NOTĂ DE FUNDAMENTARE

Secțiunea 1
Titlul actului normativ

HOTĂRÂRE
privind aprobarea Notei de fundamentare referitoare la necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului
"Sistem de alertă timpurie și informare în timp real - RO-SAT"

Secțiunea a 2-a
Motivul emiterii actului normativ

1. Descrierea situației actuale

a) Context

Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO este instituție publică înființată prin H.G. nr. 494/2011 ca structură independentă de expertiză și cercetare-dezvoltare în domeniul securității cibernetice, a cărei misiune este prevenirea, analiza, identificarea și răspunsul la incidentele din cadrul infrastructurilor cibernetice ce asigură funcționalități de utilitate publică ori asigură servicii ale societății informaționale.

Comisia Europeană a comunicat în data de 26.08.2010 către Parlamentul European, Consiliul European, Comitetul Economic și Social European și Comitetul Regiunilor strategia privind Agenda digitală pentru Europa. Printre domeniile de acțiune stabilite de Agenda digitală pentru Europa se enumeră și nevoia de încredere și securitate. Comisia afirmă că europenii nu vor adopta o tehnologie în care nu au încredere și menționează că utilizatorii trebuie să se simtă confortabil și în siguranță când se conectează online. În acest domeniu de acțiune, privind încrederea și securitatea tehnologiilor digitale, Comisia corelează direct gradul de utilizare a tehnologiilor digitale cu încrederea utilizatorilor în acestea, și oferă ca soluție întărirea securității în societatea digitală prin responsabilizarea în egală măsură a cetățenilor, a organismelor private și a celor de stat.

Comisia menționează că pentru a putea reacționa în timp real, în Europa trebuie creată o rețea performantă și extinsă de echipe de intervenție în caz de urgență informatică (Computer Emergency Response Teams – CERT). Cooperarea dintre echipele CERT și forțele de ordine este esențială, pentru prevenirea criminalității cibernetice și intervenirea în caz de urgență (de exemplu atacuri informatice).

În conformitate cu prevederile Agendei Digitale pentru Europa, Guvernul României a înființat prin Hotărârea nr. 494/11.05.2011 Centrul Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO. În vederea transpunerii în plan național a obiectivelor din cadrul Agendei Digitale pentru Europa, Guvernul României a aprobat prin Hotărârea 245/07.04.2015 Strategia națională privind Agenda Digitală pentru România 2020. În cadrul Domeniului de Acțiune I: "eGuvernare, Interoperabilitate, Securitate Cibernetică, Cloud Computing, Open Data, Big Data și Media Sociale" la cap. 2.2 "Securitate Cibernetică – Securitatea Rețelelor și a Sistemelor Informatice" Guvernul României identifică drept cerință de bază și prioritate națională securitatea și încrederea în serviciile electronice publice. Strategia recunoaște înființarea CERT-RO ca dezvoltare pozitivă în domeniul securității cibernetice și subliniază necesitatea dezvoltării capacității operaționale a CERT-RO. În acest sens, sub-capitolul 2.2.4. „Linii Strategice de Dezvoltare" vizează dezvoltarea capacităților naționale pentru managementul riscului în securitatea cibernetică și răspunsul la incidentele cibernetice în cadrul unui program național. Guvernul

României a aprobat prin Hotărârea 271/15.05.2013 Strategia de securitate cibernetică a României şi Planul de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică.

Astfel, Guvernul României îşi propune definirea şi menţinerea unui mediu virtual sigur, cu un înalt grad de reziliență şi de încredere, bazat pe infrastructurile cibernetice naţionale, care să constituie un important suport pentru securitatea naţională şi buna guvernare, pentru maximizarea beneficiilor cetăţenilor, mediului de afaceri şi ale societăţii româneşti, în ansamblul ei. Pentru atingerea acestor obiective, strategia vizează, în cadrul direcţiilor de acţiune, consolidarea potenţialului de cunoaştere, prevenire şi contracarare a ameninţărilor şi minimizarea riscurilor asociate utilizării spaţiului cibernetic, precum şi dezvoltarea entităţilor de tip CERT.

