VENDIM
Nr. 315, datë 6.5.2026

PËR DISA NDRYSHIME NË VENDIMIN NR. 718, DATË 29.10.2004, TË KËSHILLIT TË MINISTRAVE, "PËR LISTËN E PERSONAVE TË SHPALLUR SI FINANCUES TË TERRORIZMIT", TË NDRYSHUAR

Në mbështetje të nenit 100 të Kushtetutës dhe të neneve 5, pika 1, 14, pika 1, 18, pika 1, 25, pika 1, e 28, pika 1, të ligjit nr. 157/2013, "Për masat kundër financimit të terrorizmit", të ndryshuar, me propozimin e ministrit për Evropën dhe Punët e Jashtme, Këshilli i Ministrave

VENDOSI:

Në listën e personave të shpallur sipas rezolutave të Këshillit të Sigurimit "Lista e OKB-së", që i bashkëlidhet vendimit nr. 718, datë 29.10.2004, të Këshillit të Ministrave, të ndryshuar, bëhen ndryshimet e mëposhtme:

1. Në listën e shkronjës "A", të titulluar "Lista e individëve anëtarë ose bashkëpunëtorë me talibanët", ndryshohen të dhënat për 2 (dy) individë të renditur në listën e konsoliduar të Këshillit të Sigurimit të OKB-së për individët e shpallur anëtarë ose bashkëpunëtorë me talibanët.

2. Në listën e shkronjës "B", të titulluar "Lista e kompanive që i takojnë ose bashkëpunojnë me talibanët", ndryshohen të dhënat për 1 (një) kompani të renditur në listën e konsoliduar të Këshillit të Sigurimit të OKB-së për kompanitë e shpallura financuese ose bashkëpunëtore me talibanët.

Ky vendim hyn në fuqi menjëherë dhe botohet në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama

NDRYSHIME NË LISTËN E INDIVIDËVE DHE KOMPANIVE TË SHPALLUR ANËTARË OSE BASHKËPUNËTORË ME TALIBANËT

SIPAS REZOLUTAVE TË KËSHILLIT TË SIGURIMIT

("LISTA E OKB-së")

A. LISTA E INDIVIDËVE ANËTARË OSE BASHKËPUNËTORË ME TALIBANËT

1. KHALIL: AHMED: HAQQANI
2. ABDUL RAUF: ZAKIR

B. LISTA E KOMPANIVE QË U TAKOJNË OSE BASHKËPUNOJNË ME TALIBANËT

1. *HAJI KHAIRULLAH HAJI SATTAR MONEY EXCHANGE*

Shënim. Gjenealitetet e tjera për personin, emri i të cilit është radhitur më sipër, mbahen në Agjencinë e Inteligjencës Financiare.

VENDIM
Nr. 316, datë 6.5.2026

PËR MIRATIMIN E METODOLOGJISË SË VLERËSIMIT TË PROFILIT TË RREZIKUT TË FURNITORËVE DHE OFRUESVE TË PAJISJEVE TË RRJETIT 5G

Në mbështetje të nenit 100 të Kushtetutës dhe të pikës 7, të nenit 55, të ligjit nr. 54/2024, "Për komunikimet elektronike në Republikën e Shqipërisë", me propozimin e ministrit të Infrastrukturës dhe Energjisë, Këshilli i Ministrave

VENDOSI:

1. Miratimin e metodologjisë së vlerësimit të profilit të rrezikut të furnitorëve dhe ofruesve të pajisjeve të rrjetit 5G, sipas tekstit që i bashkëlidhet këtij vendimi.

2. Ngarkohen Autoriteti i Komunikimeve Elektronike dhe Postare, Autoriteti Kombëtar për Sigurinë Kibernetike dhe Ministria e Infrastrukturës dhe Energjisë për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama

METODOLOGJIA E VLERËSIMIT TË PROFILIT TË RREZIKUT TË FURNITORËVE DHE OFRUESVE TË PAJISJEVE TË RRJETIT 5G

Neni 1
Qëllimi

Ky dokument ka për qëllim përcaktimin e metodologjisë për vlerësimin e profilit të rrezikut në nivel kombëtar, të furnitorëve dhe ofruesve të pajisjeve të rrjetit, komponentëve kritikë dhe pjesëve të ndjeshme të 5G-së.

Neni 2
Fusha e zbatimit

Kjo metodologji zbatohet për rrjetet 5G, që qëndrojnë më vete, dhe për rrjetet, që nuk qëndrojnë apo zhvillohen më vete dhe për aq sa është e aplikueshme për MVNO-në.

Neni 3
Parimet e përgjithshme

1. Metodologjia për vlerësimin e profilit të rrezikut të furnitorëve dhe ofruesve të pajisjeve të rrjetit, komponentëve kritikë dhe pjesëve të ndjeshme të 5G-së (në vijim, metodologjia), bazohet në kritere objektive, transparente dhe proporcionale, sipas nivelit të rrezikut.

2. Metodologjia zbaton, për aq sa është e mundur, parimin e neutralitetit teknologjik.

3. Metodologjia bazohet në kriteret e vlerësimit të rrezikut të koordinuara me Bashkimin Evropian, për sigurinë kibernetike të rrjeteve 5G, si dhe praktikat e mira të zhvilluara për këtë qëllim për rritjen e sigurisë së rrjeteve 5G.

