SINTEZA
obiecțiilor și propunerilor/recomandărilor instituțiilor abilitate la avizarea repetată
la proiectul hotărârii de Guvern
cu privire la Legea privind securitatea cibernetică

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
1.	**Agenția de Guvernare Electronică** nr. 3007 – 36 din 28.02.2023		Analizând argumentarea autorului proiectului de neacceptare a unor propuneri din avizul Agenției nr.3007-19 din 31.01.2023, expuse în sinteză la proiect, susținem, în principiu, argumentele invocate. În acest context, vă comunicăm că, în limitele competențelor instituției, avizăm favorabil versiunea definitivată a proiectului de lege și nu avem obiecții sau propuneri.	
2.	**Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației** nr. 02-DRAS/ 308 din 01.03.2023		Lipsa obiecțiilor, suplimentar celor incluse în Sinteza obiecțiilor și propunerilor/recomandărilor la proiect.	
3.	**Agenția Națională pentru Reglementare în Energetică** nr. 06-01/820 din 01.03.2023		Lipsa obiecțiilor și propunerilor.	
4.	**Cancelaria de Stat** nr. 29 - 69 -2272 din 02.03.2023		Lipsa obiecțiilor și propunerilor.	
5.	**Aparatul Președintelui Republicii Moldova** *Nr.2/1-05-277 din 03.03.2023*		Ca urmare a examinării repetate a proiectului de hotărâre a Guvernului privind aprobarea proiectului de lege privind securitatea cibernetică (număr unic 41/ME/2023), Aparatul Președintelui Republicii Moldova informează despre lipsa obiecțiilor și propunerilor adiționale	

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
6.	**Ministerul Afacerilor Externe și Integrării Europene al Republicii Moldova** nr. DI/3/041.1-2595 din 03 martie 2023		Lipsa obiecțiilor și propunerilor.	
7.	**Serviciul Tehnologia Informației Și Securitate Cibernetică** nr. 1.4/362/23 din 01.03.2023	*1)*	I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică", în limitele competenței funcționale, reiterează obiecțiile prezentate prin avizul cu nr. 1.4/228/23 din 02.02.2023, neacceptate de către autor. De asemenea, obiectăm repetat asupra faptului că legea privind securitatea cibernetică trebuie să instituie cerințele, măsurile și mecanismele pentru asigurarea securității cibernetice, inclusiv a sistemelor informaționale.	**Se acceptă.** Proiectul a fost ajustat în conformitate cu obiecții și propunerile pertinente înaintate de către părțile interesate în procesul de consultare publică și avizare oficială, inclusiv cu cele ale Serviciului Tehnologia Informației și Securitate Cibernetică care sunt concludente.
		2)	2. La art. 2: 1) Având în vedere obiecția de mai sus, lista de noțiuni se va completa cu cea de „sistem informațional", ținând cont de faptul că legea nr. 476/2003 cu privire la informatizare și la resursele informaționale de stat, stabilește la art. 3 definiția acesteia.	**Nu se acceptă.** Aceasta ține de obiectul de reglementare a Legii nr. 467/2003. Pentru necesitățile de reglementare ale proiectului de lege este utilizată noțiunea de rețea și sistem informatic.
		3)	2) În ceea ce privește pct. 11), autorul va defini separat noțiunile de „rețea" și „sistem informatic", întrucât redacția utilizată este confuză iar noțiunile nu sunt determinate și precise. Se va reține că legea nr. 100/2017 cu privire la actele normative, stabilește la art. 54 alin. (1) lit. d) că: „d) noțiunea se redă prin termenul respectiv, evitând-se definiția acesteia sau utilizarea frazeologică, aceleași noțiuni se exprimă prin aceiași termeni;", or legea nr. 1069/2000 cu privire la informatică, definește deja „sistemul informatic".	**Nu se acceptă.** Definirea separată a acestor noțiuni nu intră în obiectul de reglementare a acestui proiect de lege. Pentru necesitățile de reglementare în proiectul de lege au fost definite noțiunile strict necesare și suficiente pentru a asigura corectitudinea înțelesului normelor juridice.

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		4)	3. La art. 3: 1) În conținutul lit. f) de la alin. (2), se utilizează sintagma „risc sistemic semnificativ". Astfel, pentru a nu lăsa loc de interpretări și neclarități, autorul fie va completa art. 2 cu definiția acesteia, fie va reformula cuprinsul lit. f).	**Nu se acceptă.** Modul de aplicare a acestei norma și în special de determinare a faptului că un risc este sistemic și semnificativ va fi reglementat prin actul normativ ce va fi aprobat în temeiul art. 4 alin. (2).

Nr. d/o	Participantul la avizare		Continutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		5)	4. La art. 6: 1) Alin. (1) stabileşte că Guvernul va realiza coordonarea strategică la nivel naţional în domeniul securităţii cibernetice prin intermediul autorităţii administraţiei publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securităţii cibernetice. Propunem să se stabilească expres cine va fi această autoritate, întrucât redacţia utilizată trezeşte imprecizii, din următoarele puncte de vedere. Prin art. 21 alin. (2) lit. c) din proiectul de lege, se stabileşte în sarcina Guvernului, determinarea, în termen de 12 luni din data publicării prezentei legi, autoritatea administraţiei publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securităţii cibernetice. Pe de altă parte, autorul indică în Nota informativă că: „Ministerul Economiei este autoritatea administraţiei publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul ... securitatea cibernetică ...". Dar, constatăm că potrivit pct. 5 din Regulamentul cu privire la organizarea şi funcţionarea Ministerului Economiei, aprobat prin anexa nr. 1 la Hotărârea Guvernului nr. 143/2021: „Ministerul are misiunea de a... elabora politici publice eficiente în domeniile prevăzute la punctul 6, de a monitoriza calitatea politicilor...". Totodată, remarcăm că securitatea cibernetică nu se regăseşte printre domeniile de competenţă ale Ministerului Economiei. De asemenea, potrivit pct. 2 din Statutul IP STISC, aprobat prin anexa nr. 1 la Hotărârea Guvernului nr. 414/2018: „Serviciul este o instituţie publică a cărei activitate are scopul de a asigura ..., precum şi implementarea politicii statului în domeniul securităţii cibernetice".	**Nu se acceptă.** Stabilirea ministerului sau altei autorităţi administrative centrale în subordinea Guvernului care este sau va fi responsabilă de realizarea politicii de stat în domeniul securităţii cibernetice ţine de competenţa Guvernului. Stabilirea în lege a acestui fapt va limita nejustificat discreţia legală a Guvernului de a organiza conducerea generală a administraţiei publice.

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		6)	2) La alin. (2) este insuficient reglementat rolul Consiliului şi atribuţiile sale, precum şi componenţa acestuia. Considerăm necesar a se completa.	**Nu se acceptă.** Prevederea respectivă stabileşte misiunea Consiliului şi obligativitatea Guvernului de a constitui un astfel de Consiliul. Modul de organizare şi funcţionare a acestuia este o prerogativă discreţionară a Guvernului în conformitate cu prevederile Legii nr. 136/2017cu privire la Guvern. Înserarea unor prevederi suplimentare ar restrânge marja discreţionară a Guvernului şi ar putea avea riscul din cauza unei supra-reglementări, de a îngreuna implementarea prevederilor legii.
		7)	2) La art. 7 alin. (3) la lit. h), se indică că autoritatea competentă exercită atribuţiile agentului constatator pentru cauze contravenţionale în domeniul securităţii reţelelor şi sistemelor informatice în conformitate cu prevederile Codului contravenţional. Reieşind din cele menţionate în analiza de impact la proiectul de lege, se constată posibilitatea de a se crea sau numi o instituţie publică în calitate de autoritate competentă. Astfel, atragem atenţia că din definiţia dată instituţiei publice la art. 307 din Codul civil, în coroborare cu prevederile Codului contravenţional, instituţia publică nu poate exercita atribuţiile agentului constatator. Or, potrivit alin. (1) al art. 385 din Codul contravenţional: „Agentul constatator este reprezentantul autorităţii publice care soluţionează, în limitele competenţei sale, cauza contravenţională în modul prevăzut de prezentul cod", iar potrivit art. 7 din Codul administrativ, Autoritatea publică acţionează în regim de putere publică.	**Precizare.** Conceptul instituţional propus în proiect în ce priveşte autoritatea competentă, în coroborare cu prevederile Legii nr. 98/2012 privind administraţia publică centrală de specialitate ne permit să stabilim că autoritatea competentă va face parte din categoria autorităţilor publice – autorităţi administrative subordonate ministerului sau altei autorităţi administrative centrale (art. 14 din Legea nr. 98/2012).
		8)	7. Noţiunile de „autentificare multifactor" şi „autentificare continuă", utilizate de către autor la ultima liniuţă a alin. (2) de la art. 11, se vor defini.	**Se acceptă.** Prevederea respectivă a fost revizuită, astfel fiind exclusă referirea la aceste noţiuni. Totuşi ţinem să relevăm că definirea acestor termeni nu intră în obiectul de reglementare al proiectului de lege şi urmează a fi dată în legile cadru care reglementează domeniul tehnologiei informaţiei şi comunicaţiilor.

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		9)	8. La lit. b) alin. (4) al art. 12, autorul utilizează noțiunea „nivelul agreat al serviciilor", pe care propunem să o definească, pentru claritate.	**Nu se acceptă.** Definirea acestor termeni nu intră în obiectul de reglementare al proiectului de lege și urmează a fi dată în legile cadru care reglementează domeniul tehnologiei informației și comunicațiilor și s/sau legislați a civilă.
		10)	9. La art. 13: 1) Subliniem că alin. (1) se contrazice cu art. 12, în partea de notificare a incidentelor cibernetice.	**Se acceptă parțial.** Alineatul (1) din art. 13 a fost transferat în art. 12 ca lin. (10) cu următoarea redacție „Obligația prevăzută la alineatul (1) nu restrânge dreptul furnizorului de servicii de a notifica autoritatea competentă cu privire la amenințările cibernetice și la incidentele evitate la limită, precum și la incidentele cibernetice care nu au un impact semnificativ prevăzut la alineatul Totuși ținem să remarcăm că spre deosebire de art. 12, care stabilește obligația furnizorilor de servicii de a notifica incidentele cibernetice semnificative, art. 13 alin. (1) stabilește dreptul furnizorilor de servicii de a notifica și celelalte categorii de incidente.

