um öryggi net- og upplýsingakerfa rekstraraðila nauðsynlegrar þjónustu og reglugerð nr. 1255/2020, um öryggi net- og upplýsingakerfa veitenda stafrænnar þjónustu. Þá hefur verið sett reglugerð nr. 480/2021, um netöryggissveit Fjarskiptastofu. Til að tryggja öryggi og ásættanlega vernd við rekstur net- og upplýsingakerfa ber rekstraraðilum stafrænna grunnvirkja og veitendum stafrænnar þjónustu að uppfylla þær lágmarkskröfur sem fram koma í framangreindum reglugerðunum.

Fjarskiptastofa hefur eftirlit með framkvæmd netöryggislaga gagnvart veitendum stafrænnar þjónustu og rekstraraðilum nauðsynlegrar þjónustu á sviði stafrænna grunnvirkja. Netöryggislöggjöfin skilgreinir stafrænnar þjónustu sem þjónusta í skilningi b-liðar 1. mgr. 1. gr. tilskipunar 2015/1535/ESB sem fellur undir skilgreiningu netöryggislaganna á hugtökunum netmarkaður, leitarvél á netinu eða skýjavinnsluþjónusta. Þá eru stafræn grunnvirki skilgreind í lögnum sem tengi- og skiptipunktur, þjónustuveitendur lénsheitakerfis og skráningarstofur höfuðléna. Það eru þó ekki allir aðilar sem reka framangreinda þjónustu sem falla innan gildissviðs netöryggislaganna. Viðkomandi rekstraraðili þarf einnig að teljast vera mikilvægur í efnahagslegu og samfélagslegu tilliti. Þannig eru settar ákveðnar kröfur í lögnum og framangreindri reglugerð nr. 866/2020, sem uppfylla þarf svo aðili teljist rekstraraðili nauðsynlegrar þjónustu.

Samkvæmt netöryggislögnum ber þeim stjórnvöldum sem fara með eftirlitshlutverk á grundvelli laganna að tilnefna þá aðila sem uppfylla skilyrði laganna um mikilvægi til samgöngu- og sveitarstjórnarráðuneytisins. Ráðherra birtir á grundvelli þeirra tilnefninga skrá í B deild Stjórnartíðinda⁴. Í lok árs 2023 voru 68 á skrá ráðherra yfir rekstraraðila nauðsynlegrar þjónustu og þar af tíu sem skilgreindir eru sem rekstraraðilar stafrænna grunnvirkja og falla þar með undir eftirlit Fjarskiptastofu. Gera má ráð fyrir í reglubundnum uppfærslum á skrá ráðherra geti fjöldi aðila breyst.

Fyrir þá rekstraraðila nauðsynlegrar þjónustu sem hlíta eftirliti stofnunarinnar þá hefur stofnunin heimild til að afla allra upplýsinga og gagna um skipulag net- og upplýsingaöryggis sem stofnunin telur nauðsynleg vegna framkvæmdar eftirlitsins. Stofnunin hefur heimild til að gera úttektir og prófanir til að kanna hvort rekstraraðilarnir uppfylli kröfur netöryggislaganna og reglugerða sem settar eru á grundvelli þeirra. Þá hefur stofnunin heimildir til að rannsaka þær áhættur og atvik sem upp koma í net- og upplýsingakerfum aðila til að kanna hvort kröfur laganna og afleiddra réttarheimilda hafi verið uppfylltar á þeim tímapunkti þegar áhætta var til staðar eða atvik varð.

Fjarskiptastofa hefur heimild til að biðja rekstraraðili nauðsynlegrar þjónustu að framkvæma sértækt áhættumat á einstökum hlutum net- og upplýsingakerfa vegna áhættu sem getur steðjað að kerfunum sem og vegna útvistunar á rekstri þeirra.

⁴ stjornartidindi.is/Advert.aspx?RecordID=8f219edf-99a8-4c4a-b620-f5daf32b1f4a



Þá fer Fjarskiptastofa með hlutverk samhæfingarstjórnvalds sem sinnir almennri stefnumörkun um eftirlit með lágmarkskröfum netöryggislaganna og reglugerð nr. 866/2020 með það að markmiði að stuðla sem best að samræmi og jafnræði við framkvæmd laganna.

Eftirlit Fjarskiptastofu með veitendum stafrænnar þjónustu takmarkast við rannsóknir eða úttektir ef upp kemur rökstuddur grunur um að fyrirtæki uppfylli ekki kröfur í 7. og 8. gr. netöryggislaganna eða afleiddum réttarheimildum. Stofnunin hefur heimild til að afla allra upplýsinga og gagna um skipulag net- og upplýsingaöryggis sem stofnunin telur nauðsynleg vegna framkvæmdar eftirlitsins.

