SECRETARIATUL GENERAL AL GUVERNULUI
DEPARTAMENTUL PENTRU RELAȚIA CU PARLAMENTUL
B-dul Primăverii nr. 22, sector 1, București, Tel: 0213143400 int.3000, Email: drparlament@gov.ro

Nr. 9994, 10156, 10157, 10158, 10159/DRP

11 -09- 2026

PARLAMENTUL ROMÂNIEI
CAMERA DEPUȚATILOR
SECRETAR
Intrare Nr. 66-7/10
2026 Luna 09 Ziua 15

Către: **Doamna Ramona-Ioana BRUYNSEELS**
Secretar al Camerei Deputaților

Ref. la: **Răspunsuri la întrebări/interpelări formulate de deputați**

Stimată doamnă secretar,

Vă transmitem, alăturat, răspunsurile instituțiilor vizate cu privire la unele întrebări/interpelări formulate de deputați, potrivit tabelului anexat.

Cu deosebită considerație,

NINI SĂPUNARU

SECRETAR DE STAT

6067A

Nr. 10156 / DRP
DATA 10 -09- 2026

Ministerul Dezvoltării,
Lucrărilor Publice și Administrației

Cabinet ministru
Bd. Libertății nr. 16,
Latura Nord, sector 5
București, cod poștal 050706

Tel : +4 0372 111 506
Fax: +4 0372 111 337
www.mdlpa.ro

Nr. 207137/08.09.2026

Către: DOMNUL DEPUTAT FLORIN BOGDAN VELCESCU
PARLAMENTUL ROMÂNIEI - CAMERA DEPUTAȚILOR

Referitor la: întrebarea dumneavoastră, înregistrată la Camera Deputaților cu **nr. 6067A/2026,** având ca obiect **"Atacul cibernetic asupra ANCPI din 14 iulie 2026"**

Stimate domnule deputat,

Ca urmare a întrebării dumneavoastră prin care solicitați informații privind *atacul cibernetic ce a avut loc în data de 14.07.2026 asupra infrastructurii informatice a Agenției Naționale de Cadastru și Publicitate Imobiliară (ANCPI) și care a blocat activitatea agenției timp de mai multe săptămâni*, vă comunicăm următoarele:

Cu privire la **primul punct** din întrebare, "*Care a fost conținutul avertizărilor scrise transmise conducerii ANCPI cu privire la vulnerabilitățile infrastructurii informatice înainte de 14 iulie 2026 și ce măsuri a dispus conducerea instituției ca urmare a acestora?*", precizăm că în cadrul cooperării interinstituționale, ANCPI a primit notificări și alerte referitoare la riscuri și vulnerabilități de securitate cibernetică. Aceste comunicări au vizat aspecte tehnice aferente unor componente ale infrastructurii informatice și au fost analizate și gestionate potrivit procedurilor aplicabile.

La nivelul ANCPI au fost adoptate, în diferite etape, măsuri de protecție, actualizare, realizare a copiilor de siguranță și modernizare a infrastructurii informatice, în funcție de necesitățile tehnice și de recomandările primite.

Ulterior identificării incidentului au fost dispuse măsuri suplimentare pentru limitarea efectelor și consolidarea securității, printre care izolarea infrastructurii afectate, restricționarea temporară a conexiunilor și a accesului la distanță, schimbarea credențialelor administrative și a cheilor de securitate, verificarea bazelor de date și a copiilor de siguranță, actualizarea mecanismelor de protecție, extinderea autentificării multifactor și reconstruirea etapizată a infrastructurii în Cloudul Guvernamental.

Conținutul tehnic integral al notificărilor, modul în care acestea au fost gestionate și eventuala lor legătură cu împrejurările producerii incidentului sunt analizate în cadrul investigațiilor tehnice și al cercetării penale aflate în desfășurare. Din considerente privind protejarea infrastructurii și pentru a nu afecta aceste verificări, în acest moment nu pot fi comunicate informații tehnice sau operaționale suplimentare.

Până la finalizarea investigațiilor nu se poate concluziona că o anumită avertizare ar fi anticipat mecanismul concret al incidentului sau că aceasta nu ar fi fost gestionată corespunzător.

