LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL VALSTYBĖS INFORACINIŲ IŠTEKLIŲ SVARBOS VERTINIMO TVARKOS APRAŠO PATVIRTINIMO“ IR LIETUVOS RESPUBLIKOS EKONOMIKOS IR INOVACIJŲ MINISTRO ĮSAKYMO „DĖL VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ SVARBOS VERTINIMO METODIKOS PATVIRTINIMO“ PROJEKTŲ DERINIMO PAŽYMA

Pastabos ir pasiūlymai	Argumentai, kodėl neatsižvelgta į institucijų pastabas ir pasiūlymus
Lietuvos Respublikos teisingumo ministerijos 2023-05-03 raštas Nr. (1.6 Mr) 2T-494	
1. Atkreiptinas dėmesys į tai, jog Nutarimo projekto 3 punktu pavedimas per jame nurodytą terminą atlikti jų steigiamų, kuriamų ir (ar) valdomų VII svarbos vertinimą, ir atsižvelgiant į vertinimo rezultatus, patikslinti informacinių sistemų, kuriuose tvarkomi VII sudarantys duomenys, nuostatus, peržiūrėti VII saugos politiką ir patikslinti ją įgyvendinančius saugos dokumentus formuojamas institucijoms, steigiančioms ir (ar) valdančioms VII, o pagal Aprašo 20 bei 23 punktus analogiškus veiksmus atlikti VII valdanti institucija gali įgalioti ir VII tvarkančią instituciją. Siekiant suvienodinti minėtas nuostatas bei mažinti VII valdančioms institucijoms tenkančių atlikti veiksmų apimtį, Nutarimo projekto 3 punktas tikslintinas, numatant galimybę šiuos veiksmus atlikti įgalioti ir VII tvarkančią instituciją.	**Atsižvelgta iš dalies.** Vyriausybė negali pavesti VII tvarkančioms institucijoms atlikti VII svarbos vertinimo, kadangi pagal galiojantį valstybės informacinių išteklių valdymo teisinį reguliavimą tokius įgaliojimus suteikia VII valdytojai. Dėl to, Nutarimo 2 punktas netikslintinas. Atkreipiame dėmesį, kad Nutarimo 2 punkte įvardintus veiksmus VII valdytojai galės pavesti atlikti VII tvarkančiai institucijai pagal Nutarimo projektu tvirtinamo Aprašo 9 punktą, kuriame įvardinti už VII svarbos vertinimą atsakingi asmenys ir VII vertinime dalyvaujantys asmenys pagal VIIVĮ gali būti ir VII tvarkytojo atstovai.
2. VIIVĮ 1 straipsnio 8 dalyje nurodoma, kad jis netaikomas, kai valstybės informaciniai ištekliai tvarkomi valstybės saugumo ir gynybos tikslais, kai būtina apsaugoti esminius valstybės saugumo interesus. Pirma, vietoje VIIVĮ 1 straipsnio 8 dalies kartojimo Aprašo 2 punkte siūlytina daryti nuorodą į minėtą VIIVĮ nuostatą. Antra, Aprašo 2 punkte, skirtingai nei minėtoje VIIVĮ nuostatoje, nurodoma kad jis netaikomas ir įslaptintos informacijos tvarkymui. Lieka neaišku, kodėl žemesnės galios teisės aktu numatoma platesnė jo netaikymo sritis nei VIIVĮ, kurį įgyvendinant tvirtinamas Aprašas. Todėl Aprašas tikslintinas šiuo aspektu (arba platesnė netaikymo sritis turėtų būti aiškiai pagrįsta Projektų lydraštyje teikiant Vyriausybei). Šios pastabos aktualios ir Metodikos 2 punktui.	**Atsižvelgta iš dalies.** Įvertinant esamą praktiką, pagal kurią VIIVĮ nuostatos netaikomos ir tvarkant įslaptintą informaciją, nepaisant to, kad tai nėra nustatyta minėtame įstatyme, siūloma Apraše ir Metodikoje tai reglamentuoti, siekiant teisinio aiškumo ir atliekant VII svarbos vertinimą, nepalikti teisinio reguliavimo spragų. Priešingu atveju, jeigu Apraše ir Metodikoje nebūtų nustatoma, kad jų nuostatos netaikomos VII, kuriuose tvarkoma įslaptinta informacija, kiltų šių teisės aktų taikymo problemų VSD, STT, FNTT ir kitoms institucijoms, kurios steigdamos, kurdamos ir (ar) valdydamos šiuos VII, vadovaujasi ne VIIVĮ, o Įslaptintos informacijos ryšių ir informacinių sistemų steigimo ir įteisinimo taisyklėmis, patvirtintomis Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 820 „Dėl Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo įgyvendinimo“.