Í október 2024 áttu aðildarríki Evrópusambandsins að hafa innleitt nýja tilskipun á sviði netöryggis, NIS2. Markmið hinnar nýju tilskipunar er líkt og forvera hennar að ná háu sameiginlegu netöryggisstigi í öllu Evrópusambandinu. Meðal stærstu breytinga í NIS2 er að tilskipunin setur lágmarkskröfur á mun fleiri aðila en forveri hennar gerði, en NIS2 er ætlað að ná til allra þeirra nauðsynlegu og þýðingarmiklu aðila sem veita þjónustu á fjölmörgum sviðum atvinnulífsins. Þá nær hún einnig til opinberra aðila. Þá er ábyrgð á netöryggi sett á æðstu stjórnenda aðilanna, en í því felst m.a. að þeir skulu staðfesta stjórnkerfi net- og upplýsingaöryggis, hafa yfirsýn með innleiðingu þess og bera ábyrgð á skorti á hlítingu. NIS2 tilskipunin er ekki eingöngu að leggja kröfur á aðila heldur eru einnig settar kröfur á aðildarríkin þar sem sérstaklega er kveðið á um aukið samstarf á Evrópuvísu. Tilskipunin hefur ekki verið innleidd á Íslandi en unnið er að innleiðingu hennar inn í EES-samningsins hjá EFTA-skrifstofunni í Brussel. Ekkert er því til fyrirstöðu að aðilar undirbúi sig fyrir gildistöku hennar, og í raun og veru verður það að teljast æskilegt í ljósi viðamikilla ráðstafana sem fyrirtæki kunna að þurfa að ráðast í vegna innleiðingar gjörðarinnar. Fjarskiptastofa mun leitast við að veita fræðslu, innsýn og leiðbeiningar eftir því sem við á um hina nýju tilskipun.



4. Markmið eftirlits

Meginmarkmið eftirlits Fjarskiptastofu er það stuðla að auknu öryggi og viðnámsþrótti hjá net- og upplýsingakerfum fjarskiptafyrirtækja, stafrænum grunnvirkjum og hjá veitendum stafrænnar þjónustu gagnvart net- og upplýsingaöryggisógnum. Það er markmið Fjarskiptastofu að í lok árs 2027 sé öryggisskipulag, áhættustýring og viðbúnaður aðila í samræmi við alþjóðleg bestu viðmið um framkvæmd á þessu sviði.

Markmiðið er að eftirlit sé framkvæmt með þeim hætti að það sé áhættumiðað, skilvirkt fyrir stofnunina og eftirlitskylda aðila og tímanlegt. Að auki er haft að leiðarljósi að eftirlit með net- og upplýsingaöryggi fjarskiptafyrirtækja og rekstraraðilum nauðsynlegrar þjónustu sé samræmt og að aðilar njóti jafnræðis.

Það er stefna stofnunarinnar að vinna að aukinni sjálfvirknivæðingu eftirlitsins, sem veitir aðilum og Fjarskiptastofu upplýsingar um stöðu öryggisskipulags, áhættustýringar og öryggisráðstafana tímanlega og endurspegli stöðu net- og upplýsingaöryggi eftirlitsskyldra aðila á hverjum tíma.

Fjarskiptastofa áréttar mikilvægi góðs samstarfs við eftirlitskylda aðila enda telur stofnunin að framkvæmd eftirlits með þeim hætti sé farsælast til þess að ná sameiginlegum markmiðum aðila, þ.e. að tryggja öryggi og virkni þeirrar efnahags- og samfélagslega mikilvægu þjónustu sem viðkomandi fyrirtæki veitir.

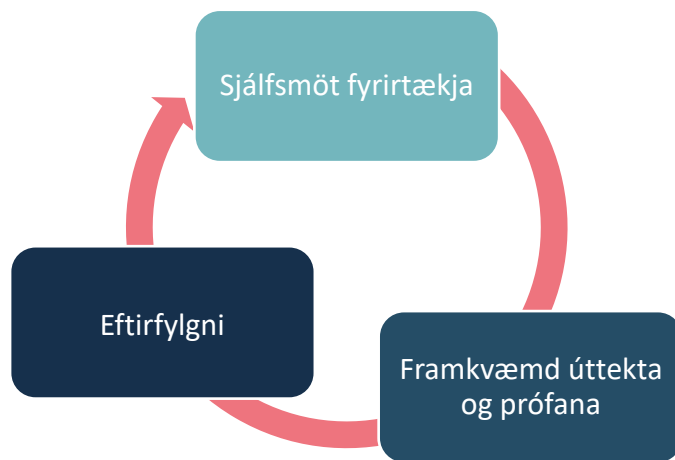
Mörg fagsvið Fjarskiptastofu hafa hlutverki að gegna þegar kemur að því að tryggja virkni fjarskiptainnviða. Framkvæmd eftirlits með öryggisskipulagi, ráðstöfunum og áhættustýringu fyrirtækja er að stærstum hluta í höndum sérfræðinga Fjarskiptastofu á sviði stafræns öryggis. En stofnunin getur einnig leitað til utanaðkomandi sérfræðinga í einstaka prófunar- eða úttektarverkefnum.

Fjarskiptastofu er umhugað um að byggja traust á milli aðila og gætir fyllsta öryggis við vinnslu upplýsinga sem fyrirtæki afhenda stofnuninni á grundvelli eftirlits. Stofnunin hefur hlotið ISO/IEC 27001 vottun auk þess sem það starfsfólk stofnunarinnar sem sinnir eftirliti á þessu sviði hefur fengið öryggisvottun ríkislögreglustjóra. Þá er vert að nefna að þagnarskylda gildir um alla starfsmenn Fjarskiptastofu sbr. 25. gr. laga nr. 75/2021, um Fjarskiptastofu, sbr. X. kafli stjórnarsýslulaga nr. 37/1993. Loks er kveðið á um sérstaka þagnarskyldu í 84. gr. fjarskiptalaga og 19. gr. netöryggislaga sem nær til framkvæmd eftirlits með netöryggi.

