

OHT	Meede	Kuidas rakendada?	Praegune praktika	Meetme arengud	Meetme takistused/probleemkohad	Täiendav ettepanek:
Kolmandate riikide tehnoloogia pole keelustatud EU või riiklikul tasandil	Seaduse muutmine	Seaduse muutmiseks on tarvis EU-ülest või riiklikku otsust kolmandate riikide tehnoloogia välistamiseks.	Hetkel pole Euroopa-üleselt, riiklikku kokkulepet ega kehtestatud juhiseid kolmandate või konkreetsete riikide tehnoloogia välistamiseks, kuna see toob kaasa majanduslikku kahju (sanktsioonid, majanduslikud piirangud, jne)	Riikides lähtutakse riskipõhisusest.	Majanduslikud piirangud, riskide hindamise praktikad on erinevad, teadmus madal.	* Kriitilise taristu ja julgeoleku kaitsmine, elutähtsate teenuste koordineerivate asutuste nõuete kehtestamine kriitilise taristu kaitseks.
					Blacklist/whitelisti koostamine seaduse tasandil ei ole lubatud	
Kriitilises taristu hankimisel osaleb kolmanda riigi esindaja.	Piirang tehnilises kirjelduses	Tehnilises kirjelduses tuleb piirata kolmandate riikide esindajate osalemist riigihankes.	Nt Poola lisab tehnilise kirjeldusse punkti, et ei soovi hankesse kolmandate riikide ettevõtjaid.	EL KOM töötab eelnõu kallal, mis lubab liikmesriikidel kehtestada erandeid strateegilise julgeoleku huvides. Eeldatavalt jõustub 2026 augustis.	Ei tohi piirata EL riike, EL kandidaatriike, WTO lepinguga liitunud riike või vabakaubanduslepinguga riike. Meetmega saab välistada ettevõtjaid aga sellega ei ole võimalik välistada konkreetseid tooteid või teenuseid. Ettevõtte saame välistada ainult juhul kui pakkuja on konkreetselt välistatav riik.	* Lisada tehnilisse kirjeldusse, et täitja võib välistada tooted, mis kujutavad endast ohtu julgeolekule. * Lisada tehnilisse kirjeldusse piirang välistamiseks tooteid, mis on toodetud ja disainitud kolmandates riikides. * Kehtestada/viidata protseduurides kolmandate riikide nimekirjale/ohuhinnangutele, kelle puhul tuleb rakendada täiendavat kontrolli, täiendavalt hinnata riske või nõuda infoturbejuhi kooskõlastust.

