GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din 5 martie 2025

Chișinău

Pentru modificarea unor hotărâri ale Guvernului
(modificarea actelor normative subsidiare în conformitate
cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe)

Guvernul HOTĂRĂŞTE:

1. Hotărârea Guvernului nr. 1206/2016 cu privire la Centrul Național de Coordonare Integrată a Acțiunilor de Ordine Publică (Monitorul Oficial al Republicii Moldova, 2016, nr. 379-386, art. 1303), cu modificările ulterioare, se modifică după cum urmează:

1.1. în anexa nr. 2, după cuvintele „Administrația Națională a Penitenciarelor” se introduc cuvintele „Agenția pentru Securitate Cibernetică”;

1.2. în anexa nr. 3, după cuvintele „Directorul adjunct al Administrației Naționale a Penitenciarelor” se introduc cuvintele „Directorul Agenției pentru Securitate Cibernetică”.

2. Regulile privind prestarea serviciilor poștale, aprobate prin Hotărârea Guvernului nr. 1457/2016 (Monitorul Oficial al Republicii Moldova, 2017, nr. 24-29, art. 46), cu modificările ulterioare, se modifică după cum urmează:

2.1. punctul 4 se completează cu subpunctul 4^1) cu următorul cuprins:

„4^1) securitatea rețelelor și sistemelor informatice utilizate la prestarea serviciilor poștale și, dacă sunt incluși în Lista furnizorilor de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, să îndeplinească obligațiile de asigurare a securității cibernetice stabilite de legea respectivă”;

2.2. se completează cu punctul 136^1 cu următorul cuprins:

„**136^1.** Agenția pentru Securitate Cibernetică exercită funcția de supraveghere și control de stat asupra respectării de către furnizorii de servicii poștale incluși în Lista furnizorilor de servicii a obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, conform prevederilor Legii nr. 131/2012 privind controlul de stat.

Furnizorii de servicii poștale incluși în Lista furnizorilor de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică sunt obligați să asigure accesul Agenției pentru Securitate Cibernetică la informațiile, bunurile și încăperile deținute de aceștia, care sunt necesare pentru realizarea obiectivelor controlului.”

3. La punctul 8 subpunctul 34) din Statutul Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică”, aprobat prin Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat (Monitorul Oficial al Republicii Moldova, 2018, nr. 157-166, art. 474), cu modificările ulterioare, cuvintele „Centrul guvernamental de reacție la incidente de securitate cibernetică” se substituie cu cuvintele „Centrul guvernamental de răspuns la incidentele cibernetice”.

4. Regulamentul privind modul de utilizare a platformei de interoperabilitate (MConnect), aprobat prin Hotărârea Guvernului nr. 211/2019 (Monitorul Oficial al Republicii Moldova, 2019, nr. 132-138, art. 254), cu modificările ulterioare, se modifică după cum urmează:

4.1. punctul 6:

4.1.1. la subpunctul 14), textul „ , inclusiv” se substituie cu cuvântul „și”;

4.1.2. la subpunctul 15), după cuvintele „precum și pentru” se introduc cuvintele „prevenirea și”;

4.2. la punctul 8 subpunctul 19), după cuvintele „și pentru” se introduc cuvintele „prevenirea și”.

5. Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat (Monitorul Oficial al Republicii Moldova, 2020, nr. 180-187, art. 614) se modifică după cum urmează:

5.1. în hotărâre:

5.1.1. pe tot parcursul textului:

5.1.1.1. cuvintele „incident de securitate cibernetică”, la orice formă gramaticală, se substituie cu cuvintele „incident cibernetic”, la forma gramaticală corespunzătoare;

5.1.1.2. cuvintele „Centrul guvernamental de reacție la incidente de securitate cibernetică” se substituie cu cuvintele „Centrul guvernamental de răspuns la incidentele cibernetice”;

5.2. în anexă:

5.2.1. pe tot parcursul textului, cuvintele „incident de securitate cibernetică”, la orice formă gramaticală, se substituie cu cuvintele „incident

cibernetic”, la forma gramaticală corespunzătoare;

5.2.2. la punctul 3, textul „*incident de securitate cibernetică* – eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică” se substituie cu textul „*incident cibernetic* – astfel cum este definit la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică.”;

5.2.3. punctul 5:

5.2.3.1. la subpunctul 8), cuvintele „incidente de securitate informațională” se substituie cu cuvintele „incidente cibernetice”;

5.2.3.2. la subpunctul 12), cuvintele „sistemelor informaționale și a rețelelor” se substituie cu cuvintele „rețelelor și a sistemelor informatice”;

5.2.3.3. subpunctul 14) va avea următorul cuprins:

„14) furnizează imediat furnizorilor de servicii persoane juridice de drept public care au notificat un incident cibernetic un răspuns care să cuprindă recomandări și instrucțiuni operaționale privind punerea în aplicare a măsurilor necesare pentru soluționarea incidentului respectiv”;

5.2.3.4. la subpunctul 16), cuvintele „platforme de management al incidentelor cibernetice și schimbului de informații” se substituie cu cuvintele „platforme guvernamentale de management al incidentelor cibernetice”;

5.2.3.5. se completează cu subpunctele 16^1)-16^4) cu următorul cuprins:

„16^1) asigură securitatea rețelelor și a sistemelor informatice proprietate a statului la nivel guvernamental;

16^2) notifică echipa de răspuns la incidentele cibernetice la nivel național și informează cu privire la incidentele cibernetice notificate de furnizorii de servicii persoane juridice drept public, în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică;

16^3) facilitează interacțiunea dintre furnizorii de servicii persoane juridice drept public și Agenția pentru Securitate Cibernetică, precum și echipa de răspuns la incidentele cibernetice la nivel național, asigurând îndeplinirea de către acestea a obligațiilor privind securitatea cibernetică stabilite de Legea nr. 48/2023 privind securitatea cibernetică;

16^4) cooperează cu echipa de răspuns la incidentele cibernetice la nivel național, inclusiv în cadrul unei platforme de management al incidentelor cibernetice și pentru schimbul de informații”;

5.2.3.6. la subpunctul 18), după cuvintele „Serviciul de Informații și Securitate al Republicii Moldova” se introduc cuvintele „și Agenția pentru Securitate Cibernetică”;

5.2.4. se completează cu punctul 6^1 cu următorul cuprins:

„**6^1.** Notificarea incidentelor cibernetice cu impact semnificativ de către CERT Gov către echipa de răspuns la incidentele cibernetice la nivel național (în continuare – *CSIRT național)* nu exclude dreptul entităților publice de a notifica și CSIRT-ul național cu privire la incidentele cibernetice.”;

5.2.5. la punctul 7 subpunctul 1), cuvintele „necesare pentru asigurarea securității cibernetice” se substituie cu cuvintele „tehnice și organizatorice pentru

gestionarea riscurilor de securitate a rețelelor și a sistemelor informatice pe care le utilizează”;

5.2.6. punctul 8 va avea următorul cuprins:

„**8.** Instituția Publică «Serviciul Tehnologia Informației și Securitate Cibernetică» va crea și asigura funcționarea unei platforme guvernamentale de management al incidentelor cibernetice.”;

5.2.7. punctul 11 subpunctul 3) se completează cu litera a[1]) cu următorul cuprins:

„a[1]) notificarea CSIRT-ului național, în condițiile stabilite de Legea nr. 48/2023 privind securitatea cibernetică, cu privire la:

– incidentele cibernetice cu impact semnificativ asupra securității rețelelor sau a sistemelor informatice ale statului ori asupra continuității serviciilor;

– incidentele cibernetice al căror impact semnificativ asupra securității rețelelor sau a sistemelor informatice ale statului ori asupra continuității serviciilor nu este evident, dar poate fi presupus în mod rezonabil;

– impactul semnificativ al unui incident cibernetic care a afectat un terț asupra continuității serviciului prestat de persoanele juridice de drept public, în cazul în care serviciul respectiv depinde de serviciile terțului afectat”;

5.2.8. punctul 12 se completează cu cuvintele „și cu Agenția pentru Securitate Cibernetică”.

6. Programul național de securitate în domeniul aviației civile, aprobat prin Hotărârea Guvernului nr. 124/2021 (Monitorul Oficial al Republicii Moldova, 2021, nr. 212-218, art. 365), cu modificările ulterioare, se modifică după cum urmează:

6.1. la punctele 557[1] și 557[2], textul „STISC” se substituie cu cuvintele „Agenția pentru Securitate Cibernetică”;

6.2. se completează cu punctele 560[1] și 560[2] cu următorul cuprins:

„**560[1].** Operatorii aeroportuari, transportatorii aerieni, FSNA și alte entități definite în prezentul Program trebuie să asigure securitatea rețelelor și a sistemelor informatice utilizate la prestarea serviciilor și, dacă sunt incluși în Lista furnizorilor de servicii în sectoarele și subsectoarele critice conform Legii nr. 48/2023 privind securitatea cibernetică, să îndeplinească obligațiile privind asigurarea securității cibernetice stabilite de legea respectivă.

560[2]. Agenția pentru Securitate Cibernetică exercită funcția de supraveghere și control de stat asupra respectării de către operatorii aeroportuari, transportatorii aerieni, FSNA și alte entități definite în prezentul Program incluși în Lista furnizorilor de servicii a obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat. Aceștia sunt obligați să asigure accesul Agenției pentru Securitate Cibernetică la informațiile, bunurile și încăperile deținute, necesare pentru realizarea obiectivelor controlului.”

7. Regulamentul sanitar privind supravegherea și monitorizarea calității apei potabile, aprobat prin Hotărârea Guvernului nr. 651/2023 (Monitorul Oficial al Republicii Moldova, 2023, nr. 387-390, art. 928) se completează cu punctele 73 și 74 cu următorul cuprins:

„**73.** Furnizorii de apă potabilă trebuie să asigure securitatea rețelelor și a sistemelor informatice utilizate la prestarea serviciilor și, dacă sunt incluși în Lista furnizorilor de servicii în sectoarele și subsectoarele critice conform Legii nr. 48/2023 privind securitatea cibernetică, să îndeplinească obligațiile privind asigurarea securității cibernetice stabilite de legea respectivă.

74. Agenția pentru Securitate Cibernetică exercită funcția de supraveghere și control de stat asupra respectării de către furnizorii de apă potabilă incluși în Lista furnizorilor de servicii a obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat. Aceștia sunt obligați să asigure accesul Agenției pentru Securitate Cibernetică la informațiile, bunurile și încăperile deținute, necesare pentru realizarea obiectivelor controlului.”

8. Ministerul Dezvoltării Economice și Digitalizării, în comun cu Agenția pentru Securitate Cibernetică și Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, va analiza și va prezenta, în termen de trei luni de la data publicării prezentei hotărâri în Monitorul Oficial al Republicii Moldova, propuneri privind stabilirea și delimitarea competențelor și responsabilităților aferente exercitării atribuțiilor de posesor și deținător al Registrului de stat al incidentelor de securitate cibernetică, în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică și va înainta propuneri pentru modificarea Hotărârii Guvernului nr. 388/2022 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică”.

9. Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

Prim-ministru **DORIN RECEAN**

Contrasemnează:

Viceprim-ministru,
ministrul dezvoltării
economice și digitalizării Dumitru ALAIBA

NOTA DE FUNDAMENTARE
la proiectul de hotărâre de Guvern pentru modificarea unor hotărâri ale Guvernului (aducerea actelor normative subsidiare în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe)

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ
Proiectul a fost elaborat de Ministerul Dezvoltării Economice și Digitalizării, cu suportul proiectului „Asistență rapidă Republicii Moldova în domeniul securității cibernetice”, finanțat de Comisia Europeană și implementat de Academia de Guvernare Electronică din Estonia.
2. Condițiile ce au impus elaborarea proiectului actului normativ
2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ
Articolul 23 al.(1) lit. c) din Legea nr. 48/2023 privind securitatea cibernetică stabilește obligația Guvernului de a aduce actele sale normative în concordanță cu legea în cauză.
2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative
La 16 martie 2023, Parlamentul a adoptat Legea nr. 48/2023 privind securitatea cibernetică, ce urmează să intre în vigoare la 1 ianuarie 2025. Scopul principal al acestei legi este de a asigura legalitatea în spațiul cibernetic prin reglementarea principalelor elemente indispensabile implementării unui model de guvernanță eficient la nivel național în vederea protecției și asigurării securității rețelelor și sistemelor informatice, utilizate de către persoanele juridice, publice sau private, în procesul de prestare a serviciilor considerate a fi esențiale pentru susținerea unor activități societale și economice critice. Un element juridic fundamental în procesul de reglementare a acestui domeniu a fost legislația Uniunii Europene, mai ales având în vedere statutul de țară candidat la aderarea la Uniunea Europeană al Republicii Moldova. Prin această lege s-a urmărit, deși doar parțial, armonizarea cadrului normativ național cu prevederile Directivei NIS2 (Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148) și implicit, cu elementele esențiale ale Directivei NIS1 (Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune). Astfel, Legea privind securitatea cibernetică cuprinde un set de reglementări care au ca scop în principal: • stabilirea cadrului general privind cooperarea și coordonarea strategică la nivel național și internațional, prin reglementarea expresă a constituirii unui consiliul coordonator cu rol consultativ al Guvernului, dedicat exclusiv domeniului securității cibernetice și stabilirea obligativității adoptării unei strategii naționale în acest domeniu; • desemnarea/instituirea de către Guvern a unei autorități competente în domeniul securității cibernetice la nivel național, care să includă în competența sa, de rând cu funcțiile de coordonare, cooperare internă, supraveghere și control de stat, și pe cele de echipă națională de răspuns la incidentele cibernetice și de punct unic de contact la nivel național; • reglementarea legală primară a procesului de coordonare și gestionare a crizelor în domeniul securității cibernetice și atribuirea competenței legale în această materie viitoarei autorități responsabile; • stabilirea cadrului legal primar în ce privește obligațiile de asigurare a securității cibernetice nu doar de către persoanele juridice de drept public, ci și de către cele de drept privat, în mod special în ce privește obligațiile de implementare a măsurilor de securitate și

în ce privește obligațiile de notificare a incidentelor cibernetice semnificative, și împuternicirea autorității competente la nivel național în acest domeniu cu exercitarea funcțiilor de supraveghere și control de stat al modului în care persoanele vizate îndeplinesc aceste obligații;

- determinarea cadrului normativ primar pentru identificarea persoanelor juridice ca fiind furnizori de servicii esențiale, împuternicire atribuită de asemenea autorității respective, ca parte componentă a funcției de supraveghere etc. Potrivit prevederilor Legii privind securitatea cibernetică, Guvernul este învestit cu competență de intervenție, de diferită natură (normativă, organizatorică și tehnică), pe un șir de chestiuni în vederea punerii în aplicare a prevederilor acesteia, dintre care în mod special ținem să le evidențiem pe cele care sunt pertinente obiectului de reglementare a proiectului propus spre avizare și anume:
- aprobarea listei sectoarelor, subsectoarelor și, respectiv, a tipurilor și categoriilor de persoane juridice care prestează servicii în aceste sectoare și/sau subsectoare și care vor cădea sub incidența prevederilor legii și a cadrului metodologic de identificare a acestora (art. 4 alin. (2));
- desemnarea/constituirea, reglementarea modului de organizare și funcționare, a structurii și efectivului-limită a entității care va exercita funcțiile autorității competente (art. 7 alin. (1));
- modul de aplicare a măsurilor de supraveghere de către autoritatea competentă (art. 18 alin. (5));
- modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin conform Legii privind securitatea cibernetică (art. 19 alin. (5)). Suplimentar, la 21 martie 2024, a fost aprobat în a doua lectură proiectul de lege pentru modificarea unor acte normative (modificarea cadrului legal în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică). Legea nr. 58/2024 pentru modificarea unor acte normative are ca obiectiv general să aducă în concordanță cu Legea privind securitatea cibernetică prevederile legale existente. Intervențiile propuse prin respectiva inițiativă legislativă constau în principal în următoarele:
- asigurarea interconexiunii dintre normele Legii privind securitatea cibernetică și cele cuprinse în legile sectoriale care reglementează activitatea viitorilor furnizori de servicii și eliminarea/revizuirea unor prevederi care ar putea suscita interpretări echivoce sau contradictorii în procesul aplicării legii;
- finalizarea instituirii cadrului normativ primar necesar stabilirii modelului de guvernanță în domeniul securității cibernetice la nivel național.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul de hotărâre de Guvern are ca obiectiv general aducerea în concordanță a hotărârilor de Guvern cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe. În acest context, finalitățile urmărite prin adoptarea actului normativ sunt determinate de diferitele categorii de intervenții normative propuse în proiect și constau, în principal, în următoarele:

- Alinierea cadrului normativ secundar care stabilește rigori în domeniul securității cibernetice la măsurile de securitate stabilite de Legea nr. 48/2023 privind securitatea cibernetică;
- Revizuirea unor prevederi din hotărârile de guvern sectoriale care ar putea suscita interpretări echivoce sau contradictorii în aplicarea Legii privind securitatea cibernetică și legislației sectoriale care reglementează activitatea viitorilor furnizori de servicii.