Vert er að taka fram að eftirlit Fjarskiptastofu með skipulagi net- og upplýsingaöryggis fyrirtækjanna er aðgreint frá starfsemi netöryggissveitarinnar CERT-IS, og sinnir ekki meðhöndlun á áhættu eða atvikum þegar þau koma upp. Netöryggissveitinni er þó skylt að miðla upplýsingum til eftirlitshluta Fjarskiptastofu um atvik sem tilkynningarskyld eru skv. fjarskiptalögunum og netöryggislögum. Þá er það einnig hlutverk CERT-IS að upplýsa stafrænt öryggi um stöðumynd netóгна en slíkar upplýsingar er mikilvægar upplýsingar við forgangsroðun áhættumiðaðs eftirlits stofnunnarinnar.

5. Áhættumiðað eftirlit Fjarskiptastofu

5.1 Hringrás eftirlits



Eftirlit Fjarskiptastofu hefur hvorki upphaf né endi heldur er um að ræða sífelluverkefni. Eftirlitinu er annars vegar skipt upp í fyrirbyggjandi eftirliti (ex-ante) og hinsvegar í eftirá eftirlit (ex-post). Fyrirbyggjandi eftirlit felst í því að afla upplýsinga um stöðu net- og upplýsingaöryggis m.a. með sjálfsmötum fyrirtækja, framkvæmd úttekta, prófunum og eftirfylgni bindandi fyrirmæla. Fjarskipta-fyrirtæki og rekstraraðilar stafrænna grunnvirkja lúta bæði fyrirbyggjandi

og eftirá eftirlit en eftirlit með veitendum stafrænnar þjónustu er eingöngu eftirá. Það er stefna Fjarskiptastofu að eftirlitið sé áhættumiðað, þ.e.a.s. verkefnum er forgangsraðað með tilliti til áhættu og er sífelld þekkingaröflunin lykilinn að þeirri forgangsroðun. Við forgangsroðun er horft til þjóðaröryggis, almannahagsmuna og hagsmuna notenda af því að mikilvæg þjónusta haldist órofin.

Fjarskiptafyrirtæki og rekstraraðilar stafræna grunnvirki gegna misstöru hlutverki í rekstri og veitingu nauðsynlegrar þjónustu og er því stærð og hlutverk haft í huga við forgangsroðun eftirlits en eins og gefur að skilja þá eru alvarlegri afleiðingar samfara útfalli þjónustu þeirra fyrirtækja sem hafa umtalsverða markaðshlutdeild.

Forgangsroðun áhættumiðaðs eftirlits Fjarskiptastofu tekur mið af eftirfarandi atriðum;

- niðurstöðum fyrri úttekta og prófana Fjarskiptastofu,
- niðurstöðum sjálfsmats fyrirtækja,
- atvikum sem upp hafa komið,
- breytingum í umhverfi fyrirtækisins,
- ISO 27001 vottun,
- niðurstöðum ytri úttekta og
- niðurstöðu áhættumata.

5.2 Sjálfsmat aðila

Fjarskiptastofa hefur lagt fyrir stærstu fjarskiptafyrirtæki og rekstraraðila stafrænna grunnvirkja sjálfsmat til að leggja mat á fyrirkomulag öryggismála og umgjörð áhættustýringar. Kóngulóaritið hér að neðan er dæmi um mögulega niðurstöðu sjálfsmat. Stefnt er að því að leggja slíkt sjálfsmat fyrir a.m.k. stærstu fjarskiptafyrirtækin og rekstraraðila stafrænna grunnvirkja á þriggja ára fresti. Er slíkt í samræmi við núverandi framkvæmd en stofnunin hefur tvisvar framkvæmt sjálfsmat á rekstraraðilum nauðsynlegrar þjónustu og einu sinni á stærstu fjarskiptafyrirtækjum landsins. Til viðbótar þá vinnur stofnunin nú í samvinnu við önnur eftirlitsstjórnvöld að framkvæmd sjálfmata á öðrum mikilvægum innviðum á



grundvelli netöryggislaganna. Um er að ræða aðgerð á aðgerðaráætlun ráðherra á sviði netöryggis.

Sjálfsmat



Tilgangur slíkrar þekkingaröflunar er að átta sig á stöðu öryggismála og öryggisvitundar hjá hverju fyrirtæki fyrir sig og heildarinnar ásamt því að veita fyrirtækjunum sjálfum tækifæri á að meta öryggisskipulag sitt m.t.t. viðurkenndra viðmiða um netöryggi frá ENISA, lögum fjarskipti nr. 70/2022, netöryggislögum nr. 78/2019 og afleiddum réttarheimildum hér á landi.

Eins og áður hefur komið fram nýtast niðurstöður sjálfsmats jafnframt sem mikilvægt innlegg fyrir afmörkun og forgangsroðun frekara eftirlits með fjarskiptafyrirtækjunum í formi úttekta og prófana.

5.3 Úttektir og prófanir

Fjarskiptastofa sannreynir fylgni við fjarskipta- og netöryggislög og afleiddar réttarheimildir með framkvæmd úttekta og prófana.

Áætlanagerð

Umfang úttekta og prófana er valið með hliðsjón af áhættu og forgangsroðunar m.a. m.t.t. fjármagns, mannafla og öðrum aðföngum, en stefnt er að því að á þriggja ára tímabili séu framkvæmdar úttektir og prófanir til að ná heildstæðri mynd af fylgni a.m.k. stærstu fjarskiptafyrirtækja og rekstraraðila stafrænna grunnvirkja við þær kröfur sem á þeim hvíla. Sérstök innri eftirlitsáætlun er gerð til þriggja ára en er endurmetin á að lágmarki sex mánaða fresti sem og þegar verulegar breytingar verða á áhættu og/eða lagaumhverfinu.