În ceea ce privește **punctul doi**, *"Din ce motiv ANCPI nu s-a înscris în sistemul de siguranță NIS, gestionat de DNSC, deși avea această obligație legală din septembrie 2025? Cine poartă răspunderea administrativă pentru această neconformare?"*, precizăm că ANCPI este înscrisă în Registrul entităților gestionat de Directoratul Național de Securitate Cibernetică (DNSC), decizia de identificare și înscriere fiind emisă ulterior producerii incidentului de securitate cibernetică.
Procedura de înscriere presupune transmiterea notificării, analizarea de către DNSC a informațiilor comunicate și emiterea deciziei de identificare și înscriere a entității.
Faptul că decizia de înscriere a ANCPI în Registrul entităților gestionat de Directoratul Național de Securitate Cibernetică a fost emisă ulterior producerii incidentului nu permite, prin el însuși, stabilirea unei legături de cauzalitate între data înscrierii și producerea incidentului și nici atribuirea automată a unei răspunderi administrative.
Stabilirea unei eventuale răspunderi revine autorităților competente și poate fi realizată numai după finalizarea verificărilor privind obligațiile legale aplicabile, împrejurările concrete și atribuțiile persoanelor implicate. În lipsa unui act definitiv de constatare, indicarea unei persoane responsabile ar fi prematură.

Referitor la **punctul trei**, *„Vă solicit transmiterea raportului integral (sau, dacă anumite secțiuni fac obiectul unei anchete penale, un rezumat detaliat neconfidențial) privind cauzele tehnice ale atacului și gradul de compromitere a infrastructurii ANCPI"*, menționăm faptul că documentele tehnice întocmite în cadrul investigațiilor conțin informații privind arhitectura infrastructurii informatice, configurațiile sistemelor, vulnerabilitățile analizate și mecanismele de securitate. Comunicarea integrală a acestor informații într-un document destinat difuzării ar putea genera riscuri suplimentare pentru securitatea sistemelor și ar putea afecta investigațiile tehnice și cercetarea penală aflate în desfășurare. Din aceste considerente, raportul tehnic integral nu poate fi comunicat în cadrul prezentului răspuns. Documentele pot fi puse la dispoziția autorităților și instituțiilor competente, în condițiile legii și prin canalele instituționale corespunzătoare.
Ca un rezumat, fără a include informații confidențiale, precizăm că, în data de 14 iulie 2026, ANCPI a identificat un acces neautorizat asupra unor componente ale infrastructurii informatice. Potrivit constatărilor preliminare, accesul inițial a vizat o aplicație web expusă public, fiind ulterior afectată disponibilitatea unor componente informatice. Imediat după identificarea incidentului au fost dispuse măsuri de izolare a infrastructurii, limitare a propagării, conservare a probelor digitale, verificare a sistemelor și protejare a bazelor de date. Aplicația e-Terra nu a fost identificată ca sursă inițială a incidentului. Funcționarea acesteia a fost oprită temporar, cu caracter preventiv, pentru efectuarea verificărilor de integritate și securitate și pentru reconstruirea infrastructurii necesare funcționării sale într-un mediu securizat.

Până la această dată, nu a fost confirmată compromiterea bazelor de date care gestionează evidențele de cadastru și publicitate imobiliară și nici exfiltrarea unor date din acestea. Verificările efectuate asupra infrastructurii de stocare, a bazelor de date și a copiilor de siguranță nu au confirmat compromiterea integrității datelor administrate prin sistemul e-Terra.
Stabilirea mecanismului complet de producere a incidentului, a naturii și întinderii componentelor afectate și a existenței unor eventuale transferuri neautorizate de informații face în continuare obiectul investigațiilor tehnice și al cercetării penale. Concluziile vor putea fi formulate numai după finalizarea acestor activități.