În proiectul de hotărâre de Guvern sunt propuse modificări la 7 hotărâri de Guvern, care pot fi divizate, în funcție de factorii ce le determină, finalitățile pe care le urmăresc și efectele pe care le vor produce, în următoarele categorii:

1. Prima categorie de modificări propuse în proiect (pct. 5) constau în necesitatea alinierii cadrului normativ secundar care stabilește rigori în domeniul securității cibernetice la măsurile de securitate stabilite de Legea nr. 48/2023 privind securitatea cibernetică.
Modificările propuse vizează Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat și au ca obiectiv corelarea prevederilor acesteia cu prevederile Legii privind securitatea cibernetică în partea ce vizează obligațiile de notificare a Agenției pentru Securitate Cibernetică. Adițional, reieșind din faptul că desemnarea unei autorități competente la nivel național în domeniul securității cibernetice este o entitate nouă cu domenii noi de competențe, se propune completarea normelor care stabilesc obligativitatea cooperării CERT Gov inclusiv cu Agenția pentru Securitate Cibernetică și nemijlocit echipa de răspuns la incidentele cibernetice la nivel național, precum și remiterea raportului privind riscurile și incidentele de securitate cibernetică identificate, măsurile întreprinse și planificate pentru remedierea acestora în adresa Agenției pentru Securitate Cibernetică. Recepționarea și analiza raportului respectiv, va permite Agenției să-și realizeze atât funcția de cercetare și dezvoltare a acesteia, cât și celelalte funcții care sunt stabilite în competența acesteia prin Regulamentul de organizare și funcționare a Agenției pentru Securitate Cibernetică, aprobat prin Hotărârea Guvernului nr. 1028/2023.
Totodată, sunt corelate funcțiile CERT Gov din Hotărârea de Guvern cu cele stabilite în Legea nr. 48/2023. Suplimentar, se propune ajustarea terminologiei și noțiunile la cele stabilite de Legea privind securitatea cibernetică, nemijlocit incidente cibernetice și Centrul guvernamental de răspuns la incidentele cibernetice.
2. A doua categorie de modificări se referă nemijlocit la terminologie, vizând pct. 3. Această hotărâre de Guvern operează cu o terminologie diferită decât cea care se utilizează în Legea nr. 48/2023 privind securitatea cibernetică. În acest sens, se propun substituirea sintagmelor „Centrul guvernamental de reacție la incidente de securitate cibernetică” cu „Centrul guvernamental de răspuns la incidentele cibernetice”.
3. A treia categorie vizează hotărârile de Guvern de la punctele 2, 6 și 7 și rezidă în alinierea și completarea hotărârilor de Guvern sectoriale cu Legea nr. 48/2023 privind securitatea cibernetică și legile care au ca obiect de reglementare a activități din domenii și subdomenii, corespondente sectoarelor sau subsectoarelor enumerate în anexele I și II ale Directivei NIS2 și pentru care au fost operate modificări prin Legea nr. 58/2024 pentru modificarea unor acte normative (modificarea cadrului legal în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică). Aceste modificări vin cu completări la prevederile generale privind limitele competenței de supraveghere și control, ce urmează a fi exercitată de Agenția pentru Securitate Cibernetică, și obligațiile exprese de asigurare a securității cibernetice de către diferitele categorii de furnizori de servicii.
4. Suplimentar, în proiectul de hotărâre de Guvern se include un punct tranzitoriu ce vizează Registrul de stat al incidentelor de securitate cibernetică. Astfel, se stabilește în sarcina Ministerul Dezvoltării Economice și Digitalizării, în comun cu Agenția pentru Securitate Cibernetică și Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, de a analiza și prezenta, în termen de 3 luni de la data publicării hotărârii de Guvern, propuneri privind determinarea și delimitarea competenței și responsabilităților în ce privește exercitarea atribuțiilor de posesor și deținător al Registrului de stat al incidentelor de securitate cibernetică în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică și corespunzător de modificare a Hotărârii Guvernului nr. 388/2022 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică”.
5. O altă intervenție vizează modificarea Hotărârii Guvernului nr. 1206/2016 privind Centrul Național de Coordonare Integrată a Acțiunilor de Ordine Publică. Se propune completarea

Listei autorităților publice reprezentate în cadrul Centrului, precum și a componenței Consiliului de decizie, prin includerea Agenției pentru Securitate Cibernetică și, respectiv, a Directorului Agenției în componența Consiliului. Această modificare este propusă ca urmare a analizei cadrului național de gestionare a crizelor. În contextul funcțiilor Agenției pentru Securitate Cibernetică, care sunt direct corelate cu ordinea publică și securitatea statului, se consideră imperativă includerea acesteia în platformele de coordonare integrată a acțiunilor de ordine publică.
3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare
Opțiunile alternative nu există deoarece la nivel de lege este stabilită obligația alinierii cadrului normativ secundar care stabilește rigori în domeniul securității cibernetice la măsurile de securitate stabilite de Legea nr. 48/2023 privind securitatea cibernetică.
4. Analiza impactului de reglementare
4.1. Impactul asupra sectorului public
Proiectul nu presupune careva reforme structurale sau instituționale.
4.2. Impactul financiar și argumentarea costurilor estimative
Implementarea prevederilor proiectului nu necesită alocarea resurselor financiare suplimentare de la bugetul de stat.
4.3. Impactul asupra sectorului privat
Proiectul vine să completeze inițiativa de legiferare realizată prin Legea nr. 48/2023 privind securitatea cibernetică și legile conexe, având ca obiectiv primordial alinierea cadrului normativ secundar la legislația primară. Respectiv, proiectul nu impune careva obligații suplimentare pentru sectorul privat decât cele stabilite prin Legea nr. 48/2023 privind securitatea cibernetică.
4.4. Impactul social 4.4.1. Impactul asupra datelor cu caracter personal 4.4.2. Impactul asupra echității și egalității de gen
Nu este aplicabil
4.5. Impactul asupra mediului
Nu este aplicabil
4.6. Alte impacturi și informații relevante
Nu este aplicabil
5. Compatibilitatea proiectului actului normativ cu legislația UE
5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională
Nu este aplicabil
5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE
Proiectul de hotărâre de Guvern are ca obiectiv aducerea în concordanță a hotărârilor de Guvern cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe. Legea nr. 48/2023 privind securitatea cibernetică a transpus parțial prevederile Directivei NIS2 (Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148).
6. Avizarea și consultarea publică a proiectului actului normativ
În conformitate cu prevederile art. 9 din Legea nr. 239/2008 privind transparența în procesul decizional pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării mded.gov.md și pe platforma de consultare particip.gov.md, la data de 2 mai 2024 a fost publicat anunțul referitor la inițierea procesului de elaborare a proiectului de

hotărâre de Guvern (link de acces - https://particip.gov.md/ro/document/stages/anunt-de-initiere-a-procesului-de-elaborare-a-proiectului-hotararii-guvernului-pentru-modificarea-unor-hotarari-ale-guvernului-aducerea-actelor-normative-subsidiare-in-concordanta-cu-legea-nr-482023-privind-securitatea-cibernetica-si-legile-conexe/12512), iar anunțul de consultare publică a proiectului a fost publicat la data de 16 iulie 2024 (link de acces - https://particip.gov.md/ro/document/stages/*/12836).

Totodată, proiectul a fost supus procesului de avizare cu elaborarea Sintezei obiecțiilor și propunerilor.

7. Concluziile expertizelor

Proiectul a fost remis conform procedurii legale Centrului Național Anticorupție pentru efectuarea expertizei anticorupție a acestuia, care a constatat că proiectul nu conține factori de risc care să genereze apariția riscurilor de corupție.

Proiectul a fost supus expertizei juridice și modificat corespunzător.

Proiectul nu cade sub incidența analizei impactului de reglementare, dat fiind faptul că nu reglementează activitatea de întreprinzător. Prin urmare, proiectul nu cade sub incidența Metodologiei de analiză a impactului în procesul de fundamentare a proiectelor de acte normative, aprobată prin Hotărârea Guvernului nr. 23/2019.

8. Modul de încorporare a actului în cadrul normativ existent

Proiectul elaborat se încadrează în prevederile cadrului normativ în vigoare, respectiv aprobarea acestuia nu implică necesitatea modificării altor acte normative. Totodată, având în vedere amploarea efectelor pe care le va avea proiectul de hotărâre de Guvern și modificările propuse prin Legea nr. 58/2024 pentru modificarea unor acte normative, este important ca autoritățile administrației publice centrale de specialitate, responsabile de realizarea politicii statului în domeniile reglementate de actele normative propuse spre adoptare, să efectueze o evaluare a actelor normative ale acestora în vederea identificării necesității de revizuire a acestora.

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Măsurile de bază necesare pentru implementarea prevederilor proiectului constau în următoarele aspecte:

În partea ce ține de implementarea modificărilor la Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat, CERT Gov urmează să asigure:

- furnizarea entităților publice care au notificat un incident cibernetic imediat a unui răspuns cu privire la incidentul cibernetic care să cuprindă recomandări și instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de soluționare a incidentului respectiv;
- notificarea CSIRT-ul național, în condițiile stabilite de Legea nr. 48/2023 privind securitatea cibernetică, cu privire la incidentele cibernetice cu impact semnificativ asupra securității rețelelor sau sistemelor informatice ale statului ori asupra continuității serviciilor.

Secretar de stat **Cătălina PLINSCHI**

SINTEZA

obiecțiilor și propunerilor/recomandărilor la proiectul Guvernului pentru modificarea unor hotărâri ale Guvernului (aducerea actelor normative subsidiare în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe)

AVIZARE I

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Cancelaria de Stat** *(Nr. 22-69-8273 din 23.07.2024)*	**1.**	În temeiul art.54 alin.(1) lit.a) și lit.c) din Legea nr.100/2017 cu privire la actele normative, conținutul proiectului se expune într-un limbaj simplu, clar și concis, pentru a exclude orice echivoc, iar terminologia utilizată în textul proiectului este constantă și uniformă, respectiv la pct.2 din proiectul hotărârii Guvernului se recomandă: 1) la subpct.3, revizuirea și ajustarea sintagmei „reglementările interne aplicabile" cu terminologia utilizată în subpct.12 „reglementări interne aplicabile în domeniul TIC”.	**Se acceptă.** Sintagma „*reglementările interne aplicabile*" a fost substituită cu sintagma „*reglementări interne aferente sistemului de management al securității informației”*.
		2.	2) la subpct.15 lit.d), prin care se propune modificarea cuprinsului pct.21 subpct.10, sintagma „efectuarea periodică a testului de penetrare” ar trebui să includă un interval clar definit pentru a evita interpretări neuniforme și ambiguități în aplicare.	**Nu se acceptă.** Periodicitatea efectuării testului de penetrare în cadrul instituției se stabilește în politica de securitate cibernetică a acesteia, care poate varia în funcție de domeniul, funcțiile și atribuțiile pe care le exercită aceasta.
2.	**Aparatul Președintelui Republicii Moldova**	Lipsa de obiecții.		

	(Nr. 2/2-06-947 din 01.08.2024)			
3.	**Ministerul Infrastructurii și Dezvoltării Regionale** *(Nr. 21-3958 din 29.07.2024)*	Lipsa de obiecții și propuneri.		
4.	**Ministerul Energiei** *(Nr. 10-1995 din 29.07.2024)*	Lipsa obiecțiilor și/sau propunerilor.		
5.	**Ministerul Finanțelor** *(Nr. 07/3-03-133/1185 din 25.07.2024)*	Lipsa de obiecții și propuneri.		
6.	**Ministerul Mediului** *(Nr. 13-05/2139 din 29.07.2024)*	Lipsa de obiecții și propuneri.		
7.	**Ministerul Sănătății** *(Nr. 27/2936 din 29.07.2024)*	Lipsa de propuneri și obiecții.		
8.	**Ministerul Agriculturii și Industriei Alimentare** *(Nr. 21-03/2424 din 30.07.2024)*	Lipsa de propuneri și obiecții.		
9.	**Ministerul Apărării** *(Nr. 11/1056 din 23.07.2024)*	Lipsa obiecțiilor și propunerilor.		
10.	**Ministerul Afacerilor Interne** *(Nr. 38/ 3064 din 25.07.2024)*	**3.**	**1.** La pct. 1 subpct. 1) se recomandă revizuirea termenului *„sistemelor informatice utilizate la prestarea serviciilor poştale”* în sensul prevederilor pct. 2 din Regulile privind prestarea serviciilor poştale, aprobate prin Hotărârea Guvernului nr.1457/2016, care utilizează noțiunea de *„sistem informaţional destinat prestării serviciilor poştale electronice”*, care este totalitate de resurse şi tehnologii informaţionale interdependente, de metode şi de personal din proprietatea furnizorului de serviciu poştal universal, destinată interacţiunii dintre	**Nu se acceptă.** Modificările propuse prin prezentul proiect de hotărâre de Guvern au drept scop alinierea cadrului normativ secundar la Legea nr. 48/2023 privind securitatea cibernetică, inclusiv la terminologia cu care operează aceasta. La rândul său, Legea nr. 48/2023 transpune Directiva NIS 2 care

			furnizorul de serviciu poştal universal şi utilizatori la prestarea serviciilor poştale electronice.	operează cu termenul de *reţele şi sisteme informatice*. Totodată, prin modificările propuse se urmărește asigurarea securității rețelelor și sistemelor informatice utilizate pentru prestarea tuturor serviciilor poștale, nu doar a celor electronice (de exemplu, poșta electronică, poșta electronică recomandată, ștampila poștală electronică de certificare, cutia poștală electronică pentru scrisori). Sistemul informațional destinat prestării serviciilor poștale electronice reprezintă totalitatea resurselor și tehnologiilor informaționale interdependente, a metodelor și a personalului aflate în proprietatea furnizorului de servicii poștale universale, destinate interacțiunii dintre furnizor și utilizatori în cadrul prestării acestor servicii.
		La pct. 2 Cerințele minime obligatorii de securitate cibernetică aprobate prin Hotărârea Guvernului nr. 201/2017:		
		4.	1) la subpct. 3), examinând modificarea propusă în contextul reglementărilor pct. 8 subpct. 3), 13, 15 supct. 5) din Cerinţele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr.201/2017 se consideră că substituitea termenului nu este relevantă, întrucât formularea *„reglementări interne aplicabile”* nu indentifică domeniul de aplicatibilitate, comparativ cu sintagmele care se intenţionează să fie substituite care indică expers domeniul de aplicare, şi	**Se acceptă.** Sintagma „regulament intern de securitate cibernetică” și „regulament intern de securitate” la orice formă gramaticală, se substituie cu cuvintele „reglementări interne aferente sistemului de management al securității informației” la forma

			anume *„securitatea cibernetică”* sau „securitatea internă”. Or, reglemenări aplicabile interne pot fi din diferite domenii, cum ar fi protecţia datelor cu caracter peroanal, privind politica de cadre etc. Prin urmare, se denotă că autorul proiectului la pct. 2 subpct. 3) a optat sau pentru textul „Reglementări interne aplicabile în domeniul TIC” sau „Reglementări interne aplicabile în domeniul politicii de securitate cibernetică”.	gramaticală corespunzătoare pe tot parcursul textului.
		5.	2) La subpct. 4) nu este clară ideea modificării propuse, deoarece apare o imprecizie cu referire la textul în conținutul căruia urmează a fi realizată intervenția normativă. Astfel, în redacția propusă se înțelege că urmează a fi modificat doar subpct. 2 al pct. 1 din Hotărâre, însă autorul proiectului a inclus și textul subpct. 1) din pct. respectiv.	**Precizare.** Modificarea propusă vizează atât subpunctul 1) cât și subpunctul 2), ambele urmând fi substituite cu textul „*rețele și sisteme informatice (în continuare – sisteme).*”
		6.	3) la subpct. 8) Persoana (subdiviziunea) responsabilă are următoarele atribuții: - la lit. e) se propune de substituit textul „criptării de la un capăt la altul” cu cuvintele „criptării integrale”; - la lit. o), în scopul stabilirii unei terminologii unice se va atrage atenţia că la pct. 2 subpct. 3) din proiect s-a optat pentru textul *„reglementări interne aplicabile”*, astfel se va revedea noţiunile utilizate; - la subpct. (8) nu este clară modalitatea de informare *„continuă”* a conducerii instituției despre situația actuală a securității cibernetice, motiv pentru care, se recomandă stabilirea unui termen rezonabil şi pertinent pentru o astfel de informare.	**Se acceptă parțial.** Modificările propuse prin prezentul proiect de hotărâre de Guvern au drept scop alinierea cadrului normativ secundar la Legea nr. 48/2023 privind securitatea cibernetică, inclusiv la terminologia cu care operează aceasta, care operează cu sintagma *criptării de la un capăt la altul.* Referitor la stabilirea unui termen unic pentru toate instituțiile cu privire la conducerii instituției este greșit, acesta urmând să varieze de la o instituție la alta în funcție de domeniul, funcțiile sau atribuțiile acestea.

