Vabariigi Valitsuse määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ eelnõu seletuskirja juurde

Lisa 2

SE 531 KOOSKÕLASTUSTE JA MÄRKUSTE TABELI II OSA TÄIENDATUD TAGASISIDE

	II Kavandatavate rakendusaktidega seotud tagasiside	
	Käesoleva lisa eesmärk on lihtsustada Vabariigi Valitsuse määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ tagasisidestamist. Dokumendis on kajastatud muutmata kujul SE 531 kooskõlastamise raames esitatud märkuseid SE 531 lisana esitatud rakendusaktide kavandite osas. Muudetud kujul on esitatud Majandus- ja Kommunikatsiooniministeeriumi kommentaarid ja selgitused esitatud märkustele, kajastamaks käesoleva eelnõu hetkeolukorda ja vastavaid selgitusi. Palume arvestada, et muutmata märkuste viited määruse eelnõu paragrahvide numbritele on ajakohastamata. Samuti juhime tähelepanu, et olulise lisandina SE 531 raames esitatud rakendusakti kavandile käesoleva määruse eelnõu poolt on käsitletav 2. jao 3. jaotis (Pilvsüsteem).	
	1. Justiitsministeerium esitas järgnevad märkused seoses eelnõu § 7 lõike 5 alusel kehtestatava Vabariigi Valitsuse määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ kavandiga	
21.	Määruse eelnõu § 3 lg 3 kohaselt kehtestab Eesti Infoturbestandardi (E-ITS) valdkonna eest vastutav minister määrusega. Kuna tegu on üleriigilise standardiga, mis loob kohustusi kõikidele teenuse osutajatele, teeme ettepaneku vastav standard kehtestada Vabariigi Valitsuse määruse tasandil.	**Mittearvestatud.** EITS on infoturberaamistik. Küberturvalisuse tagamise korraldamise eest vastutava ministri määruse kohaldamisala saab olla, vastava volituse korral, võrdeline küberturvalisuse seaduse kohaldamisalaga. Selgitame, et sarnaselt hetkel kehtiva ISKE-ga on ka E-ITS pidevat kaasajastamist ning täiendamist nõudev dokument. Majandus- ja Kommunikatsiooniministeeriumi valitsemisala asutus RIA korraldab E-ITS-i täiendamise ning uuendamisega seotud teenuseid, võttes selle aluseks varasemase rakendamise praktikat ning muutusi infotehnoloogilises maailmapildis ja õigusraamistikes. Tulenevalt

		eeldatavast vajadusest E-ITS-i korduvalt muuta ja ajakohastada, ei ole Vabariigi Valitsuse määruse vorm sobilik E-ITS-i kehtestamiseks.
22.	Määruse eelnõu § 4 lg 1 kohaselt viiakse auditeerimine läbi vastavalt küberturvalisuse seaduse (KüTS) § 7 lg-le 5 ning määruse § 3 lg 3 kohaselt. Tõenäoliselt on siin kogemata tekkinud viide valele sättele, sest KüTS § 7 lg 5 sisaldab volitusnorme määruste kehtestamiseks, kuid ei reguleeri auditeerimise korraldust. Palun vaadake viide üle.	**Arvestatud.** Määruse eelnõu § 4 lõikest 1 eemaldatakse viited KüTS § 7 lõikele 5 ja määruse eelnõu § 3 lõikele 3. Selgitame, et infoturbe korralduse, sh etalonturbe rakendamise, auditeerimine ei ole eraldiseisev E-ITS-st, vaid on selle üks osa E-ITS-i tingimustest tulenevalt. Kavandatava ministri määruse eelnõu kehtestab ühe E-ITS-i dokumendina ka auditeerimisjuhendi. Tagasiside aluseks olev määruse eelnõu § 4 kehtestab aga Vabariigi Valitsuse tasandil nõuded auditi läbiviimise sagedusele, sätestab auditi järeldusotsuse edastamise kohustuse ning auditi läbiviimise kohustuse erandid.
23.	Määruse eelnõu § 4 lg 2 seab teenuse osutajale (kelleks on sisuliselt kõik Justiitsministeeriumi haldusala asutused) kohustuse auditi järeldusotsuse edastamiseks. Piisavaks tuleks pidada, kui vastava otsuse edastab auditi tellija (st KüTS EN sõnastuse vaatest üks teenuse osutajatest).	**Teadmiseks võetud.** Selgitame, et eesmärk on võimaldada ühisauditite tellimist ning läbiviimist. Eelnõu seletuskirjas on täiendavalt kirjeldatud auditi edastamise delegeerimist.
24.	Määruse eelnõu § 4 lg 3 p 2 kohaselt loetakse auditi läbiviimise kohustus täidetuks, kui tegu on perearstiga. Juhime tähelepanu, et perearstid töötlevad mh eriliigilisi isikuandmeid, mistõttu kontroll teabeturbe osas võib osutuda olulisemaks kui mõne muu asutuse väiksema andmekogu puhul.	**Teadmiseks võetud.** Määruse eelnõus on auditi läbiviimise erandit muudetud perearsti määratlusest mikroettevõtja määratlusele. Selgitame, et lisaks perearstidele võivad ka muud KüTS-i mõistes teenuse osutajad töödelda olulise kaitseväärtusega andmeid, kuid see ei ole auditeerimise erandi loomise aluseks.