4. Metodologjia bazohet në qasjen e vlerësimit të rrezikut sipas 5G *toolbox-it* të Bashkimit Evropian për sigurinë kibernetike të rrjeteve 5G.

5. Vlerësimi i rrezikut bëhet mbi bazën e kritereve, si më poshtë vijon:

a) strategjike;

b) teknike; si dhe

c) dobësitë joteknike, që lidhen për rrjetet 5G.

6. Metodologjia i shërben zbatimit të masave të sigurisë të përcaktuara në ligjin nr. 54/2024, "Për komunikimet elektronike në Republikën e Shqipërisë" (në vijim, ligji nr. 54/2024), si dhe synon garantimin e vijueshmërisë së ofrimit të shërbimeve.

7. Metodologjia synon, gjithashtu:

a) përforcimin e sigurisë në projektimin, vendosjen dhe funksionimin e rrjeteve 5G;

b) ngritjen e standardeve bazë të sigurisë për pajisjet, rrjetet dhe shërbimet;

c) zbutjen e rreziqeve të sigurisë së rrjetit nga furnitorët dhe ofruesit e rrjetit;

ç) shmangien ose kufizimin e varësive të mëdha nga çdo furnizues i vetëm në rrjetet 5G;

d) promovimin e një tregu të larmishëm, konkurrues dhe të qëndrueshëm për pajisjet e rrjetit 5G, duke përfshirë edhe ruajtjen e kapaciteteve në zinxhirin e vlerës 5G, sipas praktikave të mira.

8. Masat për zbutjen dhe trajtimin e rrezikut të jenë të mirëbalancuara dhe të koordinuara të mbështetura në standardet e harmonizuara në nivel evropian dhe në skemën e certifikimit për 5G.

Neni 4
Përkufizimet

1. Termat e përdorur në këtë dokument kanë të njëjtin kuptim me përkufizimet e ligjit nr. 54/2024, "Për komunikimet elektronike në Republikën e Shqipërisë".

2. Në këtë metodologji, termat e mëposhtëm kanë këto kuptime:

a) "**Rrjet 5G**", tërësia e të gjitha elementeve përkatëse të infrastrukturës së rrjetit dhe teknologjia e komunikimeve pa tel, që përdoret për lidhjen dhe ofrimin e shërbimeve me vlerë të shtuar e me karakteristika të avancuara të performancës, si me shpejtësi e kapacitet shumë të lartë të të dhënave, vonesë e ulët në komunikim, besueshmëri mjaft e lartë, ose që mbështet një numër të madh pajisjesh të lidhura, ku mund të përfshihen elementet e trashëguara të rrjetit, bazuar në gjeneratat e mëparshme të teknologjisë së rrjeteve të lëvizshme pa tel, të tilla si 4G ose 3G. Rrjetet 5G do të kuptohen që përfshijnë të gjitha pjesët përkatëse të rrjetit të lëvizshëm.

b) "**MVNO**", një operator i rrjetit të lëvizshëm virtual;

c) "**5G *toolbox* i BE-së**" nënkupton rekomandimet e miratuara nga Komisioni Evropian me rekomandimin 2019/534/BE, të datës 26 mars 2019, mbi sigurinë kibernetike të rrjeteve 5G.

Neni 5
Procedura e vlerësimit

1. Për vlerësimin e profilit të rrezikut të furnitorëve dhe ofruesve të pajisjeve të rrjetit, komponentëve kritikë dhe pjesëve të ndjeshme të 5G-së, AKEP-i u kërkon operatorëve, sipas përcaktimeve në vendimin e Këshillit të Ministrave, "Për miratimin e listës me përbërësit kritikë dhe pjesët e ndjeshme të rrjeteve 5G", informacion:

a) se cilët janë furnitorët për secilin komponent të rrjetit;

b) se cili është vendi i origjinës nga i cili kontrollohet furnitori apo furnitorët;

c) nëse pajisjet e rrjetit janë të certifikuara sipas njërës prej pikave të mëposhtme:

i. skemës së certifikimit për sigurinë kibernetike të BE-së;

ii. skemës kombëtare të certifikimit të sigurisë kibernetike, miratuar me vendim të Këshillit të Ministrave sipas ligjit për sigurinë kibernetike;

iii. nëse furnizuesi ose ofruesi i pajisjeve të rrjetit është i certifikuar, sipas standardeve ISO/IEC për sigurinë, të lëshuar nga organe të akredituara/ njohura nga autoritet shqiptare ose në BE;

ç) të përcaktuar sipas pikës 3, të nenit 55, të ligjit nr. 54/2024.

2. Kërkesat sipas pikës 1 të këtij neni plotësohen me dokumentacion përkatës ligjor për shkronjat "a" dhe "c" ose me vetëdeklarim apo raporte për kërkesat e tjera.

3. Operatorët e rrjeteve 5G paraqesin pranë AKEP-it informacionin e kërkuar jo më vonë se 30 ditë nga kërkesa e AKEP-it. Për vlerësimin e parë pas hyrjes në fuqi të këtij vendimi, afati për paraqitjen e informacionit është jo më shumë se 60 ditë nga marrja e kërkesës.

