EXPUNERE DE MOTIVE

Secțiunea 1: **Titlul proiectului de act normativ**	
LEGE pentru aprobarea Ordonanței de urgență a Guvernului privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil	
Secțiunea a 2-a: **Motivul emiterii actului normativ**	
2.1. Sursa proiectului de act normativ	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) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (Text cu relevanță pentru SEE)
2.2. Descrierea situației actuale	Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului (denumită în continuare Directiva NIS1), transpusă în legislația națională prin Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice a vizat consolidarea capacităților în materie de securitate cibernetică în întreaga Uniune, abordarea adecvată a amenințărilor la adresa rețelelor și a sistemelor informatice utilizate pentru a furniza servicii esențiale în sectoare-cheie și asigurarea continuității acestor servicii atunci când se confruntă cu incidente. Directiva a vizat crearea unui ecosistem unitar al securității cibernetice la nivelul Uniunii Europene, care să includă cerințe comune privind crearea capacităților minime de asigurare a rezilienței cibernetice, răspuns și recuperare în urma incidentelor și planificarea, schimbul de informații, cooperarea și cerințele minime de securitate pentru (1) Operatorii de Servicii Esențiale și (2) Furnizorii de Servicii Digitale care activează în domeniile prevăzute de anexa la directivă.

	Viziunea NIS1 a fost aceea de a promova o cultură de securitate cibernetică, iar obligațiile statelor membre au cuprins: 1. Adoptarea unei strategii de securitate a rețelelor și sistemelor informatice; 2. Stabilirea uneia sau mai multor autorități naționale competente în domeniul NIS; 3. Stabilirea unui punct național unic de contact; 4. Stabilirea și dotarea corespunzătoare a uneia sau a mai multor echipe naționale de răspuns la incidente de securitate cibernetică (echipa CSIRT națională); 5. Inițierea unui proces de identificare a operatorilor de servicii esențiale (OSE); 6. Stabilirea cerințelor minime de securitate pentru operatorii de servicii esențiale și furnizorii de servicii digitale (FSD); 7. Stabilirea cerințelor de notificare a incidentelor de securitate survenite la nivelul rețelelor și sistemelor OSE și FSD; 8. Crearea cadrului național și a mecanismelor care să garanteze aplicarea prevederilor Directivei; 9. Crearea cadrului național de cooperare și răspuns coordonat la incidentele de securitate survenite la nivelul rețelelor OSE și FSD; 10. Participarea în organismele și în cadrul mecanismelor de cooperare la nivelul Uniunii, respectiv la Grupul de Cooperare în vederea coordonării la nivel strategic și în cadrul Rețelei CSIRT în răspunsul comun la incidentele cu impact la nivel European; 11. Raportarea periodică de date privind progresul transpunerii și eficiența aplicării, permițând Comisiei evaluarea la nivel UE a acestora. Cu privire la aplicabilitate, Directiva NIS1 și legea de transpunere au vizat un **număr limitat de sectoare** ale vieții economice, respectiv: ***Energia, Transporturile, Sectorul bancar, Infrastructuri ale pieței financiare, Sănătate, Furnizarea și distribuirea de apă potabilă, Infrastructura digitală***. De la intrarea în vigoare a Legii nr. 362/2018, s-au înregistrat progrese semnificative în ceea ce privește creșterea nivelului de reziliență cibernetică la nivelul României, aceasta creând un cadru național unitar pentru securitatea rețelelor și sistemelor informatice

	din perspectiva apartenenței la sistemul european, în același timp delimitându-se de componenta de securitate națională și apărare cibernetică, care a fost reglementată ulterior. Domeniul securității cibernetice este unul deosebit de dinamic atât prin prisma evoluției rapide a tehnologiilor, dar și a dinamicii actorilor de amenințare. În intervalul scurs de la adoptarea Directivei NIS1, amenințările și atacurile cibernetice au cunoscut un trend ascendent fără precedent în istoria TIC. Se remarcă atât (1) diversificarea și creșterea gradului de sofisticare a metodelor de atac utilizate, (2) implicarea a noi categorii de actori rău intenționați, concomitent cu (3) sporirea fără precedent a gradului de dependență al societății de tehnologiile informației și comunicațiilor, impulsionată și de pandemia de COVID-19. Toate aceste evoluții au făcut relevat necesitatea adaptării mecanismelor și cadrului legal european și a celor naționale pentru a face față noilor provocări. Reexaminarea Directivei (UE) 2016/1148 a Parlamentului European și a Consiliului a arătat că aceasta a servit drept catalizator pentru abordarea instituțională și de reglementare a securității cibernetice în Uniune, deschizând calea pentru o schimbare semnificativă a mentalității. Directiva NIS1 a asigurat definirea cadrelor naționale privind securitatea rețelelor și a sistemelor informatice ca parte a unui ecosistem european unitar al securității cibernetice, elaborarea de strategii naționale de securitate a rețelelor și a sistemelor informatice, crearea de capacități naționale, precum și punerea în aplicare a unor măsuri care să vizeze infrastructurile și entitățile esențiale identificate în fiecare stat membru. Reexaminarea Directivei (UE) 2016/1148 din perspectiva adaptării la noul peisaj al amenințărilor a evidențiat deficiențe inerente care împiedică soluționarea în mod eficace a provocărilor actuale și a celor emergente în materie de securitate cibernetică.

	O deficiență importantă o reprezintă imposibilitatea aplicării unitare la nivelul Uniunii a dispozițiilor Directivei NIS1, întrucât măsurile adoptate de statele membre au creat diferențe între criteriile de evaluare a impactului incidentelor, între modalitățile de identificare a operatorilor, de stabilire a cerințelor de securitate și de punere a acestora în practică. Toate aceste elemente au avut ca efect **fragmentarea sistemului unitar de securitate cibernetică** al Uniunii. În prezent, cerințele în materie de securitate cibernetică impuse entităților care furnizează servicii sau desfășoară activități care sunt semnificative din punct de vedere economic variază considerabil de la un stat membru la altul în ceea ce privește conținutul acestora, nivelul lor de detaliere și metoda de supraveghere. Disparitățile amintite implică costuri semnificative atât pentru state, cât și pentru entitățile în cauză și creează dificultăți pentru entitățile care oferă bunuri sau servicii în mai multe state ale Uniunii. Se remarcă nu doar diferențe între obligațiile impuse acestor entități economice, ci chiar cerințe contradictorii de la un stat la altul, afectând în mod substanțial activitățile economice. Totodată, posibilitatea ca cerințele de securitate să fie concepute sau puse în aplicare în mod necorespunzător într-un stat membru poate avea repercusiuni asupra nivelului de securitate cibernetică din alte state membre, în special având în vedere interconectările și furnizarea de servicii transfrontaliere, creând astfel vulnerabilități. În urma centralizării dificultăților întâmpinate și a lecțiilor învățate, a fost elaborată și adoptată Directiva NIS2, care aduce ca noutăți: • Extinderea domeniului de aplicare; • Eliminarea diferențierii dintre Furnizori și Operatori (OSE/FSD) și utilizarea termenului de entități; • Introducerea unui criteriu uniform de identificare a subiecților reglementării, respectiv raportarea la dimensiunea entităților vizate și la sectoarele esențiale, precum și