Kriitilises taristus on kasutusel konkreetse kolmanda riigi tootja tehnoloogia.	Riskianalüüs	Koostada tootja-põhine riskianalüüs, mis põhjendab selgelt, kuidas konkreetse tootja tooted kujutavad endast julgeolekuriski ning mille alusel on nende välistamine hankes õigustatud.	Riigikontroll rõhutab, et põhjendused peavad olema konkreetse toote või teenusepõhised. Tooma välja toote tehnilise ohu ja mõju kirjelduse julgeoleku vaatest.	RaM kavandab RHS muudatust: lisandub kohustus arvestada julgeoleku riske. See loob selgema aluse selliste toodete välistamiseks. Millal on oodata selle jõustumist?	Vastutus. Riskianalüüsi koostamine ja selle tulemuste eest vastutavad tooteomanik, teenusehaldur ning infoturbejuht. Hankeosakond ei vastuta riskianalüüsi sisu ega otsuste eest, kuid võib vajadusel juhtida tähelepanu võimalikule julgeolekuriskile või analüüsi puudumisele.	* Kehtestada asutuses hankimise juhised, mis peavad arvesse võtma julgeoleku riski hindamist ja meetmeid. * Koolitada personali riskihindamise, infoturbe ja turvalise hankimise põhimõtetest.
Julgeolekuriskidega ei arvestata asutuse tööprotsessides.	Küsida nõu asutuse infoturbejuhilt ja/või julgeolekuasutustelt	Koostada riskianalüüs ja tehniline kirjeldus, milles on selgelt määratletud, kuhu ning millisel eesmärgil tellitav toode või teenus kasutusse läheb.	KAPO ja VLA on kohustatud julgeolekuriskiga hangetega seoses nõu andma. Neid tuleks julgelt kasutada.	Infoturbejuhid peavad asutuse töötajaid harima ning ohuteadmust vastutavate töötajatega jagama, kehtestama praktikad, mis kaitsevad asutust julgeoleku riskide eest.	Julgeolekuasutuste kaasamine võib hankeprotsessi ajakava pikendada. Kuigi neil on nõustamiskohustus, ei pruugi neil alati olla piisavalt spetsialiste kõigi hangete nõustamiseks.	* Infoturbejuhid peavad ennast kurssi viima ajakohaste trendide ja julgeoleku ohtudega ning rakendama asutuses parimaid praktikaid riskide leevendamiseks (koolitused, protseduurid, täiendav kontroll jne) * Ohuteadmuse jagamine - julgeoleku riskid, julgeolekuasutuste ohuhinnangutega tutvumine.
Puudub teave/ohuhinnang kolmanda riikide riskide kohta.	Kasutada EL tööriista ja EL KOM KKK dokumenti	1) Acces2Markets tööriist: https://trade.ec.europa.eu/acces-s-to-markets/en/home 2) https://finance.ec.europa.eu/system/files/2024-01/faqs-sanctions-russia-public-procurement_en.pdf	Saab teavet kolmandate riikide turuolukorra, kaubanduslepingute, riigihangete ning teenuste ja toodete kohta. See aitab hankemenetlust ette valmistada ja toetab riskide hindamist.	Riskihindamised peavad olema asja- ja ajakohased.	Tuleb jälgida ja vaadata, et info oleks up-to-date. Spetsiifilisi tooteid võib olla raske leida.	* Kehtestada juhised, kust leiab infot kolmandate riikidega seotud ohtude kohta.
Puudub teave julgeoleku riskide maandamise kohta riigihangetes.	Rahandusministeeriumi juhised	Julgeoleku riskide maandamine riigihangetes 2024 0.pdf	Võtmeisikud (tooteomanikud, hankejuhid) ei ole juhistest teadlikud.	Plaanis täiustada Riigikantslei juhistega. Jõustuine 2026 algul	Ainus avalik juhise millele toetuda aga praktikas vähe kasutatud.	* Kehtestada asutuse sisesed juhised hangete läbiviimiseks ja riskide hindamiseks hankimisel.

Hankimisel ei saa välistada vaenuliku riigi pakkumusi.	Riigihanke erandi kasutamine	RHS §11 lg 1 p 20 erandi kohaldamine on otseselt vajalik riigi oluliste julgeolekuhuvide kaitsmiseks tingimusel, et julgeolekuhuve ei saa tagada vähem sekkuvate meetmetega	Kui avalikul konkursil ei ole tulnud soovitud tulemust ehk siis ei ole võimalik välistada vaenuliku riigi tooteid siis võib minna erandiga otsepakkumusega ettevõtte poole, kellel on vajalikud tooted.	Tuleb luua laiem arusaam, et julgeolekuaspekt ei tulene sellest, et hangitakse relvasid ja sõjapidamise vahendeid, vaid nt need võivad olla ka IT-seadmed ja muu IT-taristu.	Erandit ei julgeta kasutada - kardetakse Riigikontrolli. Riigikontroll on teadlik probleemist ja on koos RaM ja Riigikantseleiga andnud välja juhiseid riigihangetes välistamiseks.	* Harida asutuse töötajaid ja hankejuhte riigihanke erandi kasutamise võimalustest ja tingimustest.
--	-------------------------------------	---	---	--	---	---