1440a/21.07.2026

Parlamentul României
SENAT

INTREBARE

Adresată: Domnului Ambrozie-Irineu Darău - Ministrul Economiei, Digitalizării, Antreprenoriatului și Turismului

și

Domnului Dan Cîmpean - Directorul General al Directoratului Național de Securitate Cibernetică (DNSC)

De către Doamna senator:	**Niculina STELEA**
Circumscripția electorală:	**Nr. 42, București**
Grupul Parlamentar:	**A.U.R.**
Data:	**21.07.2026**

Obiectul întrebării – ***Respectarea prevederilor OUG nr. 155/2024 privind securitatea cibernetică (transpunerea Directivei NIS2) în contextul incidentelor cibernetice care au afectat infrastructuri digitale esențiale ale statului***

Stimate Domnule Ministru,

Stimate Domnule Director General,

În ultimele zile, România s-a confruntat cu mai multe incidente cibernetice care au afectat funcționarea unor sisteme informatice cu impact major asupra cetățenilor și economiei. Agenția Națională de Cadastru și Publicitate Imobiliară (ANCPI) a confirmat că aplicația e-Terra și alte sisteme informatice au devenit indisponibile în urma unui atac cibernetic, incident descris chiar de instituție drept cea mai amplă întrerupere tehnică din istoria sa.

Totodată, în spațiul public au fost semnalate incidente care au afectat și platforme informatice aferente implementării Planului Național de Redresare și Reziliență (PNRR), ceea ce ridică serioase semne de întrebare cu privire la nivelul de pregătire și reziliență al infrastructurilor digitale esențiale ale statului.

Aceste incidente survin într-un context în care România a adoptat OUG nr. 155/2024 privind instituirea cadrului național de securitate cibernetică, act normativ care transpune

Directiva (UE) 2022/2555 (NIS2) și stabilește obligații explicite atât pentru entitățile esențiale și importante, cât și pentru autoritatea competentă – Directoratul Național de Securitate Cibernetică (DNSC).

Având în vedere cele de mai sus, vă solicit respectuos să răspundeți la următoarele întrebări:

1. Sunt ANCPI și instituțiile responsabile de administrarea sistemelor informatice aferente PNRR încadrate ca entități esențiale sau importante în sensul OUG nr. 155/2024?

2. Au fost acestea identificate și înscrise în evidențele prevăzute de OUG nr. 155/2024 și au notificat DNSC cu privire la măsurile implementate pentru conformare?

3. Ce activități de supraveghere, control sau audit a desfășurat DNSC asupra acestor entități de la intrarea în vigoare a OUG nr. 155/2024 până la producerea incidentelor?

4. Au fost constatate anterior neconformități privind managementul riscurilor cibernetice, continuitatea activității, managementul vulnerabilităților, controlul accesului, backup-ul sau răspunsul la incidente?

5. Au fost dispuse măsuri obligatorii de remediere? Dacă da, care au fost acestea și în ce stadiu de implementare se aflau la data producerii incidentelor?

6. Au fost incidentele raportate către DNSC în termenele prevăzute de legislația NIS2 și de OUG nr. 155/2024? Dacă da, când au fost primite notificările inițiale, intermediare și finale?

7. Ce sprijin operațional și tehnic a acordat DNSC instituțiilor afectate în gestionarea incidentelor și în restabilirea funcționării sistemelor?

8. În urma investigațiilor, apreciază DNSC că obligațiile prevăzute de OUG nr. 155/2024 au fost respectate integral de către entitățile afectate?

9. În cazul în care vor fi constatate încălcări ale obligațiilor legale, ce măsuri administrative și sancțiuni intenționează să aplice DNSC și în ce calendar?

10. Care este numărul controalelor efectuate de DNSC, de la intrarea în vigoare a OUG nr. 155/2024, asupra entităților esențiale și importante din administrația publică centrală și care sunt principalele tipuri de deficiențe identificate?

11. Ce măsuri suplimentare intenționează DNSC să implementeze pentru creșterea rezilienței cibernetice a infrastructurilor digitale esențiale ale statului, în condițiile intensificării atacurilor cibernetice la nivel european?

12. Consideră DNSC că dispune, în prezent, de resursele umane, financiare și tehnice necesare pentru exercitarea atribuțiilor extinse conferite prin transpunerea Directivei NIS2? Dacă nu, ce măsuri sunt necesare pentru consolidarea capacității instituționale?

Având în vedere impactul major pe care indisponibilitatea acestor sisteme informatice îl are asupra cetățenilor, mediului de afaceri și funcționării serviciilor publice, consider că Parlamentul trebuie informat în mod complet cu privire la modul în care cadrul legal rezultat din transpunerea Directivei NIS2 este aplicat în practică, precum și cu privire la măsurile adoptate pentru prevenirea producerii unor incidente similare în viitor.

În acest context, vă solicit să îmi transmiteți un răspuns oficial, în scris, în termenul prevăzut de legislația în vigoare.

Vă mulțumesc anticipat pentru colaborare și aștept cu interes răspunsul dumneavoastră.

Cu considerație,

Niculina STELEA - Senator A.U.R. București