		Eesmärk on tagada auditi läbiviimise mõju proportsionaalsus subjekti IKT korralduslike võimetega. Kommenteeritava erandi puhul on tegemist väikesemahuliste organisatsioonidega, kelle IKT korralduslikud vahendid on oluliselt piiratumad ning seetõttu võib ka auditi lävendiline majanduslik mõju olla organisatsioonile ebaproportsionaalselt suur. KüTS-i subjektidest on mikroettevõtjad enamasti teede sõidetavust tagavad ettevõtjad (subjektid KüTS § 3 lg 1 p 1 alusel hädaolukorra seadusest tulenevalt) ning mitmed perearstid (subjektid KüTS § 3 lg 1 p 7 alusel). Samas perearstikeskused, mis ületavad mikroettevõtja lävendit, alluvad auditeerimiskohustusele.
25.	Määruse eelnõu § 4 lg 3 p 3 kohaselt loetakse auditi läbiviimise kohustus täidetuks valitsusasutuse hallatava riigiasutusega ning sellele isikule kohaldatakse KüTS §-s 7 sätestatud kohustusi ainult sama seaduse § 3 lõike 4 alusel. Sellest tulenevalt väheneks isegi IT-asutuste kohustused ning nii Registrite ja Infosüsteemide Keskus kui ka teised IT-majad ei ole kohustatud enam auditeid tellima. Kas see on aga olnud ikka eesmärk võttes arvesse teabe töötluse ulatust IT-majades?	**Teadmiseks võetud.** Määruse eelnõus on auditi läbiviimise erandit täpsustatud avaliku sektori asutuste suhtes. IT-asutustele erandid ei kohaldata. Selgitame, et eesmärk on vabastada asutused, mille IKT korralduslikud vahendid on oluliselt piiratumad tulenevalt IKT vahendite väiksemast olulisusest asutuse avalike ülesannete täitmisel. Avalikus sektoris sõltub asutuse IKT struktuuri mahukus ning selle IKT struktuuri turvalisuse kriitilisus ühiskonna toimepidevusele rohkem asutuse ülesannetest kui asutuse organisatsioonilisest suurusest.
26.	Määruse eelnõu 3-nda peatüki 1. jagu ületab määruse kehtestamise aluseks oleva seaduse (KüTS §-is 1 sätestatud) reguleerimis- ja kohaldamisala. Nimelt KüTS § 1 kohaselt kohaldub seadus ühiskonna toimimise seisukohast oluliste ning avaliku sektori võrgu ja infosüsteemidele. Määruse eelnõu § 5 sõnastus hõlmab aga kõiki teenuseid (st mitte üksnes võrgu- ja infosüsteeme), ületades reguleerimisala. Sellega seoses tuleks muuta § 5 sõnastust. KüTS §-is 1 sätestatud reguleerimis- ja kohaldamisala ei tohiks laiendada kõikidele teenustele. Ühtlasi tekitab segadust EITS (Eesti infoturbe standard) juhis, mis räägib omakorda hoopis äriprotsessidest, mitte võrgu- ja infosüsteemidest. Palun vaadake need sätted üle ja parandage vastavalt.	**Mittearvestatud.** Määruse eelnõu § 5 allub KüTS kohaldamisala piiridele. Selgitame täiendavalt, et KüTS reguleerimis- ja kohaldamisalaks ei ole võrgu- ja infosüsteemid (süsteem), vaid süsteemide pidamine. Teenusena käsitletakse erasektori puhul teenuseid, mille alusel isik on KüTS subjekt ning teenuste kaardistus dokumenteeritakse koos selle haldamise süsteemi, rakendatavate turvameetmete ja riskianalüüsiga. Avaliku sektori puhul on kaardistamine laiem ning teenuste kaardistamisel saab