4. AKEP-i, nga momenti i marrjes së informacionit të paraqitur nga operatorët, bën vlerësimin e detajuar të informacionit brenda 90 ditëve kalendarike.

5. Në procesin e vlerësimit, AKEP-i merr në konsideratë edhe informacionet e raportimeve periodike nga sipërmarrësit ose autoriteti përgjegjës mbi incidentet kibernetike të ndodhura gjatë vitit të fundit, si dhe raportime që mund të jenë bërë nga sipërmarrësit, bazuar në parashikimet e nenit 157, të ligjit nr. 54/2024.

6. AKEP-i, kur është e nevojshme, bashkëpunon me autoritetet kompetente për sigurinë për vlerësimin e informacioneve të përcaktuara në pikën 2, të nenit 55, të ligjit nr. 54/2024.

7. Vlerësimi i riskut nga AKEP-i mban parasysh kategorizimin e rreziqeve sipas tabelës në shtojcën 1, pjesë përbërëse e kësaj metodologjie, e cila orienton mbi skenarët dhe burimet e mundshme të rrezikut 5G, për të dalluar e përjashtuar rreziqet që nuk lidhen me furnitorët dhe që janë objekt i kësaj metodologjie. Vlerësimi i plotë i nivelit të rreziqeve, me probabilitet e ndikim, realizohet në dokumentet zbatuese sipas kësaj metodologjie.

8. AKEP-i mban parasysh, gjithashtu, nëse nga operatori janë marrë masat teknike e specifike për sigurinë e rrjeteve 5G, sipas përcaktimeve në 5G *Toolbox*, të listuara në shtojcën 2, pjesë përbërëse e kësaj metodologjie.

9. Masat teknike dhe specifike për sigurinë e rrjeteve 5G, referuar këtij vendimi, nuk anashkalojnë kërkesat për masat e sigurisë së rrjeteve dhe të shërbimeve sipas përcaktimeve në nenet 54 e 56, të ligjit nr. 54/2024, "Për komunikimet elektronike në Republikën e Shqipërisë".

10. AKEP-i mban parasysh cilësinë e përgjithshme të produkteve dhe të praktikave të sigurisë kibernetike të furnizuesit, duke përfshirë shkallën e kontrollit mbi zinxhirin e tij të furnizimit dhe nëse praktikave të sigurisë u është dhënë përparësia e duhur.

11. AKEP-i bën vlerësimin e rreziqeve nga dobësitë joteknike, që lidhen me rrjetet 5G, që përfshin mundësinë që furnizuesi të jetë subjekt i ndërhyrjeve nga një vend/qeveri e huaj, sipas kritereve të përcaktuara në paragrafin 2.37, të vlerësimit të rrezikut për 5G në Bashkimin Evropian.

12. AKEP-i, pas konsultimit me AKSK-në, bën një vlerësim të detajuar të masave të sigurisë të ndërmarra nga operatori, nivelin e rrezikut të identifikuar, si dhe një vlerësim për kohën/planin e masave dhe kohën e korrigjimit të mundshëm të tyre. Analiza e kryer i vihet në dispozicion operatorit për t'u shprehur.

13. Operatori paraqet në AKEP një plan masash për zgjidhjen dhe eliminimin e rrezikut të identifikuar brenda 30 ditëve kalendarike.

14. Në rast se masat e marra nga operatori janë të pamjaftueshme për të eliminuar rrezikun/qet e identifikuar/a, AKEP-i, pas konsultimit me AKSK-në, i paraqet ministrit propozimin për masat kufizuese, kohën e zbatimit të tyre, si dhe

propozimin për skemën e kompensimit, nëse do të jetë e nevojshme.

15. Ministri shprehet për propozimin për masat kufizuese brenda 30 ditëve.

16. Pas marrjes së mendimit të ministrisë, AKEP-i përcakton, me vendim, masat kufizuese, duke përcaktuar:

a) masat përkatëse për eliminimin e rrezikut, i cili mund të përfshijë heqjen ose zëvendësimin e pajisjeve me rrezik të lartë brenda një afati të specifikuar;

b) ndalimin e furnizimit në vijim nga një furnitor i identifikuar me rrezik të lartë;

c) sipas rastit, propozimin për mekanizmin e kompensimit, nëse do të aplikohet.

17. AKEP-i monitoron zbatimin e masave kufizuese dhe informon ministrin dhe AKSK-në për përmbushjen e tyre.

18. Operatorët e rrjetit, përpara se të kryejnë investime të reja, që lidhen me pajisje sipas përcaktimeve në vendimin e Këshillit të Ministrave, "Për miratimin e listës me përbërësit kritikë dhe pjesët e ndjeshme të rrjeteve 5G", njoftojnë paraprakisht AKEP-in.