	criteriul specific al rolului esențial al unei entități; • Extinderea ariei de aplicare la administrația publică, sub rezerva unor condiții specifice și cu anumite excepții; • Includerea unor noi tipuri de servicii și activități vizate (furnizori servicii de încredere, furnizori de telecomunicații etc.) • Propuneri de măsuri de supraveghere adecvate importanței entităților pentru sectoarele din care fac parte pentru asigurarea proporționalității obligațiilor; • Simplificarea procedurilor de înregistrare a entităților; • Reguli mai clare privind aplicarea actelor normative sectoriale; • Reguli îmbunătățite cu privire la notificarea incidentelor; • Noi instrumente la dispoziția autorităților privind controlul, supravegherea și sancționarea nerespectării obligațiilor; • Încurajarea schimbului de informații; • Încurajarea divulgării coordonate a vulnerabilităților; • Reglementări privind mecanismele de management și cooperare pentru răspunsul la crizele cibernetice; • Adresarea riscurilor privind lanțul de aprovizionare. Față de Directiva NIS1, care avea ca obiectiv general promovarea culturii de securitate cibernetică, Directiva NIS2 propune o abordare mult mai apropiată de procesele concrete de asigurare a securității cibernetice, respectiv managementul riscului. Astfel, noua directivă promovează o cultură a gestionării riscurilor, entitățile a căror activitate este vizată având obligația evaluării concrete și permanente a riscurilor și adoptarea, respectiv ajustarea măsurilor de securitate cibernetică raportat la evaluarea de risc și la condițiile economice proprii. Principiile aplicabile acestui proces sunt principiul evaluării multirisc și principiul raportării la cele mai noi tehnologii și metode de prevenire și contracarare

	atunci când entitățile își stabilesc măsurile de securitate. Pentru aplicarea proporțională, obligațiile se vor individualiza corespunzător circumstanțelor socio-economice reale ale entității, prin ajustarea măsurilor corespunzător gradului de expunere la riscul specific identificat și raportarea la situația financiară a entității în cauză. Textul Directivei rezervă Comisiei posibilitatea de a adopta acte privind cerințele tehnice și metodologice, cerințele sectoriale referitoare la măsurile de gestionare a riscurilor în materie de securitate cibernetică, precum și pentru a specifica mai în detaliu tipul de informații necesare, formatul și procedura de notificare a incidentelor, a amenințărilor cibernetice, a incidentelor evitate la limită, precum și a comunicărilor de amenințări cibernetice semnificative și, în sfârșit, cazurile în care un incident trebuie considerat semnificativ. Aceste acte vor avea în vedere asigurarea unor condiții uniforme pentru punerea în aplicare a directivei. Directiva NIS2 aduce extinderea domeniului de aplicare, obligațiile adresându-se mai multor entități și sectoare, vizând creșterea nivelului de securitate cibernetică în UE pe termen lung. Noua listă a sectoarelor de activitate este mult extinsă, cuprinzând: **Energie, Transport, Bancar, Infrastructuri ale pieței financiare, Sănătate, Furnizarea și distribuirea de apă potabilă, Infrastructură digitală, Ape uzate, Gestionarea serviciilor TIC, Administrație publică, Spațiu, Servicii poștale și de curierat, Gestionarea deșeurilor, Fabricarea, producția și distribuția de substanțe chimice, Producția, prelucrarea și distribuția de alimente, Fabricare, Furnizori digitali și Cercetare.** La nivelul României, transpunerea Directivei NIS1 prin Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice a deschis calea dezvoltării ecosistemului național de securitate cibernetică, prin dezvoltarea cadrului instituțional, modificarea cadrului strategic,

	precum și reglementarea domeniilor aferente securității și apărării cibernetice, astfel: 1. *OUG nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică*, a creat cadrul instituțional aferent aplicării directivei NIS1 prin consacrarea și conferirea capacităților necesare autorității NIS. 2. Tot în anul 2021 a fost adoptată *Strategia de securitate cibernetică a României pentru perioada 2022-2027, aprobată prin HG nr. 1321 din 30 decembrie 2021*, strategie care se află la baza evoluției securității cibernetice în România. 3. Ulterior, *Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative* a întregit cadrul normativ, adăugând prevederile aferente marjei naționale de reglementare, respectiv abordarea securității cibernetice din perspectiva securității naționale și apărare, reglementând totodată relația dintre componentele ecosistemului de la nivel național. În conformitate cu art. 41 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) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2), **statele membre au obligația să adopte și să publice măsurile necesare pentru a se conforma cu directiva menționată anterior până la 17 octombrie 2024.** Evoluții ale amenințărilor cibernetice care reclamă actualizarea rapidă a cadrului legal: Evoluția rapidă și adopția tehnologiilor emergente creează noi tipuri de interdependențe și expune infrastructura critică a statului unor riscuri complexe, neprevăzute anterior, susceptibile de a genera efecte semnificative asupra securității cibernetice, efecte care se extind și asupra autorităților și instituțiilor din administrația publică. Diversificarea și utilizarea serviciilor furnizate în mediul online au cunoscut o accelerare majoră

	datorată unui ansamblu de factori, incluzând conflictul ruso-ucrainean, pandemia de COVID-19, dezvoltarea și globalizarea mediului de afaceri, precum și reducerea costurilor pentru accesarea de noi piețe, au generat atât beneficii, cât și un nou spectru de amenințări, riscuri și vulnerabilități aferente securității cibernetice, vulnerabilități ce sunt intrinsec asociate tehnologiilor smart, precum rețelele 5G, Internetul Lucrurilor (IoT) și Inteligența Artificială (AI). De la izbucnirea conflictului armat în proximitatea teritoriului României, s-a observat o utilizare intensificată a atacurilor cibernetice ca parte a operațiunilor militare, cu efecte transfrontaliere care afectează și state neimplicate direct în conflict, spre exemplu atacul cibernetic asupra rețelei de comunicații prin satelit KA-SAT, operată de compania VIASAT, ale cărui efecte s-au extins la nivel european, impactul fiind resimțit și în România. Efectele implicării unor noi actori cibernetici în conflict, printre care grupuri de hackeri ce susțin una dintre tabere implicate în conflicte, precum Gruparea Killnet, care au desfășurat atacuri cibernetice îndreptate împotriva infrastructurilor și serviciilor esențiale din state membre ale Uniunii Europene care sprijină Ucraina, s-au resimțit inclusiv în România. Creșterea nivelului de digitalizare și interconectare a sistemelor informatice, coroborată cu dezvoltarea capabilităților actorilor maligni din mediul online a condus la o intensificare a incidentelor care generează un impact semnificativ asupra infrastructurilor din domenii de importanță critică prin compromiterea lanțului de aprovizionare. Incidente majore, precum cel din primul trimestru al anului 2024, care a afectat 26 de spitale, la nivel național, prin intermediul unui furnizor de servicii gestionate, cu impact direct asupra serviciilor vitale oferite populației, au relevat limitele legislației actuale în domeniul securității cibernetice și nevoia de a implementa reglementările europene actualizate în ceea ce privește securitatea lanțului de aprovizionare și impunerea unor obligații în vederea

