PARLAMENTUL ROMÂNIEI

SENAT

LEGE

privind înființarea și operaționalizarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie, precum și pentru modificarea și completarea unor acte normative

Având în vedere situația actuală a securității cibernetice în sectorul energetic din România, care prezintă deficiențe semnificative și vulnerabilități critice, impunându-se adoptarea unor măsuri urgente și care nu suferă amânare pentru protejarea infrastructurilor energetice împotriva amenințărilor cibernetice,

Ținând cont că atacurile cibernetice cresc în sectorul energetic, fiind de natură a opri producerea, furnizarea și transportul de energie electrică, gaze naturale sau energie termică, fiind o situație extraordinară cu care se confruntă atât statul român cât și partenerii europeni și transatlantici,

Având în vedere că aceste atacuri sunt dublate de perpetuarea războiului dus de Federația Rusă în Ucraina care începe să ia tot mai multe valențe hibride, dihotomice și asimetrice, atacurile cibernetice fiind parte componentă a acestui război, care afectează securitatea energetică a Ucrainei și se poate repercuta negativ și asupra statelor vecine, inclusiv Aliate,

Văzând faptul că ostilizarea unor actori statali și nonstatali a generat intensificarea atacurilor cibernetice sub pavilion fals împotriva României; crescând atât numărul de atacuri dar și stilul și mecanismele de operare a acestora,

Ținând cont de faptul că liberalizarea pieței energetice naționale, fluctuația prețurilor și prezența pe piața de capital a tot mai multor companii energetice constituie situația premisă de la care pleacă atacatorii cibernetici atunci când efectuează o operațiune împotriva statului român, precum și faptul atacurile cibernetice pot influența chiar direct prețurile la energie și stabilitatea Sistemului Electro energetic Național și influențează indirect funcționarea serviciilor publice și

a economiei naționale, ambele fiind dependente de furnizarea energiei electrice și termice,

Având în vedere că multitudinea atacurilor cibernetice din fiecare sector (economie, sănătate, transport, apărare etc.) obligă autoritățile naționale competente să se poată baza pe un suport tehnic real chiar din partea personalului de specialitate din respectivul sector, pentru a suplini efortul defensiv și proactiv în spațiul cibernetic, în spiritul respectării legislației naționale și europene care impun crearea de Centre de Răspuns la Incidente de Securitate Cibernetică sectoriale,

Reținând recentul atac cibernetic de tip ransomware produs asupra sistemelor informatice ale Distribuție Energie Electrică România (DEER) care a condus la punerea în indisponibilitate a unor sisteme de operare ale distribuitorului național de energie, existând riscul real ca atacul să se fi extins la nivelul infrastructurii SCADA, și văzând amploarea pagubelor unui astfel de atac,

Ținând cont de contextul creșterii riscurilor la adresa apărării și securității naționale a României, în contextul atacurilor cibernetice generate de Războiul Federației Ruse din Ucraina, care impune crearea unui Centru de Răspuns la Incidente de Securitate Cibernetică sectorial în energie, denumit în continuare *CSIRT*, capabil să sprijine efortul național și interinstituțional de prevenire și combatere a atacurilor cibernetice asupra companiilor și infrastructurii energetice,

Având în vedere faptul că, pe fondul multitudinii de atacuri cibernetice specifice sectorului energetic de tipul APT, Ransomware, atacuri de tip man-in-the-middle, Log-injection, Log-Tampering sau Log-Flooding, atacuri împotriva infrastructurii de tip Supraveghere, Control și Achiziție de Date/Sisteme de Control Industrial, denumite în continuare *SCADA/ICS*, atacuri de tip Cyber-Physical, BlackEnergy, Industroyer sau Stuxnet, este imperios necesar ca Sistemul Electroenergetic Național să funcționeze fără întreruperi și fără distrugerea sau punerea în indisponibilitate temporară a rețelelor energetice,

Luând în considerare posibilitatea crescută a unui atac cibernetic multiplu, de natură a afecta elemente de infrastructură națională din sectorul cibernetic, care ar crea panică în rândul populației civile, precum și ar deteriora poziția unor companii din sectorul energetic pe piața de capital, influențând, în final, și prețurile la energie;

Văzând că lipsa unei structuri de tipul unor centre de operațiuni de securitate cibernetică și/sau CSIRT sectoriale în energie, în contextul în care legislația europeană o recomandă încă din 2016, accentuează vulnerabilitățile și riscurile la adresa securității cibernetice a rețelelor și sistemelor informatice din energie, precum și lipsa de uniformitate și comandă unică a responsabililor de securitatea cibernetică din sector, sunt de natură a slăbi capacitatea de apărare, reacție și reziliență a României în cazul unui atac multiplu, sistemic, care vizează sistemul energetic național;

Ţinând cont că este imperativ necesară o consolidare a securităţii cibernetice a majorităţii companiilor de stat şi a operatorilor economici beneficiari ai proiectelor finanţate prin Fondul pentru Modernizare pentru a face faţă mai bine ameninţărilor cibernetice complexe şi avansate, precum şi a creşte conştientizarea importanţei securităţii cibernetice la nivel de sector;

Reţinând că înfiinţarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie este esenţială pentru a asigura monitorizarea continuă, răspunsul prompt la incidente, investigaţiile forensic şi protecţia proprie împotriva atacurilor cibernetice, ca elemente ale politicii naţionale de patriotism energetic, întrucât întârzierea punerii în aplicare a legislaţiei naţionale şi europene privind operaţionalizarea CSIRT în domeniul energetic a dus la o vulnerabilizare a sistemului, în contextul ameninţărilor cibernetice actuale, iar aceasta nu mai poate fi trecută cu vederea, drept pentru care se impune constituirea unui CSIRT sectorial, în lipsa acestuia, pagubele generate de atacurile cibernetice putând fi irecuperabile, cu consecinţe directe asupra tarifelor la energie;

Având în vedere că România, în calitate de furnizor de energie electrică pentru Republica Moldova şi Ucraina, precum şi de furnizor de securitate la nivel regional, are obligaţia de a-şi consolida urgent securitatea cibernetică a sectorului energetic pentru a-şi prezerva acest statut şi a furniza pe viitor cunoaştere strategică şi altor sectoare şi state partenere,

Ţinând cont că, în contextul construirii marilor proiecte energetice precum Hidrocentrala prin acumulare prin pompaj Tamila-Lăpuşteşti, proiectul Neptun Deep, proiectul Reactoarelor Modulare Mici SMR, proiectul reactoarelor 3 şi 4 de la CNE Cernavodă, proiectul privind realizarea unei linii de înaltă tensiune în curent continuu şi a staţiilor de conversie pe teritoriul României - proiectul HVDC, cele 11 microhidrocentrale, termocentrala de la Iemut, electrocentrala pe gaz de Ia Mintia, dar şi a celor finanţate prin Fondul pentru Modernizare care vor fi puternic digitalizate şi automatizate, România trebuie să ofere protecţie cibernetică adecvată, timpurie şi integrată operatorilor economici care vor opera acele sisteme şi reţele ale infrastructurii energetice, iar fără operaţionalizarea unei echipe CSIRT sectorial, sectorul energetic naţional apare vulnerabil în faţa atacurilor care vor viza noile tehnologii asociate marilor proiecte energetice;

Având în vedere incidentele majore din sectorul energetic românesc, precum atacul cibernetic de tip ransomware asupra Rompetrol, cu impact direct asupra unor servicii vitale oferite populaţiei, care au relevat limitele acoperirii legislaţiei actuale în domeniul securităţii cibernetice în ceea ce priveşte capacitatea instituţiilor naţionale de a răspunde în cazul unor situaţii de urgenţă şi nevoia de a implementa reglementările europene actualizate în ceea ce priveşte securitatea lanţului de aprovizionare şi supravegherea îndeplinirii obligaţiilor ce le revin entităţilor relevante, în vederea creşterii nivelului de reziliență al acestora, în corelare cu nivelul lor de risc în plan societal;

Având în vedere că adoptarea promptă și concretă a măsurilor și mecanismelor necesare creșterii rezidenței României în fața amenințărilor cibernetice și dat fiind rolul crucial al sectorului energetic în consolidarea capacităților naționale de apărare și răspuns la incidente de securitate, inclusiv cibernetică,

Având în vedere că, până cel mai târziu la data de 13 decembrie 2024, fiecare stat membru este obligat să desemneze o autoritate națională guvernamentală sau de reglementare responsabilă cu îndeplinirea sarcinilor care îi simt atribuite prin Regulamentul delegat (UE) 2024/1366 al Comisiei din 11 martie 2024 de completare a Regulamentului (UE) 2019/943 al Parlamentului European și al Consiliului prin stabilirea unui cod de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică, neimplementarea acestui regulament și neoperaționalizarea autorității competente generând vulnerabilități grave la adresa securității cibernetice din sectorul energetic românesc și putând conduce la eventuale sancțiuni împotriva României pentru neaplicarea actelor legislative obligatorii ale UE;

ținând cont că salarizarea personalului CRISCE trebuie să se realizeze la un nivel competitiv cu cel al pieței, în vederea atragerii și retenției de personal calificat, coroborată cu evaluare riguroasă a performanțelor profesionale specifice sectorului industriei de securitate cibernetică, impunându-se pe această cale derogări de la dreptul comun în materia salarizării personalului plătit din fonduri publice, dar și de la statutul profesional al personalului contractual din administrația publică;

Reținând că, printre obiectivele sectorului energetic din Programul de guvernare PSD-PNL-USR- UDMR-Grupul parlamentar al minorităților naționale din Camera Deputaților 2025-2028, este înființarea unui Centru de Răspuns la Incidente de Securitate Cibernetică în Energie, denumit în continuare CRISCE, și crearea de echipe de răspuns la incidente de securitate cibernetică - CSIRT la nivelul companiilor naționale;

Văzând considerentele Curții Constituționale a României din Decizia nr.70/2023 referitoare la respingerea obiecțiilor de neconstituționalitate a dispozițiilor art.3 alin.(1) lit.c), art.21 alin.(1), art.22, art.25, art.41, art.48 și art.50 din Legea nr.58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, care au statuat că securitatea cibernetică este parte componentă a securității naționale a României,

Senatul adoptă prezentul proiect de lege

Art.1.- (1) Începând cu data intrării în vigoare a prezentei legi, în cadrul Ministerului Energiei se înființează Centrul de Răspuns la Incidente de Securitate Cibernetică în Energie, denumit în continuare CRISCE, structură fără personalitate juridică, în directa și nemijlocita subordine a ministrului energiei, organizată la nivel de direcție generală.