Fyrir hverja úttekt, eða prófun, er markmið og umfang verkefnisins ákveðið, ásamt viðmiðunum og aðferðafræði. Skilgreint er hvaða gögnum eru nauðsynlegt að afla frá



hlutaðeigandi fyrirtæki. Leitast er við að aðferðafræðin sem valin er sé þess eðlis að markmiðum verkefnisins sé náð og að þær gefi fullnægjandi upplýsingar um virkni þeirra öryggisráðstafana sem til skoðunar eru.

Við framkvæmd eftirlits er hægt að styðjast við mismunandi matsaðferðir, sem dæmi má nefna mat á skjölum og gögnum (skrifborðsúttektir). Þá er hægt að meta stöðu aðila í gegnum spurningalista og viðtöl við starfsmenn og/eða stjórnendur fyrirtækja. Eins er hægt að framkvæma vettvangsskoðun og athuga stöðu aðila með beinum hætti á virkni stýringa ásamt tæknilegum prófunum. Framkvæmd úttektar getur stuðst við eina, tvær eða fleiri tegundir matsaðferða, allt eftir umfangi og markmiðum úttektar.

Yfirferð á gögnum (skrifborðsúttekt)

Almennt eru skrifborðsúttektir, þar sem farið er yfir skjöl og gögn frá aðilum, nauðsynlegur hluti allra úttekta. Gögn frá aðilum geta t.d. verið öryggisstefnur, áhættumat og valdar öryggisráðstafanir, neyðaráætlanir, einstaka hlutverk aðila og ábyrgðadreifing, verklagsreglur og verklýsingar, lýsingar á hönnun og uppbyggingu kerfa sem og niðurstöður innri prófana og úttektir ytri aðila.



Viðtöl

Mat í formi viðtala getur verið framkvæmt hvort sem er sjálfstætt eða til viðbótar við yfirferð gagna með skrifborðsúttekt. Í viðtölum er gjarnan aflað huglægra en gagnlegra upplýsinga um efni úttektar. Þá gefst tækifæri til að ræða dýpra um málefnið og með meiri sveigjanleika. Fjöldi viðmælenda getur verið mismunandi eftir stærð fyrirtækisins og dreifingu ábyrgðar á net- og upplýsingakerfum.



Vettvangsskoðun

Mat í vettvangsskoðun felur í sér að farið er í viðkomandi kerfi og/eða tækjarými og athugað hvort öryggisráðstöfun sé til staðar og virkni staðfest með skoðun. Hérna getur jafnframt verið um að ræða úttekt sem framkvæmd er af starfsmanni stofnunarinnar og/eða ytri aðila á vegum hennar.



Tæknilegar prófanir

Mat í formi beinnar prófunar á öryggisráðstöfun er ítarlegasta tegund mats. Í tæknilegum prófunum er reynt á öryggisráðstafanir, t.d. með veikleikaskönnun ásamt innri og/eða ytri innbrotsprófun (e. penetration test). Afmörkun prófana hverju sinni er ákvörðuð m.t.t. ástandsvitundar netöryggis og niðurstaðna sjálfsmata, úttekta, fyrri prófanna og rannsókna á atvikum.



Veikleikaskönnun felst í því að leitað er eftir veikleikum í ytra og innra umhverfi fyrirtækisins, þar á meðal veikleikum í verklagi og öryggisveilum í búnaði. Innbrotsprófun felst í að prófunaraðili setur á



síga hatt óprúttins árársaraðila og kannar hvaða öryggisráðstafanir hann getur brotið eða hvaða veikleika hann getur nýtt sér sem gætu valdið truflunum eða rofi á þjónustu. Almennt er leitað eftir að prófunin sé framkvæmd í góðu samstarfi við viðkomandi fyrirtæki. Tæknilegar prófanir eru allajafna framkvæmdar af ytri aðila á vegum stofnunarinnar en undir verkefnastjórn stofnunarinnar. Eftir atvikum getur verið kallað eftir frekari upplýsingum og gögnum frá fyrirtæki til að varpa frekari ljósi á niðurstöður veikleikaskönnunar og innbrotsprófunar.

Mat á fylgni

Mikilvægur liður við samræmda nálgun eftirlits er samræmi í mati á fylgni við lög og afleiddar réttarheimildir er varða öryggi upplýsinga og þjónustu. Afmörkun úttekta og prófanna hverju sinni er við þá þætti sem áhættan er talin hvað mest. Það felur í sér að ekki er tekin út fylgni við alla þætti viðkomandi laga og afleiddra réttarheimilda ásamt þeim stöðlum sem eiga við viðkomandi starfsemi s.s. ÍST ISO/IEC 27001, ÍST ISO/IEC 27002 og ISO/IEC 27005. Dæmi um afmörkun í úttekt á netöryggislögum er fylgni við ákvæði um skipulagslegar ráðstafanir sem hefur fimm skoðunarliði, sbr. mynd hér að neðan.