	creșterii nivelului de reziliență al acestora, în corelare cu nivelul lor de risc în plan societal. Adoptarea promptă a măsurilor și mecanismelor prevăzute de Directiva NIS2 devine imperativă pentru creșterea rezilienței României în fața amenințărilor cibernetice, dat fiind rolul crucial al acestei Directive în consolidarea capacităților naționale de apărare și răspuns la incidente cibernetice și, de asemenea, menționând și că aplicarea prevederilor contribuie la alinierea României la standardele internaționale, consolidând astfel capacitatea națională de a reacționa în mod eficient în fața evoluțiilor regionale și globale din domeniul securității cibernetice. Aspectele prezentate constituind o stare de fapt obiectivă, cuantificabilă, extraordinară, independentă de voința Guvernului, care pune în pericol interesul public și a cărei reglementare nu poate fi amânată, impunându-se astfel adoptarea unor măsuri imediate.
2.3. Schimbări preconizate	Transpunerea prevederilor 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) în legislația națională, prin integrarea experienței de la nivel european a ultimilor ani și prin abordările propuse, modernizează, completează și îmbunătățește ecosistemul asigurării rezilienței și securității cibernetice a activităților și serviciilor furnizate în sectoarele socio-economice de cea mai mare importanță la nivel național și comunitar. În același timp, lecțiile învățate în aplicarea directivei NIS1 aduc modificări la majoritatea componentelor ecosistemului existent, precum și noi componente și activități reglementate, motiv pentru care nu este posibilă simpla amendare și completare a Legii 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice. Pentru o transpunere completă a directivei NIS2 sunt necesare:

	- modificarea cadrului legislativ aferent Directivei prin act normativ cu putere de lege care va înlocui Legea nr. 362/2018; - asigurarea prin noi acte normative si administrative subsecvente aplicării acesteia; - abrogarea unor prevederi în vigoare act normativ și completarea corelativă a altor acte normative în vigoare. Proiectul de act normativ constituie o transpunere în legislația națională a unei directive a Uniunii Europene. Temeiul juridic al directivei NIS2 exclude reglementarea activităților de securitate națională și apărare aferente securității cibernetice, neaducând atingere activităților care fac parte din marja națională de reglementare a statelor membre. În România, activitățile aferente securității și apărării cibernetice, desfășurate de către instituțiile din sistemul național de apărare, ordine publică și securitate națională (SNAOPSN) sunt reglementate prin Legea nr. 58/2023, care este complementară legii de transpunere a directivei NIS, cele două acte normative adresând ca un tot unitar securitatea cibernetică națională. Legea nr. 362/2018 a vizat exclusiv spațiul cibernetic național civil, adresând în linie cu directiva NIS asigurarea securității cibernetice a activităților economice naționale, abordare care se păstrează și în privința prezentului proiect de act normativ. Prezentul proiect de act normativ urmează aceeași delimitare, asigurând totodată continuitatea complementarității celor două componente ale securității cibernetice naționale, care trebuie să fie interoperabile, funcționând ca un tot unitar. Prin Decizia nr. 455 din 4 iulie 2018 referitoare la obiecția de neconstituționalitate a dispozițiilor Legii privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, Curtea Constituțională a constatat că ritmul actual al realităților obiective este în continuă schimbare, iar

	relațiile sociale referitoare la securitatea rețelelor și sistemelor informatice vizează un interes general a cărui amploare impune calificarea acestui domeniu ca fiind în strânsă interdependență cu securitatea națională. Curtea a reținut că această teză este susținută de împrejurarea că Legea privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice reglementează cu privire la servicii publice esențiale (energie, alimentare cu apă, sănătate și transporturi), care prin natura lor pot afecta securitatea națională, motiv pentru care a decis că deși actul normativ transpune o directivă europeană dedicată domeniului civil, acesta necesită avizul Consiliului Suprem de Apărare a Țării. Ca urmare, pentru a asigura complementaritatea cu domeniul securității naționale, proiectul de act normativ a fost armonizat cu prevederile Legii 58/2023 și totodată este supus avizului CSAT. Directiva NIS1 (Legea nr. 362/2018) precum și Directiva NIS2 au ca obiect securitatea cibernetică a activităților economice aferente pieței unice a UE. Obiectivul principal îl constituie protejarea serviciilor esențiale dependente de TIC din anumite sectoare de activitate economică, a căror afectare ar avea impact negativ semnificativ asupra unor grupuri largi de populație (impact societal). Dezideratul creșterii încrederii cetățenilor în piața digitală unică poate fi realizat printr-un ecosistem unitar de asigurare a securității cibernetice, atât la nivel individual al Statelor Membre, cât ca parte în ecosistemul de la nivelul Uniunii. Ecosistemul NIS2 și prezentul proiect păstrează o serie dintre elementele instituite de directiva NIS1, în principal: - Adresarea securității cibernetice a sectoarelor economice de cea mai mare importanță; - Instituțiile și mecanismele de coordonare și relaționare la nivel național și de participare în ecosistemul UE (autorități naționale, echipe de răspuns, punct unic de contact); - Procesele de identificare a entităților care au obligații în temeiul actului normativ; - Obligația de raportare a incidentelor