3. Metodikos 4 punktu iš esmės atkartojamas (jį detalizuojant) Aprašo 5 punktas. Siekiant Projektų sistemiškumo, aiškumo bei glaustumo, siūlome tikslinti Metodikos 4 punktą ir jį performuluoti atsisakant Aprašo 5 punkte pateikto reguliavimo kartojimo.	**Atsižvelgta iš dalies.** Sutrumpinta Aprašo 8 punkto formuluotė, siekiant išvengti galimo dubliavimosi su Metodikos 4 punktu. Siekiant, kad Aprašas ir Metodika būtų maksimaliai aiškiai suprantami VII svarbos vertinimą atliksiantiems asmenims, Metodikos 4.1–4.5 papunkčiuose vietoje nuorodų į atitinkamus

Pastabos ir pasiūlymai	Argumentai, kodėl neatsižvelgta į institucijų pastabas ir pasiūlymus
	Aprašo 8.1–8.5 papunkčius, įvardijami Apraše nustatyti VII poveikio sričių pavadinimai.
Lietuvos Respublikos vidaus reikalų ministerijos 2023-05-22 raštas Nr. 1D-2606	
Aprašo 23.3 papunktyje siūloma nustatyti, kad VII valdanti ir (arba) jos įgaliota VII tvarkanti institucija, gavusi Vyriausybės įgaliotos institucijos rekomendaciją, turi įvertinti, ar pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką jų steigiama ar valdoma informacinė sistema neturėtų būti priskirta ypatingos svarbos informacinei infrastruktūrai. Pažymėtina, kad iš Aprašo nuostatų nėra aišku, kokių veiksmų turėtų būti imamasi, jeigu po šio vertinimo informacinė sistema būtų priskirta ypatingos svarbos informacinei infrastruktūrai. Siūlytume tą nurodyti	**Atsižvelgta iš dalies.** Pagal darbine tvarka iš Krašto apsaugos ministerijos gautas pastabas, patikslintos Aprašo ir Ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos (YSII metodika) sąsajos. Pagal atliktus pataisymus, VII svarbos vertinimą atlikti reikės visiems VII, nepriklausomai nuo to, ar jie yra įtraukti į ypatingos svarbos infrastruktūros (YSI) sąrašą, o atlikus vertinimą ir nustačius, kad VII priskirtas ypatingos svarbos VII rūšiai ir jį sudaranti informacinė sistema neįtraukta į YSI sąrašą, pagal Aprašo 19.5 papunktį, institucijos turės patikrinti, ar pagal YSII metodiką, informacinės sistemos nereikia įtraukti į YSI sąrašą. Visi su tuo susiję veiksmai šiuo atveju atliekami vadovaujantis YSII metodika.
Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos 2023-05-08 el. paštu gautas laiškas (suderinta darbine tvarka, esminių pastabų neturi)	
Pažymime, kad siekiant tinkamai įgyvendinti Nutarimo projektą <...> išlieka tikslingumas Nutarimo projektu tvirtiname Apraše (toliau – Aprašas) numatyti galimybę VII svarbos vertinimą atlikti kai tam tikslui suburiama kompetentingų specialistų komanda, skiriamas finansavimas ir įvertinami kiti reikiami resursai (duomenų apsaugos pareigūno kompetencija ir žinios nelaikytos pakankamomis, kad galėtų tinkamai įvertinti, pvz. poveikį žmogaus teisėms ir laisvėms ar pan. <...>), taip pat akcentuotina ir tai, kad Projektų nuostatomis turi būti užtikrintas pareigų atskyrimo principas.	**Atsižvelgta iš dalies.** Siekiant pareigų atskyrimo principo, patikslintas Aprašo 9 punktas. Jame nustatyta, kad už VII svarbos vertinimą atsakingas yra duomenų valdymo įgaliotinis (arba informacinės sistemos nuostatus rengiantis asmuo, jeigu VII svarbos vertinimas atliekamas steigiant naują informacinę sistemą), o VII svarbos vertinime pagal kompetenciją dalyvauja (bet nėra atsakingi) saugos įgaliotinis ir asmens duomenų apsaugos pareigūnas. Esminė kompetencija, kurią turi turėti už VII svarbos vertinimą atsakingi asmenys, yra savo institucijos veiklos procesų išmanymas ir supratimas, kokią įtaką šių procesų atlikimui turi atitinkami duomenys. Šią kompetenciją turi duomenų valdymo įgaliotinis, o VII svarbos vertinimo įgūdžiai, susiję su Aprašo ir Metodikos nuostatų taikymu, bus suteikiami EIM organizuojant specialius mokymus bei parengiant mokomąją medžiagą. Todėl atskiros specialistų komandos bei kitų resursų VII svarbos vertinimui papildomai skirti netikslinga.