Nr. d/o	Participantul la avizare		Continutul obiectiei/ propunerii (recomandării)	Argumentarea autorului proiectului
		11)	2) Totodată, constatăm că alin. (4) al art. 13 necesită reformularea pentru o mai mare claritate.	**Nu se acceptă.** Potrivit art. 33 alin. (1) din Legea nr. 100/2017 privind actele normative obiecțiile şi propunerile urmează a fi motivate. Astfel, propunerea formulată nu argumentează în ce constă neclaritatea normei juridice respective. Art.13 reglementează aspecte privind notificarea voluntară de către persoane juridice care nu intră în sfera de acțiune a normelor legale şi, implicit a obligațiunilor impuse de lege. Astfel, spre exemplu dacă o persoană juridică notifică autoritatea competentă despre un incident, aceasta nu va avea obligațiuni privind informarea autorității competente cu privire la evoluția acestuia, așa cum este prescris de art. 12 (alineatele 3 şi 8), Pentru că aceste obligații persoana juridică nu le avea nici până la prezentarea notificării voluntare. Totuşi , dacă urmare acestei notificări, s-au constatat anumite fapte infracționale, inclusiv imputate persoanei juridice notificatoare, această persoană juridică va fi subiect al obligațiilor stabilite de legislația penală şi procesual penală.
		12)	12. La alin. (4) al art. 16, propunem să se extindă termenul de informare de la „3 zile" la „10 zile".	**Nu se acceptă.** Urmare a definitivării proiectului art. 16 a devenit art. 17. Termenul de 3 zile este un termen rezonabil de informare a autorității competente despre faptul semnării sau retragerii din acordurile de schimb de informații. 10 zile sunt un termen excesiv pentru o simplă informare a autorității competente.
		13)	2) La alin. (5), se va substitui sintagma „instituțiile publice" cu sintagma „entitățile publice".	**Nu se acceptă.** Entități publice este o noțiune care este prea generică şi nu reflectă cercul de subiecți care sunt vizați prin această normă juridică. Alineatul respectiv a fost transferat la art. 4 alin. (4).

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
8.	**Cancelaria de Stat,** ***Centrul de armonizare a legislației*** nr. 31/02-69-2228 din 02.03.2023	*14)*	Proiectul național are drept obiectiv principal transpunerea primară și parțială în legislația națională a Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2). Astfel, proiectul național instituie norme cadru privind competențele autorităților și instituțiilor publice în materie de securitate cibernetică, reglementează cadrul național general de gestionare a crizelor în domeniul securității cibernetice, stabilește cerințele, măsurile și mecanismele pentru asigurarea securității rețelelor și a sistemelor informatice care sunt esențiale pentru funcționarea societății, precum și reflectă modul de gestionare a incidentelor cibernetice. Ca urmare a expertizei de compatibilitate a versiunii inițiale a proiectului (Declarația de compatibilitate nr. 31/02-126-1118 din 2 februarie 2023), Centrul de armonizare a legislației a constatat că proiectul în cauză asigură transpunerea parțială a Directivei 2022/2555/UE. Totodată, au fost înaintate o serie de obiecții privind compatibilitatea cu actul UE și referitoare la Tabelul de concordanță, instrument principal al procesului de armonizare legislativă. Versiunea actuală a proiectului este una îmbunătățită, fiind preluate obiecțiile referitoare la transpunerea art. 2 (1) din actul UE (aplicabilitatea normelor deopotrivă asupra entităților publice sau private, care desfășoară activități în sectoare de o importanță critică ridicată, precum și în alte sectoare de importanță critică),	**Se acceptă.**

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		15)	au fost excluse prevederile referitoare la dreptul autorității competente de a restricționa utilizarea sau accesul la un sistem informatic pentru un furnizor, care erau contrare art. 31 (5) din actul UE.	**Nu se acceptă.** Această prevedere nu a fost exclusă, alineatul (3) din art.17 a fost transferat la art. 15 alin. (2), care prevede prevenirea și soluționarea incidentelor cibernetice. Art. 32 alin. (4) și alin. (5) din Directiva NIS2 la care presupunem că a făcut referire autorul obiecției (art. 31 al NIS2 nu are un alin. (5)) nu prevăd o astfel de măsură. Procedurile de supraveghere și control specifice vor fi stabilite printr-un cadrul guvernamental subordonat legii. De asemenea, prevederile art. 32 alin.(4) și (5) din Directiva NIS2 referitoare la posibilitatea suspendării unor drepturi ale entităților esențiale nu vizează o astfel de măsură. Măsura propusă în proiectul de lege este una extraordinară, care urmează a fi aplicată ca un ultim argument în răspunsul la un incident cibernetic care are un impact semnificativ și poate perturba anumite servicii esențiale, consecințele putând fi din cele mai negative. Condițiile stabilite pentru aplicarea acestei măsuri sunt un compromis dintre limitarea discreției autorității competente, dar și aplicarea cât mai urgentă a unor remedii funcționale, care nu trebuie să depindă de incapacitatea sau incompetența unui furnizori de servicii de a reacționa prompt la astfel de provocări.

		16)	Totodată, reiterăm o serie de obiecții, care nu au fost reținute de proiectul național, dar care vor fi transpuse prin acte normative de implementare a Legii și care nu constituie impedimente pentru promovarea proiectului, după cum urmează: - Art. 4, alin. (2) din proiect stabilește că lista sectoarelor, sub sectoarelor, precum și a tipurilor și categoriilor de persoane juridice care prestează servicii în aceste sectoare și sub sectoare va fi aprobată ulterior de Guvern, ori actul UE, prin art. 3 și Anexa I și II, stabilește norme minime referitoare la entitățile esențiale și cele importante, precum și identifică (la nivel exemplificativ, cu drept de extindere a listei) sectoarele cu o importanță critică ridicată (Anexa I) și alte sectoare de importanță critică (Anexa II);	**Precizare.** Directiva NIS2 în art. 5 prevede principiul armonizării minime, ceea ce presupune că Statele membre sau cele care transpun această Directivă, cum e și cazul Republicii Moldova, pot să stabilească prevederi care asigură un nivel mai ridicat de securitate cibernetică. Această regulă de bază este incidentă și sectoarelor, subsectoarelor sau tipurilor de entități stabilite în anexele la Directiva respectivă. Cu alte cuvinte statele membre sau statele-candidat pot să stabilească și alte sectoare sau subsectoare decât cele menționate în anexe. Este ilustrativ în acest context alineatul (1) de la art. 10 din Directiva NIS2 care stabilește că CSIRT-urile naționale acoperă cel puțin sectoarele, subsectoarele și tipurile de entități menționate în anexele I și II. De asemenea, lista sectoarelor, subsectoarelor și tipologia entităților critice este una variabilă, în funcție de dinamica dezvoltării economice și sociale. Din aceste rațiuni Directiva NIS2 prevede la art. 40 procedura de revizuire a acesteia, inclusiv din perspectiva relevanței sectoarelor, subsectoarelor și tipurilor de entități esențiale și importante. Din aceste considerente preluarea listei sectoarelor, subsectoarelor și tipologiei entităților esențiale și importante în textul legii din Directiva NIS2 comportă riscul neacoperirii unor sectoare care nu sunt menționate în anexele directivei, însă sunt critice pentru Republica Moldova. În mod normal elaborarea unei legi în domeniul securității cibernetice trebuie să fie precedată de o evaluare și analiză a sectoarelor critice în țara în care o astfel de lege urmează a fi adoptată și implementată. Dat fiind stringența elaborării și promovării proiectului de lege s-a identificat o opțiune valabilă atât din punct de vedere al legalității, cât și din punct de vedere al

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				practicabilității, ca aceste sectoare, subsectoare și tipuri de entități esențiale și importante să fie stabilite de Guvern, după efectuarea unei analize profunde a sectoarelor critice și o identificare preliminară a tuturor subiecților care vor cădea sub incidența obligațiilor stabilite de legea în speță. De asemenea, ținem să evidențiem faptul că aprobarea unui act care să stabilească normele primare de reglementare a cadrului de securitate cibernetică nu este suficient pentru transpunerea Directivei NIS2. Pentru transpunerea chiar și doar parțială a acesteia este necesară realizarea unui spectru larg de măsuri de ordin juridico-normativ, instituțional, organizațional și operațional.
		17)	- Art. 6, alin. (3) din proiectul național a preluat doar la nivel de concept prevederile UE referitoare la Strategia națională de securitate cibernetică din art. 7 al Directivei UE, în speță, în ceea ce privește necesitatea existenței unui atare document de politici în RM și aprobarea acesteia de Parlamentul RM. Nu au fost transpuse prevederile UE aferente elementelor constitutive obligatorii ale Strategiei din art. 7 (1) al actului UE, spectrul de politici care sunt adoptate prin Strategie din art. 7 (2) al actului UE, precum și normele referitoare la actualizarea Strategiilor la intervale de 5 ani din art. 7 (4) al Directivei;	**Precizare.** Potrivit definiției date noțiunii de „strategie națională de securitate cibernetică", conform art.6, din Directiva NIS2, aceasta înseamnă un cadru coerent al unui stat membru care prevede obiective și priorități strategice în domeniul securității cibernetice și guvernanța necesară pentru realizarea acestora în statul membru respectiv. Articolul 7 din Directiva NIS2 detaliază elementele componente ale acestui cadru care urmează a fi implementat de Statele Membre. Analizând prevederile art. 7 din Directiva NIS2, constatăm că termenul de strategie nu este utilizat neapărat în stricto sensu ca un document unic de politici, ci ca un cadru strategic, tactic și operațional ce urmează a fi realizat de statele membre pentru asigurarea unui nivel înalt de securitate a rețelelor și sistemelor informatice. În acest context proiectul de lege este în sine un act care implementează unele aspecte menționate în art. 7 din Directiva NIS2.

Nr. d/o	Participantul la avizare		Continutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		18)	- Art. 18 și 19 din proiectul național, care se referă la supravegherea și controlul de stat asupra furnizorilor de servicii, a transpus doar normele cadru referitoare la supravegherea și controlul exercitat de autoritatea competentă din art. 31 - 33 din actul UE, urmând ca modul detaliat de exercitare a supravegherii și controlului să fie stabilit de către Guvern;	**Precizare.** Actul normativ de punere în aplicare care urmează a fi aprobat de Guvern conform prevederilor alineatului (3) al acestui articol urmează să transpună aspecte mai detaliate ale procesului de supraveghere, inclusiv din perspectiva delimitării măsurilor aplicate în funcție de categoria furnizorului de servicii, esențial sau important. Totodată ținem să relevăm faptul că delimitarea în textul legii a furnizorilor de servicii în esențiali și importanți, din perspectiva principiului armonizării minime, menționate mai sus, ar putea avea riscul includerii unor entități esențiale în categoria celor importante și invers. Din aceste considerente o analiză profundă a sectoarelor, subsectoarelor și tipologiei subiecților legii urmează a fi efectuată în procesul elaborării analizelor de impact și nemijlocit al textului actelor menționate la art. 4 alin.(2) și art. 18 alin. (3).