Shtojca 1[1]

TABELA E DOBËSIVE DHE BURIMEVE TË RREZIKUT TË RRJETEVE 5G

I: Skenari i rrezikut lidhur me pamjaftueshmërinë e masave të sigurisë	R1-Konfigurimi i gabuar i rrjeteve; R2-Mungesa e kontrollit të aksesit.
II. Skenari i rrezikut lidhur me zinxhirin e furnizimit 5G	R3-Cilësi e ulët e produktit; R4-Varësia nga çdo furnizues i vetëm brenda rrjeteve individuale dhe mungesa e diversitetit në nivel kombëtar.
III. Skenari i rrezikut lidhur me mënyrat e veprimit të aktorëve kryesorë të kërcënimeve	R5-Ndërhyrja e qeverive të huaja përmes zinxhirit të furnizimit 5G; R6-Shfrytëzimi i rrjeteve 5G nga krimi i organizuar ose grupi i krimit të organizuar që synon përdoruesit fundorë.
IV. Skenari i rrezikut lidhur me ndërvarësitë midis rrjetit 5G dhe sistemeve të tjera kritike	R7-Ndërprerje e konsiderueshme e infrastrukturave ose shërbimeve kritike; R8-Dështim masiv i rrjeteve për shkak të ndërprerjes së furnizimit me energji elektrike ose sistemeve të tjera mbështetëse.
V. Skenari i rrezikut lidhur me përdoruesit fundorë të pajisjeve	R9-Shfrytëzimi i Internetit të Gjërave (IoT), telefonave celularë ose pajisjeve inteligjente.

Shtojca 2[2]

Masa teknike (TM) për sigurinë e rrjeteve 5G					
	Siguria e rrjetit, masa bazë				
Nr.	**Masë**	**Përshkrim**	**Rreziqet**	**Aktorët**	**Veprime mbështetëse (SA)**
TM01	Zbatimi i kërkesave bazë të sigurisë (projektimi dhe arkitektura e sigurt e rrjetit)	Të sigurohet që operatorët celularë (MNO) të zbatojnë praktikat më të mira ekzistuese të sigurisë dhe rekomandimet, që nuk janë specifike vetëm për rrjetet 5G, për shembull në zhvillimin e produkteve, konfigurimin, menaxhimin e përditshëm të rrjetit, menaxhimin e incidenteve, përditësimet e sigurisë – për shembull, duke vendosur e rishikuar planet e vlerësimit të rrezikut nga ana e operatorëve celularë MNO-ve.	R1, R2, R3, R6, R7, R8, R9	AKEP-i në bashkëpunim me AKSK-në, operatorët	SA01, SA05, SA09, SA10

[1] Bazuar në aneksin 1, të *EU 5G toolbox* për masat e eliminimit të rrezikut *"Cybersecurity of 5G networks EU Toolbox of risk mitigating measures"*.

[2] Bazuar në aneksin 1, të *EU 5G toolbox* për masat e eliminimit të rrezikut *"Cybersecurity of 5G networks EU Toolbox of risk mitigating measures"*.

		Të sigurohet që operatorët celularë (MNO) të mbajnë të përditësuara informacionet mbi politikat e sigurisë, përfshirë informacionin operacional, si dhe informacionin e lidhur me procedurat e menaxhimit të ndryshimeve dhe incidenteve për sistemet kyçe të rrjetit dhe informacionit.			
TM02	Sigurimi dhe vlerësimi i zbatimit të masave të sigurisë në standardet ekzistuese të 5G-së.	Të sigurohet që operatorët celularë (MNO) dhe furnitorët e tyre të zbatojnë masat ekzistuese të sigurisë të përfshira në standardet përkatëse të teknologjisë 5G (p.sh. 3GPP) dhe t'i përdorin ato si një nivel minimal bazë sigurie për operatorët celularë MNO-të, në mënyrë që të garantohet që edhe pjesët opsionale të këtyre standardeve, që janë të rëndësishme për sigurinë, të zbatohen në mënyrë të përshtatshme.	R1, R2, R3, R6, R7, R9	AKEP-i në bashkëpunim me AKSK-në, operatorët, furnitorët	SA03, SA04, SA05, SA10
	Siguria e rrjetit – masa specifike për 5G				
TM03	Sigurimi i kontrollit të rreptë të aksesit.	Të sigurohet që operatorët celularë (MNO) të zbatojnë masa teknike të përshtatshme, fleksibël dhe të verifikueshme për të garantuar që: •të aplikohen kontrolle të rrepta të aksesit në rrjet; •të zbatohet parimi i privilegjeve minimale, duke siguruar që të drejtat e ndryshme në rrjet (p.sh. të drejtat e aksesit midis funksioneve të rrjetit, të drejtat e administratorëve të rrjetit, konfigurimi i virtualizimit) të jenë të minimizuara; •të zbatohet parimi i ndarjes së detyrave; •të jenë në fuqi procedura që sigurojnë zbatimin e vazhdueshëm të këtyre rregullave dhe përshtatjen e tyre me evolucionin e rrjetit. Gjatë përcaktimit të politikave të kontrollit të aksesit, duhet të tregohet kujdes i veçantë për të minimizuar dhe/ose shmangur sa më shumë të jetë e mundur aksesin në distancë nga palë të treta, veçanërisht nga furnitorë që konsiderohen me rrezik të lartë. Kur aksesi i tillë në distancë është i domosdoshëm, për shembull për të adresuar ndërprerjet e shërbimit, operatori celular MNO-ja duhet të zbatojë mekanizma të përshtatshëm për autentikim, autorizim, regjistrim (*logging*) dhe auditim, në mënyrë që të ketë qartësi të plotë mbi aksesin në të dhëna dhe ndryshimet në konfigurim apo në strukturën e rrjetit.	R1, R2, R3, R5, R6, R7	AKEP-i në bashkëpunim me AKSK-në, operatorët	SA05, SA10
TM04	Rritja e sigurisë së funksioneve të virtualizuara të rrjetit.	Të sigurohet që operatorët celularë (MNO) të ndjekin praktikat më të mira të sigurisë për virtualizimin e funksioneve të rrjetit. Duhet pasur parasysh se mund të ketë raste, për shembull kur një funksion rrjeti është	R1, R3, R6, R7	AKEP-i në bashkëpunim me AKSK-në, operatorët	SA01, SA05, SA10