Lietuvos Respublikos valstybinės darbo inspekcijos prie SADM 2023-05-09 raštas Nr. SD-131-11145	
Bendrajame duomenų apsaugos reglamente (BDAR) šalia trijų klasikinių duomenų saugos principų (konfidencialumo, vientisumo, prieinamumo) yra akcentuojamas ir ketvirtas atsparumo principas. <...>	**Neatsižvelgta.** Pastaboje įvardintas atsparumo principas, apibrėžiamas kaip atsparumas trikdžiams arba neteisėtiems ar tyčiniams veiksmams, ir yra susijęs

Pastabos ir pasiūlymai	Argumentai, kodėl neatsižvelgta į institucijų pastabas ir pasiūlymus
Atsparumą galima apibrėžti kaip atsparumą trikdžiams arba neteisėtiems ar tyčiniams veiksmams, kuriais yra pažeidžiamas saugomų ar persiunčiamų asmens duomenų prieinamumas, autentiškumas, vientisumas ir konfidencialumas. Atsparumas yra ypač svarbu, kai kalbama apie kritinius, ypatingos svarbos valstybės informacinius išteklius. Todėl siūlome svarstyti galimybę Metodikoje šalia konfidencialumo, vientisumo, prieinamumo įvesti dar ir atsparumo principą arba bent akcentuoti, kad vertinant valstybės informacinių išteklių svarbą būtina įvertinti ir jų atsparumą trikdžiams arba neteisėtiems ar tyčiniams veiksmams.	su duomenų bei informacinės sistemos saugumui užtikrinti taikomomis kibernetinio saugumo priemonėmis. Aprašo ir Metodikos objektas yra priskirti VII sudarančius duomenis ir juos tvarkančias informacines sistemas atitinkamai VII rūšiai, pagal VII sudarančių duomenų svarbą, kuri vertinama iš šių duomenų reikšmingumo veiklai perspektyvos. Tik atlikus VII svarbos vertinimą, pagal jo rezultatus parenkamos atitinkamos kibernetinio saugumo priemonės. Dėl to, šį principą tikslingą būtų numatyti kituose, kibernetinio saugumo politikos nustatymą ir įgyvendinimą reglamentuojančiuose teisės aktuose.