				Prin urmare, se propune ca acest termen și procedura sa fie stabilite în fișa postului și regulamentul subdiviziunii.
		7.	4) la subpct. 9) textul *„fără însă a se limita la acestea”* lasă loc de interpretare. legiuitorul obligă în mod imperativ revizuirea cel puţin o dată pe an a setului de documente dacă apar circumstanţele enumerate în norma legală. Prin urmare, nu este clar în care alte cazuri ar apărea obligația conducătorului instituției să revizuiască seturile de acte. În acest context, se recomandă excluderea textului *„fără însă a se limita la acestea”*. Mai mult, la pct. 9 nu oferă o claritate referitor la setul de acte ce urmează să fie revizuite, însă examinând prevederile pct. 8 subpct. 3) din Cerințele minime obligatorii de securitate cibernetică, se prezumă că se referă la actele enumerate în subpunctul prenotat. Prin urmare, se sugerează în primul enunț al pct. 9 după cuvintele „Setul de documente” să fie completat cu textul indicate la pct. 8 supbct. 3)” în scopul expunerii fără echivoc a normei de drept.	**Se acceptă.** Pentru a evita interpretarea eronată a prevederilor respective textul „*Setul de documente se aprobă de conducătorul instituției și trebuie să fie revizuit cel puțin o dată pe an, dacă*” se propune a fi substituit cu textul „*Setul de documente indicat la pct. 8 supbct. 3) se aprobă de conducătorul instituției și se revizuiește cel puțin o dată pe an și atunci când intervin următoarele cazuri*”.
		8.	5) la subpct. 10) lit. b), conform regulilor de tehnică legislativă, elementele structurale ale hotărârilor de Guvern se exclud, astfel, cuvântul se abrogă se va substitui cu cuvântul „se exclude”.	**Se acceptă.** Reieșind din natura sugestiei se presupune că obiecția a fost înaintată nu la subpc. 10) lit. b, dar la subpunctul 11) lit. b (subpunctul 13) lit. b) în noua redacție).
			6) la subpct. 12) se propune a fi exclus deoarece modificările propuse sunt tangențiale modificărilor înaintate prin pct. 2 subpct. 3) din proiect.	**Se acceptă.** Pentru a asigura uniformitatea terminologiei pe tot parcursul documentului și ținând cont de

				recomandările Instituției Publice „Agenția de Guvernare Electronică”, textul *„Regulamentele interne de securitate cibernetică prevăd”* se propune a fi substituit cu textul *„Reglementări interne aferente sistemului de management al securității informației prevăd, fără a se limita la acestea, următoarele”.*
		9.	7) la subpct. 15 lit. a) și c), conform pct.1 Hotărâre, cerințele minime obligatorii de securitate cibernetică se aplică în cadrul Cancelariei de Stat, ministerelor, altor autorităţi administrative centrale subordonate Guvernului, inclusiv al structurilor organizaţionale din sfera lor de competenţă (autorităţile administrative din subordine, serviciile publice desconcentrate şi cele aflate în subordine, instituţiile publice în care Cancelaria de Stat, ministerul sau altă autoritate administrativă centrală are calitatea de fondator), al autorităţilor administrative autonome şi unităţilor cu autonomie financiară (în continuare – *instituţii*). Astfel, toate autorităţilor enumerate la pct.1 din Cerinţele minime cad sub incidenţa cuvântului „instituţie”, însă, analizând conținutul normativ al Cerinţelor minime s-a remarcat că se utilizează şi cuvântul „autorităţi”. Astfel, se sugerează ca modificarea propusă să se refere la tot textul normativ al Cerinţelor minime şi nu doar la pct. 21 al acestora.	**Se acceptă** Modificările au fost operate și la pct. 6, 7 și 18 unde se operează cu cuvântul *autorități*.
		la subpct. 16) în cadrul modificărilor propuse la pct. 23 din Cerinţele minime:		**Subpunctul 19) în noua redacție**
		10.	- la subpct. 1) în contextul propunerilor de modificare a sintagmelor stipulate la pct. 2 subpct. 3) din proiect, se va revedea termenul *„reglementări interne de*	**Se acceptă.** Textul a fost ajustat uniform pe parcursul întregului proiect,

			securitate”, sau autorul proiectului utilizează acelaşi termen diferit, cum ar fi *„reglementări interne aplicabile” , „ reglementările interne pentru domeniul securității cibernetice”, „reglementări interne aplicabile în domeniul TIC”, „ reglementărilor interne ale instituției în domeniul securității cibernetice”*; *„reglementările interne ale instituției”*. Pentru excluderea interpretării dualiste se reiterează recomandarea uniformizării terminologiei în conformitate cu art. 54 alin. (1) lit. c) din Legea nr.100/2017 cu privire la actele normative.	utilizându-se terminologia de *„reglementări interne aferente sistemului de management al securității informației”*.
		11.	- la subpct. 3) drepturile şi obligaţiile sunt expuse haotic, contrar regulilor de tehnică legislativă, motiv pentru care se recomandă enumerarea drepturilor şi ulterior a obligațiilor.	**Se acceptă** Drepturile instituției și obligațiile prestatorului de servicii au fost prevăzute separat.
		12.	- la lit. c) din același subpunct 3), sunt reglemetnate aspecte ce se referă la încetarea contractului de prestări servicii, fapt ce contravine exigențelor prevăzute de Codul civil nr. 1107/2002. Astfel, nu este potrivit edclararea rezoluțiunii contractului, în strictă corespundere cu Secțiunea a 5-a din Capitolul V a Cărții a treia din Codul civil. Totodată, se atrage atenția că, în contextul contractului de prestări servicii este posibilă exclusiv încetarea raporturilor din contractul de prestări servicii, în modul stabilit de art. 1379 din codul menționat. Toto aici, în contextul digitalizării serviciilor publice, inclusiv şi celor private se sugerează substituirea cuvântului „scrisă” cu textul „pe suport de hârtie sau în format electronic”.	**Se acceptă** În vederea evitării abuzurilor în raport cu prestatorii de servicii a fost introdusă obligația respectării cadrului normativ la solicitarea încetării contractului de prestări servicii, precum și textul a fost ajustat în vederea substituirii cuvântului *„scrisă”* cu textul *„pe suport de hârtie sau în format electronic”*.
		13.	- la lit. e) , se sugerează reformularea conținutului, astfel încât să fie explicat clar dreptul prestatorului la care se	**Se acceptă.**

			face referire, având în vedere că redacția actuală creează ambiguități și premise de interpretare. Totodată, se va revedea termenul de ,,entitate", în sensul pct. 2 subpct.15 lit. c) din proiect, unde s-a optat pentru cuvântul ,,instituţie".	Prevederea respectivă a fost transferată la subpunctul nou (subpunctul 4) lit. b), constituind o obligație pentru prestatorul de servicii. Termenul de *,,entitate"* a fost substituit cu cuvântul *,,instituţie"* pe tot parcursul textului.
		14.	- la lit. f), se recomandă pentru expunerea clară a normei și de concretizat cine sunt subiecţii ,,persoanele implicate" în executarea contractului. Aparent, se concluzionează că aceştia ar fi angajaţii prestatorului de servicii.	**Nu se acceptă** Scopul normei este de a stabili obligația pentru prestatorul de servii de a se asigura că persoanele implicate în executarea contractului sunt instruite în mod corespunzător cu privire la rolurile și responsabilitățile lor înainte de a li se permite accesul la orice informație vizată în realizarea contractului respectiv, indiferent dacă relația lor este de muncă, prestări servicii sau altă formă de implicare (punctul 23, subpunctul 4), lit. c) a Cerințelor minime în noua redacție).
		15.	- se propune completarea pct. 23 cu o literă nouă, cu următorul cuprins: *,,obligația prestatorului de servicii de a asigura recuperarea integrală a prejudiciului cauzat ca urmare a activității necorespunzătoare a sistemelor informatice"*.	**Se acceptă.** Este punctul 23, subpunctul 5) a Cerințelor minime în noua redacție, care are următorul text: *„În cazul în care instituția încheie un contract cu furnizorul extern de servicii, contractul trebuie să includă și cerințe relevante de securitate, convenite cu fiecare furnizor pe baza tipului de relație cu*

				acesta. Contractul trebuie să stabilească cel puțin: *...* *5) de a monitoriza și jurnaliza toate acțiunile efectuate asupra sistemelor informaționale de către prestatorii de servicii externe entitate.*”.
		16.	**3.** Se recomandă revizuirea părții introductive din pct. 4, în partea ce ține de cuvintele „exercitarea funcțiilor de” în sensul pct. 4 din Regulamentul cu privire la tipurile și modul de stabilire a sporurilor cu caracter specific, probat prin Hotărârea Guvernului nr. 1231/2028 pentru punerea în aplicare a prevederilor Legii nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar, în care funcțiile concrete pentru care se acordă sporurile, gradul de pericol/condițiile de activitate, mărimea concretă a procentului, precum şi normele de acordare se stabilesc prin actul normativ cu caracter intern al conducătorului autorității.	**Se acceptă parțial.** Pct. 5^1) va avea următorul cuprins: „*5^1)* Pentru personalul Agenției pentru Securitate Cibernetică, sporul cu caracter specific se planifică anual la nivel de unitate bugetară în mărime de 120% față de suma anuală a salariului de bază prevăzut în schema de încadrare a autorității şi se acordă tuturor angajaţilor în funcție de eficienţa în activitate şi riscul asumat.”.
		17.	**4.** La pct. 6 subpct. 3 lit. b) este inoportun definirea noțiunii de *„incident cibernetic”*, deoarece noțiunea menționată este definită facându-se trimitere la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică. Astfel, o noțiunea poate fi explicată suplimentar, doar în cazul în care la momentul aprobării/adoptării unui act normativ se cunoaște cu certitudine că un termen este pasibil de mai multe interpretări sau dacă se imprimă un alt sens decât cel uzual și se optează pentru o anumită interpretare.	**Nu se acceptă.** Scopul acestei norme este de a stabili o definiție uniformă pentru *„incident cibernetic”* în toate actele normative, aliniată cu definiția prevăzută în Legea nr. 48/2023 privind securitatea cibernetică.
		18.	**5.** La pct. 8 subpct. 4) se sugerează substituirea cuvintelor „în anexă” cu cuvintele „în Concept”, deoarece modificările sunt incluse în conținutul conceptului, anexa conținând temeiul-cadru în textul	**Precizare.** Reieșind din faptul că la momentul actual este în proces de elaborare proiectul de Hotărâre de Guvern prin care urmează a fi aprobată procedura

			actului normativ, care se referă la obiectul determinat prin norma de trimitere.	de notificare a incidentelor cibernetice, inclusiv interacțiunea dintre furnizorul de servicii și autoritatea competentă, modul de stabilire a impactului unui incident cibernetic, și formatul informațiilor evaluărilor și rapoartelor prezentate în procesul de gestionare a unui incident cibernetic și modul de informare a destinatarilor de către furnizorii de servicii sau de către autoritatea competentă se propune excluderea modificărilor la Hotărârea Guvernului nr. 388/2022 în prezentul proiect de hotărâre de Guvern și introducerea următoarei norme tranzitoriila pct. 9 din proiect: *Ministerul Dezvoltării Economice și Digitalizării în comun cu Agenția pentru Securitate Cibernetică și Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică" vor analiza și vor prezenta, în termen de 3 luni de la data publicării prezentei hotărâri în Monitorul Oficial, propuneri privind determinarea și delimitarea competenței și responsabilităților în ce privește exercitarea atribuțiilor de posesor și deținător al Registrului de stat al incidentelor de securitate cibernetică în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică și*

				corespunzător de modificare a Hotărârii Guvernului nr. 388/2022 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică”.
11.	**Ministerul Afacerilor Externe și Integrării Europene** *(Nr. DI/3/041-7999 din 30.07.2024)*	La pct. 2 din proiectul de hotărâre, prin care se modifică Cerințele minime obligatorii de securitate cibernetică aprobate prin Hotărârea Guvernului nr. 201/2017 *(în continuare Cerințe):*		
		19.	la subpct. 16) ce prevede redacția nouă a pct. 23, subpct. 3) din Cerințe, se consideră utilă divizarea în subpuncte distincte reglementări ce ar viza drepturile și obligațiile instituției separat de cele ale prestatorului de servicii;	**Se acceptă.** Drepturile instituției și obligațiile prestatorului de servicii au fost divizate în subpuncte distincte (a se vedea subpunctul 19 din proiect: redacția pct. 23 subpct. 3) și 4).
		20.	subpunctul referitor la drepturile instituției se propune a fi completat cu o literă ce ar prevedea „dreptul instituției de a solicita dovezi din partea prestatorului de servicii a respectării cerințelor de securitate cibernetică în cadrul organizației, în scopul evitării unui atac cibernetic către instituție prin intermediul prestatorului de servicii”;	**Se acceptă** A se vedea subpunctul 19 din proiect: redacția pct. 23 subpct. 3), lit. e).
		21.	se consideră oportună completarea noii redacții a pct. 23 cu subpct. 4) care ar stabili printre clauzele contractuale faptul că „toate acțiunile efectuate asupra sistemelor informaționale de către prestatorii de servicii externe sa fie monitorizate și jurnalizate”;	**Se acceptă** A se vedea subpunctul 19 din proiect: redacția pct. 23 subpct. 5).
		22.	adițional, se propune examinarea posibilității de a completa proiectul supus avizării cu următoarele modificări suplimentare la Cerințe: - la pct. 15, subpct. 5) se propune a modifica lungimea minimă a parolei de la 7 la 12 caractere;	**Precizare.** Prezentul proiect de Hotărâre de Guvern are drept scop executarea prevederilor art. 23 alin. (2 lit. c) a Legii nr. 48/2023 privind securitatea cibernetică care stabilește obligația

			- la pct. 15, subpct. 9) și pct. 19, subpct. 6) se propune a specifica adițional că „jurnalizarea să se stocheze adițional și în locații externe securizate”; - la pct. 15, se propune a specifica adițional că „conexiunile de administrare de la distanță să fie efectuate doar prin autentificare multifactorială”; - la pct. 17, subpct. 2), lit. c), se propune a suplini cu textul „regula de baza a paravanului de protecție sa fie setată în regim de blocare implicită a tuturor conexiunilor”; - la pct. 21, subpct. 10) urmează a fi specificat că „testul de penetrare să fie efectuat de persoane competente, la nivel de infrastructură si aplicații, dar nu mai rar de 1 data pe an”; - pct. 21 se propune a fi suplinit cu două subpuncte ce ar prevedea „interzicerea accesului de pe toate serverele de procuție la rețeaua globala Internet, fără de necesitate justificată” și, respectiv, „efectuarea scanărilor de vulnerabilități periodice, dar nu mai rar decât trimestrial, cel puțin pe perimetrul extern al instituției”; - Capitolul IV se propune a fi suplinit cu un punct ce ar prevedea interzicerea utilizării sistemelor de operare și a componentelor de bază care sunt scoase din uz de către producătorul acestora; - pct. 22 se propune a fi completat cu un subpunct ce ar prevede „solicitarea dezvoltării sistemelor informaționale prin respectarea metodologiei de abordare a cerințelor și aspectelor de securitate cibernetica de la etapele incipiente a procesului de dezvoltare, de către dezvoltator (SSDLC)”; - la pct. 22, subpct. 6) se propune a specifica că „testarea de penetrare a sistemului informațional și a	pentru Guvern de a aduce actele sale normative în concordanță cu respectiva lege. Astfel, prin prezentul proiect se asiguă revizuirea unor prevederi din hotărârile de Guvern sectoriale care ar putea suscita interpretări echivoce sau contradictorii în aplicarea Legii privind securitatea cibernetică și legislației sectoriale care reglementează activitatea viitorilor furnizori de servicii. În același timp, suplimentar, după evaluarea situației reale privind sistemele informaționale de stat se va veni cu o modificare mai amplă a Cerințelor minime obligatorii de securitate cibernetică ce ar putea include și propunerile respective.