		19)	- Art. 6 și 7 din proiectul național stabilesc generic, fără o nominalizare, autoritățile naționale cu competență în domeniul securității cibernetice – autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice și autoritatea competentă la nivel național în domeniul securității cibernetice. Acest fapt denotă o implementare parțială a art. 8 din Directiva UE, care impune statelor membre desemnarea sau instituirea autorităților competente, inclusiv, prin identificarea lor nominală.	Directiva NIS2 nu instituie o astfel de cerință cum ar fi identificarea nominală a autorităților competente. Statele membre urmează să desemneze autoritățile respective în conformitate cu reglementările naționale care vizează modul de constituire și organizare a administrației publice. De asemenea, în acest context reiterăm argumentele expuse anterior în procesul de avizare. În primul rând prevederile proiectului care fac referite la autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice nu este o prevedere care transpune prevederile Directivei NIS2. Aceasta este o sintagmă legală care, prin prisma prevederilor art. 107 din Constituție și ale Legii nr. 98/2012, reprezintă un minister sau o autoritate administrativă centrală care realizează politica de stat în acest domeniu. Totodată, art. 8 din Directiva NIS2 deși impune desemnarea sau instituirea unei sau mai multor autorități competente în domeniul securității cibernetice, statele membre au marja de discreție de a institui aceste autorități în corespundere cu cadrul normativ și instituțional național. Astfel, potrivit art. 7 alin. (1) Guvernului i se deleagă atribuția de a desemna o autoritate competentă în domeniul securității cibernetice și să stabilească modul de organizare și funcționare a acesteia. Din perspectivă instituțională, conceptul propus în proiect, ca Guvernul să decidă desemnarea autorității competente în domeniul securității cibernetice se înscrie în spectrul exercitării de către Guvern a prerogativelor sale în stabilirea modului de organizare și funcționare a persoanelor juridice de drept public din structura guvernamentală. Astfel, potrivit prevederilor art. 6 literele b), d) și e) din

				Legea nr. 136/2017 cu privire la Guvern, Guvernul este împuternicit să constituie în structura sa atât autorități administrative centrale, cât și structuri organizaționale în sfera de competență a acestora și cea a ministerelor, precum și să le reglementeze modul de organizare și funcționare. Bineînțeles această marjă discreționară acordată de către Parament Guvernului este limitată, pe de o parte de obiectivele strategice ce urmează a fi realizate și de necesitatea asigurării eficienței și eficacității activității administrative, iar pe de alta de normele legale primare care reglementează administrația publică centrală de specialitate. Modul de organizare și funcționare a persoanelor juridice de drept public în structura Guvernului este stabilit de Legea nr. 98/2014 privind administrația publică centrală de specialitate. Conform proiectului autoritatea competentă în domeniul securității cibernetice, de rând cu funcțiile de echipă de răspuns la incidentele cibernetice la nivel național și de punct național unic de contact urmează să exercite și funcția de supraveghere și control a modului de realizare a obligațiilor stabilite de lege de către furnizorii de servicii, precum și alte atribuții care vizează implementarea politicii statului în domeniul securității cibernetice. Prevederile respective ale proiectului de lege în coroborare cu prevederile art. 4 pct. 1) lit. b), ale art. 14 alin. (5) și ale art. 25 alin. (2) lit. c) ne permit să identificăm forma juridică de organizare a viitoarei autorități competente și anume de autoritate administrativă subordonată unui minister sau unei autorități administrative centrale. Această opțiune specifică în exercitarea de către Guvern a acestei prerogative ar putea fi revăzută la discreția Guvernului, în limitele expuse mai sus, în funcție de evoluția situației atât la nivelul activității

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				administrative guvernamentale, cât şi la nivelul sectorului specific asigurării securității cibernetice.
		20)	Cu referire la instrumentele procesului de armonizare, se constată că în procesul de definitivare al proiectului, nu a fost ajustat Tabelul de concordanță, conform recomandărilor si sugestiilor Centrului. În acelaşi timp, având în vedere importanța proiectului care rezultă din Planul de acțiuni pentru implementarea măsurilor propuse de către Comisia Europeană în Avizul său privind cererea de aderare a Republicii Moldova la Uniunea Europeană, solicităm ca Tabelul de concordanță să fie remis în regim de lucru pentru evaluare calitativă în termen rezonabil. Menționăm că, proiectul de Lege însoțit de tot setul de acte, inclusiv Tabelul de concordanță, urmează a fi prezentat Parlamentului pentru examinare şi adoptare ulterioară. Facem mențiunea că analiza Centrului de armonizare a legislației nu are în vedere elementele de oportunitate ale soluțiilor juridice incluse în proiectul de act normativ, ci se referă strict la conformitatea acestora cu Dreptul UE aplicabil şi obligațiile juridice asumate în lumina Acordului de Asociere RM – UE.	**Se acceptă.** Tabelul de concordanță, ajustat conform obiecțiilor şi propunerilor Centru în procesul avizării proiectului, va fi prezentat ulterior în regim de lucru.

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
9.	**Ministerul Apărării** nr. 11/329 din 02.03.2023	*21)*	1. În ***Capitolul I. Dispoziții generale, Articolul 2. Principalele noțiuni și definițiile lor, se propune:*** ***introducerea noțiunii de*: "apărare cibernetică** – acțiuni desfășurate în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor și asigurării răspunsului oportun împotriva amenințărilor asupra infrastructurilor cibernetice destinate apărării naționale". Argumentare: 1) Apărarea cibernetică este o parte indispensabilă a securității cibernetice și nu poate fi tratată separat. Astfel considerăm că este necesară introducerea noțiunii de apărare cibernetică de care trebuie să cunoască toate părțile implicate în asigurarea securității și apărării cibernetice. 2) Este de menționat că Ministerul Apărării dispune de infrastructură TIC proprie, precum și de circuite, canale și servicii ce aparțin altor autorităților publice și/sau operatorilor economici pe timp de pace în scopul asigurării activităților conform responsabilităților atribuite, precum și planificarea activităților și acțiunilor în caz de instituire a stării de urgență, asediu și de război. Astfel că Ministerul Apărării este responsabil nu doar de propriile capacități defensive și propriul CERT pentru a-și proteja propriile rețele, dar și de infrastructura preluată de la terțe părți pentru toate situațiile expuse mai sus. Ca argument al includerii definiției propuse este și faptul că CERT-ul Ministerului Apărării (Armatei Naționale), precum și infrastructura TIC proprie, reprezintă o parte componentă a securității cibernetice naționale. Faptul dat este actual atât pe timp de pace, cât și în caz de instituire a stării de urgență, asediu și de război.	**Nu se acceptă.** Obiectul de reglementare al legii rezidă în instituirea cadrului instituțional și normativ pentru asigurarea unei cooperări și schimb de informații adecvat între autoritățile publice responsabile și mediul privat. Proiectul de lege are ca scop consolidarea rezilienței cibernetice din perspectivă civilă și nu militară sau de intelligence. Bineînțeles că proiectul de lege propus spre avizare este un act interdisciplinar care are conexiuni profunde cu diferite domenii, inclusiv apărarea națională și securitate națională. Totuși această caracteristică nu este proprie doar acestui act normativ, ci și altor acte care reglementează sfere de activitate civilă. Prin urmare pentru a atinge obiectivele care de curg din propunerile Ministerului Apărării, acest urmează să inițieze în comun cu autoritățile responsabile de domenii precum securitatea națională, gestionarea crizelor, analiza și revizuirea fundamentală a legislației în acest domeniu, revizuire care ar trebuie să integreze organic nu doar reglementările care sunt stabilite de proiectul de lege în speță ci și alte norma legale primare, conținute în acte normative care reglementează situațiile de urgență, starea de război, protecția civilă, etc. Materia propusă spre reglementare de către Ministerul Apărării depășește vădit atât din perspectiva obiectivelor urmărite, cât și a efectelor normelor juridice ale proiectului în speță.

		22)	2. La Capitolul I. Dispoziții generale, Articolul 3. Domeniul de aplicare, se propune de a fi reformulat aliniatul b) din punctul 3, în următoarea redacție: „activităților desfășurate de autoritățile publice în domeniile activității speciale de investigații și urmării penale în legătură cu mentenanța rețelelor și sistemelor informatice destinate prelucrării informațiilor din aceste domenii." și de a fi introdus un alineat nou, cu următorul conținut: "(8) În domeniul apărării naționale: **a)** Infrastructurile cibernetice și măsurile privind apărarea cibernetică a acestora se stabilesc de Guvern la propunerile Consiliului coordonator în domeniul securității cibernetice; **b)** Autoritățile și instituțiile publice, furnizorii de servicii și de infrastructuri critice destinate apărării naționale au obligația de a identifica și implementa, măsuri de apărare cibernetică și răspund de executarea acestora; **(c)** Ministerul Apărării împreună cu celelalte autorități și instituții publice asigură în timp de pace, furnizorii de servicii, de infrastructuri critice destinate apărării naționale, integrarea într-o concepție unitară a activităților la instituirea stării de urgență, asediu și de război; **(d)** Conducerea acțiunilor de apărare cibernetică în caz de instituire a stării de urgență, asediu și de război se realizează de către Centrul de reacție la incidente cibernetice al Armatei Naționale." Argumentare: 1) Considerăm oportună includerea aspectelor ce țin de securitatea și apărarea cibernetică în prevederile legii date pentru a nu tergiversa timpul și clarificarea situației pe domeniul securității cibernetice. Faptul dat va facilita inițierea proceselor și procedurilor de fortificare a capacităților din domeniul securității și apărării naționale, dat fiind faptul că situația actuală presupune întreprinderea măsurilor urgente în acest domeniu. Trebuie de menționat că apărare cibernetică reprezintă un element indispensabil de securitatea cibernetică și în final	**Nu se acceptă.** Obiectul de reglementare al legii rezidă în instituirea cadrului instituțional și normativ pentru asigurarea unei cooperări și schimb de informații adecvat între autoritățile publice responsabile și mediul privat. Proiectul de lege are ca scop consolidarea rezilienței cibernetice din perspectivă civilă și nu militară sau de intelligence. Bineînțeles că proiectul de lege propus spre avizare este un act interdisciplinar care are conexiuni profunde cu diferite domenii, inclusiv apărarea națională și securitate națională. Totuși această caracteristică nu este proprie doar acestui act normativ, ci și altor acte care reglementează sfere de activitate civilă. Prin urmare pentru a atinge obiectivele care de curg din propunerile Ministerului Apărării, acest urmează să inițieze în comun cu autoritățile responsabile de domenii precum securitatea națională, gestionarea crizelor, analiza și revizuirea fundamentală a legislației în acest domeniu, revizuire care ar trebuie să integreze organic nu doar reglementările care sunt stabilite de proiectul de lege în speță ci și alte norma legale primare, conținute în acte normative care reglementează situațiile de urgență, starea de război, protecția civilă, etc. Materia propusă spre reglementare de către Ministerul Apărării depășește vădit atât din perspectiva obiectivelor urmărite, cât și a efectelor normelor juridice ale proiectului în speță.

