EXPUNERE DE MOTIVE

Secțiunea 1 **Titlul proiectului de act normativ** Lege pentru aprobarea Ordonanței de urgență a Guvernului privind înființarea Directoratului Național de Securitate Cibernetică	
Secțiunea a 2-a **Motivul emiterii proiectului de act normativ**	
1. Descrierea situației actuale	Creșterea gradului de digitalizare, conectivitate, precum și utilizarea noilor tehnologii duce la agravarea riscurilor pentru securitatea cibernetică, societatea, în general, devenind astfel mai vulnerabilă la amenințările cibernetice, iar pericolele cu care se confruntă autoritățile, operatorii economici dar și cetățenii sunt extrem de mari. Implicit crește și mai mult riscul ca atacatorii cibernetici (grupări criminale, infractori, grupări extremist-teroriste sau chiar actori statali) să exploateze beneficiile inovării în scopuri răuvoitoare. Aceste amenințări transcend categoriile și afectează diverse părți ale societății în moduri diferite. Ele reprezintă un pericol major pentru cetățeni și întreprinderi și necesită un răspuns global și coerent la nivelul UE. În ultima perioadă, numărul și complexitatea incidentelor de securitate cibernetică a crescut continuu, iar situația de criză generată de răspândirea virusului SARS COV2 a scos în evidență și mai mult acest lucru. Acest aspect constituie o amenințare gravă la nivel național pentru funcționarea rețelelor și sistemelor informatice - care sunt ținte permanent pentru acțiunile rău-intenționate menite să afecteze confidențialitatea, integritatea și disponibilitatea datelor sau a sistemelor și serviciilor care susțin buna funcționare a societății și economiei României. Consecințele atacurilor și incidentelor se reflectă asupra sectoarelor importante pentru statul român și pot genera pierderi majore ori chiar pot conduce la materializarea unor riscuri la adresa securității naționale. Pașii rapizi făcuți la nivel european în reglementarea tehnologiilor 5G [Recomandarea Comisiei (UE) 2019/534 din 26 martie 2019, Regulamentul UE 881 din 2019 - Cybersecurity Act, Raportul UE privind evaluarea comună a riscurilor pe 5G, Setul de instrumente (Toolbox) pentru diminuarea riscurilor 5G, Raportul privind implementarea setului de măsuri pentru diminuarea riscurilor 5G], noua strategie de securitate cibernetică pentru decada digitală la nivel european, propunerile de adoptare a Directivei NIS 2.0 și a Directivei pentru reziliența entităților critice

	evidențiază atât preocupările intense și interesul major manifestate de factorii de decizie strategici din UE față de complexitatea problematicii securității cibernetice, cât și probabilitatea ridicată de materializare a riscurilor și amenințărilor crescute și interconectate, ceea ce presupune o adaptare rapidă legislativă, strategică și tehnico-tactică din partea României. Creșterea frecvenței și a complexității atacurilor cibernetice împotriva infrastructurilor ce susțin servicii esențiale pentru societatea si economia românească a condus la situația extraordinară de blocare a unor infrastructuri vitale dintr-o arie largă de domenii publice și private, ceea ce a scos în evidență nivelul scăzut de reziliență a rețelelor și sistemelor informatice, esențiale pentru susținerea activităților economice și societale din România. Incidentele și amenințările cibernetice perturbă furnizarea serviciilor esențiale atât la nivel național, cât și pe întregul teritoriu al Uniunii. Această stare de fapt necesită un răspuns decisiv, coordonat și eficace, precum și gestionarea activă a crizelor cibernetice atât la nivel național cât și la nivelul Uniunii Europene, ambele bazate pe instituții și autorități naționale solide și specializate în domeniul securității cibernetice, pe politici specifice și pe instrumente de solidaritate europeană și asistență reciprocă. Prezența amenințărilor cibernetice persistente orchestrate de actori statali și non-statali ce vizează atât instituții, operatori economici și infrastructuri cibernetice naționale din domeniile transporturi, sănătate, energie, financiar-bancar, alimentar, apă potabilă, servicii poștale și de curierat, termoficare, infrastructuri digitale, industria chimică și farmaceutică, protecția mediului, administrația publică, cât și persoane private, riscând, prin toate acestea, să pună în pericol buna funcționare a societății românești în ansamblul său, precum și din perspectiva apartenenței României la structurile Uniunii Europene. Mai mult, au fost identificate situații în care infrastructuri cibernetice din România sunt utilizate ca platformă de către atacatorii motivați strategic, criminal sau ideologic în scopul derulării de acțiuni ilegale care afectează atât actori naționali, cetățenii cat și alte state. În acest context, în scopul contracarării, descurajării și limitării efectelor negative ale acestor acțiuni, sunt necesare activități de investigare a incidentelor cibernetice, utilizând, după caz, metode tehnice complexe care presupun, inclusiv, analiza metadatelor corespunzătoare conexiunilor de rețea care susțin în mod fundamental activitatea de atribuire a atacurilor, precum și de identificare a victimelor. Aceste date esențiale pot fi obținute numai printr-o cooperare strânsă, pe bază de încredere, cu deținătorii acestor date , cum ar fi furnizorii de servicii de internet, de cloud, de hosting, precum și cu operatorii de telecomunicații.