		subjekt lähtuda TKTA määrusest[1]. Teenuste kaardistus dokumenteeritakse koos selle haldamise süsteemi, rakendatavate turvameetmete ja riskianalüüsiga.
27.	Vaadates määruse eelnõu § 4 ja § 6 sõnastust, siis kas mõistame õigesti, et auditid tuleb läbi viia mitte üksnes andmekogude osas, vaid kõikide võrgu- ja infosüsteemide osas, kuid turvaklass määratakse üksnes andmekogudele? Ühtlasi on hetkel rakenduslikust vaatest arusaamatu, mida mõeldud turvalisuse puudumisest tuleneva kahju hindamise all. Palun selgitage.	**Teadmiseks võetud.** Selgitame täiendavalt, et turvaklassi määramine säilitatakse andmekogude suhtes ning selle praktiline väljund rakendatavate turvameetmete osas tuleneb turvaklassi teisendamisest kaitsetarbeks, mis on osa E-ITS-i metoodikast. Teiste infosüsteemide puhul ei ole teisendamine vajalik, kuivõrd turvaklassi asemel määratletakse kaitsetarve E-ITS-i metoodika alusel. Audit viiakse läbi organisatsiooni vaatest. Andmete turvalisuse puudumisest tulenev kahju hindamine on protsess, mis koos andmete tähtsuse hindamise protsessiga moodustab andmekogu andmete turvaanalüüsi ning sellest tulenevalt määratakse andmekogu turvaklass. Täpsemad selgitused on esitatud määruse eelnõu seletuskirjas.
28.	Määruse eelnõu § 9 lõikes 3 kehtestatud käideldavuse turvaosaklassi K1 ja K2 vahel on võrdlemisi suur (K1 lubatud seisak nädalas ööpäev, K2 seisak 2 h, K3 seisak 10 min), mis võib tekitada olukorra, kus andmekogu vastutav töötleja määrab kõrgema osaklassi vaid seetõttu, et K1 osaklass võimaldab liiga pikka seisakut. Sellega seoses teeme ettepaneku vähendada osaklasside vahet.	**Mittearvestatud** Selgitame, et turvaosaklasside K lävendid ei ole määratletud lineaarse skaalana, vaid astmelise skaalana. Kui töökindlus on oluline, siis peab vastutav töötleja hindama, kas lubatav seisak nädalas on mõõdetav kuni päeva, üksikute tundide või üksikute minutite piires. Lubatavad summaarsed seisakud on pöördvõrdelised nõutava töökindlusega. See tähendab, et minimaalne nõutav töökindlus kujutab maksimaalset lubatavat seisakut vastavas osaklassis. Teisisõnu, kui K1

[1] Vabariigi Valitsuse 25.04.2017 määrus nr 88 „Teenuste korraldamise ja teabehalduse alused“, RT I, 25.03.2021, 6.