VĮ Registrų centras 2023-05-09 raštas Nr. S-17378 (1.4 E)	
Siekiant, kad informacijos svarbos vertinimas atitiktų tarptautinius saugos standartus, gerąsias IT valdymo praktikas, visuotinai pripažintų organizacijų rekomendacijas, papildomai pažymime, saugos įgaliotinio funkcija yra susijusi su saugos politikos įgyvendinimo priežiūra, pavedimų davimu VII tvarkytojo ar valdytojo darbuotojams, bet ne pačiu saugos politikos įgyvendinimu praktikoje. Vadovaujantis LST/ISO IEC 27002 standartu, <...> už informacijos svarbos įvertinimą yra atsakingi duomenų savininkai. <...> Atsižvelgdami į tai, kas išdėstyta, manome, kad informacijos svarbos vertinimo funkcijos priskyrimas saugos įgaliotiniui akivaizdžiai neatitinka tarptautinių saugos standartų, geruų IT valdymo praktikų ir visuotinai pripažintų organizacijų rekomendacijų, todėl siūlome Nutarimo projektu tvirtinamo Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo projekto 12 punkte nustatyti, kad už VII svarbos vertinimą atsakingais gali būti skiriamas informacinės sistemos duomenų valdymo įgaliotinis ar kitas asmuo, kuriam institucijoje priskirtos duomenų savininko funkcijos.	**Atsižvelgta iš dalies.** Patikslintas Aprašo 9 punktas, kuriame nustatomi už VII svarbos vertinimą atsakingi asmenys. Pagal šį punktą, už VII svarbos vertinimą atsakingu skiriamas duomenų valdymo įgaliotinis arba informacinės sistemos nuostatus rengiantis asmuo ar asmenys, jeigu VII svarbos vertinimas atliekamas steigiant naują valstybės informacinę sistemą ar registrą. Pažymime, kad VII sudarantys duomenys ir juos tvarkanti informacinė sistema priskiriami atitinkamai VII rūšiai priklausomai nuo to, kokį poveikį gali sukelti VII sudarančių duomenų konfidencialumo, vientisumo ir prieinamumo pažeidimas, o šie trys aspektai yra tampriai susiję su kibernetinio saugumo sritimi. Dėl to, Apraše įvardintoms poveikio sritims, pagal Aprašo 9 punktą nustatoma, kad VII svarbos vertinime pagal kompetenciją dalyvauja saugos įgaliotinis ir asmens duomenų apsaugos pareigūnas, tačiau jie neskiriami atsakingais už šį procesą, o tik gali prisidėti prie jo atlikimo savo kompetencijomis.
Asociacijos „Infobalt“ 2023-05-09 raštas Nr. 20230509/01	
1. <…> norime atkreipti dėmesį į tai, kad pagal šiuo metu galiojančio <...> VIIVĮ 43^3 straipsnio 2 punktą, Vyriausybės nutarimu turi būti patvirtintas valstybės informacinių išteklių, kurie turi būti prieinami karo, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais, sąrašas. Turint omenyje tai, kad Metodikos tikslas yra surūšiuoti valstybės informacinius išteklius (VII) pagal svarbą ir identifikuoti VII, kurių saugojimas pagal VIIVĮ 48 straipsnį būtų privalomas valstybiniuose duomenų centruose (toliau - **VDC**), mes manome, kad sąrašas, patvirtintas pagal VIIVĮ 43^3	**Atsižvelgta iš dalies.** Pažymime, kad koreliacija tarp Apraše nustatytų VII poveikio vertinimo sričių ir VIIVĮ 43^3 straipsnio 2 punkte įvardintų VII, užtikrinama VII svarbos vertinimo metu nustatant, kokį poveikį VII sudarančių duomenų KVP pažeidimas gali turėti šioms Apraše nustatytoms ir su VIIVĮ 43^3 straipsnio 2 dalimi susijusioms sritims: gynyba, nacionalinis saugumas ir žvalgyba, viešasis saugumas ir teisėsauga, bei viešosios ir administracinės paslaugos. Be to, pagal Aprašo 19.5 punktą yra

Pastabos ir pasiūlymai	Argumentai, kodėl neatsižvelgta į institucijų pastabas ir pasiūlymus
straipsnio 2 punktą, ir Metodikos, kuri būtų rengiama vadovaujantis VIIVĮ 8 straipsniu, poveikio vertinimo sritys turėtų koreliuoti. Visgi, Metodikos poveikio vertinimo sritys nėra susijusios su VIVĮ 43^3 straipsnio 2 punkto logika.	numatyta VII svarbos vertinimo sąsaja ir su YSII metodika.
2. Metodikoje (Metodikos II skyrius, Priedas Nr. 1) dalis poveikio vertinimo sričių dimensijų ir kriterijų pagal prigimtį turėtų būti taikomi įslaptintos arba riboto naudojimo informacijos tvarkymui, o ne apskritai visų VII atžvilgiu, pvz., „gynyba, nacionalinis saugumas ir žvalgyba“, ”viešasis saugumas ir teisėsauga“.	**Neatsižvelgta.** Tiek Aprašo, tiek ir Metodikos nuostatos yra netaikomos įslaptintos informacijos tvarkymui. Pažymėtina, kad VII gali būti sudarytas iš duomenų ar jų grupių, kurie nėra įslaptinti, bet per integracines sąsajas sąveikauja su pastaboje įvardintoms sritims priklausančiomis informacinėmis sistemomis. Dėl to, nustatant VII svarbą būtina įvertinti galimą VII sudarančių duomenų ar jų grupių KVP pažeidimo poveikį šioms sritims.