	Această stare de fapt impune ca autoritățile și instituțiile publice să țină pasul cu dinamica amenințărilor cibernetice, prin crearea de capabilități (tehnice, organizaționale, operaționale), platforme de conștientizare, informare, cooperare și colaborare, programe de educație, de cercetare-dezvoltare, precum și a unor mecanisme robuste de certificare, conformitate și standardizare. Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, este instituția înființată prin Hotărârea Guvernului nr.494/2011, modificată și completată prin Hotărârea Guvernului nr.584/2019 și prin Hotărârea Guvernului nr.256/2020. Prin Legea nr.362/2018 CERT-RO a fost desemnată ca autoritate competentă la nivel național privind securitatea sistemelor și rețelelor informatice, conform art.15 alin (1), punct unic de contact conform art.19 lit. a) și echipă CSIRT națională conform art.19 lit. B. Dinamica schimbărilor în domeniul securității cibernetice, noile cerințe ale Uniunii Europene, inclusiv responsabilitățile primite prin intrarea în vigoare a Legii 362 din 2018 au generat probleme de fond, ca urmare a depășirii capacităților funcționale actuale și a resurselor alocate către CERT-RO pentru a face față noilor provocări, riscuri și amenințări. Este nevoie stringentă de personal specializat și resurse adecvate în vederea îndeplinirii atribuțiilor și obligațiilor ce revin CERT-RO în calitate de autoritate competentă la nivel național, stabilite prin Art. 20 și Art. 24 din Legea nr. 362/2018, cât și pentru acoperirea noilor cerințe, ce rezultă din noua strategie de securitate cibernetică, a noilor propuneri de directive, respectiv Directiva NIS 2.0 și Directiva pentru reziliența entităților critice. Astfel, CERT-RO suferă cronic de o subdimensionare gravă a personalului de specialitate, fapt ce determină incapacitarea instituțională de a îndeplini atribuțiile legale în toate activitățile specifice, respectiv implementarea Directivei NIS, reglementare, certificare, standardizare, reacția la incidente cibernetice, cooperarea la nivel național și european, analiza operațională, investigarea și analiza surselor deschise, alertarea și prognoza. Ca exemplificare, CERT-RO are în prezent doar 35 de angajați, și deși au fost suplimentate posturile prin HG nr. 584/2019 cu 108 poziții (la un total de 149 poziții), nu s-a reușit încă încadrarea niciunei persoane, din cauza nealocării resurselor bugetare, a procesului greoi de încadrare de personal de specialitate prin comparație cu procesele de evaluare și selecție rapide și flexibile utilizate de operatorii economici privați, precum și a blocajului instituțional determinat de starea de alertă din timpul pandemiei de COVID-19. În acest sens, este imperios necesară încadrarea de personal de specialitate care să asigure capacitatea minimă necesară de personal pentru a adresa fără întârziere nivelul crescut de amenințare cibernetică ce pune în pericol însăși buna funcționare a sistemelor și rețelelor informatice esențiale ale statului român,