		shumë kritik ose kur përpunon informacion shumë të ndjeshëm, në të cilat virtualizimi nuk është i përshtatshëm dhe në këto raste mund të jetë e nevojshme ndarja fizike.			
TM05	Sigurimi i menaxhimit, funksionimit dhe monitorimit të sigurt të rrjetit 5G.	Të sigurohet që operatorët celularë (MNO) të operojnë qendrat e menaxhimit të rrjetit (NOC) dhe/ose qendrat e operacioneve të sigurisë (SOC) në ambientet e tyre, brenda vendit dhe/ose brenda Bashkimit Evropian. NOC-ja dhe SOC-ja përbëjnë një komponent jetik të infrastrukturës së operatorëve celularë MNO-së për zbatimin e monitorimin e masave për menaxhimin dhe funksionimin e sigurt të rrjetit. Këto qendra duhet të ofrojnë qartësi të plotë mbi rrjetin dhe të zbatojnë monitorim efektiv të rrjetit, të paktën për të gjithë komponentët kritikë dhe pjesët sensitive të rrjeteve 5G, për të zbuluar anomali dhe për të identifikuar e shmangur kërcënime, si për shembull kërcënime ndaj rrjetit qendror që vijnë nga pajisje të kompromentuara të përdoruesve ose nga pajisje IoT. Gjithashtu, të sigurohet që operatorët celularë MNO-të të mbrojnë në mënyrë të përshtatshme trafikun e menaxhimit të rrjetit të komunikimit apo shërbimit, për të shmangur ndryshimet e paautorizuara në përbërësit e rrjetit ose të shërbimit të komunikimit.	R1, R2, R3, R5,R6, R7, R9	AKEP-i në bashkëpunim me AKSK-në, operatorët	SA05, SA09, SA10
TM06	Fuqizimi i qëndrueshmërisë në nivel kombëtar	Sigurohuni që operatorët celularë (MNO) të forcojnë mbrojtjen fizike të komponentëve kritikë dhe pjesëve sensitive të rrjeteve 5G, duke ndjekur një qasje të bazuar në rrezik për teknologjitë "*Multi-access Edge Computing"* (MEC) dhe stacionet bazë, për shembull duke marrë parasysh vendndodhjen, ku këta komponentë janë vendosur e përdorur, si në rastin e përdorimit të MEC-së në spitale. Në forcimin e kontrolleve të aksesit fizik, është e rëndësishme të sigurohet që akses të ketë vetëm një numër i kufizuar personash, që janë të verifikuar për siguri, të trajnuar e të kualifikuar. Aksesi nga palë të treta, kontraktorë dhe punonjës të furnitorëve/partnerëve ose integratorëve duhet të jetë i kufizuar dhe i monitoruar, veçanërisht kur bëhet fjalë për komponentë kritikë dhe pjesë sensitive të rrjetit 5G.	R6, R7	AKEP-i në bashkëpunim me AKSK-në, operatorët	SA05, SA10
TM07	Forcimi i integritetit të softuerit, menaxhimi i përditësimeve dhe *patch*-eve.	Të sigurohet që operatorët celularë (MNO) të vendosin mjete dhe procese të përshtatshme për të garantuar integritetin e *softwar*-it, të cilat identifikojnë në mënyrë të besueshme dhe ndjekin ndryshimet dhe statusin e	R1, R3, R5, R6, R7	AKEP-i në bashkëpunim me AKSK-në, operatorët	SA02, SA10