	cibernetice - Obligațiile aferente măsurilor de prevenire a incidentelor, de răspuns la acestea și de recuperare și restabilire; - Activitatea de supraveghere și control, respectiv sancționarea neconformării cu dispozițiile legale. În acest scop, prin prezentul proiect de act normativ se propune adoptarea unui set de norme coerente, clare si transparente, menite să instituie un cadru național unitar de asigurare a securității informatice și a răspunsului la incidentele de securitate cibernetică survenite la nivelul rețelelor și sistemelor informatice ale entităților esențiale și ale entităților importante în conformitate cu cerințele 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). Spre deosebire de Legea nr. 362/2018 care transpune Directiva (UE) 2016/1148, Directiva (UE) 2022/2555 aduce următoarele elemente de noutate: • Abordarea problematicii lanțului de aprovizionare din punct de vedere al securității cibernetice; • Termene definite pentru diferite raportări - anume, la: 24 de ore de la luarea la cunoștință de producerea incidentului, la 72 de ore de la luarea la cunoștință de producerea incidentului, la o lună de la luarea la cunoștință de producerea incidentului; • Măsuri de supraveghere și control; • Implementarea la nivel național a unei politici privind divulgarea coordonată a vulnerabilităților informatice (CVD); • Stabilirea cadrului național de gestionare a incidentelor de mare amploare sau a crizelor cibernetice și participarea la sistemul european aferent, EU-CyCLONe; • Evaluări inter pares cu celelalte state membre; • Responsabilizarea conducerii entităților vizate de prezentul proiect de lege;

	• Extinderea domeniului de aplicare de la șapte sectoare la optsprezece sectoare ale vieții economice, astfel: energie, transport, bancar, infrastructuri ale pieței financiare, sănătate, furnizarea și distribuirea de apă potabilă, infrastructură digitală, ape uzate, gestionarea serviciilor TIC, administrație publică, spațiu, servicii poștale și de curierat, gestionarea deșeurilor, fabricarea, producția și distribuția de substanțe chimice, producția, prelucrarea și distribuția de alimente, fabricare, furnizori digitali și cercetare. În noua sa abordare, Directiva NIS2 elimină categoriile de subiecți din legile naționale - operatori de servicii esențiale și furnizori de servicii digitale, adoptând termenul de *entități* și criteriul principal al dimensiunii acestora, la care se adaugă elemente privind importanța acestora. În proiectul de act normativ, referințele privind dimensiunea entităților vizate sunt preluare din Recomandarea 2003/361/EC a Comisiei Europene, astfel: • microîntreprindere - sub 10 angajați și cifră de afaceri/bilanț sub 2 mil. EUR; • întreprindere mică - sub 50 angajați și cifră de afaceri/bilanț sub 10 mil. EUR; • întreprindere mijlocie - sub 250 angajați și cifră afaceri sub 50 mil. EUR sau bilanț sub 43 mil. EUR. În linie cu noua viziune a directivei, de promovare a unei culturi a gestionării riscurilor, entitățile vizate de prezentul proiect au obligația instituirii de procese interne de evaluare concretă și permanentă a riscurilor de securitate cibernetică și de a adopta, respectiv ajusta măsurile aferente, raportat la evaluarea de risc și la condițiile economice proprii. Principiile aplicabile acestui proces sunt principiul evaluării multirisc și principiul raportării la cele mai noi tehnologii și metode de prevenire și contracarare atunci când entitățile își stabilesc măsurile de securitate.

	Principiul proporționalității în stabilirea măsurilor are în vedere individualizarea acestora în acord cu circumstanțele socio-economice reale ale entității, prin ajustarea conform gradului de expunere la riscul specific identificat și raportarea la situația financiară a entității în cauză. Măsurile luate sunt de factură tehnică, operațională și organizatorică și trebuie să identifice, să evalueze și să gestioneze riscurile la adresa securității rețelelor și sistemelor informatice pe care se bazează activitatea proprie și furnizarea serviciilor. Pentru a veni în sprijinul entităților, DNSC adoptă prin decizia Directorului și publică metodologia de evaluare a nivelului de risc. Evaluarea efectivă a măsurilor luate și a gradului de conformare cu obligațiile legale se face prin efectuarea de audituri de securitate, condițiile și periodicitatea acestora variind în funcție de gradul de risc al entității. În noua viziune de la nivel european, statele membre au obligația de a se asigura că răspunderea pentru neconformarea cu cerințele legale revine conducerii entităților subiect al legii. În acest sens, și pentru a implementa principiul proporționalității cerințelor de securitate, proiectul instituie în primul rând un proces periodic de autoevaluare a maturității măsurilor de gestionare a riscurilor și de asumare de către conducerea entităților a unui plan corectiv care se comunică către DNSC, proiectul stabilind un set de categorii de măsuri ce vor fi evaluate și implementate, astfel: analiza riscurilor, evaluarea eficacității măsurilor, utilizarea criptografiei și, după caz, a criptării, securitatea lanțului de aprovizionare, securitatea achiziției, dezvoltării, întreținerii și casării rețelelor și sistemelor informatice, inclusiv gestionarea și divulgarea vulnerabilităților, securitatea resurselor umane, politicile de control al accesului și gestionarea activelor, gestionarea incidentelor, continuitatea activității, igienă cibernetică și formarea în domeniul

	securității cibernetice, utilizarea soluțiilor de autentificare etc. Proiectul prevede o serie întreagă de obligații care, conform Directivei transpuse, trebuie să revină organelor de conducere a entităților, între care: aprobarea măsurilor de gestionare a riscurilor de securitate cibernetică, supravegherea punerii în aplicare, responsabilitatea privind încălcările dispozițiilor legale, urmarea cursuri de formare pentru dobândirea cunoștințelor și competențelor necesare, stabilirea mijloacelor permanente de contact, alocarea resurselor necesare, desemnarea responsabililor cu securitatea rețelelor și sistemelor informatice etc. Raportarea incidentelor constituie o obligație principală a entităților vizate de proiect, cunoașterea privind incidentele, amenințările și atacurile cibernetice având un rol esențial în ecosistemul de securitate cibernetică. Raportarea la nivel național se face prin intermediul platformei PNRISC, iar pentru încurajarea raportării, proiectul prevede faptul că actul raportării incidentului nu atrage sporirea răspunderii entității care face raportarea. Tot în scopul cunoașterii și luării măsurilor adecvate, proiectul prevede necesitatea informării utilizatorilor finali ai unei entități privind atacurile și amenințările identificate. Conform proiectului, raportarea se face în mai multe etape, după caz: avertizare timpurie, raport de incident/evaluare inițială, rapoarte intermediare (la cererea echipei CSIRT), precum si raport final. De un interes deosebit în cazul raportărilor de incidente sunt determinarea impactului și efectelor, impactului transfrontalier, tipul de amenințare sau cauza incidentului, măsurile de atenuare a efectelor. Înregistrarea și evidența entiăților esențiale și importante: Construind pe baza experienței anterioare a registrului operatorilor de servicii esențiale din Directiva NIS1, în vederea uniformizării practicii la nivel european, Directiva NIS2 și proiectul de act