(2) CRISCE este condus de un Director de Securitate Cibernetică, denumit în continuare *CISO*, ajutat de un Director de Securitate Cibernetică adjunct, care dezvoltă relații de colaborare instituțională cu toate structurile organizatorice din cadrul Ministerului Energiei, cu entitățile din sectorul energetic, reprezentând entitățile aflate în subordinea sau sub autoritatea Ministerului Energiei sau ale altor organe de specialitate ale administrației publice centrale, cu beneficiarii proiectelor finanțate prin Fondul pentru Modernizare, cu Centrul Național de Coordonare din cadrul Organismului intermediar pentru promovarea societății informaționale din cadrul Autorității pentru Digitalizarea României, precum și cu oricare alte persoane juridice de drept public sau privat din sectorul energetic național.

(3) CRISCE îndeplinește următoarele funcții:

a) funcția de centru operațional de securitate la nivel sectorial în domeniul energiei și resurselor energetice, astfel cum este definită art.2 lit.f) din Legea nr.58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, cu modificările și completările ulterioare;

b) funcția de echipă de răspuns la incidente de securitate cibernetică la nivel sectorial în domeniul energiei și resurselor energetice, denumită în continuare CSIRT, astfel cum este definită art.2 lit.a) din Ordonanța de urgență a Guvernului nr.104/2021, aprobată cu modificări și completări prin Legea nr.11/2022, cu modificările ulterioare, precum și în conformitate cu secțiunea a 4-a din capitolul V din Ordonanța de urgență a Guvernului nr.155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil.

(4) Prin derogare de la prevederile art.37 alin.(5) din Ordonanța de urgență a Guvernului nr.155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, de la data intrării în vigoare a prezentei legi, Ministerul Energiei, prin CRISCE, îndeplinește funcția de autoritate competentă responsabilă cu îndeplinirea sarcinilor care îi sunt atribuite prin Regulamentul delegat (UE) 2024/1366 din 11 martie 2024 al Comisiei de completare a Regulamentului (UE) 2019/943 al Parlamentului European și al Consiliului prin stabilirea unui cod de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică.

(5) În vederea exercitării funcției prevăzute la alin.(2) lit.b), CRISCE are obligația de a solicita și obține prealabil autorizarea de către Directoratul Național de Securitate Cibernetică, denumit în continuare *DNSC*, în condițiile Ordonanței de urgență a Guvernului nr.155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul

cibernetic național civil și ale Ordonanței de urgență a Guvernului nr.104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, cu modificările și completările ulterioare.

Art.2.- (1) Prin derogare de la prevederile art.30, art.82 alin.(3)-(5) și ale art.84 alin.(1) din Legea nr.53/2003 - Codul muncii, republicată, cu modificările și completările ulterioare și ale art.31 alin.(1) din Legea-cadru nr.153/2017 privind salarizarea personalului plătit din fonduri publice, cu modificările și completările ulterioare, posturile structurii prevăzută la art.1 alin.(1) se ocupă cu specialiști încadrați cu contract individual de muncă pe perioadă determinată încheiat pe o perioadă de maxim 3 ani care pot fi prelungite, celelalte dispoziții ale Legii nr.53/2003 - Codul muncii, republicată, cu modificările și completările ulterioare, aplicându-se corespunzător.

(2) Funcțiile specifice de coordonare și de execuție din cadrul CRISCE sunt următoarele:

a) funcții de coordonare: manager superior securitate cibernetică, manager securitate cibernetică, coordonator superior securitate cibernetică, coordonator securitate cibernetică, arhitect integrator soluții IT;

b) funcții de execuție (studii superioare): expert securitate cibernetică, expert preluare, analiză primară și răspuns la incidente securitate cibernetică, expert investigații digitale și analiză malware, expert dezvoltare, implementare și administrare infrastructuri securitate cibernetică, expert analiză surse deschise, riscuri și amenințări securitate cibernetică, expert accesare fonduri, implementare și administrare proiecte securitate cibernetică, expert în politici, standardizare și conformitate de securitate cibernetică, expert evaluare și impact financiar securitate cibernetică, expert arhitectură securitate cibernetică și soluții IT, expert dezvoltare, implementare și administrare infrastructuri securitate cibernetică, expert preluare, analiză primară și răspuns la incidente de securitate cibernetică, expert threat intelligence, expert investigații digitale și analiză malware, expert legal politici, standardizare de securitate cibernetică, expert evaluare și impact financiar securitate cibernetică, expert politici, strategii și cooperare securitate cibernetică, expert dezvoltare competențe, aptitudini și cunoștințe specifice de securitate cibernetică;

c) funcții de execuție (studii medii): asistent securitate cibernetică, asistent preluare, analiză primară și răspuns la incidente securitate cibernetică, asistent investigații digitale și analiză malware, asistent dezvoltare, implementare și administrare infrastructuri securitate cibernetică, asistent analiză surse deschise, riscuri și amenințări securitate cibernetică, asistent accesare fonduri, implementare și administrare proiecte securitate cibernetică, asistent legal politici, standardizare

de securitate cibernetică, asistent evaluare şi impact financiar securitate cibernetică, asistent politici, strategii şi cooperare securitate cibernetică, asistent dezvoltare competenţe, aptitudini şi cunoştinţe specifice de securitate cibernetică.

(3) Funcţiile specifice de coordonare şi execuţie prevăzute la alin.(2) lit.a) şi b) pot fi ocupate potrivit alin.(1) de personal care a absolvit cel puţin studii superioare de lungă durată.

(4) Funcţiile specifice de coordonare prevăzute la alin.(2) lit.c) pot fi ocupate potrivit alin.(1) de personal care a absolvit studii liceale cu diplomă de bacalaureat.

(5) Funcţiile de coordonare şi execuţie sunt structurate pe patru nivele profesionale după cum urmează:

a) asistent;
b) junior;
c) expert;
d) senior.

Art.3.- (1) Pentru personalul încadrat cu contract individual de muncă pe durată determinată potrivit art.2 alin.(1), stabilirea numărului şi a tipurilor de posturi, precum şi ocuparea posturilor se face în baza unei proceduri interne de recrutare şi selecţie, aprobate prin ordin al ministrului energiei, cu respectarea principiilor enunţate în Legea nr.53/2003 - Codul muncii, republicată, cu modificările şi completările ulterioare şi Legea nr.153/2017 privind salarizarea personalului plătit din fonduri publice, cu modificările şi completările ulterioare.

(2) Procesul de recrutare şi selecţie va fi asigurat de către o comisie de concurs formată din minim 3 membri şi maxim 5 membri desemnată prin ordin al ministrului energiei, din care pot face parte, în funcţie de necesitate şi profilul candidaţilor, şi reprezentanţi ai autorităţilor şi instituţiilor publice prevăzute de art.10 alin.(1) din Legea nr.58/2023, la propunerea conducătorilor acestora.

(3) Membrii comisiei de concurs beneficiază de o indemnizaţie fixă pentru fiecare procedură de recrutare şi selecţie desfăşurată, în cuantum de 50% din salariul de bază minim brut pe ţară garantat în plată.

(4) Cheltuielile cu plata indemnizaţiei prevăzute la alin.(3) se asigură din sursele prevăzute la art.6 alin.(2).

(5) Personalul încadrat cu contract individual de muncă pe durată determinată potrivit art.2 alin.(1), încheie la data semnării contractului individual de muncă şi un contract de angajament pe perioada contractului individual de muncă, iar în situaţia în care persoana angajată nu respectă condiţiile contractului de angajament în sensul denunţării acestuia, CRISCE are dreptul la plata de către persoana în cauză a unei despăgubiri în cuantum de 12 câştiguri salariale medii brute

utilizate la fundamentarea bugetului asigurărilor sociale de stat pe anul respectiv care se fac venit al bugetului de stat.