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			rezumă la asigurarea securității și apărării cetățenilor, mediului privat și public. 2) În scopul reglementării domeniului de apărare cibernetică, precum și stabilirea competențelor și responsabilităților Ministerului Apărării pe domeniul dat se propune includerea expres în lege a acestui fapt.	
		23)	3. Capitolul VI. Dispoziții finale și tranzitorii, Articolul 21. Intrarea în vigoare a legii și măsuri de implementare, aliniat, (1) Prezenta lege intră în vigoare pe data de 1 ianuarie 2025, se propune de reformulat prin atribuirea unui termen ce intră în vigoare de la data publicării în monitorul oficial. Argumentare: Situația la moment presupune întreprinderea măsurilor urgente, iar faptul dat nu poate fi extins până în 2025, mai ales că implementarea prevederilor legii date presupune întreprinderea inițială a măsurilor de către autoritățile publice vizate, după care implementarea acestora de către toate părțile implicate.	**Nu se acceptă.** Implementarea prevederilor legii în speță va presupune întreprinderea unor acțiuni de ordin normativ, instituțional și organizatoric atât din partea autorităților publice responsabile, cât și din partea furnizorilor de servicii. Din acest considerent acordarea unui termen rezonabil pentru măsurile pregătitoare pentru intrarea în vigoare a legii este de o importanță practică n primul rând.

10.	**Ministerul Afacerilor Interne** *nr. 44/30-981 din 02.03.2023*	*24)*	Conform misiunii sale ministerul analizează situația și problemele din domeniile de activitate gestionate, precum și elaborează politici publice eficiente în domeniile de activitate aferente și reconfirmă propunerile asupra proiectului de hotărâre *privind aprobarea proiectului de lege privind securitatea cibernetică* **(număr unic 41/ME/2023)** prezentate anterior prin scrisoarea 44/30 – 466 din 01 februarie 2023 care nu au fost acceptate, după cum urmează: *La proiectul de lege* Proiectul conține reglementări clare privind rolul, drepturile și obligațiile echipei de răspuns la incidentele cibernetice la nivel național, dar reieșind din prevederile art. 11 *(Măsurile de securitate ale rețelelor și sistemelor informatice ale furnizorilor de servicii)* se impune obligația furnizorului de servicii să ia măsuri tehnice și organizatorice corespunzătoare și proporționale, pentru a gestiona riscurile legate de securitatea rețelelor și a sistemelor informatice pe care le utilizează în activitatea sa, precum au obligația de a notifica echipă de răspuns la incidentele cibernetice la nivel național privind incidentele cibernetice înregistrate. Aceste activități presupun crearea/existența/ extinderea Centrelor operaționale de securitate cibernetică create de furnizori de servicii, care asista beneficiarii în utilizarea sistemelor informaționale și de telecomunicații ale furnizorilor de servicii TIC în implementarea măsurilor pro active și reactive în vederea reducerii riscurilor de incidente ale securității TIC și acordarea asistenței în reacționarea la incidente, după caz cooperare si suport echipei de răspuns la incidentele „cyber". Ținând cont de prevederile Hotărârii Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale se stat, este de notat, că autorul nu vorbește despre CERT-urile Departamentale ale Guvernului - ***CERT-departamental***	**Nu se acceptă.** Modul de constituire a CERT-urilor guvernamentale nu intră în obiectul de reglementare al acestei legi. Proiectul de lege are ca scop instituirea mecanismelor de interacțiune la nivel național în procesul de asigurare a securității cibernetice prin implementarea măsurilor de securitate și realizarea obligațiilor de schimb de informații cu CSIRT-ul național a furnizorilor de servicii din mediul public și privat. Măsurile de securitate de ordin organizatoric pe care le vor lua furnizorii de servicii rămân la latitudinea acestora. Spre exemplu, Guvernul prin Hotărârea sa nr. 482/2020 a impus instituirea CERT-urilor departamentale. Un furnizor de servicii privat, în schimb, ar putea apela la externalizarea unor astfel de servicii. Efectul pe care îl produc obligațiile impuse prin normele proiectului de lege este să se asigure o protecție adecvată a rețelelor și sistemelor informatice, iar metodele urmează a fi identificate de către furnizorii de servicii în corespundere cu principiile legalității eficienței eficacității proporționalității, etc. Furnizorii de servicii au dreptul discreționar de asemenea să-și unească eforturile, spre exemplu într-un sector sau subsector în vederea constituirii unei echipe comune de răspuns la incidentele cibernetice, bineînțeles că atunci când decide organizarea măsurilor sale de securitate furnizorul de servicii trebuie să țină cont că anume el este subiectul obligațiilor impuse de lege și trebuie să se asigure că în relațiile contractuale cu anumiți furnizori de servicii de securitate aceștia vor asigura îndeplinirea corespunzătoare a acestor obligații.

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			subdiviziune sau persoană responsabilă desemnată în cadrul entităților publice care dețin infrastructuri/sisteme de tehnologia informației și comunicații și care dispun de capacitatea necesară pentru a ține evidența operativă obligatorie și a raporta incidentele de securitate cibernetică. ***Entități publice*** *ministerele, alte autorități administrative centrale subordonate Guvernului, Cancelaria de Stat și structurile organizaționale din sfera lor de competență (autoritățile administrative din subordine, serviciile publice desconcentrate și cele aflate în subordine, precum și instituțiile publice și întreprinderile de stat în care ministerul, Cancelaria de Stat sau altă autoritate administrativă centrală are calitate de fondator) și organizațiile de stat autonome înființate de Guvern.* Astfel, Ministerul Afacerilor Interne, întrunește toate condițiile prenotate și reieșind din noțiunile enunțate, proiectul de lege nu stipulează care ar fi locul, acțiunile, interacțiunile, raportările, atribuțiile, obligațiunile etc. ministerului, iar proiectul de lege pune la îndoială existența unui astfel de CERT - departamental în cadrul Ministerului Afacerilor Interne. În acest context, propunem completarea art. 8 din Proiect cu un aliniat nou care să prevadă implicarea/ desemnarea reprezentanților furnizorilor de servicii critice și autorităților responsabile de domeniu în activitățile centrul guvernamental de răspuns la incidentele cibernetice în vederea bunei cooperări in realizarea activităților de răspuns la incidentele cibernetice la nivelul rețelelor și sistemelor informatice naționale. Reieșind din cele menționate, Ministerul Afacerilor Interne, solicita respectuos luarea in calcul a obiecțiilor prezentate, intru avizarea pozitivă a proiectului de lege propus.	

11.	**Centru Național Anticorupție** *Nr. ELO23/8569 din 03.03.2023*	*25)*	**Cu referire la art. 8 din proiect** Prin norma articolului 8, Guvernul este investit cu atribuția de a institui Centrul guvernamental de răspuns la incidentele cibernetice la nivelul rețelelor și sistemelor informatice ale căror proprietar este statul. Potrivit alin.(3) al art.8, Centrul guvernamental de răspuns la incidentele cibernetice este responsabil de asigurarea securității rețelelor și sistemelor informatice ale căror proprietar este statul și de facilitarea realizării de către furnizorii de servicii - persoane juridice de drept public a obligațiilor de asigurare a securității cibernetice prevăzute de lege, inclusiv a celor de notificare și a interacțiunii acestora cu autoritatea competentă și echipa de răspuns la incidente cibernetice la nivel național. În acest sens, constatăm că norma art.8 nu stabilește expres funcția Centrului, precum și atribuțiile acestuia, lăsând acest aspect pentru a fi reglementat de către Guvern. Or, considerăm că odată ce, potrivit art.7 din lege, autorității competente îi sunt stabilite expres atribuții, necesită reglementarea expresă și a atribuțiilor Centrului, în vederea excluderii riscurilor de stabilire a unor atribuții paralele între aceste entități sau a unor atribuții care pot depăși scopul instituirii Centrului. Astfel, atât în cazul autorității competente, cât și în cazul Centrului guvernamental de răspuns la incidente cibernetice, Guvernul urmează să stabilească doar modul de organizare și funcționare a acestora. În final, menționăm că nestabilirea atribuțiilor Centrului în lege, va crește riscul stabilirii unor atribuții paralele sau a unor atribuții care pot depăși atribuțiile autorității competente în anumite direcții, ceea ce se poate răsfrânge negativ asupra finalității scopului instituirii autorității competente și a Centrului guvernamental în partea ce ține de asigurarea eficientă a securității cibernetice. **Recomandări:** Propunem autorului includerea în norma articolului 7 a	**Se acceptă parțial.** Proiectul de lege a fost ajustat prin completarea art. 12 cu un alineat nou (11) în următoarea redacție: *(11) Furnizorii de servicii – persoane juridice de drept public notifică centrul guvernamental de răspuns la incidente cibernetice cu privire la incidentele cibernetice în vederea îndeplinirii obligațiilor prevăzute de prezentul articol. Centrul guvernamental de răspuns la incidente cibernetice informează autoritatea competentă cu privire la incidentele cibernetice prevăzute de literele a) – c).* Această normă clarifică interacțiunea dintre furnizorii de servicii publici cu centrul guvernamental de răspuns la incidente cibernetice și autoritatea competentă în contextul realizării obligațiilor de notificare și elimină *riscul stabilirii unor atribuții paralele sau a unor atribuții care pot depăși atribuțiile autorității competente în anumite direcții, ceea ce se poate răsfrânge negativ asupra finalității scopului instituirii autorității competente și a Centrului guvernamental în partea ce ține de asigurarea eficientă a securității cibernetice,* după cum e menționat în expertiza anticorupție În ce privește reglementarea în lege a competenței detaliate a CERT-Gov, menționăm că stabilirea modului de organizare și funcționare cuprinde și aspectele de competență a acestui centru. Competența Guvernului în acest context este reglementată de Legea nr. 136/2017 cu privire la Guvern. Astfel conform art. 7 literele b), d) și e; Guvernul este împuternicit să decidă constituirea în structura sa a autorităților publice centrale și a structurilor organizaționale din subordinea acestora, precum și organizarea și funcționarea acestora. De asemenea notăm faptul că actualmente modul de organizare și funcționare a acestui Centru este deja