3. Metodikos uždavinys turėtų būti suformuluotas kaip VII klasifikacija pagal kritiškumą įvertinant atskirų VII poveikį kritiškai svarbių valstybės funkcijų, paslaugų ir veiklos atstatymui incidentų ir krizės atvejais, bei valstybės funkcijų, paslaugų ir veiklos tęstinumo užtikrinimui. Kaip minėta, kibernetinio saugumo reikalavimai ir iš jų išplaukiančios saugos bei patikimumo užtikrinimo priemonės yra būtent VII svarbos (kritiškumo) nustatymo bei poveikio valstybės funkcijų, paslaugų ir veiklos teikimui įvertinimo padarinys <...> ir būtina veiklos tęstinumo užtikrinimo proceso dalis. <...> Veiklos tęstinumo valdymui taikomas ISO 22313:2012 standartas, 22317 standartas, krizių valdymui – ISO 22361 standartas, rizikos valdymui – ISO 31000 standartų šeima. Manome, kad Metodika privalo remtis šiomis geriausiomis praktikomis ir metodikomis <...>.	**Atsižvelgta iš dalies.** Aprašo ir Metodikos tikslas ir yra VII priskyrimas atitinkamai rūšiai, įvertinant VII sudarančių duomenų svarbą (kritiškumą) sritims, kuriose vykdomos valstybei svarbios funkcijos, paslaugos ir kita veikla (sritys identifikuotos Aprašo 8 punkte, jų dimensijos bei poveikio vertinimo lygiai – Metodikos Priede Nr. 1). Vadovaujantis gerosiomis praktikomis, VII sudarančių duomenų svarbos vertinimui pasirinktas jų konfidencialumo, vientisumo ir prieinamumo pažeidimo galimo poveikio lygio nustatymas Apraše nurodytoms sritims. Kadangi, VII svarbos vertinimo tikslas yra tik nustatyti duomenų kritiškumą veiklai, veiklos tęstinumo užtikrinimo priemonės, vadovaujantis VII svarbos vertinimo rezultatais, turi būti parenkamos vadovaujantis kibernetinio saugumo sritį reguliuojančiais teisės aktais ir ši nuostata yra įtvirtinta Aprašo 19.1, 19.2 papunkčiuose.
4. Mūsų esminis siūlymas būtų konceptualiai pakeisti Metodikos išeitinę poziciją, VII vertinimo uždavinius, tikslą ir būdus. Pagal dabartinį VIIVĮ reguliavimą (8 straipsnis), Metodikos tikslas ir poveikis yra itin ribotas, formalus ir siauras. Pagal dabar galiojantį teisinį reguliavimą, Metodikos pagalba bus sukurta ženkli administracinė našta vien tam, kad būtų atsakyta į klausimą, kokiame duomenų centre turi būti saugomas vienas ar kitas VII pagal VIVĮ 48, 49 straipsnius.	**Iš dalies atsižvelgta.** Aprašo ir Metodikos tikslas nėra atsakyti į klausimą, kokiame duomenų centre turi būti saugomas vienas ar kitas VII. Esminis siektinas VII svarbos vertinimo poveikis ir išeitinė pozicija – didinti institucijų duomenų valdymo brandą ir stiprinti jų kompetencijas, kurių reikia įvertinti, kurie ir kodėl institucijų valdomi duomenys yra kritiniai valstybės funkcijoms bei paslaugoms, ir atsižvelgiant į šio įvertinimo rezultatus, juos panaudoti ne tik tam, kad nuspręsti, kokiame duomenų centre galima laikyti VII sudarančius duomenis, bet vertinimo rezultatais vadovautis formuojant ir įgyvendinant VII saugos politiką,

Pastabos ir pasiūlymai	Argumentai, kodėl neatsižvelgta į institucijų pastabas ir pasiūlymus
	projektuojant informacinių sistemų architektūrą ar nustatant reikalavimus įsigyjamoms IT paslaugoms (žr. Aprašo 19 punktą).