Art.4.- (1) Prin derogare de la prevederile art.248 alin.(1) din Legea nr.53/2003 - Codul Muncii, republicată, cu modificările şi completările ulterioare, performanţele profesionale ale personalului prevăzut la art.2 alin.(1) se evaluează periodic, la fiecare 12 luni calculate de la data intrării în vigoare a contractului individual de muncă, cu posibilitatea încetării contractului de muncă, pe baza criteriilor şi procedurii de evaluare, aprobate prin ordin al ministrului energiei.

(2) Criteriile de evaluare au la bază deţinerea certificatelor de calificare prevăzute, indicatori de performanţă, indicatori de impact, indicatori de realizare, indicatori de produs şi indicatori de rezultat, după caz.

(3) La elaborarea criteriilor şi procedurii de evaluare prevăzute la alin.(1), se solicită un aviz consultativ prealabil din partea autorităţilor şi instituţiilor publice prevăzute de art.10 alin.(1) din Legea nr.58/2023.

(4) Evaluarea performanţelor profesionale ale specialiştilor prevăzuţi la art.2 alin.(1) se asigură de către o comisie de evaluare formată din minim 3 membri şi maxim 5 membri desemnată prin ordin al ministrului energiei, din care pot face parte şi reprezentanţi ai autorităţilor şi instituţiilor publice prevăzute de art.10 alin.(1) din Legea nr.58/2023, cu modificările ulterioare, la propunerea conducătorilor acestora.

(5) Membrii comisiei de evaluare a performanţelor profesionale beneficiază, pentru activitatea desfăşurată, de o indemnizaţie fixă în cuantum de 50% din salariul de bază minim brut pe ţară garantat în plată.

(6) Cheltuielile cu plata indemnizaţiei prevăzute la alin.(5) se asigură din sursele prevăzute la art.6 alin.(2).

(7) Evaluarea performanţelor profesionale ale specialiştilor prevăzuţi la art.2 alin.(1) se realizează de către fiecare membru al comisiei, aprecierea îndeplinirii indicatorilor prevăzuţi la alin.(2) fiind notată cu note de la 1,00 la 5,00, nota exprimând gradul de îndeplinire a indicatorilor în realizarea obiectivelor stabilite.

(8) Nota finală a evaluării speciale a performanţelor profesionale individuale este media aritmetică a notelor prevăzute la alin.(7). Semnificaţia notelor este următoarea: nota 1,00 - nivel minim şi nota 5,00 - nivel maxim.

(9) Personalul CRISCE care a obţinut la evaluarea performanţelor profesionale nota finală cuprinsă între 4,51 şi 5,00, poate fi trecut în nivelul profesional imediat superior celui deţinut, la propunerea CISO.

(10) Personalul CIRSCE care a obținut la evaluarea performanțelor profesionale nota finală cuprinsă între 2.51 și 4,50, inclusiv, este trecut în nivelul profesional imediat inferior celui deținut la propunerea CISO.

(11) Pentru personalul CIRSCE care a obținut la evaluarea performanțelor profesionale nota finală mai mică de 2,50 inclusiv CISO, comisia de evaluare propune ministrului energiei încetarea contractului individual de muncă.

Art.5.- (1) În exercitarea funcției de centru operațional de securitate cibernetică la nivel sectorial în domeniul energetic și resurselor energetice, atribuțiile principale ale CRISCE sunt următoarele:

a) gestionarea incidentelor la nivel sectorial în domeniul energetic, ale Ministerului Energiei, ale unităților aflate în subordinea sau sub autoritatea Ministerului Energiei sau ale altor organe de specialitate ale administrației publice centrale, ale operatorilor de transport al energiei electrice și al gazelor naturale, inclusiv cele ale beneficiarilor proiectelor finanțate prin Fondul pentru Modernizare;

b) gestionarea securității cibernetice interne a Ministerului Energiei, asigurând măsurile optime pentru prevenirea și contracararea manifestării riscurilor de securitate cibernetică, în colaborare cu structurile interne responsabile de administrarea infrastructurilor și rețelelor informatice ale Ministerului Energiei;

c) asigurarea cooperării în domeniul securității cibernetice cu specific pentru sectorul energetic la nivel național, sub coordonarea DNSC, în calitate de CSIRT național, și participarea Ia grupuri de cooperare naționale și internaționale, evaluări inter pares, la Rețeaua CSIRT sau la alte formate asemănătoare la solicitarea CSIRT-ului național;

d) organizarea, monitorizarea și finalizarea, cel puțin o dată la 4 ani, a unui test de reziliență cibernetică împreună cu toți administratorii infrastructurilor critice din sectorul energetic; cadrul de testare, normele, regulamentul și condițiile de desfășurare a testelor vor fi aprobate prin ordin comun al ministrului energiei și al directorului DNSC;

e) asigurarea accesului continuu și integrat la datele și telemetria operatorilor economici din sectorul energetic, inclusiv la rețelele de tip tehnologie operațională/sisteme de control industrial, denumite în continuare *rețele de tip OT/ICS*, în scopul monitorizării eficiente și proactive a securității cibernetice;

f) implementarea de măsuri tehnice și operaționale care să faciliteze colectarea și analiza datelor de securitate cibernetică din rețelele de tip OT/ICS, inclusiv prin, dar fără a se limita la, utilizarea de log collectors și diode de date, respectând particularitățile fiecărei unități aflate în subordinea sau sub autoritatea Ministerului Energiei sau ale altor organe de specialitate ale

administrației publice centrale, ale beneficiarilor proiectelor finanțate prin Fondul pentru Modernizare, ale oricăror alte persoane juridice de drept public sau privat din sectorul energetic național pentru care CRISCE îndeplinește funcția de centru operațional de securitate cibernetică la nivel sectorial în domeniul energetic și resurselor energetice;

g) colaborarea cu operatorii economici pentru a garanta conformitatea cu standardele de securitate cibernetică și pentru a asigura protecția infrastructurilor energetice, fără a compromite funcționarea rețelelor de tip OT/ICS;

h) explorarea de soluții alternative la agenți de monitorizare, inclusiv analiza traficului de rețea și integrarea cu sistemele de monitorizare deja existente ale beneficiarilor;

i) alte atribuții stabilite prin legi speciale sau regulamentul de organizare și funcționare al CRISCE.

(2) În exercitarea funcției de echipă de răspuns la incidente de securitate cibernetică la nivel sectorial în domeniul energetic, atribuțiile principale ale CRISCE sunt următoarele:

a) asigurarea compatibilității și interoperabilității sistemelor, procedurilor și metodelor utilizate cu cele ale CSIRT-ului național;

b) prevenirea generării de incidente de securitate cibernetică prin furnizarea de expertiză preventivă pe ariile de interes, precum, dar fără a se limita la: managementul riscurilor cibernetice, securitatea rețelelor și a sistemelor informatice, prevenire, conștientizare și instruire de specialitate;

c) furnizarea unui pachet minim de servicii de tip CSIRT necesar asigurării unei protecții unitare a entităților esențiale și a entităților importante la nivel sectorial;

d) interconectarea la serviciul de alertă, monitorizare și cooperare al DNSC și să asigure un răspuns prompt la alertele și solicitările transmise de CSIRT național;

e) dispunerea de personal adecvat și calificat pentru a asigura disponibilitatea permanentă a serviciilor lor;

f) detectarea, prevenirea, combaterea și neutralizarea incidentelor, atacurilor și amenințărilor de securitate cibernetică din sectorul energetic cum sunt, dar fără a se limita la: Distributed Denial of Service, denumit în continuare DDoS, atacuri asupra lanțului de aprovizionare , Phishing și Spear Phishing care au ca țintă personalul infrastructurii energetice, Data Exfiltration, atacuri de tip Time Bomb Advanced, Firmware Tampering sau Insider Threat, Ransomware, atacuri de tip man-in-the- middle, Log-injection, Log-Tampering sau Log-Flooding, atacuri asupra SCADA/ICS, atac de tip Cyber-Physical, atacuri asupra sistemelor de control

și comunicații din sectorul energetic sau asupra sistemelor de facturare și gestionare a clienților;

g) sprijinirea și facilitarea managementului incidentelor cibernetice din cadrul entităților din sector, prin coordonarea strategică integrată a măsurilor de răspuns la incidente cibernetice la nivelul sectorului energetic;

h) gestionarea ciclului de viață al răspunsului la incidente cibernetice, de la identificare la rezoluție și analiză post-incident, la nivelul Ministerului Energiei și entităților aflate în subordine, coordonare și control, precum și la nivelul beneficiarilor proiectelor finanțate prin Fondul pentru Modernizare;

i) asigurarea de suport de specialitate pe parcursul întregului ciclu de viață al răspunsului la incidente cibernetice majore, de la identificare la rezoluție și analiză post incident, la nivelul sectorului energetic;

j) efectuarea analizei de tip Forensics în cazul unui incident major de securitate pentru a determina cauza și amploarea breșei;

k) gestionarea instrumentelor și tehnologiilor de securitate, inclusiv actualizări și corecții de securitate, denumite în continuare *patch-uri*, la nivelul Ministerului Energiei;

l) investigarea și analiza incidentelor de securitate cibernetică majore din sectorul energetic;

m) sprijinirea proceselor de recuperare și remediere post incident a rețelelor și sistemelor informatice din sectorul energetic;