		përditësimeve (*patch*-eve), gjatë kryerjes së përditësimeve të *softwar*-it dhe zbatimit të *patch*-eve të sigurisë në rrjetet 5G.			
	Kërkesat e lidhura me proceset dhe pajisjet e furnizuesve				
TM08	Rritja e standardeve të sigurisë në proceset e furnitorëve përmes kushteve të forta të prokurimit.	Sigurohuni që operatorët celularë (MNO) të kërkojnë standarde specifike sigurie nga furnitorët e pajisjeve gjatë procesit të prokurimit (p.sh. përmirësime të veçanta të sigurisë dhe demonstrim të niveleve të cilësisë, mirëmbajtje të sigurisë së pajisjes gjatë të gjithë ciklit të jetës së saj dhe integrim të sigurisë në proceset e zhvillimit të produktit).	R3, R6, R7	AKEP-i në bashkëpunim me AKSK-në, operatorët, furnitorët	SA02, SA10
TM09	Përdorimi i certifikimeve të BE-së për komponentët e rrjetit 5G, pajisjet e përdoruesve dhe/ose proceset e furnitorëve.	Komisioni Evropian ka konsideruar përfshirjen në programin e përditësuar/për vazhdimin e punës së Bashkimit (*Union Rolling Work Programme*) të skemave përkatëse në nivel BE-je për komponentët kritikë të rrjetit të përdorur në rrjetet 5G dhe/ose për pajisjet e përdoruesve të 5G-së (për shembull, për *eSIM* dhe materialin kriptografik përkatës), në kuadër të kornizës së certifikimit të BE-së. Gjithashtu, duhet të shqyrtohet në një fazë të mëvonshme, nëse certifikimi ose procesi i furnitorit mund të shtohet, gjithashtu, në programin rrotullues të punës së BE-së.	R3, R6, R7	AKEP-i në bashkëpunim me AKSK-në, EC, ENISA, palët e interesit	SA02, SA03, SA09, SA10
TM10	Përdorimi i certifikimeve të BE-së për produkte dhe shërbime të tjera TIK, që nuk janë specifike për 5G (pajisje të lidhura, shërbime *cloud*)	Komisioni Evropian ka konsideruar përfshirjen në programin afatgjatë të punës së Bashkimit Evropian të skemave të përbashkëta në nivel BE-je, në kuadër të kornizës së certifikimit të BE-së, për produkte dhe shërbime TIK, që nuk janë specifike për 5G, si për shembull: Siguria e shërbimeve *cloud* dhe teknologjive të lidhura me to, të cilat përbëjnë një pjesë të rëndësishme të vendosjes së rrjeteve 5G; Siguria e pajisjeve të lidhura (për përdoruesit fundorë), përfshirë pajisjet IoT.	R9	AKEP-i në bashkëpunim me AKSK-në, EC-në, ENISA-n, palët e interesit	SA02, SA03, SA09, SA10
	Qëndrueshmëri dhe vazhdimësi				
TM11	Forcimi i planeve të qëndrueshmërisë dhe vazhdimësisë	Sigurohuni që operatorët celularë (MNO) të forcojnë planet e tyre të qëndrueshmërisë dhe vazhdimësisë. MNO-të, operatorët celularë duhet të garantojnë se kanë plane të përshtatshme, në rast katastrofash që ndikojnë në funksionimin e vazhdueshëm të rrjetit të tyre dhe të sigurojnë që çdo varësi kritike të jetë e identifikuar dhe e zbutur sipas nevojës. MNO-të operatorët celularë duhet të kërkojnë rregullime të ngjashme edhe nga furnitorët e tyre dhe të përdorin vetëm ata furnitorë, që demonstrojnë nivele të mjaftueshme të qëndrueshmërisë afatgjatë.	R7, R8	AKEP-i në bashkëpunim me AKSK-në, furnitorët, operatorët e infrastrukturës kritike	SA07, SA08, SA10

Veprime mbështetëse (SA) për sigurinë e rrjeteve 5G				
Siguria e rrjetit				
Nr.	**Veprimi mbështetës**	**Përshkrimi**	**Aktorët**	**Masat e ndërlidhura**
SA01	Rishikimi ose zhvillimi i udhëzimeve dhe i praktikave më të mira mbi sigurinë e rrjetit	Përditësimi i udhëzimeve teknike ekzistuese për masat e sigurisë për ofruesit e shërbimeve të komunikimeve, bazuar në direktivën e BE-së për kuadrin e telekomunikacionit dhe në përputhje me nenet 54–56 të ligjit për komunikimet elektronike, duke marrë parasysh edhe nevojën për të zhvilluar praktika të mira për teknologji të reja, si virtualizimi i funksioneve të rrjetit (NFV).	AKEP-i në bashkëpunim me AKSK-në; - ENISA; - Operatorët.	SM01, TM01, TM04
SA02	Forcimi i kapaciteteve të testimit dhe auditimit në nivel kombëtar	Forcimi i kompetencave, kapaciteteve për testim dhe auditim në nivel kombëtar dhe në veçanti: mbështetja e zhvillimit të ekspertizës së ofruesve të shërbimeve të auditimit të sigurisë së sistemeve të informacionit në auditimet e sigurisë së telekomunikacioneve, përmes ndërtimit të kapaciteteve dhe investimeve të BE-së në trajnim; krijimi i një kuadri në nivel kombëtar për auditimet teknike dhe vlerësimin e sigurisë do të mundësojë një pozicion më të fortë për të kërkuar siguri nga furnitorët.	AKEP-i në bashkëpunim me AKSK-në - Komisioni Evropian (EC); - ENISA.	SM02, TM07, TM08, TM09, TM10
Standardizimi				
SA03	Mbështetja dhe formësimi i standardizimit të 5G	Rritja e përfshirjes në organet përkatëse të standardizimit, veçanërisht përmes koordinimit të forcuar në nivel kombëtar, me qëllim për të ndikuar në standardizim sipas nevojave të identifikuara. Kjo përfshin krijimin e një forumi ose grupi të autoriteteve rregullatore dhe autoriteteve të tjera përkatëse të shteteve anëtare, që raportojnë te grupi i bashkëpunimit NIS dhe EECG. Detyrat përfshijnë konvergjencën teknike përmes standardizimit dhe certifikimit, promovimin e ndërfaqeve të standardizuara për të rritur diversitetin e furnitorëve, ndërlidhjen me trupat standardizues evropianë/ndërkombëtarë dhe përfshirjen e plotë të industrisë së BE-së.	AKEP-i në bashkëpunim me AKSK-në - KE; - operatorët; - furnitorët; - ENISA.	SM05, SM06, TM02, TM09, TM10
SA04	Zhvillimi i udhëzimeve për zbatimin e masave të sigurisë në standardet ekzistuese 5G	Zhvillimi i udhëzimeve specifike kombëtare për zbatimin e masave të sigurisë, në kuadër të standardeve ekzistuese 5G (p.sh. 3GPP). Përfshin rekomandime për elementet opsionale të standardizimit dhe aspektet që nuk mbulohen nga standarde specifike, si dhe identifikimin e boshllëqeve ekzistuese në standardizimin e arkitekturave dhe funksionaliteteve për të adresuar rreziqet e identifikuara.	- AKEP-i në bashkëpunim me AKSK-në; - ENISA.	SM01, TM02
SA05	Sigurimi i zbatimit të masave të standardizuara të sigurisë përmes një skeme të certifikimit të BE-së	Të konsiderohet zhvillimi i një skeme certifikimi në nivel kombëtar për sistemet e menaxhimit të sigurisë së informacionit (ISMS) për ofruesit e shërbimeve të komunikimit elektronik, nën kuadrin e certifikimit të BE-së për sigurinë kibernetike.	- AKEP-i në bashkëpunim me AKSK-në; - ENISA; - palë të interesuara.	TM01 deri në TM06
Furnizuesit e palëve të treta				