			infrastructurii conexe de o terță parte și fixarea tuturor vulnerabilităților cu risc mai mare de cel minor de către dezvoltatori, înainte de a fi acceptat și pus in funcțiune"; - pct. 22 se propune a fi completat cu un subpunct ce prevede „elaborarea unui plan de modernizarea a sistemelor informaționale și a componentelor conexe care sunt lipsite de actualizare și nu mai sunt întreținute de către producător".	
12.	**Ministerul Educației și Cercetării** *(Nr. 08/3-09/4732 din 23.07.2024)*	Lipsa obiecțiilor și propunerilor.		
13.	**Ministerul Muncii și Protecției Sociale** *(Nr. 22/3846 din 22.07.2024)*	Lipsa obiecțiilor și propunerilor.		
14.	**Serviciul de Informații și Securitate** *(Nr. E/7938 din 05.08.2024)*	**Cerințele minime obligatorii se securitate cibernetică (Hotărârea Guvernului nr. 201/2017):**		
		23.	Înlocuirea termenilor *„incidente de securitate cibernetică"* cu *„incidente cibernetice"* propuse la subpunctul 1) și modificările echivalente în terminologie, pot duce la confuzie dacă nu sunt corelate uniform cu toate reglementările existente. Or, de exemplu la pct. 9, subpct. 3) din *Cerințele minime obligatorii se securitate cibernetică aprobate prin Hotărârea Guvernului nr. 201/2017,* se folosește sintagma *„incidentelor de securitate"*, ceea ce nu s-ar încadra în modificările propuse pct. 2, subpct. 1) din proiectul propus spre avizare. Respectiv, ar trebui să se asigure ca modificările terminologice să fie implementate uniform și coordonate cu toate reglementările și standardele relevante, inclusive cu cele internaționale, pentru a evita ambiguități.	**Se acceptă.** Pct. 9 subpct. 3) din Cerințele minime obligatorii se securitate cibernetică a fost redat cu text nou, având următorul text : *„3) s-a constatat o creștere bruscă a incidentelor cibernetice asupra sistemului sau s-a depistat cel puțin un incident cibernetic cu impact semnificativ asupra sistemului și asupra continuității serviciului ori asupra securității rețelei și/sau sistemului informatic".*

		24.	Totodată, Serviciul consideră necesar de a modifica sfera de aplicare a Hotărârii de Guvern nr. 201/2017, din considerentul că este esențial de a avea un set de cerințe minime de securitate cibernetică pentru toate entitățile publice, de altfel rămân neacoperite entități importante cum ar fi: Președinția, Parlament, CNA, Judecătorii, Procuratura etc.	**Precizare** Conform punctului 1 din versiunea actuală a Cerințelor minime obligatorii de securitate cibernetică, aprobată prin Hotărârea de Guvern nr. 201/2017, în sfera de aplicare a acesteia sunt incluse și autoritățile administrative autonome, precum și unitățile cu autonomie financiară.
		25.	Conform propunerii înaintate la subpunctul 8) „*8. Persoana (subdiviziunea) responsabilă are următoarele atribuții*", în speță subpunctul *3) coordonează elaborarea și implementarea:* i) *„măsurilor de securitate privind resursele umane"* – nu este clar despre ce fel de măsuri de securitate este vorba, respectiv, propunem excluderea prevederii sau reformularea acesteia; m) *„sistemelor securizate de comunicații de urgență în cadrul furnizorului de servicii"* – nu este clar despre ce fel de sisteme securizare este vorba, respectiv, propunem excluderea prevederii sau reformularea acesteia.	**Se acceptă.** - lit. i) va avea următorul cuprins: *măsurilor de securitate privind politicile de control al accesului și de gestionare a activelor;* - lit. m) a fost exclusă.
		Hotărârea Guvernului nr. 482/2020 privind măsuri de securitate cibernetică.		
		26.	Nu se acceptă excluderea Serviciului de Informații și Securitate din subpunctul 18), în contextul în care Serviciul trebuie să dețină informații privind riscurile și incidentele cibernetice identificate de Serviciul Tehnologia Informației și Securitatea Cibernetică, în speță în autorități publice. Respectiv, propunem expunerea în următoarea redacție „*18) întocmește și prezintă, trimestrial, în adresa Serviciului de Informații și Securitate al Republicii Moldova și Agenției pentru Securitate Cibernetică un*	**Se acceptă.**

			raport privind riscurile și incidentele cibernetice identificate, măsurile întreprinse și planificate pentru remedierea acestora.”	
		În concluzie,		
		27.	scopul proiectului propus spre examinare este de a îmbunătăți securitatea cibernetică în Republica Moldova, însă este necesară o abordare atentă pentru a evita posibilele puncte slabe și a asigura o implementare eficientă și coordonată. Serviciul consideră că această sarcină urmează a fi tratată cu maximă diligență, asigurând o coordonare strânsă între toate instituțiile implicate în securitatea cibernetică pentru a evita suprapunerile de roluri și responsabilități și a asigura o aplicare uniformă a reglementărilor. Suplimentar, considerăm necesar de a reevalua cerințele minime de securitate cibernetică stabilite în Hotărârii Guvernului 201/2017, în contextul în care acestea sunt depășite de timp, nu au fost actualizate niciodată și nu instituie cadrul elementar de protecție a sistemelor informatice.	**Se acceptă** Totodată, referitor la reevaluarea cerințelor minime de securitate cibernetică urmează a fi menționat că prezentul proiect de Hotărâre de Guvern are drept scop alinierea cadrului normativ secundar care stabilește rigori în domeniul securității cibernetice la măsurile de securitate stabilite de Legea nr. 48/2023 privind securitatea cibernetică și revizuirea unor prevederi din hotărârile de Guvern sectoriale care ar putea suscita interpretări echivoce sau contradictorii în aplicarea Legii privind securitatea cibernetică și legislației sectoriale care reglementează activitatea viitorilor furnizori de servicii. În același timp, suplimentar, după evaluarea situației reale privind sistemele informaționale de stat se va veni cu modificări la Cerințele minime obligatorii de securitate cibernetică.
15.	**IP Agenția de Guvernare Electronică**	Avizează favorabil, cu condiția luării în considerare a următoarelor propuneri:		

	(Nr. 24/3007 – 144 din 25.07.2024)	**28.**	În **pct.2 (modificări la Cerințele minime obligatorii de securitate cibernetică aprobate prin Hotărârea Guvernului nr.201/2017):** **Sbp.6),** propunem de expus în următoarea redacție: *„la punctul 7, cuvintele „Ministerului Tehnologiei Informației și Comunicațiilor” se substituie cu textul „Agenției pentru Securitate Cibernetică, i Instituției Publice „Serviciul Tehnologia Informației și Securitate Cibernetică” și și Instituției publice „Agenția de Guvernare Electronică”.* Considerăm că prezentarea informației privind persoana (subdiviziunea) responsabilă de punerea în aplicare a sistemului de management al securității cibernetice în o instituție inclusiv și AGE va permite realizarea eficientă a competențelor sale în domeniul auditului de securitate cibernetică, în special a funcției de evaluare a conformității auditului de securitate cibernetică efectuate în autoritățile publice cu cerințele minime obligatorii de securitate cibernetică, stabilită în pct.11 sbp.12) din Statutul instituției, aprobat prin Hotărârea Guvernului nr.760/2010.	**Se acceptă** **(a se vedea modificările la pct. 2 subpct. 8) lit. b)**
		29.	În **sbp.12)** textul *„Reglementări interne aplicabile în domeniul TIC” recomandăm de substituit cu textul „Reglementări interne aferente sistemului de management al securității informației prevăd, fără a se limita la acestea, următoarele:”.*	**Se accceptă** **(vezi redacția subpct. 14) în redacția nouă)**
		30.	Concomitent, considerăm oportun de completat **sbp.12)** cu încă o modificare la pct.13 din Cerințele minime obligatorii de securitate cibernetică, după cum urmează: *„se completează cu subpunctul 9) cu următorul cuprins:* *9) procedurile de clasificare și etichetare a informațiilor”.*	**Se acceptă** **(vezi redacția subpct. 14) lit. b)**
		31.	Pornind de la experiența AGE în domeniul managementului proiectelor de dezvoltare a sistemelor	**Se acceptă**

			informaționale (centralizate și sectoriale), **sbp.15)** propunem de completat cu o modificare nouă la pct.21 din Cerințele minime obligatorii de securitate cibernetică, care ar prevedea încă un aspect al asigurării securității operaționale, după cum urmează: *„se completează cu subpunctul 8[1]) cu următorul cuprins:* *„8[1]. efectuarea separării mediilor de dezvoltare, testare și operare a sistemelor;”.*	**(vezi subpct. 18) lit. c) în redacția nouă a proiectului)**
		32.	De asemenea, **sbp.15)** propunem de completat cu încă o modificare la pct.21 sbp.9) din Cerințele minime obligatorii de securitate cibernetică, în scopul excluderii divergențelor în interpretare și asigurării aplicării corecte a cerinței respective, după cum urmează: *la subpunctul 9) sintagma „auditului intern” se substituie cu cuvântul „controlului”.*	**Se acceptă** **(vezi subpct. 18 lit. d) liniuța întâia)**
		33.	La **sbp.16),** propunem de perfecționat redacțional noua redacție a pct.23 sbp.3) lit.e) din Cerințele minime obligatorii de securitate cibernetică, și anume: *„e) dreptul de audit și supraveghere a activității prestatorului de servicii care implica operarea cu informații confidențiale.”.*	**Se acceptă** **(vezi subpct. 19): redacția pct. 23 subpct. 3) lit. d)**
16.	**IP Serviciul Tehnologia Informației și Securitate Cibernetică** *(Nr. 1.4/1176/24 din 31.07.2024)*	**34.**	La pct. 1 sbp. 2) în ultimul enunț după textul „Furnizorii de servicii poștale” se va adăuga textul „incluși în Lista furnizorilor de servicii în sectoarele și subsectoarele critice”.	**Se acceptă parțial** Textul final al respectivului punct sună în felul următor: „Agenția pentru Securitate Cibernetică exercită funcția de supraveghere și control de stat al respectării de către furnizorii de servicii poștale, incluși în Lista furnizorilor de servicii, a obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică. Furnizorii de

				servicii poștale, incluși în Lista furnizorilor de servicii în conformitate cu Legea nr. 48/2023, sunt obligați să ofere acces Agenției pentru Securitate Cibernetică la informațiile, bunurile și încăperile deținute de aceștia, care sunt necesare realizării obiectivelor controlului.”.
		35.	La pct. 2. sbp. 4) textul *„rețele și sisteme informatice (în continuare – sisteme)*.” se va substitui cu textul *„rețele și sisteme informaționale (în continuare sisteme)*”, întrucât măsurile necesare pentru asigurarea securităţii cibernetice trebuie să fie realizate inclusiv pentru sistemele informaționale, a se vedea noțiunile sistem informatic și sistem informațional definite de Legea 1069/2000 cu privire la informatică și Legea nr. 467/2003 cu privire la informatizare și resursele informaționale de stat.	**Nu se acceptă** Modificările propuse prin prezentul proiect de hotărâre de Guvern au drept scop alinierea cadrului normativ secundar la Legea nr. 48/2023 privind securitatea cibernetică, inclusiv la terminologia cu care operează aceasta. La rândul său, Legea nr. 48/2023 transpune Directiva NIS 2 care operează cu termenul de *rețele sisteme informatice*. Totodată, în procesul de armonizare a legislație naționale la directivele UE, dar și în vederea excluderii discrepanțelor existente (inclusiv terminologic), urmează și cadrul normativ conex domeniului securității cibernetice a fi racordat la noile terminologii.
		36.	La pct. 2) după sbp. 5) se va completa cu un subpunct nou care va avea următorul cuprins: „6) la pct. 6, 7, 18 și 21 cuvântul „autoritățile” se substituie cu cuvântul „instituțiile”, respectiv restul subpunctelor se vor renumerota.	**Se acceptă** Modificările au fost efectuate pentru fiecare punct separat.

			Totodată, la sbpct. 15) lit. a) se exclude, având în vedere obiecția de mai sus.	
		37.	La pct. 3 sbpct. 1), 2) și 4) se va exclude, ca fiind inoportun, or completările propuse nu sunt funcții, dar sunt atribuții aferente exercitării funcției IP STISC de Centrul guvernamental de reacţie la incidente de securitate cibernetică, atribuții deja stabilite în Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securităţii cibernetice la nivel guvernamental şi modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat, mai mult aceste prevederi sunt incluse în prezentul proiect la pct. 6 lit. c).	**Se acceptă**
		38.	La pct. 6. lit. c): - propunem excluderea textului – *„subpunctul 12), sintagma „securitatea sistemelor informaționale și a rețelelor” se substituie cu sintagma „securitatea rețelelor și sistemelor informatice”* întrucât măsuri necesare pentru asigurarea securităţii cibernetice la nivel guvernamental trebuie să fie realizate inclusiv pentru sistemele informaționale. - Textul *„-subpunctul 16), după sintagma „cooperează cu”, se completează cu textul „echipa de răspuns la incidente cibernetice la nivel național”*, se exclude deoarece platforma de management al incidentelor este prevăzută pentru interacțiunea dintre CERT Gov și CERT-urile departamentale. - textul „*16[1] asigură securitatea rețelelor și sistemelor informatice proprietate a statului”* se modifică cu textul *„asigură securitatea rețelelor și sistemelor informationale proprietate a statului la nivel guvernamental”* or conform art. 8 alin. (1) din Legea nr.	**Se acceptă parțial** Referitor la substituirea sintagmei „securitatea sistemelor informaționale și a rețelelor” cu „securitatea rețelelor și sistemelor informatice,” consultați comentariul de mai sus.

			48/2023 privind securitatea cibernetică ***pentru <u>asigurarea securității cibernetice la nivel guvernamental</u>, Guvernul instituie Centrul guvernamental de răspuns la incidentele cibernetice la nivelul rețelelor şi sistemelor informatice proprietate a statului....*** - în tot conținutul lit. c) textul „*autoritățile și instituțiile publice”* se va substitui cu textul *„Furnizorii de servicii persoane juridice de drept public”*.	
		39.	La pct. 6. lit. f) se va exclude întrucât nu este clară necesitatea de substituire a sintagmei <u>„CERT Gov”</u> cu sintagma *„Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”.*	**Nu se acceptă** Rolul de creare și asigurare a funcționării unei platforme de management al incidentelor și schimbului de informații revin persoanei juridice - Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, și nu rolului (funcției) acestei persoane juridice - CERT Gov.
		40.	La pct. 6. lit. g) se va exclude, or notificarea CSIRT-ului național de către CERT Gov, nu constituie o măsură de contracarare, notificarea echipei de răspuns la incidente cibernetice la nivel național de către Cert Gov este prevăzut de prezentul proiect prin adăugarea sbpct. $16^{2})$ la pct. 5 din Hotărârea Guvernului nr. 482/2020.	**Nu se acceptă** Unul din scopurile notificării CSIRT-ului național de către CERT Gov o constituie și contracararea amenințărilor cibernetice, care este în conformitate cu art. 15 al Legii nr. 48/2023 privind securitatea cibernetică.
		41.	Avînd în vedere că Agenția pentru Securitate Cibernetică exercită funcția de supraveghere şi control, **la pct. 7. sbp. 1)** textul „Insituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică ” se va substitui cu textul „Agenția pentru Securitate Cibernetică”.	**Se acceptă**

			- De asemenea sbp. 2) se va exclude, având în vedere obiecția de mai sus.	
		42.	Cu referire la pct. 8. considerăm oportună revizuirea/modificarea Hotărârii Guvernului nr. 388/2022 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică” inclusiv în partea de substituire a IP STISC, din calitatea de responsabil de crearea, implementarea, funcționarea și dezvoltarea Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică”, precum și posesor și deținător al acestuia, cu Agenția de Securitate Cibernetică.	**Se acceptă parțial** Proiectul a fost completat cu pct. 11 cu următorul cuprins: „Ministerul Dezvoltării Economice și Digitalizării în comun cu Agenția pentru Securitate Cibernetică și Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică” vor analiza și vor prezenta, în termen de 3 luni de la data publicării prezentei hotărâri în Monitorul Oficial, propuneri privind determinarea și delimitarea competenței și responsabilităților în ce privește exercitarea atribuțiilor de posesor și deținător al Registrului de stat al incidentelor de securitate cibernetică în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică și corespunzător de modificare a Hotărârii Guvernului nr. 388/2022 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică”.