	normativ instituie un proces de luare în evidență îmbunătățit, având la bază auto-identificarea entităților și pe cale de excepție identificarea și înscrierea din oficiu a acestora. Coordonarea ecosistemului național aferent Directivei NIS este făcută de către Directoratul Național de Securitate Cibernetică (DNSC), desemnat autoritate competentă responsabilă cu securitatea cibernetică și cu sarcinile de supraveghere și asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate pentru spațiul cibernetic național civil. Totodată, DNSC îndeplinește funcția de echipă de răspuns la incidente de securitate cibernetică națională („CSIRT național''). Atribuțiile DNSC, includ: elaborarea strategiei naționale de securitate cibernetică, emiterea de norme și cerințe, elaborarea și actualizarea de ghiduri, recomandări și bune practici, participarea la formatele de cooperare la nivel european, supravegherea, verificarea și controlul respectării dispozițiilor legale în domeniul de competență, primirea de sesizări cu privire la neîndeplinirea obligațiilor, cooperarea cu autoritățile competente din celelalte state, transmiterea de solicitări și sesizări, efectuarea controlului ori luarea de măsuri de supraveghere și remediere a deficiențelor constatate, autorizarea echipelor de răspuns la incidente de securitate cibernetică ce deservesc entitățile esențiale și importante, atestarea auditorilor de securitate cibernetică, autorizarea furnizorilor de servicii de formare pentru securitate cibernetică pentru formarea auditorilor de securitate cibernetică și a echipelor de răspuns la incidente de securitate cibernetică, gestionarea procesului de divulgare coordonată a vulnerabilităților etc. DNSC va prelua sarcinile strategice și operaționale care decurg din implementarea Directivei 2022/2555, anume: • Analiza necesităților de modificare și coordonarea inițierii și adoptării următoarei versiuni a strategiei de securitate cibernetică a României, în

	strânsă cooperare cu celelalte instituții naționale cu rol în domeniul securității cibernetice abilitate prin legea 58/2023; • Funcția de autoritate națională pentru gestionarea incidentelor de securitate cibernetică de mare amploare; reprezentarea României în comitetele la nivel european și internațional privind asigurarea unui nivel ridicat de securitate cibernetică a rețelelor și a sistemelor informatice, în special grupul de cooperare EU-CyCLONe; • Consultarea și cooperarea cu autoritățile competente ale altor state membre Uniunea Europeană; • Autorizarea și supravegherea CSIRT-urilor sectoriale. Sarcina centrală a autorității este de a supraveghea respectarea măsurilor de gestionare a riscurilor și a obligațiilor de raportare prevăzute în prezentul proiect pentru entitățile esențiale și importante. DNSC acționează și ca centru de raportare a incidentelor pentru toate CSIRT-urile. Rapoartele despre amenințări cibernetice, incidente de securitate cibernetică sunt primite și analizate în consecință. CSIRT-urile (Echipe de răspuns la incidente de securitate cibernetică) au în continuare sarcina de a trata incidentele de securitate cibernetică, fiind primul punct de contact pentru toate entitățile care intră în domeniul de aplicare al prezentului act normativ afectate de un incident de securitate cibernetică. În plus, CSIRT-urile îndeplinesc și alte sarcini tehnice, precum colectarea și analiza amenințărilor cibernetice, vulnerabilităților și incidentelor de securitate cibernetică, analizarea și emiterea de alerte atunci când informațiile despre amenințările cibernetice, vulnerabilitățile și incidentele de securitate cibernetică devin disponibile. Aceste informații pot proveni și de la terți: alte CSIRT-uri, cercetători în securitate, furnizori de servicii, organizații non-profit.

	CSIRT-ul național este autorizat să efectueze scanări proactive non-intruzive ale rețelelor și sistemelor informatice accesibile publicului, la cererea unei entități esențiale. Dacă în timpul unei astfel de scanări sunt identificate sisteme și informații vulnerabile sau configurate nesigur, entitățile relevante trebuie informate, în vederea remedierii acestora. CSIRT-uri specifice unui anumit sector de activitate pot fi înființate pentru a sprijini entități esențiale și importante, care pot astfel beneficia de expertiza specifică în sectorul respectiv și pot oferi entităților esențiale și importante cel mai bun suport tehnic posibil în tratarea incidentelor și incidentelor de securitate cibernetică. În situația în care nu există echipă CSIRT specifică pentru un anumit sector, sarcinile relevante revin CSIRT-ului național din cadrul DNSC. Prin urmare, CSIRT-ul național este responsabil în mod fundamental pentru toate instituțiile care fac obiectul NIS și trebuie să îndeplinească sarcinile atribuite unui CSIRT în conformitate cu această lege în toate sectoarele. În ceea ce privește Strategia națională de securitate cibernetică, această dispoziție pune în aplicare art. 7 din Directiva 2022/2555 care impune statelor membre să adopte o strategie de securitate cibernetică. Strategia de securitate cibernetică include în special obiective strategice și măsuri de reglementare adecvate scopului de a asigura un nivel înalt de securitate a rețelelor și a sistemelor informatice de pe teritoriul României. Față de viziunea din directiva NIS1 privind obligația adoptării de strategii naționale de securitate cibernetică, noua Directivă detaliază categoriile de elemente care ar trebui să intre în cuprinsul strategiei, atât pentru a conștientiza statele membre cu privire la numeroasele aspecte care trebuie să facă obiectul politicilor publice aferente domeniului, cât și pentru a uniformiza practica la nivel european. Cu toate acestea, statele membre sunt libere să includă abordările proprii, în conformitate cu realitățile naționale. În acest sens, dincolo de rolul

	DNSC de inițiator și coordonator al procesului de actualizare a strategiei naționale de securitate cibernetică, elaborarea efectivă a acesteia va fi făcută în strânsă cooperare cu celelalte instituții naționale și organisme din domeniul securității cibernetice, conform atribuțiilor acestora din Legea nr. 58/2023. În ceea ce privește managementul incidentelor de securitate cibernetică la scară largă, DNSC este responsabilă și de gestionarea incidentelor de securitate cibernetică de mare amploare. Aceasta include participarea la EU-CyCLONe și sprijinul acestuia în îndeplinirea sarcinilor. După cum este definit în prezentul proiect, un incident de securitate cibernetică de mare amploare presupune un incident de securitate cibernetică care provoacă o perturbare a cărei amploare depășește capacitatea unui stat membru de a răspunde sau care are un impact semnificativ asupra cel puțin două state membre. În cazul în care un astfel de incident de securitate cibernetică, singur sau în împreună cu amenințări cibernetice relevante, riscuri sau alte incidente, atinge acest nivel, autoritatea competentă trebuie să măsuri. Dacă a avut loc un incident de securitate cibernetică de mare amploare, evaluarea este realizată în mod holistic și nu doar pe baza incidentului specific de securitate cibernetică. Dacă un incident de securitate cibernetică este recunoscut ca fiind de mare amploare, acest lucru trebuie prezentat de autoritatea de securitate cibernetică în cadrul EU CyCLONe. DNSC trebuie să ia măsuri preventive pentru a permite gestionarea eficientă a incidentelor de securitate cibernetică de mare amploare. Aceasta include identificarea capacităților, mijloacelor și procedurilor care pot fi implementate în cazul unui incident de securitate cibernetică de mare amploare și pe baza acesteia, adoptarea unui plan național de răspuns. DNSC transmite informațiile relevante privind planul de răspuns la incidentele de securitate cibernetică de mare amploare atât Comisiei Europene, cât și EU-CyCLONe.

