GUVERNUL ROMÂNIEI

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"

În temeiul art. 108 din Constituția României, republicată și al art. 42 alin. (1), lit. a) din Legea nr. 500/2002 privind finanțele publice, cu modificările și completările ulterioare,

Guvernul României adoptă prezenta hotărâre.

Art. 1. - Se aprobă Nota de fundamentare referitoare la necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului "Sistem de alertă timpurie și informare în timp real - RO-SAT", prevăzută în anexa care face parte integrantă din prezenta hotărâre.

Art. 2. - Finanțarea proiectului prevăzut la art.1 se realizează din fonduri externe nerambursabile și de la bugetul de stat, prin bugetul autorității desemnate la art. 5 din Ordonanța de urgență a Guvernului nr. 68/2019 privind stabilirea unor măsuri la nivelul administrației publice centrale și pentru modificarea și completarea unor acte normative, în limita sumelor aprobate anual cu această destinație, conform programelor de investiții publice aprobate potrivit legii.

Art. 3. – Centrul Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO și Serviciul de Telecomunicații Speciale răspund de modul de implementare a proiectului prevăzut la art. 1, potrivit prevederilor prezentei hotărâri.

PRIM-MINISTRU

Ludovic ORBAN

Anexă la HG nr. / 2019

NOTA DE FUNDAMENTARE

referitoare la necesitatea şi oportunitatea efectuării cheltuielilor aferente proiectului "Sistem de alertă timpurie şi informare în timp real - RO-SAT"

1. Context general:

1. Descrierea situaţiei actuale

Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică – CERT-RO este instituţie publică înfiinţată prin H.G. nr. 494/2011 ca structură independentă de expertiză şi cercetare-dezvoltare în domeniul securităţii cibernetice, a cărei misiune este prevenirea, analiza, identificarea şi răspunsul la incidentele din cadrul infrastructurilor cibernetice ce asigură funcţionalităţi de utilitate publică ori asigură servicii ale societăţii informaţionale. Comisia Europeană a comunicat în data de 26.08.2010 către Parlamentul European, Consiliul European, Comitetul Economic şi Social European şi Comitetul Regiunilor strategia privind Agenda digitală pentru Europa. Printre domeniile de acţiune stabilite de Agenda digitală pentru Europa se enumeră şi nevoia de încredere şi securitate.

Astfel, Guvernul României îşi propune definirea şi menţinerea unui mediu virtual sigur, cu un înalt grad de rezilienţă 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, 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 investigarii incidentelor de securitate cibernetică.

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 autoritățile 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 identităților electronice trebuie să fie identificate, în primul rând, serviciile de eGuvernare electronice actuale, consumatorii acestora și modalitățile de identificare și autentificare a utilizatorilor (credențialele).

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.

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 României au fost stabilite 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 și dezvoltarea cooperării între sectorul public şi cel privat în plan național, precum şi a cooperării internaționale în domeniul securității cibernetice;

În ceea ce privește 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 reziliență 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 investigarii 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 mediul 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.

Grup ţintă

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

Obiectivul general al proiectului/Scopul proiectului

Obiective proiect

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.

Indicatori prestabiliți

Indicatori prestabiliți de realizare

Denumire indicator	Unitate masură	Valoare țintă	Regiuni dezvoltate	Regiuni mai puțin dezvoltate
Audituri de securitate susținute	Audituri de securitate	120	39	81

Indicatori suplimentari proiect

Indicatori suplimentari de realizare

Denumire indicator	Unitate masură	Valoare țintă
Numar de infrastructuri cibernetice ce asigura funcționalități de utilitate publică din cadrul cărora au fost gestionate incidentele de securitate cibernetică	Infrastructuri cibernetice ce asigura funcționalități	14

Durata de realizare a întregului proiect de investiții este de 36 luni.

2. Valoarea şi finanțarea proiectului de investiții:

Descrierea investiţiei

Proiectul vizează asigurarea interoperabilităţii RO-SAT cu alte sisteme informatice, beneficiare directe ale datelor din RO-SAT, respectiv organizaţii afectate sau posibil afectate în cadrul atacurilor cibernetice raportate la CERT-RO, cărora să le poată fi transmise toate datele necesare, în timp util şi într-un format standardizat, în vederea

luării tuturor măsurilor ce se impun pentru reducerea efectelor incidentelor. RO-SAT reprezintă un sistem integrat, modern, robust, scalabil, capabil să asigure preluarea, procesarea şi transmiterea unui număr foarte mare de alerte de securitate cibernetică, din surse diferite, alerte ce vizează organizaţii publice sau private din spaţiul cibernetic naţional.

RO-SAT va funcţiona ca un sistem integrat, modular, flexibil şi scalabil, format din diverse module şi sub-module, ce vor îndeplini numeroase funcţii. Modularitatea şi flexibilitatea vor oferi posibilitatea dezvoltării ulterioare de funcţionalităţi suplimentare, care să poată apela cu uşurinţă modulele deja dezvoltate.

RO-SAT va fi accesibil utilizatorilor prin intermediul unei interfeţe WEB intuitive, ce va oferi posibilitatea administrării sistemului şi realizării majorităţii funcţionalităţilor sistemului.