	precum și pentru a corespunde cerințelor europene și internaționale în domeniul securității cibernetice. Nivelul de finanțare al CERT-RO este insuficient pentru susținerea activităților de bază și, comparativ, cu mult sub nivelul unor instituții cu responsabilități echivalente din statele membre UE sau din alte țări. Mai mult, suplimentarea posturilor CERT-RO prin HG nr. 584/2019 nu a determinat o schimbare de fond și îmbunătățire reală a proceselor, infrastructurilor proprii și culturii organizaționale. De asemenea, din lipsă de personal calificat și de fonduri adecvate, serviciile necesare de mentenanță, suport tehnic, licențiere, upgrade-uri pentru infrastructurile proprii CERT-RO au ajuns într-o stare precară din cauza căreia instituția funcționează în prezent în regim de avarie. Prin urmare eficiența și eficacitatea generală a activităților CERT-RO este nesatisfăcătoare din toate punctele de vedere: strategic, organizațional, procedural, funcțional și tehnic. Guvernul României a sesizat aceste lucruri, fapt care a generat o serie de transformări prin intermediul unor acte normative adoptate, respectiv OUG 90/2019 și OUG 4/2020, care au condus la schimbarea subordonării CERT-RO prin trecerea în coordonarea primului-ministru. De asemenea, se impune luarea în considerare a dinamicii evoluțiilor în domeniul societății digitale, precum și a cerințelor ridicate și a necesităților Pieței Unice Digitale la nivel european. Acestea necesită o abordare inovativă și proactivă în ceea ce privește măsurile de securitate cibernetică în totalitatea lor, normativ și tehnic, pentru a asigura încrederea, funcționalitatea, reziliența și eficiența acestora. Pe acest fond, Guvernul României consideră că se impune crearea unei instituții civile. Aceasta va fi autonomă, independentă, dimensionată corespunzător, pro-activă, flexibilă, capabilă, care să poată face față în mod dinamic tuturor provocărilor mai sus menționate și care să poziționeze ferm România la nivelul celor mai avansate state membre ale Uniunii Europene.
2. Schimbări preconizate	Prin propunerea de act normativ se urmărește crearea unei instituții de excelență noi, respectiv Directoratul Național de Securitate Cibernetică, denumit în continuare DNSC, prin desființarea CERT-RO, care să asigure capabilitățile și performanța necesare în domeniul securității cibernetice la nivel național pentru o perioadă de cel puțin 10 ani. În plus noua instituție va fi adaptată adecvat, putând face față provocărilor pe care dinamicele de dezvoltare tehnologică le vor ridica în spațiul cibernetic. Astfel, se propune înființarea DNSC, ca organ de specialitate al administrației publice centrale, în subordinea Guvernului și în

	coordonarea Prim-ministrului, cu personalitate juridică, finanțat integral de la bugetul de stat prin bugetul Secretariatului General al Guvernului. Centrul Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO se desființează la momentul intrării in vigoare a prezentei ordonanțe de urgență. Având în vedere dispozițiile art. 67 alin.3 din OUG nr. 57/ 2019 privind Codul administrativ, și ținând cont de deciziile Curții Constituționale nr. 455/2018 și 17/2015 prin care s-a statuat faptul că securitatea cibernetică este componentă a securității naționale, cât și in baza art. 119 din Constituția României și a legii nr. 415/2002 privind organizarea și funcționarea Consiliului Suprem de Apărare a Țării, documentele de organizare și funcționare, rapoartele de activitate ale DNSC sunt supuse aprobării CSAT, iar bugetul și numirea conducerii instituției se face cu avizul CSAT. DNSC va avea în vedere obiective majore cum sunt: asigurarea cadrului de strategii, politici și reglementări în domeniul securității cibernetice; crearea unui hub de cooperare la nivel național și internațional între instituții din domeniul public, privat, de educație și cercetare, pentru asigurarea unei viziuni realiste, comune și coerente privitor la securitatea cibernetică a României; alinierea cu celelalte state membre ale Uniunii Europene în ceea ce privește certificarea și standardizarea în domeniul securității cibernetice; alinierea țării noastre la procesele de implementare a noilor tehnologii în domeniul securității cibernetice; gestionarea crizelor de securitate cibernetică la nivel național, în cooperare cu instituțiile care au competențe și atribuții în domeniul managementului crizelor și sub autoritatea Consiliului Operativ de Securitate Cibernetica (COSC) care trebuie consolidată. DNSC va crea cadrul adecvat de lucru și de exprimare pentru specialiști români cu pregătire înaltă în domeniul securității cibernetice, generând o dezvoltare sustenabilă a acestui domeniu la nivel național cu efecte benefice directe și imediate în economia națională. Prin aceasta se vor putea crea nuclee de excelență, care vor contribui la stoparea fenomenului negativ de brain-drain și la menținerea în țară a forței de muncă înalt calificate, care în prezent migrează peste hotare. DNSC este propus a avea un număr maximum de posturi de 1250 ce este proiectat a fi atins într-un mod progresiv pe o perioadă de aproximativ 10 ani, în limita resurselor disponibile. Aceasta cifră este menită a acoperi necesarul de personal al DNSC la finalul celor 10 ani. Pentru abordarea coerentă și unitară la nivel național a problemelor legate de securitatea cibernetică și pentru asigurarea echidistanței privind procesul de reglementare, DNSC va fi sprijinit de un Comitet Director și de un Comitet de Reglementare, din care vor face parte membri ai instituțiilor cu atribuții și responsabilități în domeniul securității cibernetice.