În anul 2016 a fost adoptată Directiva 1148 a Parlamentului European şi a Consiliului, privind măsuri pentru un nivel comun de securitate a reţelelor şi a sistemelor informatice în Uniunea Europeană (Directiva NIS). În cadrul Directivei se prevede existenţa unei reţele de cooperare în răspunsul la incidente de securitate cibernetică formată din CERT-urile naţionale şi CERT-EU. Aşadar, în prezent partenerii europeni mizează pe capacitatea CERT-RO de a acţiona eficient în cadrul acestei reţele.

Necesitatea dezvoltării Sistemului de alertă timpurie şi informare în timp real privind incidentele cibernetice (RO-SAT) este prevăzută în H. G. 494/2011.

Serviciul de Telecomunicaţii Speciale este organul central de specialitate, cu personalitate juridică, ce organizează, conduce, desfăşoară, controlează şi coordonează activităţile în domeniul telecomunicaţiilor speciale pentru autorităţile publice din România şi pentru alţi utilizatori prevăzuţi de lege. Serviciul de Telecomunicaţii Speciale are ca misiune:

- asigurarea de servicii securizate de comunicaţii şi tehnologia informaţiei pentru autorităţile române, prin dezvoltarea şi administrarea de reţele de comunicaţii şi sisteme informatice având la bază principiile interoperabilităţii, standardizării şi asigurării securităţii.

- creşterea nivelului de reziliență a serviciilor şi a protecţiei infrastructurilor critice.

- consolidarea capacităţilor de cercetare-dezvoltare şi inovare, de producţie şi de mentenanţă pe întreaga durată a ciclului de viaţă a echipamentelor, sistemelor şi serviciilor administrate.

Pentru a putea realiza un management eficient al identităţilor electronice trebuie să fie identificate, în primul rând, serviciile de eGuvernare electronice actuale, consumatorii acestora şi modalităţile de identificare şi autentificare a utilizatorilor (credenţialele).

b) Justificare

Dezvoltarea rapidă a tehnologiilor moderne de informaţii şi comunicaţii - condiţie sine qua non a edificării societăţii informaţionale - a avut un impact major asupra ansamblului social, marcând adevărate mutaţii în filozofia de funcţionare a economicului, politicului şi culturalului, dar şi asupra vieţii de zi cu zi a individului. Practic, în prezent, accesul facil la TIC reprezintă una dintre premisele bunei funcţionări a societăţii moderne. Spaţiul cibernetic se caracterizează prin lipsa frontierelor, dinamism şi anonimat, generând deopotrivă oportunităţi de dezvoltare a societăţii informaţionale bazate pe cunoaştere, dar şi riscuri la adresa funcţionării acesteia (la nivel individual, statal şi chiar cu manifestare transfrontalieră).

Alături de beneficiile incontestabile pe care informatizarea le induce la nivelul societăţii moderne, aceasta introduce şi vulnerabilităţi, astfel că asigurarea securităţii spaţiului cibernetic trebuie să constituie o preocupare majoră a tuturor actorilor implicaţi, mai ales la nivel instituţional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu.

România urmăreşte atât dezvoltarea unui mediu informaţional dinamic bazat pe interoperabilitate şi servicii specifice societăţii informaţionale, cât şi asigurarea respectării drepturilor şi libertăţilor fundamentale ale cetăţenilor şi a intereselor de securitate naţională, într-un cadru legal adecvat. Din

această perspectivă se resimte necesitatea dezvoltării culturii de securitate cibernetică a utilizatorilor sistemelor informatice şi de comunicaţii, adesea insuficient informaţi în legătură cu potenţialele riscuri, dar şi cu soluţiile de contracarare a acestora.

Cunoaşterea pe scară largă a riscurilor şi ameninţărilor derivate din activităţile desfăşurate în spaţiul cibernetic, precum şi a modului de prevenire şi contracarare a acestora necesită o comunicare şi cooperare eficiente între actorii specifici în acest domeniu.