	Prezentul proiect prevede că DNSC poate participa la evaluări inter pares. Domeniul de aplicare al evaluării inter pares, inclusiv orice probleme identificate, trebuie să fie determinat de către participanți înainte de începerea evaluării inter pares. În conformitate cu art. 26 alin. (1) lit. (a) din Directiva 2022/2555, furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice accesibile publicului sunt supuși jurisdicției statului membru al Uniunii Europene în care își prestează serviciile. Prin urmare, prevederile legale le sunt aplicabile în conformitate cu condiția de a presta serviciile în România. Securitatea cibernetică este definită în cadrul art. 2 lit. y) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative și înseamnă o stare de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic ale resurselor și serviciilor publice sau private din spațiul cibernetic. Dispozițiile Legii nr. 51/1991 privind securitatea națională a României definesc în cadrul art. 1 securitatea ca acea stare de legalitate, de echilibru şi de stabilitate socială, economică şi politică necesară existenţei şi dezvoltării statului naţional român ca stat suveran, unitar, independent şi indivizibil, menţinerii ordinii de drept, precum şi a climatului de exercitare neîngrădită a drepturilor, libertăţilor şi îndatoririlor fundamentale ale cetăţenilor, potrivit principiilor şi normelor democratice statornicite prin Constituţie. Directiva 2555/2022 face trimitere în vederea definirii securității cibernetice la Regulamentul (UE) 2019/881, care identifică aceasta drept activitățile necesare pentru protejarea rețelelor și a sistemelor informatice, a utilizatorilor unor astfel de sisteme și a altor persoane afectate de amenințări cibernetice. Conform art. 4 din Tratatul privind Funcționarea

	Uniunii Europene, asupra spațiului de securitate, Uniunea se bucură de competențe partajate cu statele membre. Astfel, neconcordanța dintre conceptul de securitate definit la nivel național și cel la nivel european nu creează un conflict între cele două legislații. În cadrul Deciziei Curții Constituționale nr. 455/2018, par. 49, *Curtea a reținut că termenul „securitate națională" este unul plurivalent. Astfel, din punct de vedere al art. 53 alin. (1) din Constituție, se poate vorbi de securitate militară, economică, financiară, informatică, socială a țării.* De asemenea, amintim și par. 63 în care *Curtea constată că ritmul actual al realităților obiective este în continuă schimbare, iar relațiile sociale referitoare la securitatea rețelelor și sistemelor informatice vizează un interes general a cărui amploare impune calificarea acestui domeniu ca fiind în strânsă interdependență cu securitatea națională.* Ținând cont și de jurisprudența Curții Constituționale, subliniem faptul că definiția securității cibernetice trebuie să fie în acord cu definiția conceptului de securitate națională, astfel încât aceasta nu poate fi identificată altfel decât o stare. Având în vedere toate cele astfel amintite, învederăm faptul că nu se creează un conflict între cele două cadre legale, statele membre putând acționa autonom în acest domeniu. Pentru adresarea aspectelor întâlnite în practică și, având în vedere dezideratul Directivei NIS de creare la nivelul Uniunii a unui ecosistem unitar de asigurare a securității cibernetice – deziderat care se traduce prin expectanța de compatibilitate și interoperabilitate între sistemele de implementare națională, proiectul de act normativ adoptă definiția securității rețelelor și sistemelor informatice ca parte a asigurării securității cibernetice ce caracterizează capacitatea rețelelor și a sistemelor informatice de a rezista, la un anumit nivel de încredere, oricărui eveniment care ar putea compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate sau a serviciilor furnizate de aceste rețele și sisteme informatice puse la dispoziție

2.4. Alte informaţii	Nu este cazul.
Secţiunea a 3-a: Impactul socio-economic al proiectului de act normativ	
3.1. Descrierea generală a beneficiilor și costurilor estimate ca urmare a intrării în vigoare a actului normativ	Proiectul de act normativ nu se referă la acest subiect
3.2. Impactul social	Constituind cadrul legal care reglementează securitatea rețelelor și sistemelor informatice ce susțin serviciile oferite de entități esențiale și entități importante din domenii cheie la nivel social, este de așteptat o creștere a rezilienței acestor servicii și respectiv o reducere a riscurilor la nivel social asociate cu atacurile cibernetice. Indirect, va conduce pe termen lung la o creștere a încrederii în serviciile societății digitale și o dezvoltare a serviciilor de securitate cibernetică
3.3. Impactul asupra drepturilor și libertăților fundamentale ale omului	Proiectul de act normativ nu se referă la acest subiect
3.4. Impactul macroeconomic	Proiectul de act normativ nu se referă la acest subiect
3.4.1. Impactul asupra economiei și asupra principalilor indicatori macroeconomici	Proiectul de act normativ nu se referă la acest subiect
3.4.2. Impactul asupra mediului concurențial și domeniul ajutoarelor de stat	Proiectul de act normativ nu se referă la acest subiect
3.5. Impactul asupra mediului de afaceri	Directiva (UE) 2022/2555 și pe cale de consecință și proiectul de act normativ impune cerințe de securitate entităților esențiale și entităților importante
3.6. Impactul asupra mediului înconjurător	Proiectul de act normativ nu se referă la acest subiect
3.7. Evaluarea costurilor și beneficiilor din perspectiva inovării și digitalizării	Proiectul de act normativ nu se referă la acest subiect

3.8. Evaluarea costurilor și beneficiilor din perspectiva dezvoltării durabile	Proiectul de act normativ nu se referă la acest subiect
3.9. Alte informații	Nu este cazul

Secţiunea a 4-a:
Impactul financiar asupra bugetului general consolidat, atât pe termen scurt, pentru anul curent,
cât şi pe termen lung (pe 5 ani), inclusiv informații cu privire la cheltuieli și venituri