	Comitetul de Reglementare este o instituție cu caracter de noutate, având rolul de garant al obiectivității, transparenței, neutralității, legalității activităților de reglementare desfășurate de DNSC. Acest aspect va contribui substanțial la asigurarea unui mediu concurențial sănătos în domeniul securității cibernetice, cu efecte pozitive asupra operatorilor economici si utilizatorilor spațiului cibernetic. Adoptarea acestui act normativ creează premisele înlăturării obstacolelor întâlnite în anii anteriori în implementarea Directivei NIS prin identificarea promptă a Operatorilor de Servicii Esențiale și a Furnizorilor de Servicii Digitale, conceperea, implementarea și monitorizarea aplicării unor masuri de securitate care sa corespunda cerințelor actuale la nivel European si care sa asigure un nivel comun ridicat de securitate a rețelelor si sistemelor informatice în vederea poziționării ferme a României ca un lider recunoscut în securitatea cibernetică. Sunt necesare eforturi suplimentare pentru a spori gradul de sensibilizare a cetățenilor, organizațiilor și întreprinderilor cu privire la aspectele legate de securitatea cibernetică. Schimbările preconizate se bazează pe elemente consacrate la nivel comunitar, ce vizează domeniul securității cibernetice: piața unica digitala Europeana, servicii digitale sigure în serviciul cetățeanului, sprijinirea creșterii economice a domeniului digital și al securității cibernetice. În același timp se află în curs de pregătire, realizare sau implementare de către CERT-RO, un număr ridicat de proiecte de importanță deosebită și cu termene stricte de finalizare, cu finanțare din fonduri europene și supuse cerințelor legislației naționale și ale Uniunii Europene. Viziunea actuală de a crea un DNSC este aceea că tehnologia informației și securitatea cibernetică trebuie să ofere instrumente moderne și performante, în condiții de eficiență, pentru realizarea funcțiilor statului în raporturile cu cetățenii si celelalte instituții și autorități publice ale statului. Înființarea DNSC acoperă un vid instituțional în domeniul securității cibernetice în România întrucât creează structurile și mecanismele esențiale pentru asigurarea securității spațiului cibernetic național, precum și arhitectura de cooperare inter-instituțională flexibilă și eficientă, prin asigurarea unor roluri instituționale fundamentale după cum urmează: 1. Rol strategic pentru elaborarea și implementarea strategiei și a politicilor publice, pentru crearea unui cadru național de colaborare, cooperare, educație, instruire și conștientizare în domeniul securității cibernetice din România. În acest sens, DNSC va contribui activ la actualizarea Strategiei de Securitate Cibernetică a României, conform priorităților stabilite prin Programul de Guvernare. 2. Rol de reglementator prin elaborarea și avizarea, actelor

