DERINIMO PAŽYMA
DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS 2013 M. LIEPOS 24 D. NUTARIMO NR. 716 „DĖL BENDRŲJŲ ELEKTRONINĖS INFORMACIJOS SAUGOS REIKALAVIMŲ APRAŠO, SAUGOS DOKUMENTŲ TURINIO GAIRIŲ APRAŠO IR ELEKTRONINĖS INFORMACIJOS, SUDARANČIOS VALSTYBĖS INFORMACINIUS IŠTEKLIUS, SVARBOS ĮVERTINIMO IR VALSTYBĖS INFORMACINIŲ SISTEMŲ, REGISTRŲ IR KITŲ INFORMACINIŲ SISTEMŲ KLASIFIKAVIMO GAIRIŲ APRAŠO PATVIRTINIMO“ PAKEITIMO“, LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS 2018 M. RUGPJŪČIO 13 D. NUTARIMO NR. 818 „DĖL LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO ĮGYVENDINIMO“ PAKEITIMO“ IR LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS 1998 M. LIEPOS 23 D. NUTARIMO NR. 924 „DĖL LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTERIJOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO“ PROJEKTŲ

Suinteresuotos institucijos, į kurių pastabas ir pasiūlymus neatsižvelgta	**Suinteresuotų institucijų ir asmenų pastabos ir pasiūlymai, į kuriuos neatsižvelgta arba atsižvelgta iš dalies**	**Argumentai, kodėl neatsižvelgta arba tik iš dalies atsižvelgta į suinteresuotų institucijų ir asmenų pastabas ir pasiūlymus**
Valstybės įmonės Registrų centro 2023-01-12 raštas Nr. S-1192 (1.4 E)	2. **Siūlome** Projekte Nr. 2 numatyti Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 12 punkto pakeitimus, kuriais būtų įgyvendinta Lietuvos Respublikos valstybės kontrolės rekomendacija[1] registro ar valstybės informacinės sistemos valdytojams kartu tvirtinti bendrus saugos dokumentus, kai jų valdomų registrų ir (ar) valstybės informacinių sistemų duomenis tvarko tas pats duomenų tvarkytojas. Siūlome 12 punktą išdėstyti taip: „12. Informacinės sistemos valdytojas gali tvirtinti visų ar kelių jo valdomų informacinių sistemų bendrus saugos dokumentus. Informacinės sistemos valdytojai gali kartu tvirtinti bendrus saugos dokumentus, kai jų valdomas informacines sistemas tvarko tas pats informacinių sistemų	**Neatsižvelgta** Tokios galimybės įtvirtinimas būtų netikslingas ir nepagrįstas, nes registro ar informacinės sistemos valdytojas, kaip už registro ar informacinės sistemos saugumą ir saugumo politikos formavimą atsakingas subjektas, šias pareigas privalo įgyvendinti savarankiškai ir nepriklausomai nuo kitų subjektų. Bendrų saugos dokumentų tvirtinimas apribotų galimybes šiems valdytojams įgyvendinti šias pareigas savarankiškai ir nepriklausomai, nes bet koks saugos dokumentų keitimas turėtų būti derinamas su kitais bendrus saugos

[1] Lietuvos Respublikos valstybės kontrolė 2021 m. gruodžio 6 d. valstybinio audito ataskaitoje Nr. VAE-7 „Registrų centro tvarkomi valstybės informaciniai ištekliai“ pažymėjo, kad saugos politikos įgyvendinimą ir priežiūrą apsunkina tai, kad Registrų centro tvarkomų valstybės informacinių išteklių saugą reglamentuoja skirtingų valdytojų patvirtinta duomenų saugos politika (toks didelis Registrų centro tvarkomų informacinių išteklių saugą reglamentuojančių dokumentų kiekis apsunkina saugos politikos įgyvendinimo koordinavimą ir priežiūrą), o bendros saugos politikos nėra, ir pateikė rekomendacijas dėl bendros saugos politikos inicijavimo.