		43.	La pct. 9 în ultimul enunț după textul „Furnizorii de apă potabilă” se va adăuga textul „incluși în Lista furnizorilor de servicii în sectoarele și subsectoarele critice”.	**Se acceptă.** Este pct. 8 în redacția nouă. Pct. 72^2 va avea următorul cuprins: „72^2. Agenția pentru Securitate Cibernetică exercită funcția de supraveghere și control de stat al respectării de către furnizorii de apă potabilă, incluși în Lista furnizorilor de servicii, a obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică. Furnizorii de apă potabilă, incluși în Lista furnizorilor de servicii în conformitate cu Legea nr. 48/2023, sunt obligați să ofere acces Agenției pentru Securitate Cibernetică la informațiile, bunurile și încăperile deținute de aceștia, care sunt necesare realizării obiectivelor controlului.”.
17.	**Agenția pentru Securitate Cibernetică** *(Nr. 09-28 din 25.07.2024)*	Comunică despre susținerea inițiativei cu unele propuneri de îmbunătățire:		
		44.	La pct. 2 din proiect ce vizează modificarea *Hotărârii Guvernului nr. 201/2017,* venim cu propunerea de la lărgi cercul de subiecți cărora le incumbă obligația de a implementa cerințe minime de securitate cibernetică. Astfel, propunem ca subiecți ai actului menționa să fie și furnizorii de servicii în unul sau mai multe dintre sectoarele sau subsectoarele critice, stabilite de către Guvern, și care sunt identificați ca furnizori de servicii de către Agenția pentru Securitate Cibernetică.	**Nu se acceptă** Subiecții actuali vizați de Hotărârea Guvernului nr. 201/2017 vizează toate autoritățile publice, inclusiv autoritățile administrative autonome și unitățile cu autonomie financiară. În același timp, în conformitate cu prevederile art. 11 alin. (4), Guvernul: a) prin intermediul organismului național de standardizare, asigură

			Necesitatea respectivă de intervenție derivă pe deoparte din lipsa reglementare pentru persoanele juridice de drept privat care sunt identificați de către Agenție ca fiind furnizori de servicii și reglementările impuse de către *Legea 48/2023 privind securitatea cibernetică*, care vizează atât sectorul public cât și cel privat, ce urmează a intra în vigoare la 1 ianuarie 2025, iar cerințe minime pentru toți subiecții nu există. În această ordine de idei, dacă propunea noastră urmează a fi reținută de către autorul proiectului, atragem atenția asupra necesității cosmetice de intervenție în cuprinsul textului pentru uniformiza lărgirea cercului de subiecți (drept exemplu intervenția de completare cu pct. 7^1).	aprobarea standardelor naționale în domeniul securității informației și al securității cibernetice în baza standardelor și a specificațiilor tehnice europene și celor internaționale relevante pentru securitatea rețelelor și a sistemelor informatice; b) la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice, aprobă cerințele specifice de securitate privind rețelele și sistemele informatice în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii.
		45.	La pct. 4 din proiect ce vizează modificarea *Hotărârii Guvernului nr. 1231/2018*, considerăm necesar a oferi redacție mai clară a prevederilor pentru a putea stabili cu certitudine persoanele care urmează a beneficia de spor cu caracter specific. Astfel, pentru a implementa fidel prevederile existente din *Legea 270/2018 privind sistemul unitar de salarizare în sectorul bugetar*, propunem următoarea redacție a pct. 5^1). „ 5^1) Pentru personalul Agenției pentru Securitate Cibernetică, sporul cu caracter specific se planifică anual la nivel de unitate bugetară în mărime de 120% față de suma anuală a salariului de bază prevăzut în schema de încadrare a autorității şi se acordă tuturor angajaţilor în funcție de eficienţa în activitate şi riscul asumat.”.	**Se acceptă parțial.** Urmare a reavizării proiectului de hotărâre de Guvern, acesta urmează să aibă următorul text: „*5[1]*. Pentru personalul Agenției pentru Securitate Cibernetică sporul cu caracter specific se acordă pentru de: 1) exercitarea funcțiilor de răspuns la incidente și crize cibernetice la nivel național; 2) exercitarea funcțiilor de identificare și evidență a furnizorilor de servicii;

				3) exercitarea funcțiilor de supraveghere și control de stat al respectării de către furnizorii de servicii a cadrului normativ în domeniul securității cibernetice; 4) exercitarea funcțiilor de asigurare a cooperării la nivel național și internațional și schimb de informații în materie de securitate cibernetică, inclusiv rolul de punct național unic de contact; 5) exercitarea funcțiilor de orientare metodologică, reglementare, cercetare și dezvoltare în domeniul securității cibernetice, precum și pentru caracterul specific al suportului în realizarea funcțiilor Agenției pentru Securitate Cibernetică.”
	(Nr. 09-33 din 13.08.2024)	Suplimentar la avizul cu nr. 09-08 din 25 iulie 2024, Agenția pentru Securitate Cibernetică vine cu unele completări asupra proiectului înregistrat la ședința secretarilor generali cu nr. unic 628/MDED/2024.		
		46.	Dat fiind faptul că *Hotărârea Guvernului nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică*, a fost adoptată în baza *Legii nr. 48/2023 privind securitatea cibernetică*, iar proiectul menționat are aducerea în concordanță a cadrului normativ inferior cu prevederii legii menționate, propunem modificarea Hotărârii Guvernului nr. 1028/2023 prin proiectul avut de către minister în consultări.	**Se acceptă.**

			Necesitatea de intervenție derivă din faptul că în cadrul procesului de lucru s-a constatat că organizarea inițială a subdiviziunilor Agenției nu corespunde cu cerințele reale avute. Astfel, se propune restructurarea a 4 subdiviziuni pentru a eficientiza lucrul în cadrul Agenției, fără a suferi cheltuieli bugetare în acest sens. Totodată, în urma restructurării subdiviziunilor se va eficientiza și resursa umană necesară implementării scopului creării Agenției. În această ordine de idei, propunem completarea proiectului de hotărâre cu următoarea intervenție: „Anexa 2 la Hotărârea Guvernului nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică (Monitorul Oficial al Republicii Moldova, 2023, nr. 502-504, art. 1238), va avea următorul cuprins: **„STRUCTURA** **Agenției pentru Securitate Cibernetică** Director Director adjunct Direcția răspuns la incidente și crize cibernetice Direcția supraveghere și control Secția prevenire și analiză Secția identificare și evidență furnizori de servicii Secția management instituțional Serviciul cooperare și schimb de informații Serviciul juridic Serviciul metodologie, standarde, cercetare și dezvoltare Serviciul financiar-administrativ Serviciul securitate internă Serviciul tehnologii informaționale și comunicații”.”	

			Prin intervenția dată se propune ca Serviciul juridic să fie un serviciu autonom, serviciul managementul documentelor să fie transformat în secție și să preia funcția de resurse umane și cea de comunicare și mass-media, Secția metodologie, standarde și cercetare să se transforme în Serviciu, iar competența de Securitate internă de la managementul documentelor să treacă în serviciu distinct compus dintr-o persoană în Serviciul Securitate Internă. In urma implementării proiectului, asupra bugetului se va produce un impact pozitiv, deoarece o funcție de șef secție, se transformă în funcție de șef serviciu, iar celelalte modificări se acoperă reciproc. Astfel, această modificare va aduce economie la buget anual în sumă de 37092 lei.	
18.	**Agenția Națională pentru Reglementare în Energetică a Republicii Moldova** *(Nr. 06-01/3662 din 25.07.2024)*	Lipsa obiecțiilor și propunerilor.		
19.	**Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei** *(Nr. 01-DJAC/761 din 22.07.2024)*	Lipsa obiecțiilor și propunerilor.		
20.	**Banca Națională a Moldovei** *(Nr. 31-002/78/3802 din 25.07.2024)*	Lipsa obiecțiilor și propunerilor.		

EXPERTIZARE

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Ministerul Justiției** *(Nr. 04/2-8191 din 05.09.2024)*	1.	În conformitate cu art. 52 alin. (2) și (3) din *Legea nr. 100/2017 cu privire la actele normative*, punctele, de regulă, nu au denumire, sunt expuse fără utilizarea cuvântului „punct” şi se însemnează consecutiv cu numere ordinare, exprimate prin cifre arabe, urmate de punct, începând cu primul și terminând cu ultimul, de la începutul şi până la sfârşitul actului normativ. Pentru interpretare corectă și aplicare comodă, punctele pot fi divizate în subpuncte care se numerotează prin adăugarea consecutivă a cifrelor arabe, până la gradul de detaliere necesar. Ținând cont de regula enunțată, la punctele din proiectul hotărârii subpunctele se vor renumerota corespunzător.	**Se acceptă** Renumerotarea a fost realizată pentru punctele care au suferit modificări în procesul de revizuire a proiectului de Hotărâre de Guvern.
		2.	La pct. 1 (modificarea *Hotărârii Guvernului nr. 1457/2016*):	
			1) La subpct. 2), atragem atenția că, potrivit normelor de tehnică legislativă, în cazul completării actului normativ cu un element structural nou nu se menționează după care articol, punct, alineat, literă etc. se amplasează acesta sau pe care dintre acestea le precedă. Totodată, în cazul operațiunii de completare cu un element structural nou se va utiliza sintagma „... se completează cu „...” cu următorul cuprins:”. Ținând cont de regulile enunțate, subpct. 2) va avea următorul cuprins: „2) se completează cu punctul 1361 cu următorul cuprins:”.	**Se acceptă**
			2) Ținând cont de dispozițiile art. 52 alin. (2) din *Legea nr. 100/2017*, la cuprinsul care se propune la pct. 136^1, textul „136^1)” se va substitui cu textul „136^1”.	**Se acceptă**

			3) Primul enunț care se propune la pct. 136[1] nu reglementează o dispoziție specifică ansamblului normelor indicate la Capitolul VII, or, Capitolul VII are denumirea „Responsabilitatea furnizorilor de servicii poștale”, iar primul enunț care se propune la pct. 136[1] conține reglementări privind funcția Agenției pentru Securitate Cibernetică care are misiunea de a implementa politica de stat în domeniul securității cibernetice, în vederea asigurării unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice ale furnizorilor de servicii. Prin urmare, se va revizui elementul structural cu care urmează a fi numerotată norma enunțată or, dispoziţiile de conţinut urmează a fi sistematizate într-o succesiune logică.	**Nu se acceptă** Analizând structura actului normativ prin care sunt aprobate regulile privind prestarea serviciilor poştale, Capitolul VII care stabilește responsabilitatea furnizorilor de servicii poștale reglementează toate responsabilitățile pe care le are furnizorul de servicii, fără a le limita la un domeniu specific de competență. În consecință, se consideră oportun păstrarea atribuțiilor legate de securitatea cibernetică în cadrul Capitolului VII, asigurând astfel coerența și continuitatea logică a normelor din prezentul act normativ.
		3.	La pct. 2 (modificarea *Hotărârii Guvernului nr. 201/2017*):	
			1) În conformitate cu art. 41 alin. (1) din *Legea nr. 100/2017*, actul normativ este format din denumire, preambul, clauza de adoptare, clauza de armonizare dispoziții generale, dispoziții de conținut, dispoziții finale, dispoziții tranzitorii, anexe, formula de atestare a autenticității actului normativ. Ținând cont de prevederile legale enunțate, rezultă că clauza de adoptare este element constitutiv al actului normativ și nu al anexei. Astfel, având în vedere că prin pct. 2 subpct. 1) din proiect, clauza de adoptare se expune în redacție nouă, întru corectitudinea redactării, la pct. 2, se va indica denumirea hotărârii Guvernului, care se propune a fi modificată și nu a anexei.	**Se acceptă.** Textul a fost ajustat și renumerotat corespunzător.
			2) La subpct. 1):	

			a) Potrivit art. 54 alin. (1) lit. d) din *Legea nr. 100/2017*, aceleaşi noţiuni se exprimă prin aceiaşi termini. Ținând cont de regula enunțată, în scopul uniformizării terminologiei, la subpct.1), cuvintele „clauza de emitere” se vor substitui cu cuvintele „clauza de adoptare”, astfel cum este indicat la art. 41 alin. (1) lit. c) din *Legea nr. 100/2017*.	**Se acceptă**
			b) În conformitate cu art. 43 alin. (1) din *Legea nr. 100/2017*, în preambulul actului normativ sunt prevăzute scopul și rațiunea adoptării actului normativ. Prin urmare, din clauza de adoptare se va exclude scopul pentru care se propune adoptarea actului normativ, acesta indicându-se în nota de fundamentare, deoarece preambulul este propriu doar actelor normative deosebit de importante.	**Se acceptă**
			c) *Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017*, (în continuare - Cerințe), nu conțin reglementări cu privire la crearea tehnologiilor, sistemelor și rețelelor informaționale de către autoritățile și instituțiile publice, persoanele fizice și persoanele juridice, prin urmare din conținutul clauzei de adoptare care se propune în redacție nouă se va exclude art. 18 alin. (1) din *Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat* care oferă asemenea competență.	**Se acceptă.**
			d) În aceeași ordine de idei, din clauza de adoptare se va exclude art. 11 alin. (2) lit. e) și f) din *Legea nr. 71/2007 cu privire la registre* or, literele enunțate se referă la obligațiile posesorului registrului privind asigurarea autenticității, securității și protecției datelor din registru.	**Se acceptă.**
			e) Întru respectarea condiției preciziei, la referința la art. 24 din *Legea nr. 71/2007*, textul „art. 24” va fi succedat de textul „alin. (3)”.	**Se acceptă.**

			3) În textul Cerințelor, cuvintele „incidente de securitate cibernetică” și „incidente de securitate” sunt indicate la o singură formă gramaticală: „incidentelor de securitate cibernetică” și „incidentelor de securitate”. Prin urmare, subpct. 2) va avea următorul cuprins: „2) în tot textul cuvintele „incidentelor de securitate cibernetică” și „incidentelor de securitate” se substituie cu cuvintele „incidentelor cibernetice””.	**Se acceptă.**
			4) Prin proiect se propune completarea pct. 1 cu textul „rețele și sisteme informatice (în continuare - sisteme) și abrogarea subpct. 1) și 2). Prin urmare, întru corectitudinea redactării, în subpct. 5) din proiect se va indica că pct. 1 se completează cu textul „rețele și sisteme informatice (în continuare - sisteme)”, iar subpct. 1) și 2) se abrogă.	**Se acceptă.**
			5) Dat fiind faptul că la pct. 5 ultimul alineat se expune în redacție nouă, întru corectitudinea redactării, subpct. 6) din proiect va avea următorul cuprins: „6) la pct. 5, ultimul alineat va avea următorul cuprins:...” (observație valabilă pentru toate cazurile similare din proiect).	**Se acceptă**
			6) Deși potrivit pct. 1 din Cerințe, cu referire la autoritățile administrative autonome și unităţile cu autonomie financiară, în continuare în textul Cerințelor urmează a fi utilizată denumirea generică „instituții”, menționăm că abordarea enunțată urma a fi revizuită prin prisma art. 32 din *Legea nr. 98/2012 privind administrația publică centrală de specialitate* care utilizează noțiunea „instituții publice”. Este de menționat însă, că prevederile pct. 1 exced sfera de aplicare a instituțiilor publice or, instituțiile publice nu cuprind autoritățile administrative autonome și unităţile cu autonomie financiară, prin urmare, întru corectitudinea redactării propunem utilizarea noțiunii	**Nu se acceptă.** Noțiunea generică de „instituții”, este utilizată în Hotărârea Guvernului nr. 201/2017 încă de la adoptarea acesteia pentru a desemna toate formele de organizare juridică publice și se consideră oportună păstrarea acesteia.