n) recuperarea și remedierea post incident a rețelelor și sistemelor informatice din sectorul energetic, la nivelul Ministerului Energiei, al unităților aflate în subordinea sau sub autoritatea Ministerului Energiei sau ale altor organe de specialitate ale administrației publice centrale, al beneficiarilor proiectelor finanțate prin Fondul pentru Modernizare, al Centrului Național de Coordonare din cadrul Organismului intermediar pentru promovarea societății informaționale din cadrul Autorității pentru Digitalizarea României, precum și al oricăror persoane juridice de drept public sau privat din sectorul energetic național pentru care CRISCE îndeplinește funcția de CSIRT la nivel sectorial în domeniul energetic și resurselor energetice;

o) coordonarea dezvoltării mecanismelor tehnice și măsurilor de securitate cibernetică care protejează în mod unitar întregul sector energetic național;

p) comunicarea și raportarea amenințărilor, vulnerabilităților, riscurilor și atacurilor cibernetice către autoritățile prevăzute de art.10 din Legea nr.58/2023, respectiv altor autorități și instituții publice, conform competențelor legale, precum și societății civile, după caz;

q) monitorizarea și asigurarea răspunsului continuu la incidente, prin organizarea de echipe de permanență, asigurând astfel permanența operațională în regim 24/7;

r) colaborarea cu alte centre operaționale de securitate cibernetice, echipe de răspuns la incidente de securitate cibernetică și responsabili de securitate cibernetică, la nivel național și internațional, în vederea îmbunătățirii gradului de securitate;

s) elaborarea de strategii și proceduri de securitate cibernetică pentru sectorul energetic, sub coordonarea DNSC;

t) evaluarea periodică a eficacității măsurilor și controalelor de securitate cibernetică la nivelul Ministerului Energiei, al unităților aflate în subordinea sau sub autoritatea Ministerului Energiei sau ale altor organe de specialitate ale administrației publice centrale, al beneficiarilor proiectelor finanțate prin Fondul pentru Modernizare, precum și cu oricare alte persoane juridice de drept public sau privat din sectorul energetic național pentru care CRISCE îndeplinește funcția de CSIRT la nivel sectorial în domeniul energetic și resurselor energetice;

u) elaborarea și actualizarea continuă a politicilor și procedurilor interne de securitate cibernetică în Ministerul Energiei;

v) colectarea și analizarea informațiilor despre amenințările, riscurile și vulnerabilitățile emergente, precum și despre tehnologiile emergente relevante, pentru a preveni posibile atacuri cibernetice în sectorul energetic;

w) creșterea nivelului culturii, educației, conștientizării și igienei cibernetice în sectorul energetic;

x) coordonarea și monitorizarea proceselor și procedurilor de management al riscurilor de securitate cibernetică în sectorul energetic;

y) elaborarea de planuri și politici integrate de răspuns la incidente de securitate cibernetică la nivelul sectorului energetic;

z) monitorizarea implementării planurilor și politicilor de răspuns la incidente de securitate cibernetică la nivelul entităților din sectorul energetic;

aa) orice alte atribuții stabilite prin regulamentul de organizare și funcționare al CRISCE.

(3) În exercitarea funcției de autoritate competentă responsabilă cu îndeplinirea sarcinilor care îi sunt atribuite prin Regulamentul delegat (UE) 2024/1366 al Comisiei de completare a Regulamentului (UE) 2019/943 al Parlamentului European și al Consiliului prin stabilirea unui cod de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică, atribuțiile principale ale Ministerului Energiei sunt următoarele:

a) elaborarea, aprobarea, evaluarea și actualizarea metodologiilor și planurilor legate de securitatea cibernetică, realizarea controale minime și avansate, precum și emiterea de recomandări, inclusiv evaluările de risc și rapoartele în conformitate cu art.18, art.23, art.29, art.33-35 și art.37 alin.(1) lit.a) din Regulamentul delegat (UE) 2024/1366;

b) monitorizarea implementării și aplicării standardelor de securitate cibernetică în cooperare cu alte entități de profil și instituții europene, inclusiv ENISA;

c) consultarea și cooperarea cu autoritățile competente ale altor state membre, în vederea coordonării eficace a securității transfrontaliere a fluxurilor de energie electrică;

d) identificarea entităților cu impact ridicat și entităților cu impact critic din statul membru respectiv;

e) identificarea și clasificarea infrastructurilor critice, identificarea funcțiilor și serviciilor critice ale acestora, precum și documentarea lor;

f) elaborarea și comunicarea rapoartelor privind evaluările de risc către Comisia Europeană și alte instituții europene, în conformitate cu prevederile regulamentului;

g) dezvoltarea și implementarea de metodologii pentru monitorizarea continuă a amenințărilor cibernetice care pot afecta infrastructurile critice din sectorul energetic implicate în fluxurile transfrontaliere de energie, conform art.3 din Regulamentul delegat (UE) 2024/1366;

h) efectuarea de evaluări periodice ale riscurilor și vulnerabilităților cibernetice în conformitate cu art.5 din Regulamentul (UE) 2024/1366, incluzând, dar fără a se limita la, simulări și exerciții de testare a securității infrastructurilor energetice;

i) stabilirea de standarde minime de securitate pentru infrastructurile critice din sectorul energetic, bazate pe cerințele de la art.9 din Regulamentul (UE) 2024/1366, care includ, dar fără a se limita la, măsuri de protecție proactive și reactivă în fața atacurilor cibernetice;

j) coordonarea măsurilor de răspuns pentru a asigura o recuperare rapidă și eficientă în cazurile de atacuri cibernetice asupra infrastructurilor critice și notificarea incidentelor de securitate cibernetică în PNRISC, în condițiile capitolului IV, secțiunea 1 din Legea nr.58/2023 și a capitolului III, secțiunii a 4-a a capitolului V și a secțiunii 1 a capitolului VI din Ordonanța de urgență a Guvernului nr.155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil;

k) participarea la sistemul de alertă timpurie și cooperare la nivel european pentru a disemina alerte și informații relevante despre amenințările cibernetice, conform art.17 din Regulamentul (UE) 2024/1366;

l) menținerea interoperabilității cu alte autorități și instituții publice, persoane juridice de drept public și privat și echipe de răspuns la incidente cibernetice din Uniunea Europeană, astfel încât să se asigure o colaborare eficientă, în special pe aspecte de securitate transfrontalieră, în conformitate cu art.20 și 41 din Regulamentul (UE) 2024/1366;

m) organizarea de programe de instruire și conștientizare adresate angajaților din sectorul energetic pentru a îmbunătăți cultura de securitate cibernetică și pentru a asigura respectarea standardelor de securitate, potrivit art.24 și 25 din Regulamentul (UE) 2024/1366;

n) colaborarea cu furnizorii de tehnologii de securitate pentru a evalua conformitatea și eficiența acestora în contextul infrastructurilor critice din sectorul energetic, în acord cu art.34 și 39 din Regulamentul (UE) 2024/1366;

o) facilitarea procesului de certificare pentru infrastructurile critice din sectorul energetic, sprijinind operatorii economici în implementarea cerințelor de certificare prevăzute în Regulamentul (UE) 2019/881 privind securitatea cibernetică;

p) exercitarea oricăror alte competențe și atribuții conferite de Regulamentul (UE) 2024/1366 și legislația națională aplicabilă.

(4) Pentru îndeplinirea atribuțiilor principale prevăzute la alin.(1) și (2), specialiștii din cadrul CRISCE îndeplinesc, în principal, următoarele activități:

a) asigurarea disponibilității ridicate a canalelor de comunicații proprii, evitând punctele unice de defecțiune, dispunând de mai multe mijloace pentru a fi conectate și pentru a contacta alte entități în orice moment;

b) specificarea canalelor de comunicare prevăzute la lit.a) și aducerea la cunoștință a bazei de utilizatori și parteneri de cooperare;

c) menținerea sediilor și sistemelor informatice de suport în amplasamente securizate;

d) asigurarea unui sistem adecvat de gestionare și rutare a cererilor;

e) asigurarea confidențialității și credibilității activității CRISCE;

f) dispunerea de personal adecvat pentru a asigura disponibilitatea permanentă a serviciilor;

g) protejarea datelor confidențiale și sensibile ale beneficiarilor serviciilor lor de accesul neautorizat, sustragerea, alterarea sau distrugerea lor, prin măsuri tehnice și procedurale suficiente, adecvate și proporționale;

h) evaluarea și clasificarea incidentelor raportate în funcție de severitatea, impactul și urgența acestora, utilizând criterii predefinite și scoruri de risc pentru a asigura o prioritizare corectă a răspunsului;

i) recepționarea rapoartelor de incidente de securitate cibernetică de la entitățile din sectorul energetic, incluzând notificările automate generate de sistemele de detectare a intruziunilor și alertele transmise de personalul operativ;

j) colectarea și păstrarea dovezilor, artefactelor și amprentelor digitale relevante pentru investigarea incidentelor de securitate cibernetică, inclusiv loguri de sistem, capturi de trafic și artefacte malware;

k) efectuarea analizelor tehnice detaliate ale incidentelor pentru a identifica vectorii de atac, metodele utilizate de atacatori și vulnerabilitățile exploatate;

l) utilizarea de tehnici avansate de analiză comportamentală și de machine learning pentru a detecta activități anormale și a identifica atacurile persistente avansate, denumite în continuare *APT*, sub coordonarea directă a Serviciului Român de Informații, în acord cu art.14 alin.(2) lit.f) din Legea nr.58/2023;