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			atribuțiilor Centrului Guvernamental de răspuns la incidentele cibernetice	reglementat de Hotărârea Guvernului nr.482/2020 prin care au fost aprobate măsurile necesare pentru asigurarea securității cibernetice la nivel guvernamental

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		26)	**Cu referire la art.12 alin.(7) din proiect** Norma instituie dreptul autorității competente de a decide aplicarea normei în dependență de interes. Astfel, autoritatea competentă poate solicita expres realizarea obligațiunii de către furnizorul de servicii, totodată, poate notifica, unilateral, destinatarii posibil afectați sau publicul. Norma nu stabilește careva condiții sau cazuri de aplicare a normei diferențiate, or, norma face referință doar la faptul că modul de informare a destinatarilor de către furnizorii de servicii sau de către autoritatea competentă constituie obiectul de reglementare a unui act normativ aprobat de Guvern. În aceste condiții, prin utilizarea în normă a textului „poate solicita expres realizarea obligațiunii de către furnizorul de servicii sau își poate aroga obligația de informare" va pemite autorității competente de a decide, în aceleași situații, în mod diferit, în dependență de interes. Totodată, norma nu stabilește un termen în care autoritatea competentă, după constatarea neîndeplinirii de către furnizorul de servicii a obligației prevăzute la alin.(6), urmează să fie obligată să solicite expres acestuia realizarea obligațiunii legale. Riscurile identificate constau în aplicarea neuniformă a normei, precum și în tergiversarea intenționată de către unii participanți a luării măsurilor urgente în privința limitării impactului negativ al unui incident cibernetic semnificativ. **Recomandări:** Propunem autorului delimitarea cazurilor în care autoritatea competentă urmează să fie obligată să solicite expres realizarea obligațiunii de către furnizorii de servicii și a cazurilor în care autoritatea competentă poate să notifice, în mod unilateral, destinatarii posibil afectați sau publicul. La fel, propunem stabilirea unui termen de conformare de către autoritatea competentă de solicitare a realizării de către furnizorii de servicii a obligațiilor ce reies din norma alin.(6).	**Se acceptă.** Prima propoziție din alineatul (7) al articolului 12 a fost revizuit, rezultând următoarea redacție: *În cazul în care furnizorul de servicii nu realizează obligațiunile de notificare prevăzute de alineatul (6) în termenul respectiv, autoritatea competentă solicită expres furnizorului de servicii realizarea obligațiunii de notificare și, dacă acesta nu o realizează în termen de cel mult 3 ore din momentul solicitării, autoritatea competentă asigură notificarea destinatarilor posibil afectați sau publicul, informând despre aceasta furnizorul de servicii.*

Nr. d/o	Participantul la avizare		Continutul obiectiei/ propunerii (recomandarii)	Argumentarea autorului proiectului
		27)	**Cu referire la art.15 alin. (2) din proiect** Norma art.15 stabileşte dreptul autorităţii competente de a restricţiona sau nu utilizarea sau accesul la sistemul informativ. Cu toate acestea, norma stabileşte foarte clar întrunirea unor condiţii cumulative pentru a restricţiona utilizarea sau accesul la un sistem informativ. Or, în cazul în care sunt întrunite condiţiile (expres stabilite), considerăm că autoritatea competentă urmează să acţioneze într-un mod ferm, norma urmând să fie una imperativă, care să impună o anumită conduită de urmat (o normă cu caracter prescriptiv). Totodată, autoritatea competentă urmează să-şi exercite atribuţiile eficient şi într-un mod care să trateze într-o manieră justă şi echitabilă toţi subiecţii ce se află în situaţii identice. În acest sens, în redacţia din proiect, s-ar putea ca acţiunile pe care le va întreprinde autoritatea competentă să difere de la caz la caz, cu riscuri iminente comiterii manifestărilor de corupţie. **Recomandări:** Propunem autorului substituirea sintagmei „poate restricţiona utilizarea" cu sintagma „restricţionează utilizarea".	**Se acceptă.**

12.	**Banca Națională a Moldovei** Nr. 31-002/202703 din 03.03.2023	*28)*	Cu referire la proiectul de hotărâre privind aprobarea proiectului de lege privind securitatea cibernetică (număr unic 41/ME/2023), remis spre avizare repetată prin scrisoarea Ministerului Economiei al Republicii Moldova nr. 07-519 din 27.02.2023, Banca Națională a Moldovei, în limitele competenței sale, reiterează îngrijorările și propunerile enunțate în scrisoarea nr. 31-002/12/431 din 08.02.2023. În special, atenționăm că, în cazul în care autoritățile publice autonome, responsabile față de Parlament, vor fi incluse în lista de subiecți ai proiectului de lege, acestora nu urmează a le fi aplicabile dispozițiile proiectului de lege cu privire la, cel puțin, supravegherea continuă prin efectuare de controale pe teren, răspunderea furnizorilor de servicii conform capitolului V, inclusiv, sancționarea contravențională a acestora de către autoritate competentă, aplicarea actelor cu caracter obligatoriu emise de către autoritatea competentă, implicarea directă a acesteia în soluționarea incidentelor cibernetice și alte prevederi care ar conduce la imixtiuni în activitatea acestora. Astfel, înțelegem că proiectul de lege nu se va aplica Băncii Naționale a Moldovei, care dispune de autonomie (care urmează a fi menținută și consolidată, inclusiv în virtutea angajamentelor asumate de Republica Moldova prin Acordul de Asociere RM-UE), inclusiv cu referire la gestionarea crizelor în domeniul securității cibernetice, stabilirea mecanismelor proprii de asigurare a securității cibernetice - mecanisme, care sunt aplicate și în prezent. Pentru a evita orice echivoc, propunem completarea proiectului de lege cu o prevedere care exceptează expres Banca Națională a Moldovei de la dispozițiile proiectului de lege.	**Nu se acceptă.** În primul rând potrivit prevederilor art. 33 alin. (1) din Legea nr. 100/2017 privind actele normative, obiecțiile și propunerile părților interesate urmează a fi motivate. În al doilea rând Competența propusă în proiect a autorității competente nu este de natură să genereze imixtiuni în competența materială exercitată de către autoritățile publice care nu intră în structura guvernamentală. Ea se rezumă la supravegherea modului în care sunt onorate obligațiunile stabilite de lege în ce privește măsurile de securitate implementate pentru a asigura o protecție adecvată a rețelelor și sistemelor informatice care sunt utilizate în prestarea unor servicii esențiale în domenii critice ale vieții sociale. Obligațiile instituite de lege trebuie implementate de toate persoanele juridice de drept public, indiferent de locul acestora în structura administrației publice și natura competenței materiale exercitate. În ce privește nemijlocit Banca Națională a Moldovei și obligațiile de implementare a măsurilor de securitate sau de notificare menționăm că proiectul de lege în art. 3 alin. (5) stabilește că în cazul în care legile care reglementează activitatea furnizorilor de servicii, precum și sectoarele și subsectoarele, stabilite de Guvern, prevăd implementarea unor măsuri de securitate sau obligații de notificare a incidentelor cu impact semnificativ, ale căror efecte sunt cel puțin echivalente cu efectele obligațiilor stabilite de prezenta lege, prevederile legilor respective au caracter special în raport cu prevederile legii privind securitatea cibernetică. Astfel în situația în care legile care reglementează activitatea BNM stabilesc măsuri care asigură iun nivel mai înalt de securitate atunci vor fi aplicate prevederile legii speciale. În acest context ținem să atragem atenția că proiectul

				de lege vine să transpună parțial Directiva NIS2. Această Directivă este într-o strânsă conexiune cu Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (Regulamentul DORA). Astfel, BNM în comun cu ministerele responsabile urmează să inițieze armonizarea legislației naționale cu prevederile Regulamentului UE respectiv. Odată implementat în legislația națională în mod adecvat, acesta va asigura exceptarea anumitor categorii de entități financiare de la unele obligații stabilite de Legea privind securitatea cibernetică. O excepție urmând a fi notificarea obligatorie a incidentelor cibernetice cu impact semnificativ către CSIRT național. În acest context, amintim că proiectul de lege are ca scop instituirea mecanismelor de interacțiune la nivel național în procesul de asigurare a securității cibernetice prin implementarea măsurilor de securitate și realizarea obligațiilor de schimb de informații cu CSIRT-ul național a furnizorilor de servicii din mediul public și privat. În acest context menționăm că sectorul financiar ca oricare alt sector ar putea lua măsuri de securitate de ordin organizatoric pe care le consideră corespunzătoare riscurilor identificate. Un furnizor de servicii privat ar putea apela la externalizarea unor astfel de servicii. Efectul pe care îl produc obligațiile impuse prin normele proiectului de lege este să se asigure o protecție adecvată a rețelelor și sistemelor informatice, iar metodele urmează a fi identificate de către furnizorii de servicii în corespundere cu principiile legalității eficienței eficacității proporționalității, etc. Furnizorii de servicii

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				au dreptul discreționar de asemenea să-și unească eforturile, spre exemplu într-un sector sau subsector în vederea constituirii unei echipe comune de răspuns la incidentele cibernetice, bineînțeles că atunci când decide organizarea măsurilor sale de securitate furnizorul de servicii trebuie să țină cont că anume el este subiectul obligațiilor impuse de lege și trebuie să se asigure că în relațiile contractuale cu anumiți furnizori de servicii de securitate aceştia vor asigura îndeplinirea corespunzătoare a acestor obligații.
13.	**Ministerul Justiției** *06.03.2023 nr. 04/1858*	*29)*	În lista contrasemnatarilor la proiectul hotărârii Guvernului, cuvântul „Viceprimier" se va substitui cu cuvântul „Viceprim-ministru" astfel cum este indicat în *Legea nr. 136/2017 cu privire la Guvern*	**Se acceptă.**
		30)	În conformitate cu art. 31 alin. (2) din Legea nr. 100/2017 cu privire la actele normative, proiectele actelor normative care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene sunt marcate pe prima pagină în colțul drept de sus cu sigla „UE" și conțin clauza de armonizare conform modelului aprobat de Guvern. Prin urmare, prima pagină se va marca cu sigla „UE".	**Se acceptă.**
		31)	Potrivit art. 44 alin. (1) din Legea nr. 100/2017, pentru proiectele de legi, clauza de adoptare a actului normativ cuprinde și categoria acestora. Prin urmare, enunțul „Parlamentul adoptă prezenta lege organică" se va exclude din Capitolul I și se va indica în calitate de clauză de adoptare	**Se acceptă.**