	tvarkytojas.“	dokumentus tvirtinančiais subjektais. Be to, registrai ir informacinės sistemos pasižymi ir skirtinga funkcine struktūra, skirtinga saugomų duomenų svarba ir kitais aspektais, todėl abejotina, ar pavyktų patvirtinti bendrus informacinių sistemų saugos dokumentus, skiriant tinkamą dėmesį informacinių sistemų ypatumams ir elektroninės informacijos saugumui.
	3. **Siūlome** Saugos dokumentų gairių aprašo 3.3 papunktį, kuriuo nustatoma pareiga informacinių sistemų valdytojams saugos nuostatuose aprašyti konkrečius techninius reikalavimus (programinės įrangos, skirtos apsaugoti informacinę sistemą nuo kenksmingos programinės įrangos naudojimo nuostatas ir jos atnaujinimo reikalavimus, programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatas, kompiuterių tinklo filtravimo įrangos naudojimo nuostatas, leistinas kompiuterių naudojimo ribas ir kt. techninius reikalavimus) perkelti į Saugos dokumentų aprašo 4 punktą tokiu būdu įtvirtinant, kad minėtos nuostatos dėl konkrečių techninių reikalavimų yra informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklių turinio dalykas. Manome, kad saugos nuostatuose turėtų būti nustatyta tik saugos politika, bet ne konkretūs ją įgyvendinantys reikalavimai, kaip yra reikalaujama šiuo metu. Konkrečios organizacinės ir techninės priemonės turėtų būti reglamentuojamos saugos politiką įgyvendinančiuose saugos dokumentuose.	**Neatsižvelgta** Siūlymas nėra sietinas su projektais sprendžiama problema, be to, siekiant įgyvendinti šį siūlymą, atsirastų poreikis iš esmės peržiūrėti visų valstybės informacinių išteklių saugos dokumentus, tai sukurtų administracinę naštą valstybės informacinių išteklių valdytojams. Pažymėtina, kad iki 2024 m. spalio 17 d. į nacionalinę teisę turi būti perkeltos 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyvos 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (toliau – TIS 2 direktyva), nuostatos. Šių nuostatų perkėlimas neišvengiamai suponuotų kibernetinio saugumo ir elektroninės informacijos saugos reikalavimų peržiūrą. Krašto apsaugos ministerijos nuomone, dažna kibernetinio saugumo ir elektroninės informacijos saugos reikalavimų peržiūra ir papildomos administracinės naštos nustatymas neatitiktų kibernetinio saugumo subjektų teisėtų stabilaus teisinio reguliavimo lūkesčių. Atsižvelgiant į tai, kibernetinio saugumo ir elektroninės informacijos saugos reikalavimų peržiūrą numatoma

		įgyvendinti perkeliant TIS 2 direktyvą į nacionalinę teisę.
	5. <...> Atkreipiame dėmesį, kad šiuo metu teisės aktuose reikalavimai dėl privalomo atsparumo įsilaužimui vertinimo (angl. *Penetration Testing*) nėra nustatyti. Valstybės kontrolė 2018 m. birželio 28 d. valstybinio audito ataskaitoje Nr. VA-2018-P-900-3-6 „Ypatingos svarbos informacinių išteklių valdymas“[2] pateikė išvadą, kad „sistemiškai nėra naudojamos organizacinės saugumo priemonės, galinčios sumažinti kibernetines grėsmes: *IS kūrimo, modernizavimo, modifikavimo metu nepakankamai testuojamas saugumas*, nepakankamai ugdomas personalas; nevaldoma programinės įrangos saugi konfigūracija ir atnaujinimai, IT veiklos tęstinumo ir atsarginių kopijų netinkamas valdymas kelia grėsmę veiklos atkūrimui, saugos veiksmingumo matavimai nėra pakankami ir neprisideda prie saugumo didinimo“. Valstybės kontrolės ataskaitoje pabrėžta, kad, nors Informacinės visuomenės plėtros komitetas (IVPK) 2017 m. rekomendavo[3] kuriant ir modernizuojant informacines sistemas atlikti atsparumo įsilaužimui testavimą, tačiau ypatingos svarbos informacinių išteklių tvarkytojai neprivalo laikytis rekomendacijų, taigi ir testavimo gali neatlikti. Be to, rekomendacijose nėra išsamiai aprašyti visi reikiami atlikti saugumo testavimo veiksmai. Pažymėtina, kad Valstybės informacinių sistemų gyvavimo ciklo valdymo metodikoje[4], kuri privaloma, ir aprašo visą informacinių sistemų kūrimo eigą, reikalavimų atlikti šį testavimą nėra. Todėl papildomai ORT apraše **siūlome nustatyti, kad sukūrus valstybės**	**Neatsižvelgta** Siūlymas nėra sietinas su projektais sprendžiama problema, be to, siekiant įgyvendinti šį siūlymą, valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros valdytojams būtų sukuriama didelė tiek administracinė, tiek finansinė našta. Atsižvelgdami į tai, kad perkeliant TIS 2 direktyvos nuostatas į nacionalinę teisę (žr. argumentus dėl 3 pastabos) numatoma saugos (kibernetinio saugumo) reikalavimų peržiūra, manome, kad dažna kibernetinio saugumo ir elektroninės informacijos saugos reikalavimų peržiūra ir papildomos administracinės naštos nustatymas neatitiktų kibernetinio saugumo subjektų teisėtų stabilaus teisinio reguliavimo lūkesčių. Papildomai pažymėtina, kad dabartinis reguliavimas jau numato grėsmių ir pažeidžiamumo vertinimą, todėl valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros valdytojai turi teisę atlikti atsparumo įsilaužimams vertinimą kartu su grėsmių ir pažeidžiamumo vertinimu.