			„entități” care este mai largă și cuprinde inclusiv entitățile enunțate (obiecție valabilă și la pct. 7^1, 8, etc.).	
			7) Ținând cont că cuvântul „autorități” se propune a fi modificat la pct. 6 și 7, modificarea enunțată se va comasa la un singur subpunct și va avea următorul cuprins: 7) la pct. 6 și 7, cuvântul „autorități” se substituie cu cuvântul „entități”.	**Nu se acceptă.** Ținând cont că pct. 7 vine cu mai multe modificări, se propune păstrarea separată a modificărilor la pct. 6 și 7. Totodată, referitor la noțiunea de de „instituții” a se vedea comentariul de mai sus.
			8) Potrivit normelor de tehnică legislativă, când modificarea presupune o substituire utilizăm cuvântul „sintagma” - dacă structura reprezintă o îmbinare stabilă (denumirea unui minister, a unei agenții, bănci, a unui sistem etc.). Ținând cont de regula enunțată, la subpct. 8) lit. b), la referința la „Ministerul Tehnologiei Informației și Comunicațiilor” termenul „textul” se va substitui cu termenul „sintagma”.	**Se acceptă**
			9) La subpct. 9), reiterăm că în cazul operațiunii de completare cu un element structural nou se va utiliza sintagma „... se completează cu „...” cu următorul cuprins:”. Prin urmare, conținutul dispoziției de modificare de la subpct. 9) va avea următorul cuprins: „se completează cu punctul 7^1 cu următorul cuprins:”.	**Se acceptă**
			10) La subpct. 10):	
			a) În conformitate cu art. 3 alin. (1) lit. d) din *Legea nr. 100/2017*, la elaborarea actului normativ se va respecta principiul coerenței. În acest sens, menționăm că la pct. 7^1 se face referință la subdiviziunile instituției, iar la pct. 8 este utilizat textul „Persoana (subdiviziunea)”. Prin urmare, se va elucida acest aspect.	**Se acceptă parțial** **Precizare** Pct. 7^1 face referire la toate subdiviziunile din cadrul unei „instiuții”, pe când la pct. 8 se referă nemijlocit la persoana sau subdiviziunea reponsabilă de punerea în aplicare a sistemului de

				management al securității cibernetice.
			b) Prevederea care se propune la pct. 8 subpct. 7), în conformitate cu care persoana (subdiviziunea) responsabilă are atribuția de a verifica plenitudinea și conformitatea aplicării măsurilor de securitate, inclusiv prin efectuarea auditurilor de securitate, se va revizui prin prisma pct. 10 din *Statutul Instituției Publice „Agenția de Guvernare Electronică”, aprobat prin Hotărârea Guvernului nr. 760/2010* (în continuare - Statut), potrivit căruia unul din domeniile de competență ale Agenției este auditul de securitate cibernetică. Potrivit pct. 11 subpct. 12) din *Statut*, Agenția are funcția de a efectua și evalua conformitatea auditului de securitate cibernetică în autoritățile publice cu cerințele minime obligatorii de securitate cibernetică, aprobate de Guvern.	**Se acceptă.**
			11) La subpct. 11):	
			a) Pentru a exprima intenția de a reda un conținut nou alineatului întâi de la pct. 9, dispoziția de modificare de la subpct. 11) lit. a) din proiect va avea următorul cuprins: „alineatul întâi va avea următorul cuprins:”.	**Se acceptă**
			b) Prevederea care se propune la pct. 9 alineatul întâi: „Setul de documente indicat la pct. 8 subpct. 3) se aprobă de conducătorul instituției și se revizuiește cel puțin o dată pe an și atunci când intervin următoarele cazuri:” urmează a fi revizuită prin prisma art. 24 alin. (5) din *Legea nr. 100/2017*, în conformitate cu care documentele de politici se aprobă prin hotărâre de Guvern. În conformitate cu pct. 9 și 10 din *Regulamentul cu privire la planificarea, elaborarea, aprobarea, implementarea, monitorizarea și evaluarea documentelor de politici publice, aprobat prin Hotărârea Guvernului nr. 386/2020* (în continuare -	**Nu se acceptă** Deși se operează cu terminologie destul de simlară, Regulamentul cu privire la planificarea, elaborarea, aprobarea, implementarea, monitorizarea și evaluarea documentelor de politici publice aprobat Hotărârea Guvernului nr. 386/2020 stabiliște tipurile de documente de politici publie și documente de planificare, nu și politicile de securitate cibernetică

			Regulament), programul este un document de politici publice pe termen mediu (3-5 ani). Programul se constituie din partea descriptivă și planul de acțiuni. Ținând cont de prevederile legale enunțate, cuvintele „se aprobă de conducătorul instituției și se revizuiește cel puțin o data pe an” se vor substitui cu textul „se aprobă prin hotărâre de Guvern și se revizuiește o data la 3-5 ani”.	din cadrul autorităților/instituțiilor publice.
			12) La cuprinsul cu care se propune a fi completat pct. 11 subpct. 1), „corelate cu standardele în domeniul securității informației și în cel al securității cibernetice și cele mai bune practici pentru gestionarea incidentelor cibernetice și a riscurilor” atenționăm că, potrivit *Regulamentului,* obiectivele sunt stabilite în cadrul Strategiei.	**Nu se acceptă** A se vedea comentariul supra referitor la prevederile Hotărârii Guvernului nr. 386/2020.
			13) Potrivit normelor de tehnică legislativă, pentru exprimarea normativă a intenției de scoatere din vigoare a unor prevederi, în cazul elementelor structurale ale actului normativ se utilizează verbul „se abrogă”, iar în cazul eliminării unor cuvinte, sintagme, enunțuri se utilizează verbul „se exclude”. Ținând cont de regula de tehnică legislative enunțată, la subpct. 13) lit. b), textul „subpunctul 3) se exclude” se va substitui cu textul „subpunctul 3) se abrogă”.	**Se acceptă.**
			14) Potrivit normelor de tehnică legislativă, când modificarea presupune o substituire utilizăm termenul „cuvânt”, dacă în structura vizată nu sunt prezente și alte semne grafice (cifre, virgule, paranteze, ghilimele, bară oblică). Ținând cont de regula enunțată, la cuprinsul care se propune la subpct. 14) lit. a), termenul „textul” se va substitui cu termenul „cuvintele”.	**Se acceptă**
			15) Cuvântul „autoritățile” este indicat la pct. 18 doar în subpct. 1) din Cerințe. Prin urmare, la subpct. 17) din	**Se acceptă**

			proiect, textul „pct. 18” va fi succedat de textul „subpct. 1)”.	
			16) Potrivit regulilor de tehnică legislativă, în cazul operațiunii de completare cu un element structural nou se va utiliza sintagma „... se completează cu „...” cu următorul cuprins:”. Ținând cont de regulile expuse, dispoziția de modificare de la subpct. 18) lit. c) va avea următorul cuprins: „se completează cu subpunctul 8^1) cu următorul cuprins:”	**Se acceptă**
			17) Ținând cont de prevederile art. 2 din *Legea nr. 100/2017*, în conformitate cu care actul normativ stabilește, modifică ori abrogă norme juridice care reglementează nașterea, modificarea sau stingerea raporturilor juridice, în denumirea Capitolului VI, cuvântul „relațiile” se va substitui cu cuvântul „raporturile” (obiecție similară și la pct. 23).	**Se acceptă**
			18) La pct. 23:	
			a) Prevederile de la pct. 23 sunt confuze, or, la alineatul întâi se face referință la furnizorul extern de servicii, iar la subpct. 1) - 4) și la pct. 23^1 se face referință la prestatorul extern de servicii. Mai mult, noțiunile nu sunt uniforme, or, sunt utilizate următoarele noțiuni: furnizorul extern de servicii, furnizor, prestator de servicii, prestatorul extern de servicii. Prin urmare, noțiunile se vor uniformiza. În conformitate cu art. 3 din *Legea nr. 48/2023 privind securitatea cibernetică*, legea se aplică și persoanei juridice de tipul stabilit de Guvern dacă este prestator de servicii de încredere, în sensul legislației privind identificarea electronică și serviciile de încredere. Potrivit art. 11 alin. (2) pct. 2) lit. h) din *Legea nr. 48/2023*, în procesul aplicării măsurilor de securitate, furnizorul de servicii este obligat să implementeze măsuri tehnice și organizatorice pentru a gestiona	**Se acceptă parțial.** Se operează cu termenul de prestator de servicii. Referitor la stabilirea clară a subiecților raportului juridic, este important de menționat că pct. 23 din Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017, prevede cerințe de securitate aplicabile în cazul externalizării serviciilor de către o instituție sau autoritate publică. Totuși, aceste cerințe nu se aplică în mod necesar furnizorilor de servicii în sensul reglementărilor stabilite de Legea nr.

			riscurile de securitate a rețelelor și a sistemelor informatice pe care le utilizează care trebuie să includă măsuri legate de securitate referitoare la relațiile furnizorului de servicii cu prestatorii sau cu furnizorii direcți de servicii ai acestuia. Ținând cont de prevederile legale enunțate, se va revizui conținutul pct. 23 pentru a stabili clar subiecții raportului juridic.	48/2023 privind securitatea cibernetică. Prin urmare, este esențial să se facă o distincție clară între obligațiile care decurg din Hotărârea Guvernului nr. 201/2017 și cele prevăzute de Legea nr. 48/2023.
			b) Cuprinsul care se propune la pct. 23 subpct. 3) lit. c) se va revizui prin prisma *Legii nr. 124/2022 privind identificarea electronică și serviciile de încredere*, care operează cu noțiunea „formă electronica". Prin urmare, cuvintele „în format electronic" se vor substitui cu cuvintele „în formă electronică".	**Se acceptă**
			c) Norma care se propune la lit. d) nu se integrează armonios în text. Prin urmare, cuvintele „dreptul de" se vor substitui cu cuvintele „de a efectua".	**Se acceptă**
			d) În scopul uniformizării terminologiei, la cuprinsul care se propune la pct. 23 subpct. 3) lit. e), cuvântul „organizației" se va revizui, or, anterior în text este utilizat cuvântul „instituției".	**Se acceptă parțial** A fost precizat că organizație se referă la prestatorul extern de servicii și nu la „instituție", în sensul Hotărârii Guvernului nr. 23/2017.
		4.	La pct. 3 (modificarea *Hotărârii Guvernului nr. 414/2018*):	
			1) La subpct. 1):	
			a) la cuprinsul care se propune la subpct. 1), textul „subpunctul 20^1" se va substitui cu textul „subpunctul 20^1)" (obiecție valabilă și la subpct. 31^1), 34^1)) .	**Se acceptă**
			b) Prin proiect se propune completarea pct. 8 cu subpct. 20^1), astfel încât Serviciul Tehnologia Informației și Securitate Cibernetică să fie investit cu funcția de a asigura securitatea rețelelor și sistemelor informatice proprietate a statului. La acest aspect, menționăm că, în conformitate cu art. 8 alin. (3) din *Legea nr. 48/2023,*	**Nu se acceptă** **Precizare** Conform pct. 8. Spbct. 34) Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică" exercită rolul de Centru

			Centrul guvernamental de răspuns la incidentele cibernetice este responsabil de asigurarea securității rețelelor și sistemelor informatice proprietate a statului, prin urmare, se va elucida acest aspect.	guvernamental de răspuns la incidentele cibernetice.
			2) În aceeași ordine de idei, se va revizui prevederea care se propune la subpct. 31^{1}) și subpct. 34^{1}), în conformitate cu care, Serviciul informează Agenția pentru Securitate Cibernetică cu privire la incidentele cibernetice notificate de autoritățile și instituțiile publice, facilitează interacțiunea dintre autoritățile și instituțiile publice cu Agenția pentru Securitate Cibernetică și echipa de răspuns la incidentele cibernetice la nivel național, or, potrivit art. 8 alin. (3) din *Legea nr. 48/2023*, Centrul guvernamental de răspuns la incidentele cibernetice este responsabil de notificarea și de facilitarea interacțiunii furnizorilor de servicii persoane juridice de drept public cu autoritatea competentă și echipa de răspuns la incidentele cibernetice la nivel național.	**Nu se acceptă** A se vedea comentariul supra cu privire la rolul Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică” de Centru guvernamental de răspuns la incidentele cibernetice.
		5.	Cu referire la pct. 5, ce vizează modificarea *Hotărârii Guvernului nr. 211/2019*, ținând cont de regula, în conformitate cu care când modificarea presupune o substituire utilizăm termenul „cuvânt” sau „cuvinte”, dacă în structura respectivă nu sunt prezente și alte semne grafice (cifre, virgule, paranteze, ghilimele, bară oblică), la subpct. 1) lit. b) și subpct. 2), termenul „sintagma” se va substitui cu termenul „cuvintele”, or, sintagma se utilizează dacă structura reprezintă o îmbinare stabilă (denumirea unui minister, a unei agenții, bănci, a unui sistem etc.).	**Se acceptă**
		6.	La pct. 6 (modificarea *Hotărârii Guvernului nr. 482/2020*):	
			1) În conformitate cu art. 49 alin. (2) din *Legea nr. 100/2017*, anexele sunt parte integrantă a actului	**Se acceptă**

			normativ, au natura şi forţa juridică ale acestuia. Ținând cont de regula enunțată, la subpct. 1) și 2), cuvintele „și anexei” se vor exclude ca fiind excedente.	
			2) Cuvintele „incidente de Securitate informațională” sunt indicate doar la pct. 5 subpct. 8) al anexei la o singură formă gramaticală, prin urmare, subpct. 3) lit. a) va avea următorul cuprins: „a) la pct. 5 subpct. 8) cuvintele „incidente de securitate informațională” se substituie cu cuvintele „incidente cibernetice””.	**Se acceptă** Modificările au fost inserate la amendamentele propuse la pct. 5.
			3) Ținând cont de regulile de tehnică legislativă privind utilizarea termenilor când modificarea presupune o substituire, la subpct. 3) lit. c) liniuța a treia, termenul „sintagma” se va substitui cu „cuvintele”.	**Se acceptă**
			4) La subpct. 3) lit. c) liniuța a patra, reiterăm că, potrivit normelor de tehnică legislativă, în cazul completării actului normativ cu un element structural nou nu se menționează după care articol, punct, alineat, literă etc. se amplasează acesta sau pe care dintre acestea le precedă. Totodată, deoarece în textul actului normativ propus spre modificare subpunctele se numerotează cu cifre arabe urmate de o paranteză, cuprinsul de la liniuța a patra urma a fi expus în următoarea redacție: „se completează cu subpunctele $16^{1})$ - $16^{3})$ cu următorul cuprins:”.	**Se acceptă**
			5) La lit. c) liniuța a cincea, întru corectitudinea redactării, cuvintele „sintagma după” se vor substitui cu cuvintele „după sintagma”, termenul „textul” se va substitui cu termenul „cuvintele”, or, în structura cu care se propune a fi completat subpct. 18) nu sunt prezente și alte semne grafice.	**Se acceptă**
			6) Ținând cont de regula în conformitate cu care în cazul completării actului normativ cu un element structural nou nu se menționează după care articol, punct, alineat, literă etc. se amplasează acesta sau pe	**Se acceptă**

			care dintre acestea le precedă, dispoziția de modificare de la lit. d) va avea următorul cuprins: „se completează cu punctul 61 cu următorul cuprins:”.	
			7) În aceeași ordine de idei, conținutul dispoziției de modificare de la lit. g) urma să fie expus în următoarea redacție: „la punctul 11, subpunctul 3) se completează cu litera a^1) cu următorul cuprins:”.	**Se acceptă**
			8) Prevederea care se propune la pct. 11 subpct. 3) lit. a^1) nu se integrează armonios în text, prin urmare, în scopul alinierii la prevederile celorlalte diviziuni, verbul „notifică” se va conjuga la timpul infinitiv „notificarea”.	
			9) La lit. h), cuvintele „la sfârșit” se vor exclude, or, completarea unui text sau alineat, fără a specifica ordinea în care se inserează cuvintele, semnifică, conform regulii generale de tehnică legislativă, completarea textului la sfârșitul acestuia.	**Se acceptă**
		7.	La pct. 7 (modificarea *Hotărârii Guvernului nr. 124/2021*):	
			1) La subpct. 1), în referința la „STISC”, termenul „cuvântul” se va substitui cu termenul „abrevierea”.	**Se acceptă**
			2) Ținând cont de regulile de completare cu elemente structurale noi, dispoziția de modificare de la subpct. 2) va avea următorul cuprins: „se completează cu punctele 560^1 și 560^2 cu următorul cuprins:”.	**Se acceptă**
		8.	În cuprinsul care se propune la pct. 10 din proiect, cuvintele „corespunzător de modificare” se vor exclude ca fiind excedente.	**Se acceptă**
2.	**Centrul Naţional Anticorupţie** *(Nr. 06/2/15415 din 13.09.2024)*		În redacția propusă, proiectul nu conține factori de risc care să genereze apariția riscurilor de corupție.	