	normative cheie cu impact în domeniul securității cibernetice. 3. Rol de avizator al proiectelor cheie în domeniul securității cibernetice ale autorităților publice și monitorizarea implementării acestor proiecte. 4. Rol de autoritate națională precum și de certificare și standardizare în domeniul securității cibernetice. 5. Rol de reprezentare internațională pe domeniul securității cibernetice, în relația cu partenerii și instituțiile europene, dar și cu alte state și organisme internaționale, în vederea armonizării abordării și stimulării progresului în domeniul său de activitate. DNSC va îndeplini un rol cheie în asigurarea respectării de către România a angajamentelor asumate către partenerii strategici cat și la nivel internațional. 6. Rol de echipă de răspuns la incidente de securitate cibernetică pentru produse și servicii informatice ale sectorului guvernamental. Prin aceasta DNSC va realiza identificarea și raportarea consolidată sistematică a vulnerabilităților din produsele și serviciile informatice create, întreținute și utilizate la nivelul sectorului guvernamental, va asigura un nivel ridicat de securitate și va crește în mod natural nivelul de maturitate al procesului de dezvoltare pentru aceste produsele și servicii informatice. 7. Rol de promotor strategic al interesului național de creștere a ratei de absorbție a fondurilor europene alocate domeniului securității cibernetice și de îndrumător al participării active al entităților publice și private în programele majore de finanțări, inclusiv pentru cele pentru dezvoltarea de soluții tehnologice de securitate cibernetică de interes, care pot avea o dublă utilizare civilă și militară. Odată cu operaționalizarea Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică, găzduit de România, și a Rețelei de centre naționale de coordonare, DNSC va fi o instituție cheie ce va accesa o parte semnificativă a fondurilor europene alocate domeniului securității cibernetice ce vor fi coordonate la nivel european de către Centru. Mai mult, prin noua arhitectură instituțională a DNSC se creează pârghiile necesare pentru accesarea fondurilor europene menționate, în special a celor disponibile prin Mecanismul de Redresare și Reziliență, atât de către mediul privat cât și de mediul public din țara noastră. 8. Rol de promotor al programelor de educație și conștientizare privind securitatea cibernetică. Aceasta nu este doar o problemă legată de tehnologie, ci si una de comportament. Din acest motiv, DNSC va promova intens „igiena cibernetică” și alte măsuri preventive care, atunci când sunt introduse și aplicate cu regularitate de cetățeni, de organizații și de operatori economici, reduc la minimum expunerea acestora la riscurile cibernetice. 9. Rol de liant între administrația publică, sectorul privat și societatea civilă pentru crearea unei arhitecturi coerente și

	reziliente de securitate cibernetică la nivel național. Aceasta de va realiza prin: - un de management clar și simplificat al proceselor de cooperare și colaborare; - eliminarea suprapunerilor legate de atribuții, roluri și responsabilități; - îmbunătățirea comunicării inter-instituționale; - asigurarea unei abordări unitare și coerente în domeniul securității cibernetice, mai ales în ceea ce privește reprezentarea intereselor României la nivel internațional. Utilizarea eficientă a resurselor alocate domeniului securității cibernetice reprezintă un instrument deosebit de puternic pentru atingerea obiectivelor DNSC. Deși obiectivele strategice propuse sunt perene și asumate în mod obișnuit de toate entitățile din administrația publică, acestea nu au putut fi atinse prin modul actual de organizare și funcționare din cadrul CERT-RO. În condițiile în care atacurile cibernetice sunt în creștere, o economie și o societate conectate mai vulnerabile la amenințările și atacurile cibernetice necesită o protecție mai puternică prin instituții moderne, capabile si dedicate domeniului securității cibernetice și binelui public. Cu toate acestea, deși atacurile cibernetice sunt adesea transfrontaliere, competența și răspunsurile oferite de politicile autorităților de securitate cibernetică și de aplicare a legii sunt predominant naționale. În acest context, accesul la și analiza metadatelor corespunzătoare conexiunilor de rețea vor susține în mod fundamental activitatea de investigare a incidentelor cibernetice precum și de limitare a impactului acestora. Pentru a putea pune în practică arhitectura instituțională propusă, se impune adoptarea unui cadru legislativ nou, prin promovarea prezentei ordonanțe de urgență. DNSC preia activitățile, atribuțiile și personalul Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, cu menținerea drepturilor salariale avute la data preluării. DNSC obține venituri care se constituie integral ca venit la bugetul de stat. Un obiectiv asumat este atragerea unor noi categorii de venituri, cum ar fi furnizarea de produse și componente din domeniul securității cibernetice sau conexe acestuia sau încasări din drepturi de proprietate intelectuală și licențe, pentru a valorifica corespunzător potențialul creativ instituțional și al specialiștilor implicati.
3. Alte informații	Caracterul de urgență al actului normativ este determinat de următoarele considerente: - nevoia acută și urgentă de a limita riscurile generate de nivelul scăzut de securitate cibernetică al infrastructurilor cibernetice din sectoarele cheie ale statului român, de nivelul general scăzut de