La nivelul UE sunt întreprinse demersuri în privinţa adoptării unei strategii europene pentru securitatea cibernetică, care să armonizeze eforturile statelor membre în abordarea provocărilor de securitate din spaţiul cibernetic şi protecţia infrastructurilor informatice critice. Totodată, la nivelul UE, s-a conturat necesitatea adoptării unei politici privind lupta împotriva criminalităţii informatice. Iniţiativele subsecvente au pornit de la constatarea creşterii numărului de infracţiuni informatice, a tot mai amplei implicări a grupurilor de criminalitate organizată în criminalitatea informatică, precum şi a necesităţii unei coordonări a eforturilor europene în direcţia combaterii acestor acte. Având în vedere că atacurile cibernetice pe scară largă, bine coordonate şi direcţionate către infrastructurile cibernetice critice ale statelor membre, constituie o preocupare crescândă a UE, întreprinderea de acţiuni pentru combaterea tuturor formelor de criminalitate informatică, atât la nivel european, cât şi la nivel naţional, a devenit o necesitate stringentă.

Creşterea capacităţii de luptă împotriva criminalităţii informatice la nivel naţional, european şi internaţional implică, printre altele creşterea gradului de cooperare şi coordonare, dezvoltarea unui cadru de reglementare coerent la nivelul UE, creşterea nivelului de conştientizare a costurilor şi pericolelor pe care le implică criminalitatea informatică.

În acest context, România recunoaşte existenţa unor astfel de ameninţări şi susţine o abordare comună, integrată şi coordonată, atât la nivelul NATO, cât şi la nivelul UE, pentru a putea oferi un răspuns oportun la atacurile cibernetice. Pentru asigurarea securităţii cibernetice a România si-a stabilit următoarele obiective:

a) adaptarea cadrului normativ şi instituţional la dinamica ameninţărilor specifice spaţiului cibernetic;

b) stabilirea şi aplicarea unor profile şi cerinţe minime de securitate pentru infrastructurile cibernetice naţionale, relevante din punct de vedere al funcţionării corecte a infrastructurilor critice; c) asigurarea rezilienţei infrastructurilor cibernetice;

d) asigurarea stării de securitate prin cunoaşterea, prevenirea şi contracararea vulnerabilităţilor, riscurilor şi ameninţărilor la adresa securităţii cibernetice a României;

e) valorificarea oportunităţilor spaţiului cibernetic pentru promovarea intereselor, valorilor şi obiectivelor naţionale în spaţiul cibernetic;

f) promovarea şi dezvoltarea cooperării între sectorul public şi cel privat în plan naţional, precum şi a cooperării internaţionale în domeniul securităţii cibernetice;

In ceea ce priveste abordarea pe termen mediu si lung România îşi propune, conform Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică asigurarea stării de normalitate în spaţiul cibernetic reducând riscurile şi valorificând oportunităţile, prin îmbunătăţirea cunoştinţelor, a capabilităţilor şi a mecanismelor de decizie.

În acest sens, eforturile se vor focaliza pe următoarele direcţii de acţiune:

1. Stabilirea cadrului conceptual, organizatoric şi acţional necesar asigurării securităţii cibernetice - constituirea şi operaţionalizarea unui sistem naţional de securitate cibernetică; - completarea şi armonizarea cadrului legislativ naţional în domeniu, inclusiv stabilirea şi aplicarea unor cerinţe minimale de securitate pentru infrastructurile cibernetice naţionale; - dezvoltarea cooperării între sectorul public şi

cel privat, inclusiv prin stimularea schimbului reciproc de informaţii, privind ameninţări, vulnerabilităţi, riscuri, precum şi cele referitoare la incidente şi atacuri cibernetice.