m) desfășurarea de operațiuni și manevre cibernetice proactive și reactive, pentru a preveni și combate atacuri, amenințări, riscuri și vulnerabilități cibernetice la adresa sectorului energetic, al Ministerului Energiei, al unităților aflate în subordinea sau sub autoritatea Ministerului Energiei sau ale altor organe de specialitate ale administrației publice centrale, al beneficiarilor proiectelor finanțate prin Fondul pentru Modernizare, al Centrului Național de Coordonare din cadrul Organismului intermediar pentru promovarea societății informaționale din cadrul Autorității pentru Digitalizarea României, precum și al oricăror alte persoane fizice și juridice din sectorul energetic;

n) aplicarea de măsuri în timp real de izolare, pentru a limita răspândirea atacurilor și pentru a proteja activele critice, inclusiv segregarea segmentelor de rețea afectate și izolarea sistemelor compromise;

o) recuperarea și restabilirea funcționalității normale a sistemelor afectate, inclusiv restaurarea din backup-uri sigure și aplicarea de patch-uri de securitate;

p) desfășurarea de investigații de tip forensic detaliate pentru a analiza urmele lăsate de atacatori, a reconstrui evenimentele și a înțelege pe deplin mecanismele de atac utilizate; aceste investigații includ analizarea fișierelor de sistem, a memoriei și a altor artefacte digitale pentru a obține dovezi concrete ale atacurilor cibernetice;

q) elaborarea de rapoarte forensic detaliate care documentează toate dovezile colectate, metodele de analiză utilizate și concluziile investigației, oferind astfel suport legal și tehnic pentru eventuale acțiuni ulterioare;

r) monitorizarea continuă, în regim 24/7, a traficului de rețea și a activităților din sistemele IT, utilizând soluții avansate de securitate cibernetică, platforme pentru detectarea și răspunsul la incidente, analiză comportamentală, automatizare și orchestrare a proceselor, precum și tehnologii bazate pe inteligență artificială și machine learning;

s) analizarea și corelarea datelor din diverse surse de evenimente de securitate, incluzând loguri de sistem, alerte de securitate și fluxuri de trafic, pentru a identifica activitățile anormale și a detecta potențialele amenințări cibernetice;

t) utilizarea instrumentelor de inteligență artificială, învățare automată și inginerie socială pentru a identifica, preveni și a neutraliza amenințările cibernetice emergente și atacurile sofisticate;

u) trierea și clasificarea incidentelor de securitate cibernetică din sectorul energetic pe baza severității și impactului acestora asupra infrastructurii critice, asigurând prioritizarea corespunzătoare a răspunsului;

v) coordonarea răspunsului la incidente de securitate în colaborare cu echipele tehnice interne și externe din sectorul energetic, asigurându-se că toate acțiunile sunt documentate și că măsurile de răspuns sunt implementate eficient și sincronizat;

w) realizarea de investigații detaliate ale incidentelor de securitate pentru a identifica cauza rădăcină, vectorii de atac și impactul asupra sistemelor IT și datelor;

x) aplicarea măsurilor de remediere necesare pentru a elimina vulnerabilitățile exploatate și pentru a restabili funcționalitatea normală a sistemelor afectate, inclusiv patch-uri de securitate, actualizări de configurație și alte măsuri tehnice;

y) asigurarea comunicării clare și constante cu entitățile afectate din sectorul energetic, furnizând informații despre stadiul incidentului, măsurile de răspuns aplicate și recomandările pentru prevenirea incidentelor viitoare;

z) oferirea de suport și consultanță tehnică pentru proiectele de securitate cibernetică din sectorul energetic, asigurându-se că acestea sunt proiectate și implementate cu măsuri adecvate de securitate cibernetică;

aa) coordonarea cu echipele de administrare a sistemelor pentru a implementa patch-urile și actualizările necesare pentru a remedia vulnerabilitățile identificate, respectiv pentru aplicarea de măsuri de tipul apărare în profunzime, denumite în continuare *defense-in-depth*, sau de izolare, denumite în continuare ringed-fence acolo unde nu pot fi aplicate patch-uri;

bb) efectuarea de analize tehnice detaliate ale amenințărilor cibernetice identificate, incluzând analiza comportamentală și tehnică a malware-ului și altor vectori de atac;

cc) elaborarea de rapoarte detaliate despre incidentele de securitate cibernetică, incluzând descrierea tehnică a atacurilor, vectorilor de atac, impactului și măsurilor de remediere implementate, și transmiterea către autoritățile competente și alte părți interesate;

dd) organizarea de briefinguri periodice, din oficiu sau la cerere, pentru ministrul Energiei și alte părți relevante, informând despre starea securității cibernetice și incidentele recente;

ee) actualizarea politicilor și procedurilor de răspuns la incidente de securitate cibernetică, asigurându-se că acestea sunt aliniate cu standardele și reglementările naționale, europene și internaționale;

ff) dezvoltarea de planuri de continuitate și reziliență a sectorului energetic și de recuperare în caz de dezastru pentru a asigura revenirea rapidă la operare normală după un incident de securitate cibernetică;

gg) oferirea programe de training și conștientizare specializate pentru angajații Ministerului Energiei, entitățile și partenerii din sectorul energetic, axate pe răspunsul la incidente și pe bunele practici de securitate cibernetică;

hh) organizarea de simulări și exerciții periodice de răspuns la incidente pentru a testa și îmbunătăți capacitatea de răspuns și coordonarea în cadrul sectorului energetic;

ii) colaborarea cu alte echipe de răspuns la incidente de securitate cibernetică din țară și din străinătate pentru a partaja informații despre amenințări, riscuri și vulnerabilități și pentru a coordona răspunsul la incidente complexe și transfrontaliere;

jj) participarea activă în rețele naționale și internaționale de partajare a informațiilor despre amenințările cibernetice cum sunt, dar fără a se limita la, rețele Information Sharing and Analysis Centers, denumite în continuare *ISAC*, pentru a obține și a disemina informații critice despre amenințări și vulnerabilități;

kk) oferirea de suport tehnic și consultanță pentru entitățile din sectorul energetic în gestionarea incidentelor de securitate cibernetică și în implementarea măsurilor de prevenire și remediere a acestora;

ll) realizarea de evaluări de risc pentru proiectele și infrastructurile de securitate cibernetică din sectorul energetic, oferind recomandări pentru reducerea riscurilor identificate și pentru îmbunătățirea securității;

mm) efectuarea de teste de penetrare, atacuri și validări de securitate pentru a identifica vulnerabilitățile și pentru a verifica eficacitatea măsurilor de securitate implementate;

nn) implementarea și menținerea măsurilor de securitate interne riguroase pentru a proteja infrastructura și datele CRISCE de atacurile cibernetice; aceste măsuri includ, dar fără a se limita la, utilizarea de firewall-uri, dispersarea și izolarea punctelor și a terminalelor de lucru, sisteme de detectare și prevenire a intruziunilor, criptarea datelor și autentificarea multifactorială și alte asemenea;

oo) monitorizarea continuă a infrastructurii interne a CRISCE pentru a detecta și răspunde prompt la orice activități suspecte sau atacuri cibernetice care vizează echipa;

pp) realizarea de audituri și evaluări periodice de securitate pentru a identifica și remedia vulnerabilitățile din sistemele interne ale CRISCE;

qq) dezvoltarea și implementarea planurilor de continuitate și reziliență a activității și de recuperare în caz de dezastru pentru a asigura continuitatea operațională a CRISCE în cazul unui atac cibernetic;

rr) colaborarea loială cu autoritățile și instituțiile din sistemul național de ordine publică, apărare națională și securitate națională, precum și cu organele de urmărire penală în investigarea și răspunsul la incidentele de securitate cibernetică care implică săvârșirea de infracțiuni;

ss) analiza periodică a vulnerabilităților descoperite folosind instrumente specializate de identificare a punctelor slabe din rețelele și sistemele de securitate cibernetică ale sectorului energetic;

tt) evaluarea impactului potențial al vulnerabilităților identificate asupra securității și operațiunilor sectorului energetic, și prioritizarea acestora pentru remediere pe baza severității și riscului asociat, inclusiv elaborarea de proceduri operaționale și tehnice pentru a asigura conformitatea cu politicile de securitate cibernetică și pentru a proteja infrastructura critică din sectorul energetic;

uu) generarea de rapoarte despre incidentele de securitate și amenințările cibernetice, incluzând descrierea tehnică a atacurilor, vectorilor de atac, impactului și măsurilor de remediere implementate, și informarea periodică a conducerii Ministerului Energiei și a autorităților prevăzute la art.10 din Legea nr.58/2023 despre starea securității cibernetice din sectorul energetic;

vv) participarea la exerciții și conferințe de securitate cibernetică, comitete, comisii și consilii interinstituționale în domeniul securității cibernetice, respectiv al situațiilor de urgență, infrastructurilor critice, rezilienței și informațiilor clasificate cu componentă de securitate cibernetică;

ww) dezvoltarea şi actualizarea politicilor de securitate cibernetică pentru Ministerul Energie, unităţile aflate în subordinea sau sub autoritatea Ministerului Energiei sau ale altor organe de specialitate ale administraţiei publice centrale, beneficiarii proiectelor finanţate prin Fondul pentru Modernizare, precum şi cu oricare alte persoane juridice de drept public sau privat din sectorul energetic naţional pentru care CRISCE îndeplineşte funcţia de CSIRT la nivel sectorial în domeniul energetic şi resurselor energetice, asigurându-se că acestea sunt aliniate cu standardele naţionale şi internaţionale şi reflectă cele mai bune practici din domeniu;