		osaklass lubab liiga pikka seisakut, aga K2 lubatav seisak on liiga lühike, siis määrab vastutav töötleja turvaosaklassiks K1, sest nõutav töökindlus jääb vastutava töötleja hinnangul vahemikku 90%-99%. Eelnõu koostajad ei näe, kuidas vastutav töötleja peaks määrama kõrgema turvaosaklassi lihtsalt seetõttu, et K1 lubatav seisak on liiga pikk. Oluline on hinnata, mis lävendit nõutav töökindlus ületab.
29.	Määruse eelnõu § 11 kehtestab süsteemid, millel on oluline mõju riigi ja kohaliku omavalitsuse üksuse võimele täita avalikke ülesandeid. Ühtlasi on ka teisi võrgu- ja infosüsteeme, mis omavad olulist mõju avalike ülesannete täitmisele. Näiteks puudub nimekirjas mh riigi andmeside võrk (ASO võrk), allkirjastamise ja autentimise süsteemid, millest sõltuvad väga paljud teised võrgu- ja infosüsteemid (sh avalike ülesannete täitmine). Loetletud andmekogude ja infosüsteemide nimetused vajavad täpsustamist, palun vaadake loetelu üle.	**Mittearvestatud.** Selgitame, et lähtudes MKM-i küberturvalisuse strateegiast 2019-2022 on kõige enam kaitset vajavateks digitaalseteks varadeks põhiandmed kodanike, riigi territooriumi ja õigusloome kohta[2]. Kriitiliste andmekogude töörühm, mis käis koos MKM-i juhatamisel selgitasid välja avalike ülesannete täitmist oluliselt mõjutavad süsteemid, mis on ka küberjulgeoleku nõukogu[3] poolt kinnitatud. Sama kinnitatud loetelu alusel ongi koostatud määruses toodud loetelu. Täpsemad selgitused on esitatud eelnõu seletuskirjas.
30.	Määruse eelnõu § 12 lõike 3 kohaselt ei ole võimalik IT-asutustel rakendada ISO standardit määruse eelnõu §-is 11 toodud infosüsteemide osas. Hetkel ei ole arusaadav, miks selline erisus on tehtud. Kui asutus otsustaks rakendada ISO standardit, siis EITS rakendamine üksnes osadele süsteemidele toob kaasa täiendava ressursi kulu. Teeme ettepanku, et regulatsioon toetaks laiemalt turbestandardi valikut asutuste poolt.	**Arvestatud.** Eelnõust on viidatud säte kustutatud.
	2. Siseministeerium esitas järgnevad märkused	

[2] Majandus- ja Kommunikatsiooniministeerium. Küberturvalisuse strateegia 2019-2022, lk 24. Kättesaadav: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf.

[3] 2009. aastal alustas Vabariigi Valitsuse julgeolekukomisjoni juures tööd küberjulgeoleku nõukogu, mille ülesanne on aidata kaasa ametkondade koostöö toimimisele ja teha järelevalvet küberjulgeoleku strateegia eesmärkide elluviimise üle. Nõukogu esimees on ettevõtlus- ja infotehnoloogiaminister ning nõukogu juhib MKM-i kantsler.

31.	Seletuskirjas on toodud lause: "Eelnõu koostamise hetkel kavandatav Vabariigi Valitsuse määrus sätestab kohustuse järgida E-ITS-i ning rakendada selle järgimisest tulenevaid turvameetmeid, kusjuures E-ITS-i järgimine seisneb E-ITS tingimuste täitmises infoturbe halduse käivitamisel, rakendamisel, käigushoidmisel ning täiustamisel ja E-ITS-i tingimuste täitmise auditeerimises." Selle lause kohaselt võib aru saada, et E-ITS-i rakendamine on kohustuslik ja ainuke valik. Samas on erinevatel EITS-iga seotud kohtumistel ja koolitustel toodud välja, et võib rakendada ka ISO standardit.	**Teadmiseks võetud.** Selgitame, et E-ITS-i asemel võib tõesti rakendada ISO standardit ning vastav võimalus on ka määruse eelnõus esitatud.
32.	Juhime tähelepanu olukorrale, mis tekib kui Vabariigi Valitsuse määruse eelnõu kavand „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ pakutud sõnastuses jõustub. Antud määruse eelnõu kavandi § 3 lõige 1 ja 4 kohaselt lubatakse teenuse osutajal rakendada turvameetmeid, mis vastavad rahvusvahelise standardi ISO/IEC 27001 kehtestatud nõuetele. Samas aga piirab § 12 lõige 3 ISO/IEC 27001 standardis kehtestatud nõuete kasutamist juhul, kui tegu on § 11 nimetatud süsteemiga. Antud juhul siis on § 11 punktis 11 nimetatud rahvastikuregister. Selline piirang viib olukorrani, kus Siseministeerium ja Siseministeeriumi infotehnoloogia- ja arenduskeskus peavad hakkama juurutama paralleelselt Eesti Infoturbestandardi tingimusi ainult rahvastikuregistri jaoks, aga teiste infosüsteemide jaoks saab kasutada ISO/IEC 27001 kehtestatud nõudeid.	**Teadmiseks võetud.** Eelnõust on viidatud säte kustutatud.
33.	Eelnõus on käsitlemata, kuidas täpsemalt määratletakse andmekogude ja äriprotsesside kaitsetarvet (vana nimega turvaosaklassid). Ära on määratud, mis tase vastab endisele kõrgkäideldavusele või kõrg-terviklikkuse turvaosaklassile, kuid pole täpselt välja toodud, kuidas selleni jõutakse. Palume seletuskirja selles osas täiendada.	**Arvestatud.** Seletuskirja on täiendatud andmekogude turvaosaklasside määramise selgitamisega. E-ITS-i alusel kaitsetarbe määramine toimub E-ITS-i dokumentatsiooni alusel.