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		32)	În conformitate cu art. 41 din Legea nr. 100/2017, actul normativ este format din denumire, preambul, clauza de adoptare, iar pentru proiectele cu sigla „UE" – şi clauza de armonizare, dispoziții generale, …..". Potrivit art. 45 din Legea nr. 100/2017, dispozițiile generale sunt prevederile care determină obiectul, scopul și domeniul de aplicare, orientează întreaga reglementare, explică termenii și definesc concepte. Potrivit pct. 30 din Regulamentul privind armonizarea legislației Republici Moldova cu legislația Uniunii Europene, aprobat prin Hotărârea Guvernului nr. 1171/2018, clauza de armonizare se include după preambul și clauza de adoptare a proiectului de act normativ. Prin urmare, clauza de armonizare se va exclude din Capitolul I și se va indica după clauza de adoptare.	**Se acceptă.**
		33)	În conformitate cu pct. 31 sbp. 2) din Regulamentul privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene, clauza de armonizare utilizează calificativul de apreciere a compatibilității: transpune art., lit., pct., anexa, etc. din actul Uniunii Europene în cazul transpunerii selective a actului Uniunii Europene, în funcție de scopul specific al transpunerii, menționându-se expres componentele actului Uniunii Europene (capitolul, articolul, litera, punctul, anexa etc.) care se transpun integral. Ținând cont de prevederea dată, întru corectitudinea redactării, în clauza de armonizare cuvintele „transpune parțial" se vor exclude ca fiind excedente. Totodată, articolele din Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 nu se vor lua între paranteze rotunde. Textul „art. 36" va fi succedat de prepoziția „din". În clauza de armonizare se va indica și sursa de publicare a Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022	**Se acceptă.**

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		34)	La art. 7 alin. (3) lit. h): În avizul nr. 04/1437 din 20.02.2023, Ministerul Justiției a menționat că prevederea de la art. 7 alin. (3) lit. h) din proiectul legii, care prevede că autoritatea competentă exercită atribuțiile organului constatator pentru cauze contravenționale în domeniul securității rețelelor și sistemelor informatice în conformitate cu prevederile Codului contravențional urmează a fi exclus, or, autoritățile care exercită atribuțiile organului constatator în cauze contravenționale se indică expres în Codul contravențional. Totodată, s-a stipulat că propunerile ce vizează amendarea Codului contravențional, urmează a fi remise în adresa Ministerului Justiției, care va asigura elaborarea și definitivarea proiectului unic de modificare și completare a Codului contravențional, cu promovarea ulterioară a acestuia (obiecție valabilă și la art. 21 alin. (3)). Obiecția nu a fost acceptată de Ministerul Dezvoltării Economice și Digitalizării, deoarece norma de la art. 7 alin. (3) lit. h) constituie o normă de trimitere la actul normativ de bază care va reglementa competența și procedurile ce urmează a fi realizate în acest context. Autorul proiectului a menționat că, urmează să fie elaborat proiectul de lege privind modificarea unor acte normative pentru aducerea în concordanță cu Legea privind securitatea cibernetică, proiectul urmând să includă și propuneri de modificare a Codului contravențional în vederea atribuirii competenței respective autorității competente conform Legii privind securitatea cibernetică. Argumentul autorul proiectului nu poate fi reținut, or, după cum a menționat însăși autorul, competența de a constata contravenții se stabilește în Codul contravențional. Prin urmare, reiterăm obiecția din precedentul aviz. În acest context, se va revizui și art. 21 alin. (3) din proiect	**Se acceptă.**

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		35)	La art. 12: 1) La alin. (5) lit. b), cuvântul „sau" va fi succedat de cuvântul „prevăzute".	**Se acceptă.**
		36)	2) Potrivit normelor de tehnică legislativă, dacă se face referință la trei elemente structurale consecutive, enumerarea se redă după următorul exemplu: „a), b) și c)". Prin urmare, la alin. (5) lit. b), textul „litere a)-c)" se va substitui cu textul „literele a), b) și c)"	**Se acceptă.**
		37)	Ținând cont de obiecția expusă la pct. 6 sbp. 2) din aviz, la art. 14 alin. (1), textul „articolului 11 alineatele (1)-(3)" se va substitui cu textul „articolului 11 alineatele (1), (2) și (3)"	**Se acceptă.**
		38)	La art. 15 alin. (2) lit. b), cuvintele „nu este în măsură" sunt lipsite de claritate, motiv pentru care, se vor revizui	**Se acceptă.**
		39)	La art. 23 Ministerul Justiției în avizul precedent a menționat că, ținând cont de prevederile art. 41 alin. (1) lit. f) și g) din Legea nr. 100/2017 cu privire la actele normative, prevederile de la art. 23 alin. (3) urmează a fi excluse din proiectul legii, or, acestea nu corespund caracterului dispozițiilor finale și tranzitorii, ci se referă la cerințele cărora trebuie să corespundă echipa de răspuns. Prin urmare, a fost înaintată propunerea de a indica dispoziția de la art. 23 alin. (3) în cuprinsul legii. Autorul proiectului nu a acceptat obiecția înaintată motivând că consideră judicioasă păstrarea acestuia în dispoziții finale. Ținând cont că argumentul autorul proiectului nu este întemeiat din punct de vedere juridic, obiecția se menține	**Se acceptă.**

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
14.	**Serviciul de informație și Securitate**	*40)*	1. La obiecția Serviciului privind alin. (3) al art. 3 al proiectului, deși autorul indică că aceasta a fost acceptată, totuși nu a exclus alin. (3) al art. 3, ci l-a expus în redacție nouă, care nu poate fi acceptată. Or, art. 2 alin. (7) din Directiva (UE) 2022/2555 a Parlamentului european și a Consiliului din 14 decembrie 2022, privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2), pe care proiectul o transpune, specifică că aceasta nu se aplică entităților administrației publice care își desfășoară activitățile în domeniile securității naționale, siguranței publice, apărării sau aplicării legii, inclusiv prevenirii, investigării, depistării și urmăririi penale a infracțiunilor. Totodată, potrivit art. 5 alin. (5) a Legii nr. 245/2008 cu privire la secretul de stat, elaborarea și realizarea măsurilor de protecție a secretului de stat în cadrul autorităților publice și altor persoane juridice, precum și efectuarea controlului asupra asigurării protecției secretului de stat constituie atribuții ale autorității publice în domeniul protecției secretului de stat care este Serviciul de Informații și Securitate. Prin urmare, exceptată de la aplicarea prevederilor proiectului este anume instituția și nu doar o parte din activitatea acestuia (în speță doar activitatea de mentenanță a rețelelor si sistemelor informatice care sunt destinate prelucrării informațiilor atribuite la secret de stat).	**Precizare.** Din perspectiva transpunerii în legislația națională a Directivei NIS2 menționăm că excluderea acestei categorii de entități publice trebuie percepută prin prisma principiului armonizării minime, stabilite de art. 5 din aceeași directivă. Având în vedere că o condiție fundamentală pentru ca o persoană juridică să cadă sub incidența prevederilor legii este ca aceasta să utilizeze rețele și sisteme informatice în prestarea serviciilor esențiale. În caz contrar aplicarea normelor legale conținute în proiect nu poate fi realizată efectiv. Din aceste considerente și a fost propusă redacția alin. (3) articolul 3 din proiectul de lege. Da într-adevăr o primă examinare aceasta ar putea fi considerată ca o acceptare parțială, însă având în vedere precondițiile expuse mai sus, normele respective vor avea ca efect excluderea din sfera de aplicarea a legii a autorităților publice respective. Totuși atunci când un sistem informatic nu este utilizat în activitatea unei autorități din domeniul ordinii publice, spre exemplu, acesta urmează a fi supus măsurilor de securitate prevăzute de lege. Nu este cazul Serviciului de Informații și Securitate, deoarece activitatea acestuia practic cade în totalitate sub incidența prevederilor literei a) din acest alineat, dacă utilizează sisteme informatice. Dacă nu le utilizează nici nu poate fi vorba de aplicarea prevederilor legii asupra Serviciului.

		41)	2. Potrivit art. 1 alin. (1) al Legii nr. 753/1999 privind Serviciul de Informații și Securitate al Republicii Moldova, Serviciul este organul de stat specializat în domeniul asigurării securității naționale prin exercitarea tuturor măsurilor adecvate de informații și contrainformații, de culegere, prelucrare, verificare și valorificare a informațiilor necesare cunoașterii, prevenirii și contracarării oricăror acțiuni care constituie, potrivit legii, amenințare internă sau externă pentru independența, suveranitatea, unitatea, integritatea teritorială, ordinea constituțională, dezvoltarea democratică, securitatea internă a statului, societății si cetățenilor, statalitatea Republicii Moldova, funcționarea stabilă a ramurilor economiei naționale de importanță vitală, atât pe teritoriul Republicii Moldova, cât și peste hotare. Astfel, în vederea realizării misiunii de asigurare a securității statului și de contracarare efectivă a amenințărilor hibride, considerăm absolut argumentată și necesară completarea proiectului cu un articol nou, care va avea următorul conținut: ***„ Autoritatea competentă informează imediat Serviciul de Informații și Securitate al Republicii Moldova, dar nu mai târziu de 24 de ore din momentul în care a luat cunoștință despre un incident cibernetic care poate avea impact asupra securității statului.".*** In același timp, considerăm nejustificat argumentul autorului precum că completarea propusă ar dubla prevederile art. 7 (fără a indica la care alineat sau literă se referă), or, acesta din urmă stabilește atribuția autorității competente de a asigura interacțiunea în domeniul securității cibernetice cu autoritățile si instituțiile publice naționale și cu furnizorii de servicii, și nicidecum nu stabilește obligația acesteia de raportare către autorități competente a incidentelor cibernetice specifice (în speță - care pot avea impact asupra securității statului). Mai mult ca atât, alin. (10) al art. 23 din Directiva NIS2 stabilește obligația echipelor CSIRT, după caz, autorităților competente de a furniza autorităților competente în temeiul Directive 2022/2557 informații privind incidentele	**Se acceptă parțial.** Articolul 15 din proiect a fost completat cu alineatul (5) cu următorul cuprins: „(5) Autoritatea competentă informează Serviciul de Informații și Securitate imediat, însă nu mai târziu de 24 de ore din momentul în care a luat cunoștință despre incidentele cibernetice cu impact semnificativ, prevenite sau soluționate, care au vizat obiectivele infrastructurii critice". Sintagma „incident cibernetic care poate avea impact asupra securității statului" în contextul în care categorizarea incidentelor cibernetice este una destul de complicată, ar putea avea ca efect că autoritatea competentă să informeze SIS despre orice incident cibernetic.