SA06	Shkëmbimi i praktikave më të mira për zbatimin e masave strategjike, veçanërisht kuadri kombëtar për vlerësimin e profilit të rrezikut për furnitorët	Lehtësimi i një qasjeje të koordinuar përmes shkëmbimit të praktikave më të mira në zbatimin e masave strategjike, sidomos mbi faktorët e rrezikut që duhen marrë parasysh në vlerësimin e profilit të rrezikut të furnitorëve. Këta faktorë janë të listuar në raportin e vlerësimit të rrezikut të koordinuar të BE-së, në raportin e vlerësimit, këta faktorë mund të përfshijnë informacion të veçantë për çdo vend si niveli i penetrimit të tregut nga furnizuesit, inteligjencën mbi kërcënimet nga shërbimet e sigurisë kombëtare etj.	- AKEP-i në bashkëpunim me AKSK-në	SM01, SM03, SM04
Qëndrueshmëri dhe vazhdimësi				
SA07	Përmirësimi i koordinimit në përgjigjen ndaj incidenteve dhe menaxhimin e krizave	Nëpërmjet punës në vijim brenda grupit të dedikuar NIS, të sigurohet bashkëpunimi dhe koordinimi efektiv ndërmjet autoriteteve kombëtare dhe në nivel BE-je, në rast të incidenteve kibernetike ndërkufitare dhe krizave. Gjithashtu, shtetet anëtare mund të përfshijnë skenarë të lidhur me 5G në ushtrimet kibernetike kombëtare ose të BE-së.	- AKEP-i në bashkëpunim me AKSK-në; - ENISA.	TM11
SA08	Kryerja e auditimeve të ndërvarësive mes rrjeteve 5G dhe shërbimeve të tjera kritike	Analiza e ndërvarësive kritike midis rrjeteve 5G dhe sektorëve të tjerë kritikë, si furnizimi me energji elektrike, ujë të pijshëm dhe transport. Duhet të merren parasysh edhe varësitë rrethore (p.sh. rrjeti 5G që varet nga energjia, dhe energjia që varet nga rrjeti 5G).	- AKEP-i në bashkëpunim me AKSK-në.	TM11
Bashkëpunimi dhe koordinimi				
SA09	Fuqizimi i bashkëpunimit, koordinimit dhe mekanizmave të shkëmbimit të informacionit	Të konsiderohet përdorimi i mekanizmave ekzistues për bashkëpunim, koordinim dhe shkëmbim informacioni, duke përfshirë edhe veprimet e mbështetura nga ENISA, veçanërisht përmes vlerësimeve të rregullta të kërcënimeve.	- AKEP-i në bashkëpunim me AKSK-në; - ENISA.	TM01, TM05, TM09, TM10
Prokurimi publik				
SA10	Të sigurohet që projektet 5G të mbështetura nga fonde publike të marrin në konsideratë rreziqet kibernetike	Zhvillimi i udhëzimeve të detajuara për dispozitat e sigurisë, në lidhje me 5G në prokurimet publike dhe programet e financimit të BE-së (*Horizon, Connecting Europe Facility, Digital Europe Programme*). Këto udhëzime mund të përgatiten përmes procedurës komitologjike nga përfaqësues të emëruar nga shtetet anëtare. Programet si *CEF Digital* pritet të kenë rol kyç në zhvillimin e rrjeteve 5G në Evropë. Prandaj, udhëzimet e përmendura duhet të përdoren gjatë zbatimit të këtyre programeve. Rreziqet e sigurisë kibernetike të identifikuara në raportin e BE-së dhe mjetet e zbutjes përkatëse të përcaktuara në këtë *Toolbox,* duhet të merren në konsideratë gjatë përzgjedhjes së furnitorëve ose pjesëmarrësve të tjerë të projektit. Në nivel kombëtar, prokurimi publik nuk duhet të bazohet vetëm në çmimin më të ulët, por edhe në cilësinë, që lidhet me sigurinë, standardet e punës dhe ato mjedisore. Rekomandimi i Komisionit i 26 marsit 2019 përmend në mënyrë të veçantë zhvillimin e zbatimin e skemave të certifikimit të sigurisë kibernetike në prokurimet publike për 5G.	- AKEP-i në bashkëpunim me AKSK-në, - Komisioni Evropian (KE).	SM03 deri në SM08; TM01 deri në TM11

