

NOTĂ DE FUNDAMENTARE

Secțiunea 1 Titlul proiectului de act normativ ORDONANȚĂ DE URGENȚĂ privind înființarea Directoratului Național de Securitate Cibernetică și pentru modificarea și completarea unor acte normative	
Secțiunea a 2-a Motivul emiterii actului normativ	
1. Descrierea situației actuale	<p>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 cibernetică, iar pericolele cu care se confruntă autoritățile, operatorii economici dar și cetățenii sunt extrem de mari. Implicite crește și mai mult riscul ca atacatorii ciberneticici (grupări criminale, infractori, grupări extremist-teroriste sau chiar actori statali) să exploateze beneficiile inovării în scopuri răuvoitoare.</p> <p>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.</p> <p>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.</p> <p>Acest aspect constituie o amenințare gravă la nivel național pentru funcționarea rețelelor și sistemelor informatice - care sunt ținte permanente 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.</p> <p>Pașii rapizi făcuți la nivel european în dezvoltarea tehnologiilor 5G (RECOMANDAREA (UE) 2019/534 A COMISIEI 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) creează premisele manifestării unor riscuri și amenințări crescute și interconectate, care presupun o adaptare rapidă la aceste schimbări și o gestionare eficientă și dinamică a situațiilor nou apărute.</p>

Creșterea frecvenței și a complexității atacurilor cibernetice împotriva infrastructurilor ce susțin servicii esențiale pentru societatea și economia românească a condus la situația extraordinară de blocare a unor infrastructuri vitale dintr-o arie largă de domenii publice și private.

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 și chiar al Uniunii Europene, bazate pe politici specifice și pe instrumentele de solidaritate europeană și asistență reciprocă.

Prezența amenințărilor cibernetice persistente orchestrate de actori statali sau non-statali ce vizează atât instituții, operatori economici și infrastructuri cibernetice naționale din domeniile transporturi, sănătate, energie, financiar-bancar, alimentar, apă potabilă, 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, infrastructurile 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 cât 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 celor impactați. Aceste date esențiale pot fi obținute numai în baza unei cooperări strânse, pe baze de încredere, cu posesorii datelor implicate, cum ar fi furnizorii de servicii de internet, de cloud, de hosting, operatori de telecomunicații.

Această stare de fapt impune ca autoritățile și instituțiile publice să țină pasul cu dinamica amenințărilor cibernetice, în același ritm prin crearea de capacități (tehnice, organizaționale, operaționale), platforme de 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 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.

Astfel, CERT-RO suferă cronic de o subdimensionare gravă a personalului de specialitate, fapt ce determină incapacitarea instituțională de a îndeplini atribuțiile legale, în special în domeniul reacției la incidente cibernetice, cooperării la nivel național și european, al analizei operaționale, alertare și prognoză. Ca exemplificare, CERT-RO are în prezent doar 37 de angajați, și deși au fost suplimentate posturile prin HG 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.

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 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, ținând seama de dinamica evoluțiilor în domeniul societății digitale și a concretizării Pieței Unice Digitale la nivel european, care impun o sporire a măsurilor de securitate cibernetică în rețele, pentru a asigura încrederea, funcționalitatea, reziliența și eficiența acestora, la nivel guvernamental se consideră că se impune crearea unei noi instituții mai capabile, pro-active, flexibile care să poată face față în mod dinamic provocărilor și să poziționeze ferm România la nivelul celor mai performante 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 instituție publică, cu personalitate juridică, în coordonarea Prim-ministrului, finanțată din venituri proprii și subvenții acordate de la bugetul de stat.

Centrul Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO se desființează la momentul intrării în vigoare a prezentei ordonanțe de urgență.

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 Cibernetică (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.

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 și 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 măsuri de securitate care să corespundă cerințelor actuale la nivel European și care să asigure un nivel comun ridicat de securitate a rețelelor și 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 cibernetică: piața unică digitală Europeană, servicii digitale sigure în serviciul cetățeanului, sprijinirea creșterii economice a domeniului digital și al securității cibernetică.

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 și celelalte instituții și autorități publice ale statului.

Înființarea DNSC acoperă un vid instituțional în domeniul securității cibernetică 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 cibernetică 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 cibernetică.
3. Rol de avizator al proiectelor cheie în domeniul securității cibernetică ale autorităților publice și monitorizarea implementării acestor proiecte.
4. Rol de autoritate națională precum și de certificare și standardizare în domeniul securității cibernetică.
5. Rol de reprezentare internațională pe domeniul securității cibernetică, 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 ca 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 cibernetică 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.

8. Rol de promotor al programelor de educație și conștientizare privind securitatea cibernetică. Aceasta nu este doar o problemă legată de tehnologie, ci și 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 cibernetică.

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 cibernetică, mai ales în ceea ce privește reprezentarea intereselor României la nivel internațional.

Utilizarea eficientă a resurselor alocate domeniului securității cibernetică 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 cibernetică sunt în creștere, o economie și o societate conectate mai vulnerabile la amenințările și atacurile cibernetică necesită o protecție mai puternică prin instituții moderne, capabile și dedicate domeniului securității cibernetică și binelui public. Cu toate acestea, deși atacurile cibernetică 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 cibernetică precum și de limitare a impactului acestora.