Fjarskiptastofa viðhefur samræmda matsaðferð og einkunnargjöf en það gerir stofnuninni betur kleift að bera saman stöðu fyrirtækja og þar með öðlast yfirsýn yfir öryggi þjónustu og rekstur aðila. Aðferðafræði stofnunarinnar er með þeim hætti að hver skoðunarliður í úttektinni, t.d. *öryggisstefna*, er skipt í nokkra eftirlitsþætti, t.d. *öryggisstefna er yfirfarin og samþykkt með formlegum hætti af stjórnendum* og þar eftir viðmið og er fylgni við hvert viðmið metin með einkunnagjöf á bilinu 0-3, en í töflu hér að neðan má sjá forsendur einkunnagjafar. Í þeim tilfellum sem niðurstaða eftirlitsþáttar er lægri en 3 fær viðkomandi



fyrirtæki bindandi fyrirmæli og ráðast tímamörk úrbóta af alvarleika greinds frávíks, en í tilfelli alvarlegustu frávíkanna er tímafrestur 3 mánuðir, sjá nánar næstu töflu.

Í töflunni hér á eftir eru forsendur þeirra viðmiða sem tölulegar einkunnir byggja á. Um er að ræða fjórar einkunnir, frá 0-3, ásamt litakóðum til að auðvelda úrvinnslu og yfirsýn.

Einkunn 3 (3,0)

• **Ekkert frávik** kom upp við skoðun. Skoðunarliðir, eftirlitþættir og/eða viðmið eru í lagi. Stjórnkerfi og/eða öryggisráðstöfun hefur verið komið á og er samræmi við lágmarkskröfur.

Ekki þörf á viðbrögðum af hálfu Fjarskiptastofu.

Einkunn 2 (2,0 - 2,9)

• **Minniháttar frávik** kom upp við skoðun. Öryggisráðstöfun og skjalfesting er til staðar og innleiddar, en við skoðun kom í ljós að tækifæri til úrbóta eru fyrir hendi sem bregðast þarf við fyrir næstu úttekt Fjarskiptastofu.

Fjarskiptastofa beitir bindandi fyrir mælum.

Einkunn 1 (1,0 - 1,9)

• **Frávik** kom upp við skoðun. Öryggisráðstöfun og/eða skjalfesting er til staðar en eru ekki að fullu innleiddar. Niðurstöður kalla á viðbrögð innan sex mánaða.

Fjarskiptastofa beitir bindandi fyrir mælum.

Einkunn 0 (0,0 - 0,9)

• **Alvarlegt frávik** kom upp við skoðun. Ekki hægt að staðfesta að öryggisráðstöfun sé til staðar. Niðurstöður kalla á viðbrögð innan þriggja mánaða.

Fjarskiptastofa beitir bindandi fyrir mælum.

Niðurstöður úttektar og prófunar

Að lokinni upplýsingaöflun, framkvæmd matsaðferða og mati á fylgni, eru niðurstöður skjalfestar í drögum að skýrslu sem send er viðkomandi fyrirtækis til yfirlestrar. Yfirlesturinn er hluti af rannsókn málsins og er til þess fallinn að tryggja að málið sé nægilega upplýst og að andmælaréttur sé virtur áður en ákvörðun er tekin. Í yfirlestrarferlinu er fyrirtækinu gefinn kostur á að kynna sér niðurstöðurnar, leiðrétta misskilning og miðla frekari upplýsingum til stofnunarinnar ef þörf er á.

Ef niðurstaða úttektar eða prófunar leiðir í ljós að fyrirtæki fylgja ekki einhverjum þeim kröfum sem settar eru fram í þeim lögum og afleiddum réttarheimildum sem skoðunin afmarkast við mun Fjarskiptastofa krefjast þess að úr verði bætt með því að gefa út bindandi fyrir mæli. Hlutaðeigandi aðili fær þá hæfilegan frest til úrbóta sem tekur mið af alvarleika niðurstöðu úttektar og einkunnagjafar. Tímamörk á viðbrögð fyrirtækis sem og dagsektir eða önnur stjórnsýsluviðurlög taka mið af einkunnum. Ljóst er þó að ávallt verður leitast við að gefa fyrst



út bindandi fyrirmæli og tryggja eftirfylgni við þau, áður en meira íþyngjandi úrræðum verður beitt.

5.4 Eftirfylgni

Í þeim tilvikum þar sem gefin eru út bindandi fyrirmæli fylgir Fjarskiptastofa þeim eftir til að gæta þess að úrbætur fyrirtækisins séu fullnægjandi. Viðhafa þarf það verklag að áður en tímafrestur bindandi fyrirmæla rennur út skilar fyrirtæki umsögn og gögnum sem staðfesta að brugðist hafi verið við fyrirmælunum með fullnægjandi hætti. Að loknum tímafresti leggur Fjarskiptastofa sjálfstætt mat á hvort úrbætur séu fullnægjandi. Komi í ljós að viðkomandi fyrirtæki hafi vanrækt að fara að fyrirmælum Fjarskiptastofu um úrbætur getur stofnunin ákveðið að láta þriðja aðila vinna verkið á kostnað hlutaðeigandi sem og lagt á dagsektir þar til fyrirmælum hefur verið fullnægt að mati stofnunarinnar.



6. Sértækt eftirlit

6.1 Áherslur í sértæku eftirliti

Úttektir og prófanir eru megin eftirlitsverkefni, en ásamt þeim er öðrum aðferðum beitt þegar tilefni er til, og má þá helst nefna heildstætt áhættumat fjarskiptainnviða, sértækt áhættumat og rannsóknir á alvarlegum öryggisatvikum⁵, atvikum⁶ og áhættum⁷. Því til viðbótar er eftirlit með útvistun fjarskiptafyrirtækja á nauðsynlegri starfsemi fyrir virkni, vernd eða stjórnun fjarskipta.