34.	Riigi Infosüsteemi Amet peaks välja töötame E-ITS-i tööriista, mis aitaks kiirendada ja viia efektiivsemalt praktikasse uut infoturbe standardit. Antud vajadus ilmnes juba eelmise infoturbe standardi ISKE-ga, kus see puudus mitmeid aastaid ja paljud tegid seda oma äranägemise järgi. Mõistlik oleks seda üle riigi ühtlustada või vähemalt osa sellest.	**Teadmiseks võetud.**
	3. Rahandusministeerium esitas järgnevad märkused	
35.	Eelnõu § 1 punktiga 8 täiendatakse KüTS § 7 lõikega 5, mis sisaldab volitusnormi süsteemide küberturvalisuse tagamiseks vajalike nõuete, sh E-ITS-i kehtestamiseks. Sellega seoses tunnistatakse kehtetuks avaliku teabe seaduse § 43^9 lõike 1 punkt 4 volitusnorm infosüsteemide turvameetmete süsteemi kehtestamiseks. Muudatustega kaasajastatakse ning viiakse infoturbe tagamine andmekogude põhiselt lähenemiselt võrgu- ja infosüsteemide lähenemisele. Seega võimaldab muudatus aegunud infosüsteemide kolmeastmelise etalonturbe süsteemi asendada uue Eesti Infoturbestandardiga (E-ITS). Eelnõu seletuskirja lisa 2 (rakendusaktide kavandid) sisaldab Vabariigi Valitsuse määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ kavandit (edaspidi *kavand*). Kavandi § 10 lõike 2 kohaselt on turbeastmele kõrge (H) vastav E-ITS-i kaitsetarve väga suur (VS), turbeastmele keskmine (M) vastav kaitsetarve suur (S) ning turbeastmele madal (L) vastav kaitsetarve normaalne (N). Kavandi §-s 11 on loetelu avalike ülesannete täitmist oluliselt mõjutatavate süsteemidest. Nõustume, et on asjakohane loetleda avalike ülesannete täitmist oluliselt mõjutavad süsteemid ja maksukohustuslaste register ning e-riigikassa on olulised süsteemid. Kuivõrd nende andmeid varundatakse välisriigis asuvasse turvalisse andmekeskusesse, on vastava volitusnormi loomine igati asjakohane. Lisaks soovitame	**Arvestatud.** Eelnõust on eemaldatud säte, mis kohustab avalike ülesannete täitmist oluliselt mõjutavate süsteemide loetelus kehtestatud süsteemidele rakendama kaitsetarvet väga suur (VS).