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			semnificative si amenințările cibernetice din infrastructura entităților critice. Respectiv, menționăm că în conformitate cu prevederile Regulamentului privind protecția antiteroristă a infrastructurii critice, Serviciul de Informații şi Securitate al Republicii Moldova este desemnat în calitate de organ responsabil de coordonarea la nivel național a activității de asigurare a protecției antiteroriste a infrastructurii critice. Din aceleaşi considerente este oportună completarea proiectului cu un articol nou care va stabili obligația autorității competente de a remite trimestrial în adresa Serviciului de Informații şi Securitate al Republicii Moldova, a rapoartelor de sinteză privind incidentele de securitate cibernetică şi amenințările identificate.	

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		42)	3. Considerăm necesară completarea art. 18 alin. (2) din proiectul, după cuvântul „terța" cu textul „din contul furnizorului de servicii responsabil, cu excepția persoanelor juridice de drept public". In acest sens, menționăm că reieșind din prevederile alin (1) al aceluiași articol din proiect, furnizorii de servicii au obligația de respectare a prevederilor legale în domeniul securității cibernetice, iar autoritatea competentă exercită funcția de supraveghere a respectării acestora. Astfel, refuzul autorului de a completa pct. 18 conform propunerii Serviciului expuse în avizul anterior, va rezulta în imposibilitatea punerii efective în aplicare a prevederilor legale. Or, furnizorul de servicii nu va fi interesat în realizarea măsurilor de asigurare a securității cibernetice din cont propriu, odată ce legea oferă posibilitatea de a nu întreprinde nici o acțiune din cont propriu și apelarea la autoritatea competentă, care la necesitate va contracta din bani publici și asistență terță. Considerăm că varianta agreată de autor pe lângă faptul că va crea condiții prielnice apariției manifestărilor de corupție, aceasta nu va duce la realizarea obiectivelor principale ale proiectului.	**Se acceptă.** Sintagma „utilizând dacă e necesar asistență profesionistă terță" a fost exclus.

		43)	4. Urmând aceeași logică, dar și conducându-ne de prevederile pct. 5 al Măsurilor necesare pentru asigurarea securității cibernetice la nivel guvernamental, aprobate prin Hotărârea Guvernului nr. 482/2020, considerăm imperativă completarea art. 18 al proiectului cu un alineat nou cu următorul conținut: „In cazul persoanelor juridice de drept public, asigurarea aplicării măsurilor necesare pentru soluționarea incidentului cibernetic care nu au putut fi soluționate în timp util de către acestea, este realizată prin solicitarea asistenței Centrului guvernamental de reacție la incidente de securitate cibernetică (CERT Gov). ". Or, în lipsa reglementării propuse, persoanelor juridice de drept public li se va aplica norma stabilită la alin. (2) al art. 18 , care prevede atragerea asistenței terțelor părți la gestionarea incidentelor cibernetice, fapt ce presupune inclusiv atragerea companiilor private, contra plată, scenariu care comportă pericole de apariție a manifestărilor de corupție și care nu trebuie să existe, odată ce actualmente este instituit Centrul guvernamental de reacție la incidente de securitate cibernetică (CERT Gov), misiunea căruia constă, inclusiv, în asigurarea răspunsului la incidente de securitate cibernetică la nivel guvernamental. Totodată, menționăm că argumentul autorului precum că, în cazul completării proiectul cu astfel de prevederi ar putea apărea percepția a două CSIRT naționale nu rezistă criticilor, or, chiar proiectul face referire la Centrul guvernamental de reacție la incidente de securitate cibernetică în art. 8. Mai mult ca atât, alin. (3) al art. 8 din proiect, stabilește că Centrul guvernamental este responsabil de asigurarea securității rețelelor și sistemelor informatice ale căror proprietar este statul și de facilitarea realizării de către furnizorii de servicii - persoane juridice de drept public a obligațiilor de asigurare a securității cibernetice prevăzute de prezenta lege. Prin urmare, completarea art. 18 conform propunerii expuse supra, constituie o continuare logică și necesară în stabilirea atribuțiilor actorilor implicați în asigurarea securității	În contextul în care sintagma „utilizând dacă e necesar asistență profesionistă terță" a fost exclus. Completarea articolului cu textul propus este inutilă, având în vedere că atribuțiile CERT-Gov anume în aceasta și constau să asigure răspunsul la incidentele cibernetice în rețelele și sistemele informatice ale persoanelor juridice de drept public CSIRT național urmând să se implice în situația în care o echipă sectorială, inclusiv CERT-Gov nu este în măsură să asigure soluționarea incidentului.

Nr. d/o	Participantul la avizare		Continutul obiectiei/ propunerii (recomandării)	Argumentarea autorului proiectului
			cibernetice şi mecanismelor de punere în aplicare a legii.	

		44)	5. Având în vedere climatul de securitate din regiune și posibilitatea intensificării amenințărilor hibride asupra obiectelor de infrastructură critică, inclusiv prin atacuri cibernetice, considerăm necesară completarea proiectului cu un articol nou, care ar prevedea obligația echipelor CERT/CSIRT/CIRT/SOC ce prestează servicii de răspuns la incidente pentru operatorii de infrastructură critică, de a obține de la autoritatea competentă, autorizare pentru prestarea acestor servicii. Suplimentar, în articolul dat urmează a fi prevăzută obligativitatea că, la emiterea autorizației, autoritatea competentă va solicita opinia organului ce coordonează la nivel național activitățile de asigurare a protecției antiteroriste a infrastructurii critice. Or, lipsa unor astfel de reglementări va crea condiții prielnice pentru centre subversive de a obține (de ex. prin companii intermediare care ar propune condiții de preț avantajoase) acces la obiectele de infrastructură critică, fapt care va pune în pericol securitatea statului. In acest sens, considerăm argumentată necesitatea acordării unui control deosebit asigurării securității cibernetice a obiectivelor de infrastructură critică.	**Precizare** În viziunea noastră stabilirea unui astfel de mecanism ar crește exponențial costurile administrat8ive de implementare a legii de către furnizorii de servicii. Având în vedere nivelul de maturitate scăzut al Republicii Moldova în domeniul securității cibernetice pentru moment ca obiective prioritare ar trebui să fie instituirea unor mecanisme de reacție la nivel național în acest domeniu. Implementarea treptată a măsurilor de securitate de către furnizorii de servicii. Ulterior, așa după cum este caracteristic în general evoluției dreptului, în funcție de dezvoltarea domeniului ar putea fi implementate și alte măsuri. De asemenea este necesar de evidențiat că implementarea unui mecanism de autorizare nu are un impact financiar sporit asupra mediului privat, ci va necesita cheltuieli suplimentare și din bugetul de stat pentru implementarea practică a acestui mecanism. Deși propunerea în sine nu este una care ține de aspecte juridice, ci este mai mult una de oportunitate, totuși considerăm că acceptarea acesteia la momentul actual ar dăuna procesului de implementare, care și așa se prefigurează a fi unul destul de complex. Totodată considerăm ca fiind mai rațională examinarea oportunității instituirii unui astfel de mecanism în contextul promovării de către Serviciul de Informații și Securitate a proiectului de act normativ care va avea ca obiectiv transpunerea Directivei CER. În context ținem să evidențiem că interconexiunile dintre Directiva NIS2 și Directiva CER, de altfel destul de strânse, trebuie extrapolate la nivelul național al Republicii Moldova. Desincronizarea transpunerii acestor doua acte legislative europene este, în contextul celor expuse, un neajuns fundamental al procesului de reglementare a domeniilor respective.
		45)	6. Serviciul atenționează asupra faptului, că obiecția	**Precizare.**

			comună expusă de marea majoritate a autorităților care au participat la procesul de avizare a proiectului, constă în necesitatea stabilirii exprese a autorității competente. Or, desemnarea organului competent prin act al Guvernului, este irațională și incorectă din momentul în care atribuțiile organului competent sunt stabilite în proiect, iar Directiva NIS2 stabilește obligația statelor de desemnare a acesteia. Menționăm că, nu poate fi acceptat argumentul autorului precum că desemnarea organului competent de către Guvern, se încadrează în împuternicirile Guvernului stabilite în art. 6 lit. b), d) și e) din Legea nr. 136/2017 cu privire la Guvern și considerăm că desemnarea organului unic național, prin act a Guvernului depășește competențele acestuia. Or, potrivit art. 7 lit. b) a Legii nr. 136/2017, Guvernul stabilește modul de organizare și funcționare, domeniile de activitate, structura si efectivul-limită ale ministerelor, ale altor autorități administrative centrale subordonate Guvernului și ale structurilor organizaționale din sfera lor de competență, coordonează și controlează activitatea acestora. Potrivit art. 7 lit. d) a Legii nr. 136/2017, Guvernul înființează în subordinea sa, alte autorități administrative centrale pentru realizarea politicii statului într-un domeniu de activitate care nu intră în competența nemijlocită a ministerelor, precum și în domenii de activitate în care competențele ministerelor se intersectează, precum și le reorganizează și dizolvă. Potrivit art. 7 lit. e) a Legii nr. 136/2017, Guvernul decide asupra constituirii, reorganizării și dizolvării structurilor organizaționale din sfera de competentă a ministerelor și altor autorități administrative subordonate Guvernului. Prin urmare, având în vedere importanța, statutul și atribuțiile organului național în domeniul securității cibernetice, care urmează să acopere toate domeniile și actorii implicați la nivel național, considerăm imperativ necesară desemnarea acestuia prin lege.	Suplimentar la argumentarea prezentată în procesul avizării inițiale, menționăm că exercitarea conducerii generale a administrației publice este o funcție fundamentală constituțională a Guvernului, stabilită de art. 96 din Constituție. Funcție ce este dezvoltată în Legea nr. 136/2017 cu privire la Guvern. În primul rând Guvernul este responsabil de realizarea politicii de stat în domeniul securității cibernetice. În acest scop, Guvernul are nevoie de instrumentarul instituțional adecvat, adică să constituie sau să atribuie unei autorități existente implementarea obiectivelor strategice în acest domeniu. Ținem să evidențiem că faptul menționării în Directiva NIS2 a obligației statelor de desemnare a autorității competente, nu implică obligativitatea menționării acesteia expres într0un act normativ de nivel superior Statele membre urmează să-și reglementeze și implementeze mecanismele instituționale și funcționale în corespundere cu dreptul său intern. Suntem de acord că nominalizarea expresă în textul legii a unei autorități publice care va exercită funcțiile autorității competente este o opțiune judicioasă, totuși aceasta este o decizie cu caracter politic. O astfel de decizie poate fi luată în cunoștință de cauză doar în baza atunci unei analize profunde a opțiunilor instituționale posibile (aspectul financiar nefiind cel mai plauzibil) în vederea identificării entității cu un nivel de maturitate cel mai înalt în țară, precum și a unei analize a sectoarelor/subsectoarelor și a tipologiei furnizorilor de servicii pentru a stabili întinderea constituenței acestei autorități naționale. Soluția propusă în proiect deși nu este poate cea mai oportună, dar cu siguranță este una legală. În contextul promovării stringente a proiectului de lege, această opțiune s-a constatat a fi cea mai judicioasă, urmând ca în procesul elaborării deciziei guvernamentale, într-o