6.2 Heildstætt áhættumat fjarskiptainnviða

Árin 2020-2021 var framkvæmt, í fyrsta skipti á Íslandi, heildstætt áhættumat á ógnum sem geta valdið alvarlegum truflunum á virkni fjarskiptaneta og/eða rofi á veitingu fjarskiptaþjónustu, annað hvort á stórum landssvæðum, og/eða hvort mikinn fjölda notenda yrði fyrir áhrifum. Áhættumatið náði til átta fjarskiptafyrirtækja, en ýmist sinna þessi fyrirtæki rekstri sæstrengja, fastaneta, stofnsambanda og fjarskiptasendastaða eða eru rekstraraðilar fjarskipta- og netþjónustu.

Niðurstaða áhættumatsins gaf Fjarskiptastofu mikilvæga innsýn inn í helstu fjarskiptainnviði á öllum landssvæðum sem og hvernig fjarskiptafyrirtækin skilgreina fjarskiptastaði sína, hvernig þau meta áhættur gagnvart innviðum sínum sem og þær öryggisráðstafanir sem þau viðhafa.

Áhættumatið gaf Fjarskiptastofu öflugan grunn fyrir áframhaldandi vinnu þegar kemur að eftirliti og verkefnum er varðar öryggi og virkni fjarskipta hér á landi. Ekki einungis við hefðbundin eftirlitsverkefni heldur einnig hvernig skuli á breiðari grundvelli nálgast umræðu um mikilvæga fjarskiptainnviði eins og mögulegan „markaðsbrest“ þegar kemur að öryggi í almennum fjarskiptum⁸, um lágmarksráðstafanir, hlítingu við staðla o.fl. sem og þegar kemur að stöðu landshringsins sem baknets fyrir uppbyggingu nýrrar þjónustu, t.a.m. 5G.

Fjarskiptastofa telur einnig brýnt að áhættumat sem þetta sé reglulega endurtekið t.d. á um fimm ára fresti. Þannig næst betri og dýpri mynd af fjarskiptakerfum landsins, þróun þeirra og stöðu öryggis. Hyggst Fjarskiptastofa uppfæra umrætt áhættumat í samstarfi við stærstu fjarskiptafyrirtæki á markaði á gildistíma stefnu þessarar.

6.3 Sértækt áhættumat

Fjarskiptastofa hefur framkvæmt sértækt áhættumat á fjarskiptanetum og -þjónustu á grundvelli núgildandi laga. Var það gert í kjölfar innrásar Rússlands í Úkraínu árið 2022. Áhættumatið nýttist afar vel til að ná skjótri sýn á áfallapol fjarskiptafyrirtækja gagnvart mögulegri stigmögnun átaka í Evrópu og hefur leitt þess að sértæk verkefni hafa verið sett af

⁵ 62. tl. 1. mgr. 5.gr. laga nr. 70/2022; *Öryggisatvik*: Hver sá atburður sem hefur eða getur haft skaðleg áhrif á öryggi fjarskiptaneta og fjarskiptaþjónustu.

⁶ 1. tl. 1. mgr. 6.gr. laga nr. 78/2019; *Atvik*: Hver sá atburður sem hefur skaðleg áhrif á öryggi net- og upplýsingakerfa.

⁷ 2. tl. 1. mgr. 6.gr. laga nr. 78/2019; *Áhætta*: Aðstæður eða atburðir sem geta haft skaðleg áhrif á öryggi net- og upplýsingakerfa.

⁸ Hér er t.a.m. horft til farneta, en farsímar verða að teljast orðin öryggistæki fyrir almenning.



stað af stjórnvöldum til að tryggja uppitíma þjónustu með sem bestum hætti. Eins nýttist það inn í einstök og mikilvæg eftirlitsverkefni hjá Fjarskiptastofu.

Markmið sértækra áhættumata er einnig að virkja áhættuvitund fjarskiptafyrirtækja og rekstraraðila stafrænna grunnvirkja til að endurmeta ákveðnar ógnir út frá viðurkenndri aðferðafræði sem og leggja mat á öryggisráðstafanir sínar út frá niðurstöðu slíks mats.

Sértækt áhættumat felst í því að stofnunin óskar eftir mati fyrirtækja á því hvaða áhrif ein eða fleiri áhættur hafa á þjónustu þess fyrirtækis. Upplýsinga um áhættumat eru oft á tíðum trúnaðarmál, varða almannahagsmuni og þjóðaröryggi og ber því að tryggja leynd þeirra.

Sértækt áhættumat er alla jafna skipulagt með litlum fyrirvara og óskað er eftir að fyrirtæki framkvæmi það þegar veruleg ógn steðjar að upplýsingum, fjarskiptanetum og fjarskiptaþjónustu. Ekki er því sérstaklega gert ráð fyrir sjálfstæðu sértæku áhættumati að svo stöddu en til slíks kann þó að koma með stuttum fyrirvara ef upp koma slíkar aðstæður hér á landi eða í alþjóðlegu umhverfi.

6.4 Sértækar skoðanir

Fjarskiptastofa hefur eftirlit með framkvæmd netöryggislaga gagnvart veitendum stafrænnar þjónustu Eftirlit stofnunarinnar með þeim er eingöngu eftirá (ex-post), þ.e. ekki er farið í eftirlitsúrræði nema rökstuddur grunur sé að skortur á hlítu sé til staðar eða tilkynnt sé um alvarlegt atvik eða áhættu. Í þeim tilvikum sem upp kemur rökstuddur grunur um að veitandi stafrænnar þjónustu hlíti ekki lögum fer fram sértæk skoðun. Sértæk skoðun getur falið í sér sjálfsmat aðila, úttekt eða jafnvel prófun, en afmörkun skoðunar og eftirlitsúrræðið sem nýtt er valin m.t.t. þeirrar upplýsinga sem liggja fyrir á hverjum tíma.