xx) realizarea de audituri şi evaluări periodice şi ad-hoc, din oficiu sau la cerere, pentru a asigura conformitatea infrastructurii TIC şi a operaţiunilor din Ministerul Energiei, a beneficiarilor proiectelor finanţate prin Fondul pentru Modernizare, precum şi cu oricăror alte persoane juridice de drept public sau privat din sectorul energetic naţional pentru care CRISCE îndeplineşte funcţia de CSIRT la nivel sectorial în domeniul energetic şi resurselor energetice, cu procedurile de securitate cibernetică stabilite, în condiţiile secţiunii a 2-a a capitolului VII şi a capitolului VIII din Ordonanţa de urgenţă a Guvernului nr.155/2024 privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional civil;

yy) dezvoltarea şi livrarea de programe de training pentru angajaţii din sectorul energetic, axate pe conştientizarea securităţii cibernetice şi cele mai bune practici pentru prevenirea atacurilor cibernetice;

zz) organizarea de simulări şi exerciţii de răspuns la incidente pentru a testa şi îmbunătăţi capacitatea de răspuns a echipelor şi pentru a identifica eventualele lacune în planurile de răspuns;

aaa) dezvoltarea şi implementarea de planuri detaliate de răspuns la incidente pentru a izola, mitiga şi elimina ameninţările, vulnerabilităţile, riscurile şi atacurile identificate, asigurându-se că toate măsurile sunt documentate şi coordonate eficient;

bbb) contribuţia la dezvoltarea şi menţinerea parteneriatelor cu entităţi private pentru a partaja informaţii despre ameninţările cibernetice şi pentru a dezvolta soluţii comune de securitate;

ccc) orice alte activităţi stabilite prin legi speciale, regulamentul de organizare şi funcţionare al CRISCE.

(5) Pentru îndeplinirea atribuţiilor principale prevăzute la alin (3), Ministerul Energiei, prin specialiştii din cadrul CRISCE, desfăşoară, în principal, următoarele activităţi:

a) monitorizarea constantă a sistemelor şi infrastructurilor de securitate cibernetică din sectorul energiei electrice şi gaze naturale, pentru a detecta şi răspunde la ameninţările cibernetice;

b) colectarea și analizarea de informații despre potențiale atacuri cibernetice și alte riscuri pentru securitatea infrastructurilor critice;

c) implementarea și supravegherea măsurilor de atenuare a riscurilor identificate, în conformitate cu metodologiile aprobate;

d) coordonarea și schimbul de informații cu echipele CSIRT și alte autorități naționale și europene;

e) efectuarea de evaluări periodice ale riscurilor de securitate cibernetică în conformitate cu metodologiile aprobate;

f) dezvoltarea și actualizarea planurilor de continuitate operațională și de recuperare în caz de incidente majore;

g) organizarea de simulări și exerciții de testare a capacității de răspuns la incidente de securitate cibernetică;

h) elaborarea și prezentarea rapoartelor periodice către Comisia Europeană și alte instituții relevante;

i) asigurarea conformității cu standardele europene și internaționale aplicabile securității cibernetice în sectorul energiei;

j) participarea la forumuri și grupuri de lucru la nivel european pentru schimbul de bune practici în domeniul securității cibernetice;

k) identificarea și remedierea vulnerabilităților cibernetice raportate în infrastructurile critice de energie;

l) identificarea entităților critice care joacă un rol esențial în fluxurile transfrontaliere de energie electrică și clasificarea lor ca *entități cu impact ridicat* sau *entități cu impact critic* conform criteriilor stabilite de Regulamentul delegat (UE) 2024/1366 al Comisiei;

m) coordonarea proceselor de notificare a incidentelor de securitate cibernetică, asigurându-se că entitățile afectate raportează rapid și corect orice incident către autoritatea competentă, conform termenelor și procedurilor prevăzute de regulament;

n) stabilirea și implementarea unui cadru de colaborare interinstituțională între autoritățile naționale din domeniul energiei și securității cibernetice, pentru a asigura un răspuns coordonat la nivel național și european în caz de incidente;

o) evaluarea vulnerabilităților sistemelor digitale din infrastructura energetică și propunerea de măsuri pentru creșterea rezilienței acestor sisteme în fața amenințărilor cibernetice;

p) implementarea unor mecanisme de schimb de informații cu alte autorități naționale și europene, inclusiv utilizarea unor platforme dedicate pentru partajarea amenințărilor cibernetice și a indicatorilor de compromitere;

q) realizarea de teste și simulări pentru evaluarea capacităților de reacție la incidente cibernetice majore, inclusiv crize simultane care afectează fluxurile de energie electrică la nivel european;

r) asigurarea conformității cu cerințele de securitate impuse lanțului de aprovizionare din domeniul energiei, monitorizând respectarea cerințelor de securitate cibernetică de către furnizorii de echipamente și servicii TIC;

s) dezvoltarea condițiilor legale și procedurale pentru asigurarea securității cibernetice de-a lungul întregului lanț valoric și de aprovizionare din sectorul energetic;

t) monitorizarea implementării cerințelor tehnice și operaționale prevăzute în regulament pentru entitățile cu impact critic și cu impact ridicat, inclusiv revizuirea periodică a planurilor de securitate cibernetică și a rezultatelor auditului de securitate;

u) participarea la elaborarea și actualizarea metodologiilor de evaluare a riscurilor la nivel european, contribuind la dezvoltarea de noi standarde de securitate cibernetică adaptate la evoluțiile tehnologice din sectorul energetic;

v) participarea la gestionarea situațiilor de criză la nivel național, oferind suport și expertiză entităților afectate de atacuri cibernetice și coordonându-se cu alte autorități naționale și europene pentru a minimiza impactul asupra aprovizionării cu energie;

w) colaborarea și consultarea cu autoritățile și organismele relevante la nivel național, în scopul îndeplinirii obligațiilor relevante prevăzute de Regulamentul delegat (UE) 2024/1366;

x) cooperarea cu Agenția Uniunii Europene pentru Cooperarea Autorităților de Reglementare din Domeniul Energiei (ACER) și punerea la dispoziția acesteia a informațiilor necesare realizării sarcinilor prevăzute la art.17 din Regulamentul delegat (UE) 2024/1366 și a celorlalte obligații prevăzute în cadrul acestuia;

y) cooperarea cu Asociația Operatorilor de Transport și de Sistem din Energie Electrică din Europa, denumit în continuare *ENTSO-E,* cu Asociația Operatorilor de Distribuție din Europa, denumit în continuare EU-DSO, și cu alte organizații europene în acord cu prevederile Regulamentului delegat (UE) 2024/1366;

z) exercitarea oricăror alte activități conferite de Regulamentul delegat (UE) 2024/1366 al Comisiei și legislația națională aplicabilă.

(6) În exercitarea atribuțiilor și activităților, personalul CRISCE respectă și prevederile ordinelor și deciziilor directorului DNSC, în conformitate cu prevederile Ordonanța de urgență a Guvernului nr.104/2021, în sensul aplicării lor sectorului energetic.

(7) CRISCE nu efectuează auditul de securitate la un operator de servicii esențiale sau furnizor de servicii digitale în care Ministerul Energiei deține o participare la capitalul social al acestuia.

(8) În vederea exercitării atribuțiilor prevăzute la alin.(1) lit.f), alin.(2), lit.g), h), l), r), t), w), x), y) și z), alin.(3) lit.a), e), i) și j), alin.(4), lit.h) și u) și alin.(5) lit.a), b), c), q), r), s) și u), ministrul energiei și directorul DNSC emit ordine comune.

(9) Activitatea CRISCE se desfășoară în cel puțin un imobil special destinat, diferit de sediul Ministerului Energiei, care va avea cel puțin, dar fără a se limita la, următoarele dotări: sistem control- acces, monitorizare video, personal de securitate, baricade fizice, generatoare de rezervă și Uninterruptible Power Supply, sisteme de răcire și ventilație, rețele de comunicații redundante, sisteme de detectare a intruziunilor, sisteme de identificare conforme cu Regulamentul (UE) nr.910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, Security Information and Event Management, Managed Detection and Response, Decepție și honeypots avansate, Endpoint Detection and Response, Threat Intelligence Platforms, Cloud-native SIEMs, User and Entity Behavior Analytics, Extended Detection and Response, Security Orchestration, Automation, and Response, telefoane securizate, sisteme de videoconferință și alte mijloace de comunicare, servere și echipamente de stocare a datelor securizate, segmentarea rețelei, spațiu de gestionare a crizelor și echipamente specializate de securitate cibernetică.

(10) În vederea administrării adecvate a incidentelor majore la nivel național ori pentru administrarea unor incidente care necesită înaltă specializare și pregătire tehnică de specialitate, CRISCE poate dezvolta parteneriate și alcătui echipe mixte compuse din specialiști proprii și specialiști proveniți de la alte instituții ori entități din mediul privat, cu respectarea legii și asigurarea condițiilor privind confidențialitatea și accesul la informații în limitele legii și cu acordul părților implicate în incident.