	kaaluda ka normi lisamist, mis laiendaks krüptovõtmete hoidmise võimalusi, et vähendada võimalikke riske. Kavandi § 12 lõike 2 kohaselt on §-s 11 nimetatud süsteemide (sh riigikassa infosüsteem ja maksukohustuslaste register) kaitsetarve E-ITS-i tähenduses on väga suur (VS), mis tähendab, et täitmaks tulevikus määrust, peab nii maksukohustuslaste registrile kui riigikassa infosüsteemile rakendama kõrgmeetmeid, mis praegu vastavad turbeastmele kõrge (H).[4] Märgime, et vastavalt Vabariigi Valitsuse 7. märtsi 2019. a määruse nr 21 „Maksukohustuslaste registri põhimäärus“ § 74 lõikele 3 on infosüsteemi turbeaste keskmine (M). Määrates maksukohustuslaste registrile infosüsteemi turbeaste keskmine (M) asemel turbeastmeks kõrge (H), mis edaspidi Eesti Infoturbestandardi kohaselt tähendab, et kaitsetarve on väga suur (VS), see aga toob kaasa märkimisväärsed kulud H taseme kohustuslike meetmete, edaspidi kõrgmeetmete rakendamiseks. Muutus mõjutab samuti Maksu- ja Tolliameti ning Rahandusministeeriumi Infotehnoloogiakeskuse töökorraldust ja nõudeid andmete töötlemisele. Muutus mõjutab ka e-riigikassa süsteemi, mille turbeastmeks on hetkel määratud samuti (M). Määruse seletuskirjast ei selgu, millistele andmetele või analüüsile tugineb maksukohustuslaste registri ja e-riigikassa infosüsteemi kaitsetarve muutmine seniselt väga suurele (VS). Vastavalt standardile väljendab kaitsetarve äriprotsessi infoturbe vajadust. Hinnang äriprotsessi kaitsetarbele tuleneb eelkõige äriprotsessi poolt töödeldava teabe kaitsetarbest, sh andmekogu turvaklassist. Kaitsetarbe määramine võib toimuda näiteks äritoime analüüsi tulemuste põhjal. Kui	

[4] Lisainformatsioon täiendavalt rakendatavatest kõrgmeetmetest on kirjeldatud vastavustabelis ISKE meetmetele, kus näidatud E-ITS etalonturbe mooduli meetmete ja ISKE 8.06 meetmete omavahelisi seoseid (https://eits.ria.ee/et/versioon/2020vers1/standardi-dokumendid/vastavustabelid/#vastavustabeliskemeetmetele2).

	sellekohane analüüs on läbi viidud, siis palume vastav analüüs Rahandusministeeriumile edastada. Arvestades eeltoodut ei saa Rahandusministeerium kavandit kooskõlastada enne, kui Majandus- ja Kommunikatsiooniministeerium on teostanud analüüsi ja leidnud rahastuse kavandi § 11 punktides 9 ja 10 nimetatud süsteemide nõuetele vastavaks viimise ja ülalhoiu kuludeks tingimuses, kus tekib kohustus rakendada kõrgmeetmeid lähtudes väga suurest kaitsetarbest (VS). Samuti palume selles osas täiendada seletuskirja mõju osa, nii rahalises vaates kui ka E-ITS kehtestamise tingimuste osas.	
36.	Määruse § 12 lõiked 2 ja 3 välistavad Rahandusministeeriumi valitsemisalas ülemineku Eesti siseriiklikult, küll uuenevalt, aga rahvusvaheliselt tunnustamata infoturbe raamistikult, üldtunnustatud ISO/IEC 27001 infoturbestandardile kui kõik E-ITS-i kohustuslikud meetmed on täidetud. Peame vajalikuks jätta otsustuspädevus ministeeriumide valitsemisalasse ja hõlbustada toimivate sidusate lahenduste juurutamist ühtses tollialas, nii Euroopa Liidu üleselt, kui ka vastavalt riikide vahelisele koostööle ja kehtivatele koostöölepetele sh ühine võitlus terrorismi rahastamise ja rahapesuga. Seega peame vajalikuks, et E-ITS kohustuslike meetmete rakendamisel §-s 11 nimetatud süsteemide puhul ei välistataks ISO/IEC 27001 infoturbestandardi rakendamist.	**Arvestatud.** Eelnõust on eemaldatud säte, mis välistaks ISO kohaldamise erandi.
37.	Palume eelnõus kontrollida eelnõu ja seotud rakendusaktide kavandatavad jõustumise ajad. Näiteks kavandi § 12 lõige 2 jõustub § 15 lõike 1 kohaselt juba 2022.a, mille tulemusena peaks §-s 11 nimetatud süsteemid vastama turbeastmele (VS) ehk tänases mõistes astmele (H) juba 2022. aasta algusest. Selgitame veelkord, et süsteemidele kõrgema turbeastme nõuete rakendamine eeldab nii aja- kui finantsressursse ning protseduuriliste jm reeglite muutmist ning	**Teadmiseks võetud.** Selgitame täiendavalt, et kavandatava määrusega sätestatakse küll E-ITS-i järgimise kohustus, kuid E-ITS-i järgimise kohustuse täitmine ei tähenda, et rakendaja on järgmiseks päevaks kõik vastavad turvameetmed rakendanud. E-ITS-i järgimine on protsess, mitte seisund, ning see algab