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				perioadă temporală adecvată, să se vină cu întreg spectrul de opțiuni prin care problematica instituțională să fie rezolvată într-un mod eficient
		46)	7. O altă obiecție comună, exprimată de către majoritatea autorităților care au participat la procesul de avizare a proiectului, este necesitatea stabilirii sectoarelor/subsectoarelor menționate în Directiva NIS2. În acest sens, deşi autorul proiectului indică corect că statele membre sau cele care transpun această Directivă, cum e cazul Republicii Moldova, pot să stabilească prevederi care asigură un nivel mai ridicat de securitate cibernetică, inclusiv să stabilească si alte sectoare sau subsectoare decât cele menționate în anexe la Directiva NIS2, acesta ajunge la concluzia greșită precum că statele membre sau candidate pot să nu stabilească sectoarele în general, sau să stabilească doar o parte din ele. Or, alin. (1) al art. 10 din Directiva NIS2 stabilește că CSIRT- urile naționale acoperă cel puțin sectoarele, subsectoarele și tipurile de entități menționate în anexele I si II. Astfel, sectoarele indicate în anexe se desemnează în mod obligatoriu, statele membre sau candidate având opțiunea de a le completa pe acestea. Totodată, nu este argumentată opinia autorului precum că, preluarea listei sectoarelor/subsectoarelor comportă riscul neacoperirii unor sectoare esențiale pentru Republica Moldova, or, acesta nu a prezentat nici un studiu care ar demonstra acest lucru. Astfel, în cazul existenței unui astfel de studiu realizat de către autor, considerăm necesară includerea rezultatelor acestuia în notă informativă si analiza de impact, în caz contrar, constatăm că lista sectoarelor şi subsectoarelor stabilite în Directiva NIS este una amplă, universală şi urmează a fi transpusă în legislația națională prin lege.	**Precizare** Menținem în principiu argumentarea expusă la opinia anterioară a Serviciului înaintată în procesul de avizare. Totuși suntem de acord că listarea exhaustivă a sectoarelor, subsectoarelor a tipurilor și categoriilor de persoane juridice care ar urma să cadă sub incidența prevederilor proiectului de lege ar fi cea mai rațională și judicioasă opțiune de reglementare. Totuși această opțiune poate fi luată în considerare doar în situația în care în prealabil promovării, sau chiar elaborării textului unui astfel de proiect de lege, ar fi fost efectuată o analiză amplă a sectoarelor/subsectoarelor și a tipologiei furnizorilor de servicii pentru a stabili relevanța acestora pentru Republica Moldova, dar și o profundă analiză a legislației sectoriale în vederea stabilirii nivelului de compatibilitate (cel puțin al tipologiei respective) a acesteia cu actele legislative europene, la care se face referire expres în anexele la Directiva NIS2. Având în vedere stringența promovării proiectului, considerăm că pentru moment opțiunea propusă este una plauzibilă atât din punct de vedere juridic, cât și din punct de vedere practic. În context termenul extins de intrare în vigoare a legii, propus în textul în proiectul de lege, ne oferă o marjă temporală pentru realizarea acestei analize, rezultatul căreia nu exclude și o posibilă completare a legii.

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		47)	8. Serviciul consideră necesara completarea proiectului cu norme de transpunere a prevederilor art. 20 al Directivei NIS 2. Art.20 alin (1) al Directivei menționate, stabilește posibilitatea de tragere la răspundere a organelor de conducere a entităților esențiale și entităților importante, dacă acestea nu respectă măsurile de gestionare a riscurilor în materie de securitate cibernetică. Totodată, art. 20 alin. (2) al aceleiași Directive, obligă membrii organelor de conducere a entităților esențiale si entităților importante să urmeze o formare pentru a dobândi suficiente cunoștințe și competențe pentru a putea identifica riscurile și a evalua practicile de gestionare a riscurilor în materie de securitate cibernetică. Astfel, deși în clauza de adoptare a proiectului se indică faptul că acesta transpune prevederile art. 20 al Directivei NIS 2, proiectul nu conține astfel de reglementări. Transpunerea acestor norme va asigura punerea în aplicare a legii în mod calitativ si nu declarativ/formal.	**Nu se acceptă.** Articolul 20 din Directiva NIS2 stabilește norme generale privind măsurile de gestionare a riscurilor în materie de securitate cibernetică. Acest articol stabilește o normă generală care este ulterior dezvoltat în articolul 21 al aceleiași directive. Proiectul de lege transpune art. 20, și nu doar parțial, prin stabilirea obligațiilor pentru furnizorii de servicii de a implementa măsurile de securitate tehnice și organizatorice, măsuri care urmează a fi bazate și să fie proporționale riscurilor care au fost identificate în procesul evaluării acestora. De altfel evaluarea riscurilor este o primă obligație stabilită în art. 11 alin. (1). În mod special prevederile: art. 20 alin. (1) sunt implementate de prevederile literelor a), b),c) și d) ale alin. (2) din art. 11 al proiectului de lege, iar ale alin. (2) sunt implementate de prevederile punctul 9) litera b) din art. 11 al proiectului de lege. În ceea ce privește că organele de conducere ale entităților esențiale și importante pot fi trase la răspundere pentru încălcarea prevederilor art. 21 din Directiva NIS2, aceasta urmează a fi transpusă prin operarea modificărilor în actele normative care stabilesc răspunderea contravențională și, eventual penală. O examinare aprofundată a acestei materii urmează a fi realizată în cel mai scurt timp.

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		48)	9. Totodată, considerăm oportună completarea proiectului cu norme de transpunere a art. 28 al Directivei NIS 2, care prevede că, pentru consolidarea securității cibernetice, registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii sunt obligate să colecteze și să mențină date exacte și complete privind înregistrarea numelor de domenii într-o bază de date, iar baza de date să conțină informațiile necesare pentru identificarea și contactarea titularilor numelor de domenii. Respectiv, entitățile care prestează servicii de înregistrare a numelor de domenii se obligă să implementeze politici și proceduri, inclusiv de verificare, care să asigure că baza de date conține informații exacte și complete. Suplimentar, Serviciul consideră imperativ de a transpune în proiect, prevederile articolului menționat, din considerentul că aceasta va permite identificarea actorilor ce au o activitate malițioasă sau identificarea posesorilor de resurse din Internet ale căror pagini web au fost compromise și reprezintă o amenințare de securitate.	Aceste norme sunt deja transpuse într-o anumită măsură prin legislația privind comunicațiile electronice: Legea nr. 241/2007 comunicațiilor electronice și Hotărârea ANRCETI nr. 42/2020 privind aprobarea Regulamentului cu privire la gestionarea domeniului de nivel superior .md
15.	**Ministerul Finanțelor**	*49)*	Art.22: - la alin.(1), cuvintele „mijloacele financiare alocate anual în bugetul de stat" de substituit cu cuvintele „din bugetul de stat în limita alocațiilor aprobate prin legea bugetară anuală"; - la alin.(2) cuvintele „și în limita mijloacelor, alocate din bugetul de la care se finanțează activitatea persoanelor juridice respective" de substitut cu cuvintele „bugetul de la care se finanțează activitatea persoanelor juridice respective în limita alocațiilor aprobate prin legea/decizia bugetară anuală".	**Se acceptă.**

Nr. d/o	Participantul la avizare		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		50)	Art.23, alin.(3) de exclus, deoarece stabilirea pentru Guvern a sarcinii de a asigura autoritatea competentă cu resursele necesare, nu ține cont de procesul bugetar, în conformitate cu prevederile Legii finanțelor publice și responsabilității bugetar-fiscale nr. 181/2014, care începe cu elaborarea cadrului bugetar pe termen mediu. Prin Legea menționată sunt stabilite responsabilitățile autorităților publice centrale în domeniul finanțelor publice, printre acestea fiind prezentarea propunerilor pentru elaborarea cadrului bugetar pe termen mediu și a proiectului legii bugetului de stat. Astfel, responsabilă de prezentare a propunerilor de alocare a resurselor necesare pentru finanțarea activității autorității competente este atribuția autorității publice centrale responsabile de realizarea politicii în domeniul securității cibernetice.	**Se acceptă.**
		51)	La cap.5 Fundamentarea economico-financiară din Nota informativă, ultimul alineat de exclus deoarece costurile indicate nu corespund realității (estimări din anul 2015). Totodată, Ministerul Finanțelor consideră necesar examinarea oportunității fortificării capacităților instituționale ale instituțiilor deja existente (inclusiv IP STISC) întru evitarea creării instituțiilor noi, preponderent cu același profil. Cu atât mai mult că, conform prevederilor Legii bugetului de stat pentru anul 2023 nr.359/2022 în bugetul Cancelariei de stat sunt prevăzute mijloace financiare în sumă de 3687,9 mii lei, pentru activitatea Centrului guvernamental de reacții la incidente de securitate cibernetică, gestionat de către IP STISC (HGRM nr.482/2020)	**Se acceptă.**

MINISTRU **Dumitru ALAIBA**