6.5 Rannsókn alvarlegra öryggisatvika, atvika og áhættu

Fjarskiptafyrirtæki sem rekur almennt fjarskiptanet eða veitir almenna fjarskiptaþjónustu skal skv. 80 gr. fjarskiptalaga tilkynna án tafar til netöryggissveitarinnar CERT-IS um öll alvarleg öryggisatvik sem ógna öryggi eða virkni almennra fjarskiptaneta eða almennri fjarskiptaþjónustu. Sambærilegt ákvæði er í 8. gr. netöryggislaga en rekstraraðilum nauðsynlegrar þjónustu og veitendum stafrænnar þjónustu ber að tilkynna til CERT-IS öll alvarleg atvik eða áhættu sem ógnar öryggi net- og upplýsingakerfa þeirra.

Þegar upp kemur tilkynningaskyلت atvik hjá rekstraraðila stafrænna grunnvirkja og veitendum stafrænnar þjónustu eða tilkynningarskyلت öryggisatvik hjá fjarskiptafyrirtæki hefur Fjarskiptastofa forskoðun á atvikinu/öryggisatvikinu. Við lok á forskoðun atviks/öryggisatviks er tekin ákvörðun um hvort hefja eigi stjórnsýsluskoðun á umræddu atviki/öryggisatviki. Verklagið er á þá leið að í hvert skipti sem skyldutilkynning berst frá CERT-IS eða stofnunin fréttir af atviki þá hefur stafrænt öryggi forskoðun á atvikinu/öryggisatvikinu sem hefst með upplýsingabeiðni. Þetta er gert til að leggja frummat á alvarleika atviks/öryggisatviks og á því hvort að öryggisráðstafanir og verklag varðandi stjórnunarkerfi netöryggis sé í samræmi við kröfur þar um. Sé það niðurstaða forskoðunar að hefja skuli stjórnsýsluskoðun hefst formlegt stjórnsýsluferli sem leitt getur til töku stjórnvaldsákvörðunar.



Almennt leiða fáar forskoðanir á atvikum/öryggisatvikum til ítarlegrar stjórnsýsluskoðunar. Málum lýkur almennt með niðurstöðubræfi stofnunarinnar til hlutaðeigandi aðila, oft með ábendingum um hvar gæti verið þörf á yfirferð eða úrbótum hjá félaginu. Ekki er um bindandi fyrirmæli að ræða.

Forskoðanir eru gerðar að frumkvæði Fjarskiptastofu og hafa það markmið að framfylgja ákvæðum um lágmarkskröfur um stjórnskipulag upplýsingaöryggis, ráðstafanir og umgjörð áhættustýringar. Eiga því málsmæðferðarreglur stjórnvaldsákvæðana Fjarskiptastofu nr. 710/2020⁹, ekki við, sbr. 3. mgr. 2. gr. reglnanna. Þrátt fyrir það mun málsmæðferð við stjórnsýsluskoðun atvika taka mið af umræddum reglum eftir því sem við á.

6.6 Öryggi útivistunar og birgjakeðju farneta

Í mars 2019 gaf framkvæmdastjórn Evrópusambandsins (e. European Commission) út tilmæli varðandi öryggi 5G þjónustu til aðildarríkja sambandsins. Tilmælin fólu í sér að aðildarríki sambandsins myndu framkvæma landsbundið áhættumat á öryggi 5G neta, endurmeta öryggisráðstafanir og taka þátt í samræmdri vinnu við samræmt evrópskt áhættumat hvað þetta varðar og undirbúa samræmdar öryggisráðstafanir. Samevrópskt áhættumat varðandi 5G net var svo birt í október 2019. Áhættumatið var samstarfsverkefni ENISA, aðildarríkja og framkvæmdastjórnar Evrópusambandsins. Í kjölfar útgáfu áhættumatsins var það samstarfshópur á sviði netöryggis (NIS Cooperation Group, NIS CG) sem vann og gaf út skýrslu 23. janúar 2021 með viðeigandi öryggisráðstöfnunum, svokallaða verkfærakistu 5G netöryggis. Í skýrslunni eru leiðbeiningar/tilmæli um aðgerðir til að auka netöryggi 5G neta í sambandinu. Undanfarin misseri hefur innan Evrópusambandsins verið lögð aukin áhersla á að aðildarlönd sambandsins greini áhættur sem steðji að 5G netum landanna og uppbyggingu þeirra með tilliti til birgjakeðju 5G búnaðar.

Í kjölfar innrásar Rússlands í Úkraínu í febrúar 2022 sendu ráðherrar fjarskiptamála innan Evrópusambandsins frá sér ákall um styrkingu netöryggis fjarskiptainnviða. Um er að ræða skjal frá 9. mars 2022 en þar er m.a. óskað eftir að aðilar líkt og BEREC, ENISA og framangreindur samráðshópur, ynnu að tilmælum/leiðbeiningum, sem byggðu á niðurstöðu áhættumats, til aðildarríkja og framkvæmdastjórnar til að auka áfallapol fjarskiptaneta og fjarskiptainnviða í Evrópu, þ.m.t. 5G neta.