2. Dezvoltarea capacităţilor naţionale de management al riscului în domeniul securităţii cibernetice şi de reacţie la incidente cibernetice în baza unui program naţional, vizând: - consolidarea, la nivelul autorităţilor competente potrivit legii, a potenţialului de cunoaştere, prevenire şi contracarare a ameninţărilor şi minimizarea riscurilor asociate utilizării spaţiului cibernetic; - asigurarea unor instrumente de dezvoltare a cooperării dintre sectorul public şi cel privat, în domeniul securităţii cibernetice, inclusiv pentru crearea unui mecanism eficient de avertizare şi alertă, respectiv de reacţie la incidentele cibernetice; - stimularea capabilităţilor naţionale de cercetare-dezvoltare şi inovare în domeniul securităţii cibernetice; - creşterea nivelului de rezilienţă a infrastructurilor cibernetice; - dezvoltarea entităţilor de tip CERT, atât în cadrul sectorului public, cât şi în sectorul privat.

3. Promovarea şi consolidarea culturii de securitate în domeniul cibernetic

- derularea unor programe de conştientizare a populaţiei, a administraţiei publice şi a sectorului privat, cu privire la ameninţările, vulnerabilităţile şi riscurile specifice utilizării spaţiului cibernetic; - dezvoltarea de programe educaţionale, în cadrul formelor obligatorii de învăţământ, privind utilizarea sigură a internetului şi a echipamentelor de calcul;

- formarea profesională adecvată a persoanelor care îşi desfăşoară activitatea în domeniul securităţii cibernetice şi promovarea pe scară largă a certificărilor profesionale în domeniu;

- includerea unor elemente referitoare la securitatea cibernetică în programele de formare şi perfecţionare profesională a managerilor din domeniul public şi privat.

4. Dezvoltarea cooperării internaţionale în domeniul securităţii cibernetice

-încheierea unor acorduri de cooperare la nivel internaţional pentru îmbunătăţirea capacităţii de răspuns în cazul unor atacuri cibernetice majore;

-participarea la programe internaţionale care vizează domeniul securităţii cibernetice; -promovarea intereselor naţionale de securitate cibernetică în formatele de cooperare internaţională la care România este parte.

Necesitatea dezvoltării Sistemului de alertă timpurie şi informare în timp real privind incidentele cibernetice (RO-SAT) este prevăzută în H.G. 494/2011, cu scopul de a:

-avertiza în timp real şi emite de rapoarte cu privire la distribuţia şi natura incidentelor de securitate cibernetică;

-colabora cu autorităţile naţionale responsabile în asigurarea securităţii cibernetice, în vederea prevenirii şi înlăturării efectelor incidentelor, inclusiv prin crearea cadrului necesar realizării auditurilor de securitate;

-interveni on-site in vederea investigării incidentelor de securitate cibernetică.

Astfel vor putea fi identificate premisele de producere a incidentelor cibernetice şi/sau de lansare a unor atacuri asupra infrastructurilor cibernetice ce asigură funcţionalităţi de utilitate publică ori asigură servicii ale societăţii informaţionale.

Proiectul va încuraja şi facilita schimbul de informaţii privind ameninţările, vulnerabilităţile, riscurile, incidentele şi atacurile cibernetice.

Va fi dezvoltat un sistem robust, modern, interoperabil şi scalabil destinat procesării alertelor de securitate cibernetică primite de CERT-RO, care va fi interoperabil cu sistemele instituţiilor publice cu responsabilităţi în domeniu precum şi cu orice altă organizaţie din mediile guvernamental, de afaceri sau universitar, în vederea transmiterii corecte, coerente şi rapide a alertelor, sau a altor informaţii despre ameninţări detectate, într-un format clar, uşor de interpretat şi uşor de integrat în diverse sisteme de

securitate cibernetică. Posibilitatea transmiterii rapide şi coerente a informaţiei va spori capacitatea organizaţiei afectate de a răspunde la incidente de securitate cibernetică, prin remedierea pagubelor şi implementarea măsurilor tehnice necesare pentru evitarea pe viitor a acestor tipuri de evenimente, iar transmiterea datelor într-un format standardizat, recunoscut la nivel internaţional, va oferi posibilitatea integrării rapide şi eventual automate a măsurilor de securitate în sistemele de protecţie ale organizaţiei afectate.

Grupul ţintă este alcătuit din Poşta Română, Loteria Română şi Autoritatea Electorală Permanentă cu reţele distribuite la nivel naţional, precum şi alţi beneficiari.