	Rahandusministeerium ei saa kavandi kohast määruse eelnõu kooskõlastada enne käesoleva kirja punktis 1 nimetatud analüüsi teostamist ning lisarahastuse tagamist.	üldjuhul juhtkonna tasemel küberturvalisuse tagamise pühendumuse tegemisest ning infovarade kaardistamisest.
38.	Ühtlasi palume selgitada, kas kavandi § 11 punktides 4 ja 5 nimetatud riigi- ja kohaliku omavalitsuse register ning mittetulundusühingute ja sihtasutuste register on käsitletavad eraldi süsteemidena või on tegemist e-äriregistri keskkonna osaga.	**Teadmiseks võetud.** Selgitame, et kuigi eesmärk on tagada e-äriregistri keskkonna toimepidevus, siis tuleb süsteemide loetelus lähtuda nende süsteemide juriidilistest nimetustest. Seetõttu on määruses nimetatud registri ametlikud nimetused, mis kogumina moodustavad e-äriregistri keskkonna.
	4. Maaeluministeerium esitas järgneva märkuse	
39.	Seaduseelnõu seletuskirja lisa 2 Vabariigi Valitsuse määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ kavandi 3. peatüki 2. jao 1. alljaotises kasutatakse mõisteid „turvaklass“ ja „turbeaste“, need mõisted on siiani tulnud Vabariigi Valitsuse 20. detsembri 2007. a määrusest nr 252 „Infosüsteemide turvameetmete süsteem“. Eelnõuga tunnistatakse nimetatud määruse volitusnorm kehtetuks ja kehtima hakkav Eesti Infoturbestandard (edaspidi E-ITS) selliseid mõisteid ei kasuta, kuid samad mõisted esitatakse seletuskirja lisas rakendusakti kavandis uuesti. E-ITS annab kasutuseks võrdväärse mõiste „kaitsetarve“ ja sisustab selle võrdväärsete tasemetega, mille võrdlus turbeastmega on ka rakendusakti kavandis toodud. Samuti nimetab E-ITS turvaosaklasside tähise K-T-S ümber ingliskeelseks C-I-A (Confidentiality, Integrity, Availability). Leiame, et kahe võrdväärse mõiste turbeastme või kaitsetarbe määramise metoodika kehtestamine lisab keerukust. Sellise lähenemise otstarve aga jääb arusaamatuks. Teeme ettepaneku ühtlustada metoodikad rakendusakti ja E-ITS vahel.	**Teadmiseks võetud.** Selgitame, et kommenteeritud määruse kavandi vastava osa eesmärk on kehtestada küberturvalisuse nõuete erisused andmekogude pidamisel. Andmekogu on AvTS-s reguleeritud süsteemi eriliik, millele rakenduvad ka eelmainitud seaduse alusel mitmed nõuded. Andmekogude küberturvalisuse tagamiseks rakendati varasemalt ISKE nõudeid, mis omakorda olid koostatud andmekogu kui süsteemi vaatepunktist. E-ITS-i kehtestamisel ISKE asemele uueneb mõnevõrra ka küberturvalisuse tagamiseks rakendatavate nõuete loogika, seda ennekõike süsteemipõhise lähenemise asendamisel organisatsiooni ja selle protsesside põhiste lähenemisega. Arvestades aga vajadust säilitada andmekogude kui eriliigiliste süsteemide turbeastme määramine ennekõike andmekogu andmete tähtsusest lähtuvalt (erinevalt E-ITSi riskipõhisest kaitsetarviduse määramisest infovarade olulisuse kaudu protsessi eesmärgi täitmisel) ning säilitada riigi infosüsteemi haldussüsteemi ja seekaudu ka andmekogude põhimääruste regulatiivne sisu turvaosaklasside ja nendest