Í febrúar 2024 birti NIS Cooperation Group skýrslu sem byggði á niðurstöðum áhættumats sem aðildarríkin framkvæmdu á tímabilinu apríl 2022 og desember 2023 innan hópsins, með stuðningi framkvæmdastjórnarinnar og ENISA og í samráði við BEREC. Þar eru settar fram tegundir ógna, veikleika og sviðsmynda áhættu sem og að settar eru fram ákveðin tilmæli hvað varðar stefnumótandi og tæknileg atriði. Í þessu verkefni er nauðsynlegt að horft verði til framangreindra og væntanlegra leiðbeininga frá Evrópu, sem og annarra sem kunna að eiga við.

Stofnunin hefur hafið kortlagningu útivistunar og aðfangakeðju fjarskiptafyrirtækja á nauðsynlegri starfsemi fyrir virkni, vernd og stjórnun fjarskipta með það að markmiði að fá yfirsýn yfir ógnir sem stafa af útivistun ásamt því að kanna hlítu við sér ákvæði um útivistun í 6. og 7. mgr. 78 gr. fjarskiptalaga sem og kröfur sem tilgreindar eru í reglum, alþjóðlegum

⁹ stjornartidindi.is/Advert.aspx?RecordID=aac6a5d6-3617-4955-853c-abaf4ac5c1d3



viðmiðunum um bestu framkvæmd sem og þeim leiðbeiningum sem gefnar hafa verið út í Evrópu.

Markmið verkefnisins er að:

- kortleggja og meta regluverk og tillögur Evrópusambandsins varðandi öryggi farneta, þ.m.t. 5G,
- kortleggja aðgerðir einstakra landa innan EES í þessu samhengi,
- að greina gildandi íslensk lagaákvæði varðandi öryggi farneta með tilliti til öryggis útvistunar og birgjakeðju farneta og þróunar innviða þeirra,
- að fá fram áhættumat íslensku fjarskiptafélaganna á öryggi útvistunar og birgjakeðju farneta,
- og setja fram tillögur um aðgerðir FST og annarra stjórnvalda til að auka öryggi far neta á Íslandi.



7. Lokaorð

Í þessu skjali hefur Fjarskiptastofa sett fram sýn sína á eftirliti með net- og upplýsingaöryggi stafræna grunnvirkja, veitendum stafrænnar þjónustu og fjarskiptafyrirtækjum. Í upphafi skjalsins er farið yfir stefnuna og því næst er almenn umfjöllun um net- og upplýsingaöryggi. Í næstu tveimur köflum er fjallað um þá löggjöf sem stefnan nær til, þ.e. annars vegar fjarskiptalögin og hins vegar netöryggislögin.

Markmið eftirlits Fjarskiptastofu er til umfjöllunar í fjórða kafla, en meginmarkmið þess er að stuðla að auknu öryggi og viðnámsþrótti í net- og upplýsingakerfum fjarskiptafyrirtækja, stafrænum grunnvirkjum og hjá veitendum stafrænnar þjónustu gagnvart net- og upplýsingaöryggisógnum. Markmið Fjarskiptastofu er að í lok árs 2027 verði öryggisskipulag, áhættustýring og viðbúnaður aðila í samræmi við alþjóðleg bestu viðmið um framkvæmd á þessu sviði.

Í köflum fimm og sex er umfjöllun um högun eftirlits Fjarskiptastofu og aðferðafræði. Fimmti kafli fjallar um almennt eftirlit stofnunarinnar, sem nær til sjálfsmats fyrirtækja, úttekta og prófana og eftirfylgni með bindandi fyrirmælum. Í sjötta kafla er fjallað um sértækt eftirlit, en til þess telst áhættumat fjarskiptainnið, sértækt áhættumat, rannsóknir og kortlagning á öryggi útvistunar og birgjakeðju farneta.

Að mati stofnunarinnar er mikilvægt að sjónarmið hagsmunaaðila á þessa sýn stofnunarinnar komi fram. Fjarskiptastofa leggur sig fram að upplýsa og óska eftir umsögnum eftirlitskyldra aðila þegar verulegar breytingar eru á stefnumörkun eftirlits eða aðferðafræði eftirlits, þar með talið er að viðhafa opið samráð um stefnu um fyrirkomulag og framkvæmd eftirlits. Í febrúar 2025 óskaði Fjarskiptastofa eftir sjónarmiðum og athugasemdum frá hagsmunaaðilum hvað varðar efni þessara stefnu með því að setja drögin í opið samráð á heimasíðu stofnunar og útsendingu tilkynningar á póstlista Fjarskiptastofu. Fjarskiptastofu þakkar fyrir innsendar umsagnir en stofnunni bárust þrjár umsagnir. Niðurstaða yfirferðar var ekki tilefni til efnislegra breytinga en framsetning og orðalag var breytt á völdum stöðum til að bæta skýrleika og gagnsæi stefnunnar.

Stofnunin áréttar sem fram hefur komið í skjali þessu að markmið stofnunarinnar hlýtur að fara saman með markmiðum eftirlitskyldra aðila, þ.e. stuðla að auknu öryggi og viðnámsþrótti net- og upplýsingakerfa hjá aðilunum gagnvart net- og upplýsingaöryggisógnum. Óskar stofnunin því eftir farsælu samstarfi við rekstraraðila stafrænna grunnvirki, veitendur stafrænnar þjónustu og fjarskiptafyrirtækja til að ná þessum markmiðum.