	cunoştinţe specifice, conştientizare şi pregătire, precum şi de nivelul inacceptabil de granularitate în ceea ce priveşte competenţele instituţionale cu efecte negative privind cooperarea şi colaborarea la nivel naţional şi internaţional; - nevoia recuperării imediate a întârzierilor înregistrate în implementarea Directivei (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice, pentru care s-a declanşat procedura de infringement împotriva României în cauza nr. 2019/2214. Finalizarea acestei proceduri va obliga statul român la plata unor penalizări importante, care vor afecta substanţial bugetul de stat; - nevoia ca România să ţină pasul cu ritmul alert al dezvoltărilor tehnologice în domeniul securităţii cibernetice la nivel european, ţinând seama de faptul că în prezent o serie de elemente nu sunt acoperite (certificare-standardizare, cercetare-dezvoltare, noi tehnologii), iar întârzierile se vor transforma în decalaje care nu vor putea sau vor fi greu de surmontat; - corectarea urgentă a situaţiei îngrijorătoare ca statul să fie depăşit în capacităţile sale de răspuns adecvat în domeniul securităţii cibernetice – datorită dezvoltărilor înregistrate pe plan internaţional şi la nivelul sectorului privat, sau ca urmare a neadaptării legislaţiei şi dezvoltărilor instituţionale la cerinţele pieţei. Se impune, aşadar, cu celeritate înfiinţarea DNSC, pentru ca noua autoritate să contribuie la implementarea strategiei naţionale de securitate cibernetică a României, a cadrului naţional de cooperare precum şi a obligaţiilor ce revin din noua strategie europeană de securitate cibernetică pentru decada digitală. Consecinţa negativă directă a neadoptării măsurilor propuse prin prezenta ordonanţă de urgenţă este aceea a expunerii României la riscuri critice inacceptabile a tuturor infrastructurilor cibernetice naţionale cu consecinţe incomensurabile.
Secţiunea a 3-a **Impactul socioeconomic al proiectului de act normativ**	
1. Impactul macroeconomic	Proiectul de act normativ va contribui în mod direct la sprijinirea creşterii economice prin susţinerea încrederii, stabilităţii, rezilienţei şi securităţii pieţei unice digitale în România cu efecte benefice asupra unei dezvoltări economice echilibrate şi sustenabile la nivel naţional. De asemenea, prin sprijinirea masurilor securităţii cibernetice, va asigura un cadru propice pentru progresul transformării digitale şi al adoptării noilor tehnologii e.g. 5G, inteligenţă artificială, blockchain, quantum computing, Internet of Things (IOT), în România. Valorificarea şi capacitarea, la nivel naţional, pe termen mediu şi lung a resursei umane din domeniu prin atragerea şi păstrarea specialiştilor romani, încurajarea şi susţinerea sistemului de

	învățământ românesc astfel încât securitatea cibernetică să capete o pondere importantă în structura economiei naționale și PIB.
1[1].Impactul asupra mediului concurențial și domeniului ajutoarelor de stat	Proiectul de act normativ are ca efect crearea unei instituții care a va sprijini și stimula în mod direct inovarea, noile tehnologii, produse și servicii, precum și mediul concurențial în domeniul securității cibernetice din România. Nu va exista impact asupra ajutoarelor de stat.
2. Impactul asupra mediului de afaceri	Proiectul de act normativ va contribui în mod direct la creșterea accelerata a domeniului produselor și serviciilor de securitate cibernetice în România. Va crea premisele creșterii ratei de absorbție a fondurilor europene pentru care România este eligibilă, în domeniul securității cibernetice, în special în noul context determinat de proximitatea Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică, găzduit de București.
3. Impactul social	Proiectul de act normativ nu se refera la acest subiect.
4. Impactul asupra mediului (***)	Proiectul de act normativ nu se refera la acest subiect.