INFORMARE

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Cancelaria de Stat** *(Nr. 22-69-9764 din 30.08.2024)*		Lipsa obiecțiilor și propunerilor.	
2.	**Aparatul Președintelui Republicii Moldova**		Nu a prezentat avizul la etapa de informare.	
3.	**Ministerul Infrastructurii și Dezvoltării Regionale**		Nu a prezentat avizul la etapa de informare.	
4.	**Ministerul Energiei** *(Nr. 10-2367 din 09.09.2024)*		Lipsa obiecțiilor și propunerilor.	
5.	**Ministerul Finanțelor** *(Nr. 07/3-03-165/1442 din 16.09.2024*	1.	La pct.4 al proiectului hotărârii Guvernului, *nu se susține noua redacție a punctului 5[1] la Hotărârea Guvernului nr.1231/2018* pentru punerea în aplicare a prevederilor Legii nr.270/2018 privind sistemul unitar de salarizare în sectorul bugetar. În proiectul definitivat a fost introdusă o modificare esențială la punctul prenotat, prin excluderea criteriilor specifice atribuite funcțiilor urmare a încadrării și identificării personalului cu drept de a beneficia de sporul cu caracter specific stabilit la art. 17 alin. (2) lit. b[2]) din Legea nr. 270/2018. În acest sens accentuăm că conform pct. 3 și 4 din anexa nr. 4 la hotărârea Guvernului nr. 1231/2018, sporurile cu caracter specific se acordă personalului pentru compensarea efortului depus sau a riscului asumat în condiţiile specifice de activitate prevăzute de prezentul Regulament, pentru timpul lucrat în aceste condiţii. Funcţiile concrete pentru care se acordă sporurile, gradul de pericol/condiţiile de activitate, mărimea concretă a procentului, precum şi normele de acordare se stabilesc prin actul normativ cu caracter intern al conducătorului autorităţii. Prin urmare, cele expuse în pct. 4 din proiect, precum că sporul vizat „se acordă tuturor angajaților în funcție de eficiența în	**Se acceptă parțial.** Urmare a reavizării proiectului de hotărâre de Guvern, acesta urmează să aibă următorul text: „*5[1]*. Pentru personalul Agenției pentru Securitate Cibernetică sporul cu caracter specific se acordă pentru de: 1) exercitarea funcțiilor de răspuns la incidente și crize cibernetice la nivel național; 2) exercitarea funcțiilor de identificare și evidență a furnizorilor de servicii; 3) exercitarea funcțiilor de supraveghere și control de stat al respectării de către furnizorii de servicii a cadrului normativ în domeniul securității cibernetice;

			activitate...” nu formează în sine scopul de reglementare a plății vizate, precum stabilirea caracterului specific al activităţilor, compensarea efortului depus sau a riscului asumat în aceste condiții. Reieșind din cele relatate, Ministerul Finanțelor insistă asupra necesității redactării pct.4 din proiect vis-a-vis de completarea Hotărârii Guvernului nr.1231/2018 privind sporul cu caracter specific ce urmează a fi acordat personalului Agenției.	4) exercitarea funcțiilor de asigurare a cooperării la nivel național și internațional și schimb de informații în materie de securitate cibernetică, inclusiv rolul de punct național unic de contact; 5) exercitarea funcțiilor de orientare metodologică, reglementare, cercetare și dezvoltare în domeniul securității cibernetice, precum și pentru caracterul specific al suportului în realizarea funcțiilor Agenției pentru Securitate Cibernetică.”
6.	**Ministerul Mediului**		Nu a prezentat avizul la etapa de informare.	
7.	**Ministerul Sănătății** *(Nr. 27/3366 din 30.08.2024)*		Lipsa obiecțiilor și propunerilor.	
8.	**Ministerul Agriculturii și Industriei Alimentare** *(Nr. 21-03/2741 din 30.08.2024)*		Lipsa obiecțiilor și propunerilor.	
9.	**Ministerul Apărării** *(Nr. 11/1219 din 03.09.2024)*	2.	Lipsa obiecțiilor și propunerilor. Totodată, considerăm oportună și actuală, odată cu operarea modificărilor în Legea 270/2018, privind sistemul unitar de salarizare în sectorul bugetar, includerea tuturor angajaților din echipele de răspuns la incidentele cibernetice de toate nivelele (departamentale, sectoriale etc.), a sporului cu caracter specific, planificat anual la nivel de unitate bugetară în mărime de 50% față de suma anuală a salariului de bază prevăzut în schema de încadrare a autorității şi să se acorde în funcție de eficienţa în activitate şi riscul	**Nu se acceptă** **Precizare** Prin prezentul proiect de hotărâre de Guvern se urmărește aducerea în concordanță a hotărârilor de Guvern cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe, inclusiv Legea 270/2018. Finalitățile urmărite prin adoptarea prezentului proiect de hotărâre de Guvern constau, în principal, în

			asumat, precum și în scopul motivării și menținerii specialiștilor calificați.	alinierea cadrului normativ secundar care stabilește rigori în domeniul securității cibernetice la măsurile de securitate stabilite de Legea nr. 48/2023 privind securitatea cibernetică și evizuirea unor prevederi din hotărârile de guvern sectoriale care ar putea suscita interpretări echivoce sau contradictorii în aplicarea Legii privind securitatea cibernetică și legislației sectoriale care reglementează activitatea viitorilor furnizori de servicii. Astfel, prin acesta nu se urmărește modificarea unor legi, ci doar a hotărârilor de Guvern care urmează a fi raliate la legislația primară.
10.	**Ministerul Afacerilor Interne** *(Nr. 38/3552 din 05.09.2024)*		Lipsa obiecțiilor și propunerilor.	
11.	**Ministerul Afacerilor Externe**		Nu a prezentat avizul la etapa de informare.	
12.	**Ministerul Educației și Cercetării**		Nu a prezentat avizul la etapa de informare.	
13.	**Ministerul Muncii și Protecției Sociale** *(Nr. 22/4739 din 16.09.2024)*		Lipsa obiecțiilor și propunerilor.	
14.	**Serviciul de Informații și Securitate** *(Nr. E/9791 din 13.09.2024)*		Lipsa obiecțiilor și propunerilor.	
15.	**IP Agenția de Guvernare Electronică**		Nu a prezentat avizul la etapa de informare.	

16.	**IP Serviciul Tehnologia Informației și Securitate Cibernetică** *(Nr. 1.4/1336/24 din 03.09.2024)*		Se reiterează următoarele obiecții:	
		3.	La **pct. 3, sbpct. 1), 2) și 4) se vor exclude**, întrucît potrivit pct. 8 sbpct. 34) din Statutul IP STISC aprobat prin Hotărârea Guvernului 414/2018 IP STISC exercită funcția de Centrul guvernamental de reacţie la incidente de securitate cibernetică, iar atribuțiile aferente exercitării funcției IP STISC de Centrul guvernamental de reacţie la incidente de securitate cibernetică, sunt stabilite în Hotărârea Guvernului nr. 482/2020 *privind aprobarea unor măsuri necesare pentru asigurarea securităţii cibernetice la nivel guvernamental şi modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat*, mai mult aceste prevederi sunt incluse în prezentul proiect la pct. 6 lit. c). Astfel, pentru evitarea dublării reglementărilor din alte acte normative, a interpretării defectuoase a normelor juridice cât și în vederea aplicării eficiente a acestora, considerăm imperios ca atribuțiile aferente funcției de CERT Gov să se regăsească doar într-un singur act normativ.	**Se acceptă**
		4.	La pct. 6, sbpct 3 lit. c) textul „însă nu mai târziu de 24 ore” se va substitui cu textul „însă nu mai târziu de 48 ore”.	**Nu se acceptă** Termenul de 24 ore este corelat și sincronizat cu termenul stabilit în art. 12, alin. (2) al Legii nr. 48/2022 privind securitatea cibernetică care stabilește obligativitatea pentru autoritatea competentă de a prezenta, fără întârzieri nejustificate și nu mai târziu de 24 de ore de la recepționarea informației privind incidentele cibernetice, furnizorului de servicii un răspuns inițial cu

				privire la incidentul cibernetic cu impact semnificativ și, la solicitarea furnizorului de servicii, recomandări sau instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de soluționare a incidentului respectiv, inclusiv de atenuare a impactului acestuia și de continuitate a activității.
		5.	La pct. 6, sbpct 3 lit. c), Textul *„-subpunctul 16), după sintagma „cooperează cu”, se completează cu textul „echipa de răspuns la incidente cibernetice la nivel național”*, se va exclude deoarece platforma de management al incidentelor este prevăzută pentru interacțiunea dintre CERT Gov și CERT-urile departamentale, argumentul autorului precum că afectează principiul cooperării nu este viabil în cazul dat, or Platforma care se menționează în Hotărârea Guvernului 482/2020 este destinată pentru a asigura cooperarea dintre CERT urile departamentale și entitățile publice stabilite la pct. 5 din hotărâre cu CERT Gov. STISC va asigura cooperarea cu echipa de răspuns la incidentele cibernetice la nivel naţional în conformitate cu legea, inclusiv prin notificări, rapoarte, după caz prin platforma prevăzută la art. 7 alin. (4) pct. 7 din Legea 48/2023.	**Se acceptă parțial** În vederea evitări interpretărilor eronate, se propune completarea cu un subpunct suplimentar care prevede cooperarea cu cu echipa de răspuns la incidentele cibernetice la nivel național, cu următorul cuprins: *16^4) cooperează cu echipa de răspuns la incidentele cibernetice la nivel național, inclusiv în cadrul unei platforme de management al incidentelor cibernetice și pentru schimbul de informații;*”.
		6.	Textul *„16^1 asigură securitatea rețelelor și sistemelor informatice proprietate a statului” se modifică cu textul „asigură securitatea rețelelor și sistemelor informationale proprietate a statului la nivel guvernamental”* or conform art. 8 alin. (1) din Legea nr. 48/2023 privind securitatea cibernetică ***pentru asigurarea securităţii cibernetice la nivel guvernamental, Guvernul instituie Centrul***	**Se acceptă**

			guvernamental de răspuns la incidentele cibernetice la nivelul reţelelor şi sistemelor informatice proprietate a statului...., obiecția dată vine în vederea asigurării executării art. 8 alin. (1) din Legea 48/2023, or din textul prevederii legale citate rezultă expres și neîndoielnic faptul că Certul guvernamental de răspuns la incidente cibernetice asig ură securitatea cibernetică la nivel guvernamental.	
17.	**Agenția pentru Securitate Cibernetică**		Nu a prezentat avizul la etapa de informare.	
18.	**Agenția Națională pentru Reglementare în Energetică a Republicii Moldova** *(Nr. 06-01/4286 din 29.08.2024)*		Lipsa obiecțiilor și propunerilor.	
19.	**Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei** *(Nr. 03–DJAC/994 din 03.09.2024)*		Lipsa obiecțiilor și propunerilor.	
20.	**Banca Națională a Moldovei** *(Nr. 31-002/95/4496 din 11.09.2024)*		Lipsa obiecțiilor și propunerilor.	

AVIZARE II

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului

1.	**Cancelaria de Stat** *(Nr. 22-69-12529 din 14.11.2024)*		***La proiectul hotărârii:***	
		1.	La pct.3 subpct.2) din proiect, prin care se modifică Hotărârea Guvernului nr.201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică: a) la lit. f), g) și q) unde se propune substituirea cuvântului „autorității” cu „instituției” pentru o mai marea claritate și pentru a se exclude orice echivoc, se recomandă utilizarea sintagmei „entități publice”, sintagmă consacrată în Hotărârea Guvernului nr.482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și Hotărârea Guvernului nr.414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat. b) la lit. q) înaintea textului „ - cuvântul „entității” se substituie cu cuvântul „instituției” se va completa cu textul „- subpunctul 9) lit.b):”.	**Se acceptă parțial** a) Cuvântul *“instituție”* pe tot parcursul textului este corelat cu pct. 1 al Cerințelor minime obligatorii de securitate cibernetică, care stabilește termenul generic de instituție pentru: ministere, alte autorități administrative centrale subordonate Guvernului, inclusiv structurile organizaționale din sfera lor de competență (autorități administrative subordonate, servicii publice desconcentrate și cele aflate în subordine, precum și instituțiile publice în care Cancelaria de Stat, un minister sau o altă autoritate administrativă centrală are calitatea de fondator), autoritățile administrative autonome și unitățile cu autonomie financiară.” b) completat cu lit. b) la subpunctul 9).
		2.	La pct.5 din proiect, prin care se completează Regulamentul cu privire la tipurile şi modul de stabilire a sporurilor cu caracter specific, aprobat prin Hotărârea Guvernului nr.1231/2018 pentru punerea în aplicare a prevederilor Legii nr.270/2018 privind sistemul unitar de salarizare în sectorul bugetar, cu un nou punct 5^1 , se va exclude textul „exercitarea funcțiilor de”. Potrivit	**Se acceptă parțial.** În vederea asigurării uniformității pe tot parcusul actului normativ a fost revăzut textul punctului 5^1 care va avea următorul cuprins:

			pct.54 alin.(1) lit.c) din Legea nr.100/2017 cu privire la actele normative, terminologia utilizată în textul proiectului actului normativ este constantă, uniformă și corespunde celei utilizate în alte acte normative.	„*5[1]*. Pentru personalul Agenției pentru Securitate Cibernetică sporul cu caracter specific se acordă pentru: 1) exercitarea funcțiilor de răspuns la incidente și crize cibernetice la nivel național; 2) exercitarea funcțiilor de identificare și evidență a furnizorilor de servicii; 3) exercitarea funcțiilor de supraveghere și control de stat al respectării de către furnizorii de servicii a cadrului normativ în domeniul securității cibernetice; 4) exercitarea funcțiilor de asigurare a cooperării la nivel național și internațional și schimb de informații în materie de securitate cibernetică, inclusiv rolul de punct național unic de contact; 5) exercitarea funcțiilor de orientare metodologică, reglementare, cercetare și dezvoltare în domeniul securității cibernetice, precum și pentru caracterul specific al suportului în realizarea funcțiilor Agenției pentru Securitate Cibernetică.*”*
		3.	La pct.6 din proiect se va revizui numerotarea reglementărilor, deoarece reglementarea de la subpct. 5) este parte a pct.5 al proiectului.	**Se acceptă.**

		4.	Cu privire la modificările propuse în pct.10 din proiect, prin care Hotărârea Guvernului nr.1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică, se completează cu pct. 6^1, se impune completarea Notei de fundamentare a proiectului cu argumente care să justifice atribuirea responsabilităților Cancelariei de Stat, Ministerului Dezvoltării Economice și Digitalizării, precum și Agenției Proprietății Publice, în vederea asigurării resursele necesare funcționării Agenției pentru Securitate Cibernetică, conform cerințelor specificate. În acest sens, este necesară o evaluare detaliată a costurilor aferente implementării acestor cerințelor și identificarea surselor de finanțare. Reieșind din cele menționate, proiectul și Nota de fundamentare urmează a fi revizuite și consultate suplimentar.	**Se acceptă** Notă informativă a fost completată cu informații privind costurile aferente implementării cerințelor, dar și sursele de acoperire a acestora. Suplimentar, urmează a fi remarcat că aceste costuri au fost prezentate în nota informativă și analiza de impact care au însoțit Legea nr. 48/2023 privind securitatea cibernetică și Hotărârea Guvernului nr. 1028/2023 cu privire la cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică.
2.	**Serviciul de Informații și Securitate** *(Nr. E/12533 din 13.11.2024)*		Lipsa obiecțiilor și propunerilor.	
3.	**IP Serviciul Tehnologia Informației și Securitate Cibernetică** *(Nr. 1.4/1627/24 din 13.11.2024)*		Comunică și reiterează următoarele obiecții.	
		5.	1) La pct. 3, sbpct. 2) lit. q) sintagma „*10) efectuarea periodică a testului de penetrare”* se va substitui cu textul „*10) efectuarea periodică a testului de vulnerabilitate”*. Această modificare se propune deoarece testul de vulnerabilitate este automatizat și din punct de vedere economic este mai avantajos a fi utilizat de către entitățile publice, având în vedere în special periodicitatea cu care trebuie efectuat. Testul de penetrare însă este util a fi realizat la sistemele informaționale la momentul inițial până la lansare sau în cazul în care au avut loc careva dezvoltări asupra acestuia, și de regulă nu este necesar să fie realizat periodic, iar instituirea obligației ca entitățile publice să	**Se acceptă**

			efectueze periodic teste de penetrare care va putea fi realizat doar de către companii specializate, presupune cheltuieli majore asupra bugetului de stat. Referitor la testul de vulnerabilitate comunicăm că, STISC va lansa un sistem pentru testarea vulnerabilităților, oferit gratuit, la solicitare entităților publice, și cu control al resurselor supuse testărilor. Totuși, dacă autorul proiectului insistă asupra necesității de realizare periodică a testului de penetrare de către entitățile publice, este absolut necesar a se analiza care va fi impactul financiar asupra bugetului de stat cu reflectarea acestui aspect în Nota de fundamentare.	
		6.	2) La **pct. 4, sbpct. 1), 2) și 4) se vor exclude**, întrucât potrivit pct. 8 sbpct. 34) din Statutul IP STISC aprobat prin Hotărârea Guvernului 414/2018, IP STISC exercită funcția de Centru guvernamental de reacţie la incidente de securitate cibernetică, iar atribuțiile aferente exercitării funcției IP STISC de Centru guvernamental de reacţie la incidente de securitate cibernetică, sunt stabilite în Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securităţii cibernetice la nivel guvernamental şi modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat. Mai mult, aceste prevederi sunt incluse în prezentul proiect la pct. 7, sbpct. 3 lit. b). Astfel, pentru evitarea dublării reglementărilor din alte acte normative, a interpretării defectuoase a normelor juridice cât și în vederea aplicării eficiente a acestora, considerăm imperios ca atribuțiile aferente funcției de CERT Gov să se regăsească doar într-un singur act normativ.	**Se acceptă**

		7.	3) La pct. 7, sbpct 3 lit. b) având în vedere timpul de reacție care se instituie pentru CERT Gov în cazul unui incident cibernetic *„pentru a furniza imediat, însă nu mai târziu de 24 a unui răspuns cu privire la incidentul cibernetic”*, apare necesitatea organizării în cadrul CERT Gov a unei echipe dedicate 24/24 (7/7) pentru monitorizarea, examinarea și reacția la incidentele de securitate cibernetic. Cu acest scop, au fost analizate necesitățile STISC pentru a putea asigura executarea acestor prevederi, și astfel comunicăm că completarea statelor de personal ale STISC cu încă 9 funcții de inginer manager de securitate informaționale dedicate acestui scop impune necesitatea unui buget suplimentar de circa 3,6 mln lei anual pentru salarizare. În context menționăm că recrutarea unor specialiști competenți în domeniul securității cibernetice, capabili să lucreze 24/24 este un proces anevoios și greu realizabil, iar asigurarea unei salarizării competitive este o condiție absolut necesară. Prin urmare, se impune completarea Notei de fundamentare a proiectului cu informația privind costurile aferente realizării de către STISC a sarcinii privind furnizarea furnizorilor de servicii persoane juridice de drept public care au notificat un incident cibernetic imediat, însă nu mai târziu de 24 ore de la recepționarea notificării, un răspuns cu privire la incidentul cibernetic care să cuprindă recomandări și instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de soluționare a incidentului respectiv.	**Se acceptă** Nota de fundamentare a fost completată.
		8.	4) La pct. 7 se va adăuga un subpunct nou, cu următorul conținut: „În conținutul Hotărârii textul *„platforme de management al incidentelor cibernetice și pentru schimbul de informații”* se va substitui cu textul	**Se acceptă** A fost completat cu modificări la anexă.