- mii lei -

Indicatori	**Anul Curent**	**Următorii 4 ani**				**Media pe 5 ani**
1	**2024 2**	**2025 3**	**2026 4**	**2027 5**	**2028 6**	**7**
4.1. Modificări ale veniturilor bugetare, plus/minus, din care: a) *buget de stat*, din acesta: (i) impozit pe profit (ii) impozit pe venit b) *bugete locale*: (i) impozit pe profit c) *bugetul asigurărilor sociale de stat*: (i) contribuții de asigurări *d) alte tipuri de venituri*						

4.2. Modificări ale cheltuielilor bugetare, plus/minus, din care: a) *buget de stat*, din acesta: (i) cheltuieli de personal (ii) bunuri și servicii b) *bugete locale*: (i) cheltuieli de personal (ii) bunuri și servicii c) *bugetul asigurărilor sociale de stat*: (i) cheltuieli de personal (ii) bunuri și servicii *d) alte tipuri de venituri*						
4.3. Impact financiar, plus/minus, din care: a) *buget de stat* b) *bugete locale*						
4.4. Propuneri pentru acoperirea creșterii cheltuielilor bugetare	Proiectul de act normativ nu se referă la acest subiect					
4.5. Propuneri pentru a compensa reducerea veniturilor bugetare	Proiectul de act normativ nu se referă la acest subiect					
4.6. Calcule detaliate privind fundamentarea modificării veniturilor și/sau cheltuielilor bugetare	Proiectul de act normativ nu se referă la acest subiect					
4.7. Prezentarea, în cazul proiectelor de acte normative a căror adoptare atrage majorarea cheltuielilor bugetare, a următoarelor documente: **a) fișa financiară prevăzută la art. 15 din Legea nr. 500/2002 privind finanțele publice, cu modificările și completările ulterioare, însoțită de ipotezele și metodologia de calcul utilizată;** **b) declarație conform căreia majorarea de cheltuială respectivă este compatibilă cu obiectivele și prioritățile strategice specificate în**	Nu este cazul Nu este cazul					

strategia fiscal-bugetară, cu legea bugetară anuală și cu plafoanele de cheltuieli prezentate în strategia fiscal-bugetară	
4.8. Alte informații	Aplicarea prevederilor actului normativ în cauză nu are impact financiar

Secțiunea a 5-a
Efectele proiectului de act normativ asupra legislației în vigoare

5.1. Măsuri normative necesare pentru aplicarea prevederilor proiectului de act normativ: a) acte normative în vigoare ce vor fi modificate sau abrogate, ca urmare a intrării în vigoare a proiectului de act normativ; b) acte normative ce urmează a fi elaborate în vederea implementării noilor dispoziții	a) • Legea nr. 362 din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, publicată în Monitorul Oficial al României nr. 21 din 9 ianuarie 2019 cu excepția măsurilor adoptate sau impuse în temeiul dispozițiilor din Capitolele IV și V, care rămân în vigoare până la revizuirea acestora, conform art. 65. • art. 4 alin. (1) pct. 54^1 și 54^2, precum și Capitolul IV: Securitatea rețelelor și serviciilor de comunicații electronice din Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, publicată în Monitorul Oficial al României, Partea I, nr. 925 din 27 decembrie 2011, aprobată cu modificări și completări prin Legea nr. 140/2012, cu modificările și completările ulterioare; • Legea nr. 146/2014 privind autorizarea plății cotizațiilor la Forumul Internațional al Echipelor de Răspuns la Incidente de Securitate Cibernetică (Forum of Incident Response and Security Teams-FIRST) și la Forumul TF/CSIRT Trusted Introducer (TI) din cadrul Asociației Transeuropene a Rețelelor din Domeniul Cercetării și al Educației (Transeuropean Research and Education Network Association-TERENA) în scopul menținerii participării Centrului Național de Răspuns la Incidente de Securitate Cibernetică CERT-RO la aceste două organisme neguvernamentale, actualizată;

	• Legea nr. 106/2015 privind aprobarea Ordonanței Guvernului nr. 3/2015 pentru modificarea și completarea Legii nr. 146/2014 privind autorizarea plății cotizațiilor la Forumul Internațional al Echipelor de Răspuns la Incidente de Securitate Cibernetică (Forum of Incident Response and Security Teams - FIRST) și la Forumul TF/CSIRT Trusted Introducer (TI) din cadrul Asociației Transeuropene a Rețelelor din Domeniul Cercetării și al Educației (Transeuropean Research and Education Network Association - TERENA) în scopul menținerii participării Centrului Național de Răspuns la Incidente de Securitate Cibernetică CERT - RO la aceste două organisme neguvernamentale; b) • Criteriile și pragurile de determinare a gradului de perturbare a unui serviciu și metodologia de evaluare a nivelului de risc al entităților, în temeiul art. 10 alin. (2), în termen de 20 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I; • Măsurile de gestionare a riscurilor, în temeiul art. 12 alin. (1), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I; • Normele metodologice privind raportarea incidentelor, în temeiul art. 15 alin. (17), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I; • Cerințele privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor, în temeiul art. 18 alin. (10), în termen de 15 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I; • Planul de management al crizelor de securitate cibernetică la nivel național pe timp de pace, în temeiul art. 28 alin. (2), în termen de 180 de zile de la data publicării prezentei

	ordonanțe de urgență în Monitorul Oficial al României, Partea I; • Normele tehnice privind compatibilitatea și interoperabilitatea sistemelor, procedurilor și metodelor utilizate de către CSIRT-uri și criteriile de stabilire a numărului de persoane calificate, în temeiul art. 31 alin. (2), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I; • Pachetul minim de servicii de tip CSIRT, în temeiul art. 32 alin. (5), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I; • Regulamentul privind autorizarea și verificarea CSIRT-urilor, condițiile de valabilitate pentru autorizațiile acordate și tematicile pentru formarea personalului CSIRT-urilor, în temeiul art. 34 alin. (2) lit. a), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I; • Normele de aplicare și metodologia de prioritizare pe bază de risc a activităților de supraveghere, verificare și control, în temeiul art. 47 alin. (8), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I; • Regulamentul privind autorizarea, verificarea și revocarea furnizorilor de servicii de formare pentru securitate cibernetică pentru auditori și CSIRT-uri și condițiile de valabilitate pentru autorizațiile acordate acestora, în temeiul art. 54 alin. (3), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I; • Normele de aplicare a dispozițiilor privind supravegherea, verificarea și controlul pentru CSIRT-uri, furnizorii de servicii specifice CSIRT, precum și pentru auditorii de securitate cibernetică, în temeiul art. 56 alin. (2), în termen de 120 de zile de la data

	publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I; • Regulamentul privind atestarea și verificarea auditorilor de securitate cibernetică și condițiile de valabilitate pentru atestatele acordate, în temeiul art. 58 alin. (2) lit. b), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I. • Tematicile pentru specializarea auditorilor în vederea atestării, în temeiul art. 58 alin. (2) lit. e), în termen de 180 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I; • Tematicile pentru specializarea personalului din cadrul CSIRT-urilor în vederea autorizării, în temeiul art. 31 alin. (3), în termen de 180 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I.
5.2. Impactul asupra legislației în domeniul achizițiilor publice	Proiectul de act normativ nu se referă la acest subiect
5.3. Conformitatea proiectului de act normativ cu legislația UE	Proiectul de act normativ transpune 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) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (Text cu relevanță pentru SEE)
5.3.1. Măsuri normative necesare transpunerii directivelor UE	Proiectul de act normativ transpune 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) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (Text cu relevanță pentru SEE)
5.3.2. Măsuri normative necesare aplicării actelor legislative UE	Proiectul de act normativ nu se referă la acest subiect