		tulenevate turbetasemete osas, on alljaotise eesmärk võtta üle kehtetuks tunnistatavast infosüsteemide turvameetmete süsteemist andmekogude turbeastmete regulatsioon ning ühildada see E-ITSi rakendamisega organisatsioonis, mis on andmekogu vastutav või andmekogu majutav volitatud töötleja. Kavandatava määruse kooskõlastamisel esitatav seletuskiri käsitleb ka iga konkreetse sätte eesmärki ja vajalikkust täiendavalt.
	5. Sotsiaalministeerium esitas järgneva märkuse	
40.	Eelnõu seletuskirja lisast 2 (rakendusaktide kavandid) nähtub, et üleminekusätteid on plaanitud sätestada ka KüTS § 7 lõike 5 alusel kehtestatava määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ §-s 14. Palume kaaluda auditeerimise kohustuse ülemineku tähtaegade sätestamist seaduse tasemel ning vastavalt täiendada eelnõu ja seletuskirja rakendussätete osa. Nimetatud rakendusakti kavandi §-s 14 sätestatud üleminekusätetest ei selgu üleminekuperioodi kestus. Nimetatud paragrahvis sätestatu kohaselt on teenuseosutaja kohustatud E-ITS nõuetele vastava auditeerimise viima läbi nelja aasta jooksul pärast viimast ISKE järgi tehtud turvameetmete süsteemi auditeerimist. Samas on märgitud, et E-ITS nõuetele vastava esimene auditeerimine peab teenuseosutajal olema läbi viidud *mitte hiljem kui* 2025. aasta 1. jaanuariks. Kuivõrd ajavahemik 2023. aasta 1. jaanuarist kuni 2025. aasta 1. jaanuarini ei ole neli aastat, palume üleminekuperioodi täpsustada ja seletuskirjas vastavalt lahti selgitada.	**Teadmiseks võetud.** Selgitame, et auditeerimise kohustus on üks osa E-ITS-i järgimise kohustusest. Sellest tulenevalt puudub vajadus reguleerida auditeerimise kohustuse ülemineku tähtaegade sätestamist seaduse tasemel. Sarnaselt sätestas Vabariigi valitsuse ISKE määrus esimese auditi läbiviimise tähtajad. Olukorras, kus hiljemalt 2022. aastal läbiviidud ISKE audit võimaldaks järgmise E-ITS-i auditi läbiviimise tähtaega viia kaugemale kui 2025. aasta 1. jaanuar, rakendatakse E-ITS auditi läbiviimise tähtajaks 2025. aasta 1. jaanuari. ISKE auditi läbiviimine ei tähenda, et nõuded on täidetud järgnevaks neljaks („L“ turbeastmega andmekogude suhtes) aastaks. See tähendab, et auditi läbiviimise hetkel on teada küberturvalisuse tagamiseks rakendatud meetmed. Ei eeldata, et õigusakti jõustumisele järgneval päeval on E-ITS-i järgimisega jõutud auditeeritava tasemeni, kuid E-ITS-i järgimise kontrollimise viimaseks tähtajaks jääb kolm aastat pärast nõuete järgimise kohustuse tekkimist.
	6. Eesti Energia AS esitas järgneva märkuse	
41.	Lisaks ei saa nõustuda eelnõus oleva Vabariigi Valitsuse määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 5 lõikega 3, mis	**Teadmiseks võetud.**

	kohustab säilitada dokumentatsiooni 7 aastat selle koostamisest ja see tuleb teha RIA-le kättesaadavaks vastava taotluse korral. Hetkel kehtiva seaduse § 7 lõike 2 punkti 6 järgi tuleb dokumente säilitada 3 aastat (see punkt tunnistatakse eelnõuga kehtetuks). 7 aastat on infotehnoloogias väga pikk aeg ja on raske mõista, mis väärtust pakuvad RIA-le 7 aasta tagused riskianalüüsid või sel hetkel rakendatud turvameetmete info. Eriti arvestades veel nõuet, et sõltumatu audit või sertifitseerimine tuleb läbi viia iga 3 aasta järel.	Selgitame, et tähtaja määratlemisel on lähtutud asjaolust, et see tähtaeg katab ära vähemalt kaks auditiperioodi (3+3 aastat) ning ühe aastase täiendava tähtaja. Nimetatud tähtaeg võimaldab järelevalveasutusel ka planeerida enda järelevalvelisi tegevusi.