La beneficiari vor fi amplasate echipamente şi sisteme de tip senzor SOC (Security Operation Center) de monitorizare în timp real a reţelelor din locaţiile beneficiarilor şi vor fi realizate audituri de securitate în scopul creşterii nivelului de securitate.

Proiectul reprezintă pentru instituţiile publice care deţin sau administrează la nivel teritorial infrastructuri cibernetice ce asigură funcţionalităţi de utilitate publică o oportunitate de evaluare a stării de securitate cibernetică a infrastructurii TIC, precum şi de identificare a ameninţărilor cibernetice prin intermediul senzorului ce urmează a fi dezvoltat în cadrul proiectului, fără a implica costuri din partea beneficiarilor.

Auditarea se realizează de către CERT-RO şi partenerul STS cu ajutorul facilităţilor oferite de echipamentele achiziţionate în cadrul proiectului. Prin proiectul RO-SAT, CERT-RO va asigura achiziţionarea, livrarea şi instalarea echipamentelor de securitate, singura obligaţie a beneficiarului fiind asigurarea funcţionării optime a acestuia şi utilizarea în scopul declarat în cadrul proiectului. Totodată, între CERT-RO şi instituţiile beneficiare vor fi stimulate schimburile de informaţii cu privire la alertele/incidentele de securitate cibernetică detectate de echipamentele din cadrul proiectului, schimburile de informaţii cu privire la sursele de ameninţare, metodele şi mijloacele folosite de acestea, cu respectarea dispoziţiilor legale în vigoare, informarea în timp real privind incidentele cibernetice, capabilităţile de reacţie rapidă în cazul identificării unor posibile indicii ce pot preceda apariţia unor atacuri cibernetice

1.[1] Prezentul act normativ nu transpune legislație comunitară și nu creează cadrul pentru aplicarea directă a acesteia.

2. Schimbări preconizate

Obiectivul general al proiectului: Proiectul propus spre finanţare prin POC are ca obiectiv general creşterea capacităţii operaţionale a CERT-RO în vederea asigurării capabilităţilor naţionale de prevenire, identificare, analiză şi reacţie la incidentele de securitate cibernetică. Prin implementarea RO-SAT se urmăreşte creşterea nivelului de securitate a spaţiului cibernetic naţional (instituţii publice, companii private, utilizatori individuali), precum şi creşterea capacităţii de răspuns la incidente de securitate cibernetică a CERT-RO. Îmbunătăţirea stării de securitate prin cunoaşterea, prevenirea şi contracararea vulnerabilităţilor, riscurilor şi ameninţărilor la adresa securităţii cibernetice a organizaţiilor din România este stipulată ca obiectiv al Strategiei Naţionale de Securitate Cibernetică.

Obiectivele specifice ale proiectului

1. Dezvoltarea unui sistem naţional de avertizare în timp real a persoanelor fizice şi/sau juridice vizate de atacuri cibernetice şi/sau afectate de incidente cibernetice, precum şi pentru informarea şi cooperarea cu autorităţile competente;

2. Amplasarea unor sisteme de tip senzor SOC (Security Operation Center) de monitorizare în timp real a reţelelor din locaţiile beneficiarilor: Poşta Română, Loteria Română şi Autoritatea Electorală Permanentă, reţele distribuite la nivel naţional precum şi la alţi beneficiari 3. Realizarea unui număr de cel puţin 120 audituri de securitate pentru reţelele din locaţiile beneficiarilor în care vor fi amplasate echipamente;

4. Instruirea unui număr de 20 specialişti. Domeniile de interes sunt: procesarea alertelor generate de terminalele SOC, managementul terminalelor SOC, managementul sistemului de alertă timpurie şi informare în timp real, intervenţia rapidă în caz de atac cibernetic, investigarea atacurilor cibernetice, ethical hacking etc;

5. Operaţionalizarea a patru echipe de intervenţie on-site în vederea derulării investigaţiilor în cazul incidentelor de Securitate cibernetică.