5.4. Hotărâri ale Curții de Justiție a Uniunii Europene	Proiectul de act normativ nu se referă la acest subiect
5.5. Alte acte normative și/sau documente internaționale din care decurg angajamentele asumate	Proiectul de act normativ nu se referă la acest subiect
5.6. Alte informații	Nu este cazul
Secțiunea a 6-a Consultările efectuate în vederea elaborării proiectului de act normativ	
6.1. Informații privind neaplicarea procedurii de participare la elaborarea actelor normative	Nu este cazul
6.2. Informații privind procesul de consultare cu organizații neguvernamentale, institute de cercetare și alte organisme implicate	Proiectul de act normativ a fost dezbătut și agreat în forma prezentată în cadrul Comitetului de reglementare al Directoratului Național de Securitate Cibernetică, înființat prin OUG nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică. De asemenea, DNSC a transmis spre dezbatere, pe site-ul DNSC, subiecte abordate în Directiva (UE) 2555/2022. Menționăm faptul că pe tot parcursul elaborării actului normativ au fost consultate organismele implicate, de exemplu, în cadrul ședinței de lucru organizate în data de 29.09.2024 cu entități precum Institutul Național de Statistică (INS), Agenția Spațială Română (ROSA) și Consiliul Concurenței. În perioada de transparență decizională, au fost transmise pe adresa de e-mail a DNSC pusă la dispoziție pe site-ul DNSC observații de către persoane fizice, dar și de către organisme precum Motion Picture Association EMEA și Asociația Operatorilor Mobili din România. Toate observațiile transmise, atât în termenul indicat pe site, cât și cele transmise ulterior termenului indicat au fost analizate și integrate, după caz. Menționăm, de asemenea, faptul că și Internet Corporation for Assigned Names and Numbers (ICANN) a transmis un punct de vedere privitor la transpunerea Directivei 2022/2555. Acest punct de vedere a fost pus la dispoziția tuturor entităților

	interesate și avut în vedere în elaborarea actului normativ.
6.3. Informații despre consultările organizate cu autoritățile administrației publice locale	Nu este cazul
6.4. Informații privind puncte de vedere/opinii emise de organisme consultative constituite prin acte normative	Nu este cazul
6.5. Informații privind avizarea de către: **a) Consiliul Legislativ** **b) Consiliul Suprem de Apărare a Țării** **c) Consiliul Economic și Social** **d) Consiliul Concurenței** **e) Curtea de Conturi**	Consiliul Suprem de Apărare a Țării a transmis Hotărârea nr. 250/2024. Proiectul prezentului act normativ a fost avizat de Consiliul Legislativ prin avizul nr. 1323/2024.
6.6. Alte informații	Nu este cazul
Secțiunea a 7-a **Activități de informare publică privind elaborarea și implementarea proiectului de act normativ**	
7.1. Informarea societății civile cu privire la elaborarea proiectului de act normativ	Proiectul de act normativ a fost elaborat cu îndeplinirea procedurii de consultare publică prevăzută de Legea nr. 52/2003 privind transparența decizională în administrația publică, republicată, cu modificările ulterioare, inclusiv prin publicarea proiectului pe pagina de internet a Directoratului Național de Securitate Cibernetică la data de 15.10.2024. Menționăm, de asemenea, faptul că s-a urmărit în toată perioada elaborării actului normativ ca persoanele să fie informate în prealabil asupra problemelor de interes public care urmau a fi dezbătute și consultate în legătură cu acestea. În acest sens, amintim invitația la consultare publică privind transpunerea Directivei NIS 2, promovată în spațiul public în data de 30.04.2024 (pe site-ul DNSC și pe alte pagini oficiale ale DNSC), invitație în cadrul căreia au fost indicate subiecte de interes pentru cetățeni.

	În procesul de elaborare, s-au organizat diferite întâlniri în cadrul cărora au fost dezbătute fie subiectele abordate în Directiva 2022/2555, fie propunerile cu privire la prevederile de transpunere a acesteia. Din rândul acestor ședințe, amintim: ședința de lucru din data de 23.09.2024 cu Grupul de lucru pe probleme de proprietate intelectuală, întâlnirea organizată în data de 27.09.2024 cu Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București, RoTLD și experți în domeniul proprietății intelectuale, întâlnirea organizată în data de 13.09.2024 cu reprezentanți ai Asociației Patronale a Industriei de Software și Servicii (ANIS), Camerei Americane de Comerț în România (AMCHAM Romania), Consiliului Investitorilor Străini (FIC). Menționăm, de asemenea, grupurile de lucru cu experții voluntari pentru sprijinirea elaborării normelor de transpunere, cu care s-au organizat întâlniri recurente încă de la începutul procesului de elaborare a actului normativ.
7.2. Informarea societății civile cu privire la eventualul impact asupra mediului in urma implementării proiectului de act normativ, precum si efectele asupra sănătății și securității cetățenilor sau diversității biologice	Nu este cazul
Secțiunea a 8-a Măsuri privind implementarea, monitorizarea și evaluarea proiectului de act normativ	
8.1. Măsurile de punere în aplicare a proiectului de act normativ	DNSC își continuă activitatea ca autoritate competentă național în domeniul securității cibernetice pentru spațiul cibernetic național civil, iar în temeiul prezentei legi va fi responsabilă de coordonarea activităților desfășurate de autoritățile competente sectorial, desemnate în temeiul prezentei legi, precum și punct unic de contact în relația cu Comisia Europeană și celelalte state membre
8.2. Alte informații	Nu este cazul

Față de cele prezentate, a fost elaborat proiectul de Lege pentru aprobarea Ordonanței de urgență a Guvernului privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, pe care îl supunem Parlamentului spre adoptare.

PRIM–MINISTRU

[redacted]

ION-MARCEL CIOLACU