[2] https://www.valstybeskontrole.lt/LT/Product/Download/3621

[3] Projektų, kurių įgyvendinimo metu kuriamos elektroninės paslaugos ir informacinių technologijų sprendimai, techninės priežiūros rekomendacijos patvirtintos Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2017 m. lapkričio 22 d. įsakymu Nr. T-126 „Dėl Projektų, kurių įgyvendinimo metu kuriamos elektroninės paslaugos ir informacinių technologijų sprendimai, techninės priežiūros rekomendacijų patvirtinimo“.

[4] Patvirtinta Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2014 m. vasario 25 d. įsakymu Nr. T-29 „Dėl Valstybės informacinių sistemų gyvavimo ciklo valdymo metodikos patvirtinimo“

	informacinius išteklius arba ypatingos svarbos informacinę infrastruktūrą, turi būti atliktas jų atsparumo įsilaužimams vertinimas, kurį turi atlikti nuo minėtų informacinių išteklių kūrėjo nepriklausomi auditoriai.	
	7. Registrų centras tvarko skirtingų valdytojų (Lietuvos Respublikos ekonomikos ir inovacijų ministerijos, Lietuvos Respublikos kultūros ministerijos, Lietuvos Respublikos susisiekimo ministerijos, Lietuvos Respublikos sveikatos apsaugos ministerijos, Lietuvos Respublikos teisingumo ministerijos, Lietuvos Respublikos žemės ūkio ministerijos, Nacionalinio bendrųjų funkcijų centro) registrus ir valstybės informacines sistemas. Vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 37 punktu ir 44 punktu, rizikos įvertinimo ir rizikos valdymo priemonių planą bei pastebėtų trūkumų šalinimo planą turi tvirtinti kiekvienas valdytojas atskirai, nors priemonės gali būti identiškos, pvz. tą pačią priemonę informacinių sistemų tvarkytojui įrengti signalizaciją turi tvirtinti net 7 valdytojai, kas praktikoje tiek informacinių sistemų valdytojui, tiek informacinių sistemų tvarkytojams sukelia nepagrįstą ir neproporcingą administracinę naštą. Siekiant optimalaus saugos valdymo, **siūlome** pakeisti minėtus aprašo punktus numatant, kad informacinių sistemų valdytojas **ar jo įgaliotas informacinių sistemų tvarkytojas** prireikus gali tvirtinti bendrą tvarkomų informacinių sistemų rizikos įvertinimo ir rizikos valdymo priemonių planą bei pastebėtų trūkumų šalinimo planą.	**Neatsižvelgta** Žr. argumentus dėl 2 pastabos.
	9. Nors Teisės aktų projektais siekiama panaikinti besidubliuojančius saugos reikalavimus, sistemiškai vertinant elektroninės informacijos saugos ir kibernetinio saugumo sritį reglamentuojančius teisės aktus pastebėtina, kad priėmus siūlomus projektus ir toliau išliks atskiras šių sričių reglamentavimas, kadangi greta ORT aprašo liks galioti Bendrųjų elektroninės informacijos saugos reikalavimų aprašas ir Saugos dokumentų turinio gairių aprašas, kurie konkuruoja su ORT aprašu ir jį	**Neatsižvelgta** Siekiant įgyvendinti šiuos siūlymus, yra būtina išsami Lietuvos Respublikos kibernetinio saugumo ir Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymų peržiūra ir pakeitimas. Atsižvelgdami į tai, kad perkeliant TIS 2 direktyvos nuostatas į nacionalinę teisę (žr. argumentus dėl 3 pastabos) numatoma kibernetinio

	dubliuoja. Siekiant vieningo reglamentavimo, siūlytume iš esmės peržiūrėti galiojantį teisinį reguliavimą ir pilnai konsoliduoti elektroninės informacijos saugos ir kibernetinio saugumo teisinį reglamentavimą, atsižvelgiant į naujausią gerąją saugos užtikrinimo praktiką ir informacinių ir ryšių technologijų raidą.	saugumo ir elektroninės informacijos saugos reikalavimų peržiūra, manome, kad dažna kibernetinio saugumo ir elektroninės informacijos saugos reikalavimų peržiūra ir papildomos administracinės naštos nustatymas neatitiktų kibernetinio saugumo subjektų teisėtų stabilaus teisinio reguliavimo lūkesčių.