3. Alte informaţii

Proiectul "Sistem de alertă timpurie şi informare în timp real - RO-SAT" a fost depus ca urmare a apelului 1 de proiecte lansat prin POC 2014-2020, Axa Prioritară 2 - Tehnologia Informaţiei şi Comunicaţiei (TIC) pentru o economie digitală competitive, Acţiunea 2.3.2 Asigurarea securităţii cibernetice a sistemelor TIC şi a reţelelor informatice.
La data de 20 septembrie a.c. a fost semnat contractul de finanţare nr. 2/2.3.2/20.09.2019.

Secţiunea a 3-a
Impactul socio - economic al proiectului de act normativ

1. Impact macro-economic

Proiectul de act normativ nu se referă la acest subiect.

1¹ Impactul asupra mediului concurenţial şi domeniul ajutoarelor de stat

Proiectul de act normativ nu se refera la acest subiect.

2. Impact asupra mediului de afaceri

Proiectul de act normativ nu se referă la acest subiect.

2¹ Impactul sarcinilor administrative

Proiectul de act normativ nu se referă la acest subiect.

2² Impactul asupra întreprinderilor mici şi mijlocii

Proiectul de act normativ nu se referă la acest subiect.

3. Impact social

Proiectul de act normativ nu se referă la acest subiect.

4. Impact asupra mediului

Proiectul de act normativ nu se referă la acest subiect.

5. Alte informaţii

Beneficiarul investiţiei este Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO şi Serviciul de Telecomunicaţii Speciale.

În vederea implementării proiectului, CERT-RO are semnate protocoale cu beneficiari, precum Posta Română, AEP, Loteria Română etc.

Proiectul reprezintă pentru instituţiile publice care deţin sau administrează la nivel teritorial infrastructuri cibernetice ce asigură funcţionalităţi de utilitate publică o oportunitate de evaluare a stării de securitate cibernetică a infrastructurii TIC, precum şi de identificare a ameninţărilor cibernetice prin intermediul senzorului ce urmează a fi dezvoltat în cadrul proiectului. Şi după finalizarea proiectului vor putea fi efectuate audituri de securitate, atât la nivelul infrastructurilor identificate deja, cât şi la nivelul altor infrastructuri cibernetice.
Prin operaţionalizarea centrului integrat de management şi monitorizare, vor fi stimulate schimburile de informaţii cu privire la alertele/incidentele de securitate cibernetică, schimburile de informaţii cu privire

la sursele de amenințare, metodele şi mijloacele folosite.
De asemenea, se va asigura informarea în timp real privind incidentele cibernetice, capabilitățile de reacţie rapidă în cazul identificării unor posibile indicii ce pot preceda apariția unor atacuri cibernetice.

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 patru ani				Media pe cinci ani
1	2	3	4	5	6	7
	2019	2020	2021	2022	2023	2024-2028
1. Modificări ale veniturilor bugetare, în plus/minus, din care: a) buget de stat, din acesta: i. impozit pe profit ii. impozit pe venit iii. TVA b) bugete locale i. impozit pe profit c) bugetul asigurărilor sociale de stat: i. contribuții de asigurări						
2. Modificări ale cheltuielilor bugetare, în plus, din care: a) **buget de stat**, din acesta: i. cheltuieli de personal ii. bunuri şi servicii iii. asistență socială b) bugete locale: i. cheltuieli de personal ii. bunuri şi servicii iii. asistență socială c) bugetul asigurărilor sociale de stat: i. cheltuieli de personal ii. bunuri şi servicii	679 0	2.655 0	34.482 0	31.808 0	0 0	