			„platforme guvernamentale de management al incidentelor cibernetice”. Această obiecție intervine în vederea evitării confuziilor cu privire la platforma de management a incidentelor cibernetice și pentru schimbul de informații care se menționează în Hotărârea Guvernului 482/2020 și care este destinată pentru a asigura cooperarea dintre CERT urile departamentale și entitățile publice cu CERT Gov și platforma menționată în proiectul de hotărâre examinat.	
		9.	5) La pct. 6, sbpct 3 lit. b) textul *„16[1] asigură securitatea rețelelor și sistemelor informatice proprietate a statului”* se va modifica cu textul „*asigură securitatea rețelelor și sistemelor informaționale proprietate a statului la nivel guvernamental”*. În context comunicăm că STISC menține această obiecție (expusă și în avizul anterior), și atrage atenția asupra necesității delimitării atribuțiilor sale aferente asigurării securității sistemelor informaționale de atribuțiilor altor entități. Astfel, deoarece conform art. 8 alin. (1) din Legea nr. 48/2023 privind securitatea cibernetică ***„pentru asigurarea securității cibernetice la nivel guvernamental, Guvernul instituie Centrul guvernamental de răspuns la incidentele cibernetice la nivelul reţelelor şi sistemelor informatice proprietate a statului****....*, din textul prevederii legale citate rezultă expres și neîndoielnic faptul că Certul guvernamental de răspuns la incidente cibernetice asigură securitatea cibernetică la nivel guvernamental, iar prevederea propusă de autorul proiectului, prin interpretarea extensivă a legii și instituirea atribuției STISC de a asigura securitatea tuturor sistemelor informaționale de stat, creează condiții de executare defectuoasă a legii. Respectiv cu scopul evitării acestui rezultat, STISC	**Se acceptă**

			insistă ca prevederea de la 16[1] sa includă sintagma „la nivel guvernamental” în vederea asigurării executării art. 8 alin. (1) din Legea 48/2023. Suplimentar comunicăm că structura și efectivul limită al STISC, la moment, este astfel organizat pentru asigurarea securității sistemelor informaționale de stat la nivel guvernamental, precum este statuat în Hotărârea Guvernului 482/2020. Mai mult, având în vedere atribuțiile STISC privind asigurarea funcționării și securității Sistemului de telecomunicații al autorităților administrației publice, comunicăm că asigurarea securității rețelelor se realizează doar până la punctul de interconectare cu rețeaua beneficiarului.	
4.	**Agenția pentru Securitate Cibernetică** *(Nr. 9-76 din 12.11.2024*		Lipsa obiecțiilor și propunerilor.	

AVIZARE III

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Cancelaria de Stat** *(Nr. 22-69-759 din 24.01.2025)*		Cu titlul general, menționăm că proiectul hotărârii a fost restituit pentru examinare pe platforma Grupului de lucru privind examinarea inițiativelor de instituire/reorganizare a autorităților administrative și a structurilor organizaționale din sfera lor de competență, în ședința din 17 ianuarie 2025. Conform celor agreate în ședința Grupului de lucru, autorul urma să excludă din proiect intervențiile la Hotărârea Guvernului nr. 1231/2018 pentru punerea în aplicare a prevederilor Legii nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar și Hotărârea Guvernului nr. 1028/2023 cu privire la	**Se acceptă** Proiectul a fost modificat conform poziției expuse de Cancelaria de Stat și Grupul de lucru privind examinarea inițiativelor de instituire/reorganizare a autorităților administrative și a structurilor organizaționale din sfera lor de competență.

			constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică. De asemenea, urma să se excludă din Nota de fundamentare referințele legate de fortificarea capacităților Serviciului Tehnologia Informației și Securitate Cibernetică, pentru care nu au fost estimate costurile și indicată sursa de acoperire. Totodată, la etapa de avizare repetată, aviz nr.22-69-12529 din 14-11-2024, s-a obiectat propunerea autorului de completare a hotărârii Guvernului nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică, cu un punct suplimentar 6^1 care impunea atribuirea unui șir de responsabilități, inclusiv Cancelariei de Stat, dar și s-a comunicat necesitatea revizuirii și consultării suplimentare a proiectul hotărârii și a notei de fundamentare. Astfel, urmare a examinării proiectului, se constată că autorul a menținut intervenția normativă în Hotărârea Guvernului nr. 1028/2023, dar și referințele din Nota de fundamentare cu privire la fortificarea capacităților Serviciului Tehnologia Informației și Securitate Cibernetică.	
		La proiectul hotărârii:		
		1.	1. La pct.2, subpct. 2.2 textul normei urmează a fi completat cu textul „conform prevederilor Legii nr. 131/2012 privind controlul de stat” după cuvintele „Legea nr. 48/2023 privind securitatea cibernetică”.	**Se acceptă**
			La pct. 3:	
		2.	a). la subpct. 3.2.6 și 3.2.7.1, prin care se propune substituirea cuvântului „autorității” cu „instituției”, pentru o mai marea claritate și pentru a se exclude orice echivoc, se recomandă utilizarea sintagmei „entități publice”, sintagmă consacrată în Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare	**Precizare** În contextul proiectului HG privire la modul de implementare a măsurilor de securitate a rețelelor și sistemelor informatice de către furnizorii de servicii în sectoarele critice (număr

			pentru asigurarea securității cibernetice la nivel guvernamental și Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat.	unic 49/MDED/2025), care prevede abrogarea Hotărârii Guvernului nr. 201/2017 ”Cu privire la aprobarea Cerințelor minime obligatorii de securitate cibernetică”, prevederile pct.3 au fost excluse din proiect.
		3.	b). la subpct. 3.2.17.5 textul „10) efectuarea periodică a testului de penetrare” se va substitui cu textul „10) efectuarea periodică a testului de vulnerabilitate”. Această modificare este justificată prin faptul că testul de vulnerabilitate, fiind automatizat, este mai economic pentru entitățile publice, mai ales având în vedere periodicitatea necesară. În schimb, testul de penetrare este indicat în etapele inițiale, înainte de lansarea sistemelor informaționale sau în cazul unor modificări semnificative aduse acestora. De regulă, acesta nu necesită realizare periodică, iar obligativitatea de a efectua periodic teste de penetrare, care pot fi realizate doar de companii specializate, ar genera costuri semnificative pentru bugetul de stat. În cazul în care se consideră indispensabilă realizarea periodică a testului de penetrare de către entitățile publice, este esențial să se efectueze o analiză detaliată a impactului financiar asupra bugetului de stat, și reflectarea acestuia în Nota de fundamentare.	**Precizare** În contextul proiectului HG privire la modul de implementare a măsurilor de securitate a rețelelor și sistemelor informatice de către furnizorii de servicii în sectoarele critice (număr unic 49/MDED/2025), care prevede abrogarea Hotărârii Guvernului nr. 201/2017 ”Cu privire la aprobarea Cerințelor minime obligatorii de securitate cibernetică”, prevederile pct.3 au fost excluse din proiect.
		4.	La pct. 5-7 se va revedea numerotarea subpunctelor din proiect, în scopul asigurării corespunderii cu numerotarea punctelor.	**Se acceptă**
			La pct. 6:	
		5.	a). la subpct. 7.3.3.3 (care va fi renumerotat în 6.3.3.3) textul „însă nu mai târziu de 24 ore de la recepționarea notificării” se va exclude. În cazul menținerii acestei prevederi și a instituirii unei astfel de obligații pentru CERT Gov în gestionarea incidentelor cibernetice,	**Se acceptă** Sintagma „însă nu mai târziu de 24 ore de la recepționarea notificării” a fost exclusă.

			devine necesară organizarea unei echipe dedicate, operabile 24/24 (7/7), pentru monitorizarea, examinarea și reacția la incidentele de securitate cibernetică. În acest sens, Nota de fundamentare se va completa cu informații privind costurile asociate și sursa de acoperire realizării de către Serviciului Tehnologia Informației și Securitate Cibernetică a acestei sarcini, care implică furnizarea unui răspuns către furnizorii de servicii persoane juridice de drept public ce au notificat un incident cibernetic, în termenul stabilit de 24 ore de la recepționarea notificării.	
		6.	b). la subpct 7.3.3.4 (care va fi renumerotat în 6.3.3.4) textul „16[1] asigură securitatea rețelelor și sistemelor informatice proprietate a statului” se va substitui cu textul „asigură securitatea rețelelor și sistemelor informaționale proprietate a statului la nivel guvernamental”. În context, se accentuează necesitatea delimitării atribuțiilor Serviciului Tehnologia Informației și Securitate Cibernetică aferente asigurării securității sistemelor informaționale de atribuțiilor altor entități. Astfel, conform art. 8 alin. (1) din Legea nr. 48/2023 privind securitatea cibernetică, „pentru asigurarea securității cibernetice la nivel guvernamental, Guvernul instituie Centrul guvernamental de răspuns la incidentele cibernetice la nivelul rețelelor şi sistemelor informatice proprietate a statului...”. Din textul acestei prevederi legale rezultă clar și fără echivoc faptul că Centrul guvernamental de răspuns la incidentele cibernetice este responsabil pentru asigurarea securității cibernetice la nivel guvernamental. Propunerea autorului proiectului, privind extinderea atribuțiilor Serviciului Tehnologia Informației și Securitate Cibernetică pentru a include securitatea tuturor	**Se acceptă**

			sistemelor informaționale de stat, depășește cadrul legal instituit și poate conduce la executarea defectuoasă a legii. Pentru a evita această situație, Serviciul Tehnologia Informației și Securitate Cibernetică insistă ca prevederea de la punctul 16^1 să includă explicit sintagma „la nivel guvernamental”, asigurând astfel conformitatea cu art. 8 alin. (1) din Legea nr. 48/2023. De asemenea, menționăm că structura și efectivul limită al Serviciului Tehnologia Informației și Securitate Cibernetică sunt organizate în prezent pentru a asigura securitatea sistemelor informaționale de stat exclusiv la nivel guvernamental, conform Hotărârii Guvernului nr. 482/2020. În plus, având în vedere atribuțiile Serviciului Tehnologia Informației și Securitate Cibernetică privind funcționarea și securitatea Sistemului de telecomunicații al autorităților administrației publice, subliniem că securitatea rețelelor este asigurată doar până la punctul de interconectare cu rețeaua beneficiarului.	
		7.	La pct. 7, subpct. 8.2 (care urmează a fi renumerotat în 7.2), prin care se introduce un punct nou 560^2 , textul normei urmează a fi completat cu cuvintele „conform prevederilor Legii nr. 131/2012 privind controlul de stat” după cuvintele „Legea nr. 48/2023 privind securitatea cibernetică”.	**Se acceptă**
		8.	La pct. 8, prin care se introduce un punct nou 72^2 , textul normei urmează a fi completat cu textul „conform prevederilor Legii nr.131/2012 privind controlul de stat” după cuvintele „Legea nr. 48/2023 privind securitatea cibernetică” .	**Se acceptă**
		9.	Pct.9 din proiect se va exclude.	**Se acceptă** Totodată, menționăm că prevederile Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului privind măsuri pentru un

				nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS 2), inclusiv prevederile Articolului 11 din Directivă, urmează ulterior obligatoriu a fi integral transpuse în cadrul normativ național, fiind una din condiționalitățile impuse RM în procesul de aderare la UE.
			La nota de fundamentare:	
		10.	Compartimentul 4.2 Impactul financiar și argumentarea costurilor estimative se va revizui în conformitate cu Notele de la NOTA DE FUNDAMENTARE, aprobate prin Anexa nr. 1 la Legea nr. 100/2017 cu privire la actele normative.	**Se acceptă** **Precizare** Drept urmare a poziției expuse de Cancelaria de Stat și Grupul de lucru privind examinarea inițiativelor de instituire/reorganizare a autorităților administrative și a structurilor organizaționale din sfera lor de competență, referințele legate de fortificarea capacităților Serviciului Tehnologia Informației și Securitate Cibernetică au fost excluse din Nota de fundamentare. Totodată, în contextul proiectului HG privire la modul de implementare a măsurilor de securitate a rețelelor și sistemelor informatice de către furnizorii de servicii în sectoarele critice (număr unic 49/MDED/2025), care prevede abrogarea Hotărârii Guvernului nr. 201/2017 ”Cu privire la aprobarea Cerințelor minime obligatorii de securitate cibernetică”, prevederile pct.3 au fost excluse din proiect.

2.	**Ministerul Finanțelor** *(Nr. 07/3-03-10/106 din 30.01.2025)*	11.	Potrivit modificărilor/completărilor la proiectul hotărârii, autorul la etapa de definitivare înaintează propuneri privind completarea/modificarea *prevederilor Hotărârii Guvernului nr. 1028/2023 cu privire la constituirea, organizarea şi funcționarea Agenției pentru Securitate Cibernetică (pct.9 al proiectului)*. Suplimentar, autorul indică în compartimentul 4.2 din nota de fundamentare că proiectul necesită alocarea resurselor suplimentare în sumă de cca 10,0 mil lei pentru investițiile inițiale în dezvoltarea și configurarea infrastructurii digitale și a sistemelor informaționale (achiziționarea de echipamente specializate, crearea de software personalizat). Mai mult, ulterior va fi nevoie de alte cheltuieli pentru mentenanța și actualizarea sistemelor informaționale, asigurarea securității și reacția de cel mult 24 ore la incidente cibernetice etc, care nu sunt cuantificate de autor. În context, ținând cont că implicarea partenerilor de dezvoltare va reduce semnificativ presiunea financiară asupra bugetului de stat, se necesită *completarea impactului financiar cu informația detaliată privind costurile necesare pentru fiecare măsură, sumele alocate în bugetul de stat şi suportul partenerilor de dezvoltare planificat* în acest sens.	**Precizare** Prevederile pct.9 al proiectului (propuneri privind completarea/modificarea prevederilor Hotărârii Guvernului nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică) au fost excluse din proiect drept urmare a avizului înaintat de Cancelaria de Stat.
		12.	Cu titlul de informare, în Legea bugetului de stat pentru anul 2025 nr. 310/2024 în bugetul Ministerului Dezvoltării Economice și Digitalizării, la subprogramul 1504 „Tehnologii informaționale” au fost aprobate cheltuieli în sumă de 20,4 mil lei, dintre care 15,7 mil lei pentru cheltuieli de personal, 1,5 mil lei pentru reparații curente și cca 3,2 mil lei alte cheltuieli. Respectiv, costurile indicate de autor în nota de fundamentare nu sunt planificate în bugetul de stat	**Precizare** Prevederile pct.9 al proiectului (propuneri privind completarea/modificarea prevederilor Hotărârii Guvernului nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică) au fost excluse din proiect drept urmare

			pentru anul 2025, mai mult, nici în CBTM pentru anii 2025-2027. În concluzie, impactul financiar al proiectului urmează a fi ajustat prin prisma celor expuse mai sus, dat fiind faptul că conform prevederilor art.17 alin.(2) din Legea finanțelor publice și responsabilității bugetar-fiscale nr. 181/2014, pe parcursul anului bugetar nu pot fi puse în aplicare decizii care conduc la majorarea cheltuielilor bugetare, dacă impactul financiar al acestora nu este prevăzut în buget, iar conform art. 131 alin. (6) din Constituția RM, nici o cheltuială bugetară nu poate fi aprobată fără stabilirea sursei de finanțare.	a avizului înaintat de Cancelaria de Stat.
		13.	Deasemenea, menționăm că în conformitate cu anexa nr.2 din Legea nr.100/2017 cu privire la actele normative, proiectul prezentat spre reavizare trebuie să includă și sinteza obiecțiilor/propunerilor și recomandărilor, care lipsește din documentele de proiect.	**Se acceptă**

Secretar de stat **Cătălina PLINSCHI**