Secțiunea a 4-a
Impactul financiar asupra bugetului general consolidat, atât pe termen scurt, pentru anul curent, cât și pe termen lung (pe 5 ani)

- mii lei -

Indicatori	Anul curent	Următorii 4 ani				Media pe 5 ani
1	2	3	4	5	6	7
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						
2. Modificări ale cheltuielilor bugetare, plus/minus, din care:						
a) buget de stat, din acesta:						
(i) cheltuieli de personal						

(ii) bunuri şi servicii						
b) bugete locale:						
(i) cheltuieli de personal						
(ii) bunuri şi servicii						
c) bugetul asigurărilor sociale de stat:						
(i) cheltuieli de personal						
(ii) bunuri şi servicii						
3. Impact financiar, plus/minus, din care:						
a) buget de stat						
b) bugete locale						
4. Propuneri pentru acoperirea creşterii cheltuielilor bugetare						
5. Propuneri pentru a compensa reducerea veniturilor bugetare						
6. Calcule detaliate privind fundamentarea modificărilor veniturilor si/sau cheltuielilor bugetare	Veniturile DNSC se estimează la 1,2 milioane lei în 2021 (6 luni) respectiv 7,4 milioane lei (medie anuală) pe perioada 2022-2025. Finanţarea DNSC se va realiza cu încadrarea în prevederile bugetare anuale aprobate potrivit legii. Posturile nou înfiinţate se vor ocupa eşalonat cu încadrarea în prevederile bugetare aprobate cu aceasta destinaţie şi cu respectarea prevederilor Art. 38 din OUG 114/2018.					
7. Alte informaţii	Proiectul de act normativ îşi propune să creeze bazele unei noi instituţii capabile să genereze venituri la bugetul de stat. Veniturile DNSC provin din: a) tarife pentru servicii din activităţile prevăzute la art. 32 alin. (2) lit. c) şi e), respectiv la art. 33 alin. (2) lit. c) şi e) şi art. 22 alin. (1) lit. l) din Legea nr. 362/2018, stabilite prin decizie a Directorului DNSC care se publică în Monitorul Oficial al României, Partea I; b) tarife pentru înscrierea în Registrul naţional al activelor, produselor şi serviciilor de securitate cibernetică; c) tarife pentru autorizarea laboratoarelor civile de testare, evaluare şi certificare a securităţii cibernetice a produselor şi serviciilor care sunt utilizate în cadrul reţelelor şi sistemelor informatice; d) tarife pentru avizarea, verificarea şi validarea conformităţii privind securitatea cibernetică;					

	e) tarife pentru certificarea securității cibernetice a soluțiilor, produselor și serviciilor de tehnologia informației și comunicațiilor, inclusiv a noilor tehnologii; f) venituri din servicii de specialitate; g) venituri din furnizare de produse și componente din domeniul securității cibernetice sau conexe acestuia; h) venituri din drepturi de proprietate intelectuală și licențe; i) venituri din comisioane pentru parteneriate și proiecte, j) alte venituri aprobate prin hotărâre de guvern.
Secțiunea a 5-a **Efectele proiectului de act normativ asupra legislației în vigoare**	
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.	Se abrogă Hotărârea Guvernului nr. 494/2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, publicată în Monitorul Oficial al României, Partea I, nr. 388 din 2 iunie 2011, cu modificările și completările ulterioare. Se abrogă art. II din Ordonanța de Urgență nr. 4/2020 privind stabilirea unor măsuri la nivelul administrației publice centrale și pentru modificarea unor acte normative, publicată în Monitorul Oficial al României, Partea I, nr. 38 din 20 ianuarie 2020. Se modifică și se completează HG nr. 271 /2013 din perspectiva componenței Consiliul Operativ de Securitate Cibernetică, ca efect al dispozițiilor art. 2 alin.(5) din prezentul proiect de act normativ, referitor la desemnarea DNSC ca membru permanent în Consiliul Operativ de Securitate Cibernetică. Se modifică și se completează Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice cu modificările și completările ulterioare, publicată în Monitorul Oficial al României, Partea I, nr. 21 din 9 ianuarie 2019. Se modifică și se completează Legea nr. 55/2020 privind unele măsuri pentru prevenirea și combaterea efectelor pandemiei de COVID-19, cu modificările și completările ulterioare.
2. Conformitatea proiectului de act normativ cu legislația comunitară în cazul proiectelor ce transpun prevederi comunitare	Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune. Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate

	Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică). Recomandarea (UE) 2019/534 a Comisiei din 26 martie 2019 Securitatea cibernetică a rețelelor 5G.
3. Măsuri normative necesare aplicării directe a actelor normative comunitare	Proiectul de act normativ nu se refera la acest subiect
4. Hotărâri ale Curții de Justiție a Uniunii Europene	Proiectul de act normativ nu se refera la acest subiect
5. Alte acte normative și/sau documente internaționale din care decurg angajamente	Proiectul de act normativ nu se refera la acest subiect
6. Alte informații	Nu au fost identificate

Secțiunea a 6-a
Consultările efectuate în vederea elaborării proiectului de act normativ

1. Informații privind procesul de consultare cu organizații neguvernamentale, institute de cercetare și alte organisme implicate	Nu este cazul.
2. Fundamentarea alegerii organizațiilor cu care a avut loc consultarea, precum și a modului în care activitatea acestor organizații este legată de obiectul proiectului de act normativ	Nu este cazul.
3. Consultările organizate cu autoritățile administrației publice locale, în situația în care proiectul de act normativ are ca obiect activități ale acestor autorități, în condițiile Hotărârii Guvernului nr.521/2005 privind procedura de consultare a structurilor asociative ale autorităților administrației publice locale la elaborarea proiectelor de acte normative	Nu este cazul.
4. Consultările desfășurate în cadrul consiliilor interministeriale, în conformitate cu prevederile Hotărârii Guvernului nr.750/2005 privind constituirea consiliilor interministeriale permanente	Nu este cazul.
5. Informații privind avizarea de către: **a) Consiliul Legislativ** **b) Consiliul Suprem de Apărare a Țării** **c) Consiliul Economic și Social** **d) Consiliul Concurenței**	Consiliul Suprem de Apărare a Țării a avizat favorabil proiectul prezentului act normativ prin avizul nr. 131/2021. Consiliul Legislativ a avizat

e) Curtea de Conturi	favorabil proiectul prezentului act normativ prin avizul nr. 763/2021. Consiliul Concurenței a emis adresa nr. 8641/2021. Curtea de Conturi a avizat favorabil proiectul prezentului act normativ prin Hotărârea Plenului Curții de Conturi nr. 285/2021.
6. Alte informații	Nu au fost identificate.
Secțiunea a 7-a Activități de informare publică privind elaborarea și implementarea proiectului de act normativ	
1. Informarea societății civile cu privire la necesitatea elaborării proiectului de act normativ	Au fost respectate dispozițiile legii 52/2003 privind transparenta decizionala în administrația publică, republicată.
2. Informarea societății civile cu privire la eventualul impact asupra mediului în urma implementării proiectului de act normativ, precum și efectele asupra sănătății și securității cetățenilor sau diversității biologice	Proiectul de act normativ nu se referă la acest subiect.
3. Alte informații	Sunt incidente dispozițiile art. 7 alin. (13) Legii nr.52/2003 privind transparența decizională în administrația publică, republicată.
Secțiunea a 8-a Măsuri de implementare	
1. Măsurile de punere în aplicare a proiectului de act normativ de către autoritățile administrației publice centrale și/sau locale - înființarea unor noi organisme sau extinderea competentelor instituțiilor existente	
2. Alte informații	Nu au fost identificate.

Faţă de cele prezentate, a fost elaborat proiectul de Lege pentru aprobarea Ordonanţei de urgenţă a Guvernului privind înființarea Directoratului Național de Securitate Cibernetică, pe care îl supunem Parlamentului spre adoptare.

PRIM – MINISTRU

[redacted]

FLORIN-VASILE CIȚU

[redacted]