3. Impact financiar, plus/minus, din care: a) buget de stat b) bugete locale	 -679 0	 -2.655 0	 -34.482 0	 -31.808 0	 0	
4. Propuneri pentru acoperirea creşterii cheltuielilor bugetare						
5. Propuneri pentru a compensa reducerea veniturilor bugetare						
6. Calcule detaliate privind fundamentarea modificărilor veniturilor şi/sau cheltuielilor bugetare	Proiectul de act normativ nu se referă la acest subiect.					
7. **Alte informaţii**:	Finanţarea proiectului se realizează din fonduri externe nerambursabile şi de la bugetul de stat, prin bugetele Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO şi Serviciului de Telecomunicatii Speciale a României, în limita sumelor aprobate anual cu această destinaţie, conform programelor de investiţii publice aprobate potrivit legii. Potrivit cererii de finanţare, **bugetul total de 69.624 mii lei** este distribuit pentru cele 2 instituţii partenere după cum urmează: **Buget CERT-RO: 69.600 mii lei,** din care: cofinantarea FEDR este de: 58.697 mii lei, si Bugetul de stat: 10.903 mii lei (10.898 mii lei cheltuieli eligibile şi 5 mii lei cheltuieli neeligibile). **Buget STS: 24 mii lei,** din care: FEDR este de: 20 mii lei şi Bugetul de stat: 4 mii lei.					

Secţiunea a 5-a
Efectele proiectului de act normativ asupra legislaţiei în vigoare

1. Măsuri normative necesare pentru aplicarea prevederilor proiectului de act normativ:
1[1].Compatibilitatea proiectului de act normativ cu legislaţia în domeniul achiziţiilor publice.

a) impact legislativ - prevederi de modificare şi completare a cadrului normativ în domeniul achiziţiilor publice, prevederi derogatorii;
Nu este cazul.

b) norme cu impact la nivel operaţional/tehnic - sisteme electronice utilizate în desfăşurarea procedurilor de achiziţie publică, unităţi centralizate de achiziţii publice, structură organizatorică internă a autorităţilor contractante.
Nu este cazul.

2. Conformitatea proiectului de act normativ cu legislaţia comunitară în materie cazul proiectelor ce transpun prevederi comunitare
Proiectul de act normativ nu se referă la acest subiect.

3. Măsuri normative necesare aplicării directe a actelor normative comunitare
Proiectul de act normativ nu se referă la acest subiect.

4. Hotărâri ale Curţii de Justiţie a Uniunii Europene
Proiectul de act normativ nu se referă la acest subiect.

5. Alte acte normative și sau documente internaționale din care decurg angajamente
Proiectul de act normativ nu se referă la acest subiect.

6. Alte informații:
Nu este cazul.

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

1.Informații privind procesul de consultare cu organizațiile neguvernamentale, institute de cercetare și alte organisme implicate
Proiectul de act normativ nu se referă la acest subiect.

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
Proiectul de act normativ nu se referă la acest subiect.

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
Proiectul de act normativ nu se referă la acest subiect.

4. Consultările desfășurate în cadrul consiliilor interministeriale în conformitate cu prevederile Hotărârii Guvernului nr.750/2005 privind constituirea consiliilor interministeriale permanente
Proiectul de act normativ nu se referă la acest subiect.

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
Proiectul de act normativ nu se referă la acest subiect.

6. Alte informații:
Nu este cazul.

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 întreprinse demersurile legale prevăzute de art. 7 din Regulamentul privind procedurile, la nivelul Guvernului, pentru elaborarea, avizarea și prezentarea proiectelor de documente de politici publice, a proiectelor de acte normative, precum și a altor documente, în vederea adoptării/aprobării, aprobat prin Hotărârea Guvernului nr. 561/2009.

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:

Nu este cazul.
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 Proiectul de act normativ nu se referă la acest subiect.
2. Alte informații Nu este cazul.

Față de cele prezentate mai sus, a fost elaborat prezentul proiect de **Hotărâre privind aprobarea Notei de fundamentare referitoare la necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului "Sistem de alertă timpurie și informare în timp real - RO-SAT",** care, în forma prezentată, a fost avizat de ministerele interesate și pe care îl supunem spre aprobare.

MINISTRUL TRANSPORTURILOR, INFRASATRUCTURII ȘI COMUNICAȚIILOR
Lucian Nicolae BODE

AVIZ FAVORABIL:

MINISTRUL FINANȚELOR PUBLICE
Vasile-Florin CÎȚU

MINISTRUL FONDURILOR EUROPENE
Ioan Marcel BOLOȘ