Art.6.- (1) Prin derogare de la prevederile art.62 alin.(4) din Ordonanța de urgență a Guvernului nr.57/2019 privind Codul administrativ, cu modificările și completările ulterioare, organigrama, statul de funcții, regulamentul de organizare și funcționare al CRISCE se stabilesc prin ordin al ministrului energiei, care se publică în Monitorul Oficial al României, Partea I.

(2) Cheltuielile de înființare, organizare și funcționare, inclusiv cheltuielile de personal ale CRISCE, sunt cele prevăzute la art.8 alin.(2) din Ordonanța de urgență a Guvernului nr.60/2022 privind stabilirea cadrului

instituțional și financiar de implementare și gestionare a fondurilor alocate României prin Fondul pentru modernizare, precum și pentru modificarea și completarea unor acte normative, aprobată cu completări prin Legea nr.376/2024, cu modificările și completările ulterioare, și sunt finanțate exclusiv din dobânzile acumulate în conturile Ministerului Energiei aferente sumelor primite din Fondul pentru modernizare, precum și din venituri proprii.

(3) Prevederilor prezentei legi nu îi sunt aplicabile prevederile art.II-IV din Ordonanța de urgență a Guvernului nr.34/2023 privind unele măsuri fiscal-bugetare, prorogarea unor termene, precum și pentru modificarea și completarea unor acte normative, aprobată cu modificări și completări prin Legea nr.230/2023, cu modificările și completările ulterioare.

Art.7.- Prin derogare de Ia prevederile art.I alin.(1) și (4) din Ordonanța de urgență a Guvernului nr.156/2024 privind unele măsuri fiscal-bugetare în domeniul cheltuielilor publice pentru fundamentarea bugetului general consolidat pe anul 2025, de la prevederile art.1 alin.(3) și art.39 din Legea-cadru nr.153/2017, cu modificările și completările ulterioare, precum și de la legile anuale de salarizare a personalului plătit din fonduri publice, salarizarea personalului CIRSCE și celelalte drepturi de personal, inclusiv drepturile bănești și cheltuielile de cazare pentru perioada delegării și detașării în altă localitate sau în afara țării în interesul serviciului, se stabilesc prin ordin al ministrului energiei, prin utilizarea de date și informații asigurate de Inspecția Muncii, Institutul Național de Statistică sau alte surse externe care dețin astfel de analize, ținând cont de vechimea în muncă, experiența profesională, nivelul studiilor și a pregătirii profesionale.

Art.8.- (1) Ministerul Energiei, prin CRISCE, poate realiza venituri din prestații de servicii de securitate cibernetică, în limitele atribuțiilor și activităților prevăzute la art.5, persoanelor fizice și juridice de drept public sau privat din sectorul energetic.

(2) Serviciile și tarifele prevăzute la alin. (1) se stabilesc în baza unei metodologii de calcul realizată în baza unor standarde de cost stabilite prin ordin al ministrului energiei, cu avizul prealabil și conform al DNSC și al Consiliului Concurenței, care se publică în Monitorul Oficial al României, Partea I.

(3) Tarifele reglementate din sectorul energetic aferent costurilor cu auditul de securitate cibernetică, pentru serviciile prestate de CRISCE către operatorii economici se recuperează prin tarife de rețea sau alte mecanisme similare stabilite de prevederile legale aplicabile, potrivit Regulamentului delegat UE 2024/1366.

(4) Sumele încasate din sursele prevăzute la alin.(1) constituie venituri proprii ale activității finanțate integral din venituri proprii pe lângă Ministerul Energiei conform art.9 alin.(1) și vor fi folosite în conformitate cu prevederile bugetului de venituri și cheltuieli al ministerului, conform clasificației bugetare distincte, pentru funcționarea, organizarea și dezvoltarea CRISCE.

(5) Prin excepție de la prevederile alin.(1), prestarea serviciilor către Ministerul Energiei, unitățile din sectorul energetic aflate în subordinea sau sub autoritatea Ministerului Energiei sau ale altor organe de specialitate ale administrației publice centrale, beneficiarii proiectelor finanțate prin Fondul pentru Modernizare, către Centrul Național de Coordonare din cadrul Organismului intermediar pentru promovarea societății informaționale din cadrul Autorității pentru Digitalizarea României, precum și către operatorii naționali de transport al energiei electrice și al gazelor naturale se realizează cu titlu gratuit.

Art.9.- (1) Pentru înființarea, funcționarea, organizarea și dezvoltarea CRISCE se înființează pe lângă Ministerul Energiei o activitate finanțată integral din venituri proprii.

(2) Veniturile proprii ale activității prevăzute la alin.(1) se constituie din contravaloarea în lei a sumelor primite din prestarea serviciilor de securitate cibernetică prestate în temeiul art.8, precum și din dobânzile prevăzute la art.8 alin.(4^1) din Ordonanța de urgență a Guvernului nr.60/2022, aprobată cu completări prin Legea nr.376/2024, cu modificările și completările ulterioare, și virate în contul de venituri al activității deschis la Activitatea de Trezorerie și Contabilitate Publică a Municipiului București pe numele Ministerului Energiei și se aprobă la o subdiviziune distinctă de venituri bugetare și se înregistrează ca venituri ale bugetului respectiv la data transferului sumelor în Iei în contul de trezorerie.

(3) Cheltuielile aferente îndeplinirii activității prevăzute la alin.(1) se suportă din veniturile proprii prevăzute la alin.(2).

(4) Bugetul de venituri și cheltuieli pentru activitatea finanțată integral din venituri proprii prevăzută la alin.(1) se întocmește la venituri pe surse de proveniență, iar la cheltuieli după natura și destinația acestora, potrivit clasificației bugetare și se aprobă în subanexă distinctă la bugetul Ministerului Energiei.

(5) Excedentul anual rezultat din execuția bugetului de venituri și cheltuieli se reportează în anul următor și se utilizează cu aceleași destinații.

(6) Execuția de casă a bugetului de venituri și cheltuieli al activității prevăzute la alin.(1) se realizează prin Trezoreria Statului, conform prevederilor legale în vigoare.

(7) Ministerul Energiei implementează şi operaţionalizează CRISCE, care reprezintă infrastructură de securitate naţională, prin Regia Autonomă *Rasirom*, care are rolul de contractor- integrator, cu respectarea prevederilor Ordonanţei de urgenţă a Guvernului nr.114/2011 privind atribuirea anumitor contracte de achiziţii publice în domeniile apărării şi securităţii, aprobată cu modificări şi completări prin Legea nr.195/2012, cu modificările şi completările ulterioare.

Art.10.- (1) Ministerul Energiei, prin CRISCE, în situaţia în care solicită şi primeşte date şi informaţii de la orice persoană fizică şi juridică în temeiul prezentei legi ia măsuri adecvate pentru a proteja interesele de securitate şi comerciale ale acestora, ale persoanelor care furnizează datele şi informaţiile respective, precum şi ale persoanelor la care se referă datele şi informaţiile respective.

(2) Transmiterea de date şi informaţii obţinute potrivit prezentei legi de la orice persoană fizică şi juridică de drept public sau privat poate fi efectuată numai pentru îndeplinirea atribuţiilor legale ale CRISCE care obţine aceste date şi informaţii, cu garantarea păstrării confidenţialităţii datelor cu caracter personal şi a protecţiei intereselor şi secretelor de serviciu şi comerciale ale persoanelor fizice şi juridice de drept public şi privat

Art.11.- (1) Prelucrările de date cu caracter personal ce intră sub incidenţa prezentei legi se efectuează cu respectarea reglementărilor legale privind protecţia persoanelor fizice şi juridice în ceea ce priveşte prelucrarea datelor cu caracter personal.

(2) Notificările realizate în temeiul prezentei legi nu afectează obligaţiile operatorilor de date cu caracter personal stabilite potrivit art.33 şi 34 din Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor).

(3) În scopul îndeplinirii atribuţiilor ori furnizării serviciilor prevăzute de prezenta lege, precum şi în scopul prevenirii şi răspunsului la incidentele de securitate cibernetică ori al cooperării Ia nivel naţional, comunitar şi internaţional în prevenirea şi răspunsul la incidentele de securitate cibernetică, Ministerul Energiei, prin CRISCE, primeşte, prelucrează şi transmite date şi informaţii ce pot constitui sau pot conţine date cu caracter personal, în limitele legislaţiei aplicabile, cu asigurarea respectării prevederilor alin.(2).

Art.12.- Prezenta lege se completează cu prevederile corespunzătoare din Legea nr.58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative, cu modificările şi completările ulterioare, Ordonanţa de urgenţă a Guvernului nr.155/2024 privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional civil, precum şi cu Ordonanţa de urgenţă a Guvernului nr.104/2021 privind înfiinţarea Directoratului Naţional de Securitate Cibernetică, cu modificările şi completările ulterioare.