	<p>Pentru a putea pune în practică arhitectura instituțională propusă, se impune adoptarea unui cadru legislativ nou, prin promovarea prezentei ordonanțe de urgență.</p> <p>DNSC precum activitățile, atribuțiile și personalul Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, cu menținerea drepturilor salariale avute la data preluării.</p>
3. Alte informații	<p>Caracterul de urgență al actului normativ este determinat de următoarele considerente:</p> <ul style="list-style-type: none"> - nevoia acută și urgentă de limita riscurile generate de nivelul scăzut de securitate cibernetică al infrastructurilor cibernetică din sectoarele cheie ale statului român, de nivelul general scăzut de cunoștințe specifice, conștientizare și pregătire, precum și de nivelul inacceptabil de granularitate în ceea ce privește competențele instituționale cu efecte negative privind cooperarea și colaborarea la nivel național și internațional; - nevoia recuperării imediate a întârzierilor înregistrate în implementarea Directivei (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice, pentru care s-a declanșat 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 substanțial bugetul de stat; - nevoia ca România să țină pasul cu ritmul alert al dezvoltărilor tehnologice în domeniul securității cibernetică la nivel european, ținând 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 situației îngrijorătoare ca statul să fie depășit în capacitățile sale de răspuns adecvat în domeniul securității cibernetică – datorită dezvoltărilor înregistrate pe plan internațional și la nivelul sectorului privat, sau ca urmare a neadaptării legislației și dezvoltărilor instituționale la cerințele pieței. <p>Se impune, așadar, tranșarea cu celeritate a chestiunii înființării DNSC, pentru ca noua autoritate să procedeze la inițierea fără întârziere a actualizării Strategiei Naționale de Securitate Cibernetică a României, în scopul creării cadrului național armonizat de acțiune a autorităților și instituțiilor publice cu responsabilități specifice privind securitatea cibernetică.</p> <p>Consecința negativă directă a neadoptării măsurilor propuse prin prezenta ordonanță de urgență este aceea a expunerii României la riscuri critice inacceptabile a tuturor infrastructurilor cibernetică naționale cu consecințe incommensurabile.</p>
Secțiunea a 3-a Impactul socioeconomic al proiectului de act normativ	
1. Impactul macroeconomic	<p>Proiectul de act normativ va contribui în mod direct la sprijinirea creșterii economice prin susținerea încrederii, stabilității, rezilienței și</p>

	<p>securității pieței unice digitale în România cu efecte benefice asupra unei dezvoltări economice echilibrate și sustenabile la nivel național.</p> <p>De asemenea, prin sprijinirea măsurilor securității cibernetice, va asigura un cadru propice pentru progresul transformării digitale și al adoptării noilor tehnologii e.g. 5G, inteligență artificială, blockchain, quantum computing, IOT, în România.</p> <p>Valorificarea și capacitatea, la nivel național, pe termen mediu și lung a resursei umane din domeniu prin atragerea și păstrarea specialiștilor romani, încurajarea și susținerea sistemului de învățământ românesc astfel încât securitatea cibernetică să capete o pondere importantă în structura economiei naționale și PIB.</p>					
1¹. 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 accelerată a domeniului produselor și serviciilor de securitate cibernetică în România.					
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 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						
3. Impact financiar, plus/minus, din care:						
a) buget de stat						
b) bugete locale						
4. Propuneri pentru acoperirea creșterii cheltuielilor bugetare						
5. Propuneri pentru a compensa reducerea veniturilor bugetare						
6. Calcule detaliate privind fundamentarea modificărilor veniturilor si/sau cheltuielilor bugetare						

7. Alte informații	Nu au fost identificate.	Nu are impact bugetar. Cheltuielile prevăzute se încadrează în bugetul aprobat.
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.	Proiectul de act normativ nu se refera la acest subiect.	
2. Conformitatea proiectului de act normativ cu legislația comunitară în cazul proiectelor ce transpun prevederi comunitare	<p>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.</p> <p>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).</p> <p>Recomandarea (UE) 2019/534 a Comisiei din 26 martie 2019 Securitatea cibernetică a rețelelor 5G.</p>	
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 e) Curtea de Conturi	Prezentul proiect necesită avizul: Consiliului Suprem de Apărare a Țării, Consiliului Legislativ, Consiliului Concurenței, Curții de Conturi
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 transparența decizională 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 competențelor instituțiilor existente	
2. Alte informații	Nu au fost identificate.

Față de cele prezentate, a fost elaborat proiectul de Ordonanță de Urgență a Guvernului privind înființarea Directoratului Național de Securitate Cibernetică, pe care îl supunem Guvernului spre adoptare.

Secretarul General al Guvernului
Antonel TĂNASE

Directorul general al Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO
Dan CÎMPEAN

Avizăm favorabil:

Ministrul Finanțelor Publice
Florin-Vasile CÎȚU

Ministrul Muncii și Protecției Sociale
Viorica-Violeta ALEXANDRU

Ministrul Afacerilor Interne
Marcel-Ion VELA

Ministrul Apărării Naționale
Ionel-Nicolae CIUCĂ

Ministrul Afacerilor Externe
Bogdan AURESCU

Ministrul Educației Naționale
Monica Cristina ANISIE

Directorul Serviciului de Informații Externe
Gabriel VLASE

Directorul Serviciului Român de Informații
Eduard-Raul HELLVIG

**Directorul Serviciului de Protecție și Pază
Lucian-Silvian PAHONȚU**

**Directorul Serviciului de Telecomunicații
Speciale
Ionel-Sorin BĂLAN**

**Directorul General al Oficiului Registrului
Național al Informațiilor Secrete de Stat
Marius PETRESCU**

**Președintele Autorității Naționale pentru
Administrare și Reglementare în
Comunicații
Sorin Mihai GRINDEANU**

**Președintele Autorității Naționale de
Supraveghere a Prelucrării Datelor cu
Caracter Personal
Ancuța Gianina OPRE**

**Ministrul Justiției
Marian-Cătălin PREDOIU**