Shtojca 3

Lista e shkurtimeve

3GPP	Projekti i Partneritetit të Gjeneratës së 3-të
5G	Gjenerata e 5-të
AKEP	Autoriteti i Komunikimeve Elektronike dhe Postare
AKSK	Autoriteti Kombëtar për Sigurinë Kibernetike
BE	Bashkimi Evropian
CEF	Lehtësi për lidhjen e Evropës
EC	Komisioni Evropian
EECC	Kodi Evropian për Komunikimet Elektronike
EECG	Grupi Evropian për Certifikimin e Sigurisë Kibernetike eSIM-SIM/Kartë e/i integruar
IoT	Interneti i Gjërave
ISMS	Sistemet e menaxhimit të sigurisë së informacionit MEC Përpunim të skajshëm me akses të shumëfishtë
MNO	Operator Rrjeti i Lëvizshëm
NIS	Sistemet e rrjetit dhe informacionit
NFV	Virtualizimi i funksioneve të rrjetit
NOC	Qendrat e Menaxhimit të Rrjetit
TIK	Teknologjia e informacionit dhe komunikimit
TM	Masa teknike
SA	Veprime mbështetëse
SM	Masat strategjike
SM01	Forcimi i rolit të autoriteteve kombëtare
SM02	Kryerja e auditimeve të operatorëve dhe kërkimi i informacionit
SM03	Vlerësimi i profilit të rrezikut të furnitorëve dhe aplikimi i kufizimeve për furnitorët e konsideruar me rrezik të lartë – përfshirë masat e përjashtimit për një eliminim efektiv të rrezikut për asetet kyçe
SM04	Kontrolli i përdorimit të "*Managed Service Providers*" (MSPs) dhe furnitorëve të pajisjeve të mbështetjes nga palë të treta
SM05	Sigurimi i diversifikimit të furnitorëve për MNO individuale përmes strategjive me shumë furnitorë
SM06	Forcimi i qëndrueshmërisë në nivel kombëtar
SM07	Identifikimi i aseteve kyçe dhe nxitja e një ekosistemi 5G të larmishëm, dhe të qëndrueshëm në BE
SM08	Mirëmbajtja dhe ndërtimi i diversifikimit dhe i kapaciteteve për teknologjitë e rrjeteve të ardhshme
SOC	Qendrat e operacioneve të sigurisë
URWP	Programi i përditësuar/në vazhdim i punës së Unionit

VENDIM
Nr. 317, datë 6.5.2026

PËR SHPRONËSIMIN, PËR INTERES PUBLIK, TË PRONARËVE TË PASURIVE TË PALUAJTSHME, PRONË PRIVATE, QË PREKEN NGA REALIZIMI PROJEKTIT "NDËRTIM RRUGA KASHAR – NYJA VAQAR, FAZAT I DHE II"

Në mbështetje të nenit 100 të Kushtetutës dhe të neneve 5, 20 e 21, të ligjit nr. 8561, datë 22.12.1999, "Për shpronësimet dhe marrjen në përdorim të përkohshëm të pasurisë pronë private për interes publik", të ndryshuar, me propozimin e ministrit të Infrastrukturës dhe Energjisë, Këshilli i Ministrave

VENDOSI:

1. Shpronësimin, për interes publik, të pronarëve të pasurive të paluajtshme, pronë private, që preken nga realizimi i projektit "Ndërtim rruga Kashar – Nyja Vaqar, fazat I dhe II".

2. Shpronësimi bëhet në favor të Autoritetit Rrugor Shqiptar.

3. Pronarët e pasurive të paluajtshme, pronë private, që shpronësohen, kompensohen në vlerë të plotë, sipas masës përkatëse, që paraqitet në tabelën që i bashkëlidhet këtij vendimi, për pasuritë e llojit "arë", "vreshtë", "pemëtore", "ullishte" dhe "ndërtesë", me një vlerë të përgjithshme prej 126 284 521 (njëqind e njëzet e gjashtë milionë e dyqind