Art.13.- Ordonanţa de urgenţă a Guvernului nr.60/2022 privind stabilirea cadrului instituţional şi financiar de implementare şi gestionare a fondurilor alocate României prin Fondul pentru modernizare, precum şi pentru modificarea şi completarea unor acte normative, publicată în Monitorul Oficial al României, Partea I, nr.459 din 9 mai 2022, aprobată cu completări prin Legea nr.376/2024, cu modificările şi completările ulterioare, se modifică şi se completează după cum urmează:

1. **La articolul 8, alineatul 2 va avea următorul cuprins:**

„(2) Reprezintă cheltuieli administrative cheltuielile pentru informare, comunicare şi promovare referitoare la sprijinul şi rezultatele aferente Fondului pentru modernizare, precum şi cheltuielile privind organizarea şi funcţionarea structurilor de specialitate din cadrul Ministerului Energiei/organismelor delegate cu gestionarea finanţării investiţiilor din Fondul pentru modernizare, constând în:

a) cheltuieli privind asigurarea activităţii de management, de evaluare şi control pentru implementarea Fondului pentru modernizare;

b) cheltuieli pentru asistenţă tehnică, inclusiv pentru angajarea de personal în afara organigramei, pe perioadă determinată, în condiţiile procedurii reglementate prin Hotărârea Guvernului nr.234/2023 pentru aprobarea Regulamentului-cadru privind criteriile pe baza cărora se stabileşte procentul de majorare salarială pentru persoanele prevăzute la art.16 alin.(1) şi (2) din Legea-cadru nr.153/2017 privind salarizarea personalului plătit din fonduri publice, precum şi condiţiile de înfiinţare a posturilor în afara organigramei în cadrul instituţiilor şi/sau autorităţilor publice care implementează proiecte finanţate din fonduri europene nerambursabile şi/sau prin Mecanismul de redresare şi reziliență, respectiv pentru angajarea de personal în afara organigramei, în condiţiile de înfiinţare a posturilor pentru personalul Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie din cadrul Ministerului Energiei;

c) cheltuieli pentru consultanţă, inclusiv activităţile prevăzute la art.3 din Legea nr.51/1995 pentru organizarea şi exercitarea profesiei de avocat, republicată, cu modificările şi completările ulterioare;

d) cheltuieli cu personalul, inclusiv, dar fără a se limita la, salariile şi alte drepturi asimilate salariilor, sporuri, indemnizaţii, stimulente, cheltuieli cu selecţia şi evaluarea personalului, cheltuieli pentru asigurarea de programe de pregătire profesională la nivelul instituţiilor de învăţământ superior, cursuri, examene, certificări de specialitate, cheltuieli cu deplasările şi diurna;

e) cheltuieli cu spaţii de birouri şi clădiri, inclusiv achiziţia servicii de curăţenie, mobilier şi dotările necesare desfăşurării activităţii în condiţii optime, autovehicule şi utilităţi, precum şi orice alte tipuri de cheltuieli necesare desfăşurării activităţii;

f) cheltuieli pentru achiziţionarea şi/sau dezvoltarea şi/sau adaptarea de aplicaţii, soluţii şi servicii hardware şi software sau alte tipuri de echipamente TIC, după caz, inclusiv soluţii de tip cloud şi securitate cibernetică.

g) cheltuieli pentru informare, comunicare şi promovare referitoare la sprijinul şi rezultatele aferente Fondului pentru modernizare;

h) cheltuieli aferente susţinerii proiectelor pilot care promovează soluţii inovatoare pentru reducerea emisiilor de gaze cu efect de seră precum şi studii şi analize necesare dezvoltării proiectelor propuse la finanţare din Fondul pentru Modernizare;

i) cheltuieli pentru achiziţia de autovehicule şi pentru acoperirea costurilor de funcţionare şi exploatare a acestora;

j) cheltuielile de tipul celor prevăzute la lit.a)-i) pentru înfiinţarea, organizarea şi funcţionarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie din cadrul Ministerului Energiei."

2. La articolul 8, după alineatul (4) se introduce un nou alineat, alin.(4^1), cu următorul cuprins:

„(4^1) Cheltuielile administrative necesare înfiinţării, organizării şi funcţionării Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie din cadrul Ministerului Energiei sunt finanţate din dobânzile acumulate în conturile Ministerului Energiei."

3. La articolul 8, după alineatul (6), se introduce un nou alineat, alin.(7), cu următorul cuprins:

„(7) Prin derogare de la prevederile art.1 alin.(3) din Legea-cadru nr.153/2017, cu modificările şi completările ulterioare, la nivelul Ministerului Energiei/organismelor delegate se acordă stimulente financiare personalului

implicat în gestionarea, coordonarea şi controlul fondurilor puse la dispoziţie României prin Fondul pentru modernizare. Acestea vor fi considerate cheltuieli administrative, conform art.8 alin.(2) lit.d) şi vor fi decontate în baza art.8 alin.(4). Metodologia de acordare a stimulentelor financiare se aprobă prin ordin al ministrului energiei/act administrativ al conducătorului organismului delegat."

Art.14.- Alineatul (3) al articolului LXXVI din Legea nr.296/2023 privind unele măsuri fiscal-bugetare pentru asigurarea sustenabilităţii financiare a României pe termen lung, publicată în Monitorul Oficial al României, Partea I, nr. 977 din 27 octombrie 2023, cu modificările şi completările ulterioare, va avea următorul cuprins:

„(3) Curtea Constituţională, Curtea de Conturi, Avocatul Poporului, Administraţia Prezidenţială, Autoritatea Electorală Permanentă, Consiliul Economic şi Social, Consiliul Legislativ şi Ministerul Energiei, numai pentru înfiinţarea, organizarea şi funcţionarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie, nu aplică prevederile din capitolul III - Măsuri de disciplină economico-financiară, cu excepţia art.XXIV, XXVI şi XXVII, iar Autoritatea de Supraveghere Financiară nu aplică prevederile art.XVII din secţiunea 1 şi ale art.XLVII din secţiunea a 3-a ale capitolului III - Măsuri de disciplină economico-financiară."

Art.15.- (1) În vederea exercitării funcţiei prevăzute la alin.(2) lit.b), CRISCE va solicita autorizarea DNSC în maximum 120 de zile de la data intrării în vigoare a prezentei legi.

(2) Ordinul ministrului energiei prevăzut la art.3 alin.(1) pentru stabilirea numărului şi a tipurilor de posturi, precum şi a procedurii interne de recrutare şi selecţie se emite în maximum 45 de zile de la data intrării în vigoare a prezentei legi.

(3) Ordinul ministrului energiei prevăzut la art.3 alin.(2) privind desemnarea comisiei de concurs se emite în maximum 45 de zile de la data intrării în vigoare a prezentei legi şi cuprinde cuantumul indemnizaţiei fixe a membrilor comisiei.

(4) Ordinul ministrului energiei prevăzut la art.4 alin.(1) pentru aprobarea criteriilor şi procedurii de evaluare se emite în maximum 60 de zile de la data intrării în vigoare a prezentei legi.

(5) Ordinul ministrului energiei prevăzut la art.4 alin.(4) privind desemnarea comisiei de evaluare se stabileşte în maximum 60 de zile de Ia data intrării în vigoare a prezentei legi şi cuprinde cuantumul indemnizaţiei fixe a membrilor comisiei.

(6) Ordin comun al ministrului energiei şi al directorului DNSC prevăzut la art.5 alin.(1) lit.d) se emite în termen de 90 de zile de la data intrării în vigoare a prezentei legi.

(7) Ordinele ministrului energiei prevăzut la art.6 alin.(1) privind stabilirea organigramei, statului de funcţii şi a regulamentului de organizare şi funcţionare şi procedurile interne ale CRISCE se emit în maximum 45 de zile de la data intrării în vigoare a prezentei legi.

(8) Ordinul ministrului energiei prevăzut la art.7 alin.(1) se emite în maximum 45 de zile de la data intrării în vigoare a prezentei legi.

(9) Ordinul ministrului energiei prevăzut la art.8 alin.(2) se emite în maximum 90 de zile de la data intrării în vigoare a prezentei legi.

Art.16.- Ordinul ministrului energiei/actul administrativ al conducătorului organismului delegat pentru aprobarea Metodologiei de acordare a stimulentelor financiare prevăzută la art.8 alin.(7) din Ordonanţa de urgenţă a Guvernului nr.60/2022 privind stabilirea cadrului instituţional şi financiar de implementare şi gestionare a fondurilor alocate României prin Fondul pentru modernizare, precum şi pentru modificarea şi completarea unor acte normative, aprobată cu completări prin Legea nr.376/2024, cu modificările şi completările ulterioare, inclusiv cu cele aduse prin prezenta lege, se emite în termen de 10 zile de la data intrării în vigoare a prezentei legi

Art.17.- Prevederile art. XX - XXII din Ordonanţa de urgenţă a Guvernului nr.107/2024 pentru reglementarea unor măsuri fiscal-bugetare în domeniul gestionării creanţelor bugetare şi a deficitului bugetar pentru bugetul general consolidat al României în anul 2024, precum şi pentru modificarea şi completarea unor acte normative nu se aplică în cazul Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie.

Art.18.- Prevederile art.I-II, IV, VI, VII şi XV din Ordonanţa de urgenţă a Guvernului nr.156/2024 privind unele măsuri fiscal-bugetare în domeniul cheltuielilor publice pentru fundamentarea bugetului general consolidat pe anul 2025, pentru modificarea şi completarea unor acte normative, precum şi pentru prorogarea unor termene, nu se aplică în cazul Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie din cadrul Ministerului Energiei.

Acest proiect de lege se consideră adoptat de Senat în forma inițială, în condițiile articolului 75 alineatul (2) teza a III-a din Constituția României, republicată.

p. PREȘEDINTELE SENATULUI

MIHAI COTEȚ