Prin sistemul RO-SAT se va dezvolta o platformă de alertă timpurie a factorilor de decizie, precum şi a deţinătorilor de sisteme informatice din România cu privire la ameninţările existente în spaţiul cibernetic. În acest sens se vor colecta alerte/date despre incidente de securitate cibernetice prin intermediul unor terminale de tip SOC dispuse la nivel naţional, acestea urmând a fi procesate în cadrul unei platforme centrale de tip cyberintelligence.

Alertele colectate de la terminalele de tip SOC vor fi integrate cu alerte/date ce provin din modulele dezvoltate in cadrul proiectului (DarkNET, HoneyNET, Crawling siteuri, Scanner vulnerabilităţi etc.), precum şi din surse externe, respectiv din reţeaua de cooperare internaţională a CERT-urilor şi de la companiile de securitate cibernetică (feed-uri publice şi feed-uri contracost). Pentru realizarea acestui sistem sunt necesare: - dezvoltarea unui sistem de terminale SOC personalizate pentru specificul naţional de securitate cibernetică actual - personalizarea unei platforme de cyber threat intelligence ce va conţine componente de machine learning, inteligenţă artificială, prelucrare a unui volum mare de date (big data analytics) necesare pentru analiza, corelarea, procesarea, integrarea şi generarea unor informaţii referitoare la ameninţări din spaţiul cibernetic - operaţionalizarea echipelor de reacţie rapidă la incidentele de securitate cibernetică al căror rol va fi acela de a asigura intervenţia la nivel naţional (stoparea atacurilor cibernetice, limitarea efectelor/pierderilor, coordonarea în vederea restabilirii funcţionării normale şi prelevarea probelor pentru efectuarea investigaţiilor aferente).

Modulele software ce vor alcatui platforma RO-SAT sunt următoarele:
A. Modulul "Darknet"
B. Modulul "HoneyNet"
C. Modulul "Senzor SOC"
D. Modulul "Scanner vulnerabilităţi"
E. Modulul "Crawling website-uri"
F. Modulul "OSINT"
G. Modulul "Cyber Threat Intelligence"
H. Modulul colectare, normalizare şi îmbogăţire
I. Modulul "Big Data Security Analytics" J. Modulul "Security Operations Center"
K. Modulul "Diseminare date" (API)
Sistemul va fi instalat în locaţii fizice, astfel:
- Nodul principal – reprezintă locaţia de bază în care va funcţiona sistemul, la sediul CERT-RO
- Locaţii Poşta Română: 2 locaţii centrale , 7 locaţii regionale
- Locaţii Loteria Română: 2 locaţii centrale - Locaţii Autoritatea Electorală Permanentă: 3 locaţii centrale

Proiectul va include soluţii hardware şi software pentru toate locaţiile menţionate anterior precum şi pentru alte locaţii. Totodată, în cadrul proiectului vor fi realizate audituri de securitate pentru reţelele din locaţiile beneficiarilor în care vor fi amplasate echipamentele.

Valoarea totală a proiectului de investiţii este de **69.624 mii lei.**
Valoarea eligibilă a proiectului este de **69.624 mii lei**.

Din care:

	mii lei
Cheltuieli de investiții	**64.305**
Din care:	
Dotări independente	25.643
Cheltuieli de expertiză, proiectare, asistență tehnică, pentru teste și predare la beneficiar, precum și alte categorii de lucrări de intervenții	-
Alte cheltuieli de investiții	38.662

Finanțarea proiectului se realizează din Fondul European de Dezvoltare Regională (FEDR) şi bugetul de stat din Programul Operațional Competitivitate, în conformitate cu contractul de finanțare nr. 2/2.3.2/20.09.2019, încheiat cu Ministerul Fondurilor Europene, în calitate de Autoritate de Management pentru Programul Operațional Competitivitate 2014-2020 şi Ministerul Comunicațiilor şi Societății Informaționale, în calitate de Organism Intermediar pentru Promovarea Societății Informaționale pentru Programul Operațional Competitivitate 2014-2020 aferentă Axei Prioritare 2 - Tehnologia Informației și Comunicației (TIC) pentru o economie digitală competitive, Acţiunea 2.3.2 Asigurarea securităţii cibernetice a sistemelor TIC şi a reţelelor informatice.

Proiectul a primit în data de 25.04.2019 avizul pozitiv nr.223 CTE al Comitetului Tehnico-Economic pentru Societatea Informațională pentru Proiectul tehnic și în data de 30.05.2019 avizul pozitiv nr. 294 CTE pentru Studiul de fezabilitate, în conformitate cu prevederile H.G. nr. 941/2013 privind organizarea și funcționarea Comitetului Tehnico-Economic pentru Societatea Informațională.

Caracteristicile principale ale proiectului de investiții - "Sistem de alertă timpurie și informare în timp real - RO-SAT"

Caracteristici principale:

Valoarea totală a cheltuielilor de investiții (inclusiv TVA)	mii lei	**64.305**
Eşalonarea cheltuielilor de investiții		
- Anul I	mii lei	**185**
- Anul II	mii lei	**1.214**
- Anul III	mii lei	**32.048**
- Anul IV	mii lei	**30.858**

Finanţarea investiţiei

Finanțarea proiectului de investiții se realizează din fonduri externe nerambursabile, prin Programul Operațional Competitivitate 2014-2020, în conformitate cu contractul de finanțare nr.

2/2.3.2/20.09.2019 și de la bugetul de stat conform HG 494/2011, în limita sumelor aprobate anual cu această destinație, conform programelor de investiții publice aprobate potrivit legii.