În ceea ce privește **punctul patru**, *"Care este valoarea totală a contractelor active de securitate cibernetică și mentenanță IT ale ANCPI la data atacului, cine sunt operatorii economici contractanți, prin ce proceduri de achiziție au fost atribuite aceste contracte și ce clauze contractuale privind testarea periodică a securității sistemelor și obligația de raportare a vulnerabilităților conțineau?"*, precizăm că la data de 14 iulie 2026, ANCPI nu avea în derulare contracte distincte având ca obiect prestarea unor servicii integrate de securitate cibernetică pentru întreaga infrastructură informatică a instituției.
Serviciile de mentenanță și suport tehnic sunt prevăzute în cadrul contractelor aferente fiecărei aplicații informatice, în funcție de obiectul, caracteristicile și cerințele tehnice specifice acesteia. În consecință, nu există o valoare totală evidențiată distinct sub forma unor *„contracte de securitate cibernetică și mentenanță IT"* și niciun set unic de clauze aplicabil tuturor sistemelor informatice ale ANCPI. Obligațiile prestatorilor sunt stabilite prin fiecare contract, în raport cu serviciile și componentele informatice care fac obiectul acestuia.
Singurul instrument contractual care vizează în mod direct o soluție de protecție informatică este acordul-cadru încheiat în anul 2023, având ca obiect furnizarea serviciilor de suport tehnic aferente soluției antivirus implementate la nivelul stațiilor de lucru din cadrul ANCPI. Acordul-cadru include servicii de suport tehnic din partea producătorului soluției, actualizarea versiunilor aplicației, actualizarea semnăturilor de securitate și asigurarea funcționării corespunzătoare a soluției de protecție antivirus instalate pe calculatoarele utilizatorilor. Rolul acestui acord-cadru este de a asigura suportul tehnic și menținerea la zi a soluției antivirus utilizate pentru protejarea stațiilor de lucru împotriva amenințărilor informatice, în conformitate cu specificațiile tehnice și obligațiile contractuale asumate. Obiectul nu îl reprezintă însă testarea periodică a securității tuturor aplicațiilor și componentelor infrastructurii ANCPI și nici furnizarea unui serviciu general de monitorizare și raportare continuă a vulnerabilităților la nivelul întregului sistem informatic.
Datele referitoare la operatorii economici, valorile contractuale și procedurile de atribuire aferente fiecărui contract, precum și acordului-cadru menționat, pot fi prezentate distinct, pe baza evidențelor structurilor de specialitate competente.

Cu privire la **punctul cinci**, *"A verificat ministerul, la momentul atribuirii sau ulterior, eventualele incompatibilități sau conflicte de interese privind operatorii economici contractanți pentru servicii de securitate cibernetică a ANCPI?"*, precizăm că, până în prezent, nu ne-a fost comunicat niciun act de

constatare sau o decizie definitivă a unei autorități competente prin care să fie confirmată existența unor incompatibilități ori conflicte de interese privind operatorii economici menționați.
În absența unei asemenea constatări, premisa existenței unor incompatibilități sau conflicte de interese nu poate fi considerată dovedită, neputând fundamenta atribuirea unei răspunderi.

În ceea ce privește **punctul șase**, *"Ce măsuri de verificare a respectării regimului incompatibilităților și conflictelor de interese au fost aplicate în legătură cu atribuirea de contracte publice de către ANCPI și structurile sale teritoriale către operatori economici cu legături cu persoane din conducerea instituției sau cu rude ale acestora?"*, menționăm faptul că procedurile de achiziție publică derulate de ANCPI și de instituțiile subordonate se desfășoară cu respectarea dispozițiilor legale aplicabile, inclusiv a obligațiilor privind prevenirea, identificarea și gestionarea situațiilor de incompatibilitate și conflict de interese. În cadrul acestor proceduri sunt aplicate mecanismele de verificare și control prevăzute de legislația achizițiilor publice și sunt solicitate declarațiile și documentele necesare persoanelor implicate. Procedurile pot fi supuse verificării instituțiilor cu atribuții de control, potrivit competențelor acestora.
Oficiile de cadastru și publicitate imobiliară și Centrul Național de Cartografie au personalitate juridică proprie, iar procedurile de achiziție derulate de acestea sunt organizate și asumate la nivelul fiecărei autorități contractante.
ANCPI nu a primit o constatare definitivă a unei autorități competente care să confirme premisa atribuirii unor contracte către operatori economici aflați în legăturile descrise în întrebare.

Referitor la punctul șapte, *„Ce măsuri disciplinare sau de altă natură intenționează ministerul să dispună față de conducerea ANCPI, având în vedere concluziile preliminare ale DNSC potrivit cărora incidentul putea fi prevenit?"*, precizăm faptul că atât cauzele incidentului, legăturile de cauzalitate, cât și eventualele responsabilități fac obiectul investigațiilor tehnice și al cercetării penale aflate în desfășurare. Până la finalizarea acestora, nu pot fi formulate concluzii definitive și nu pot fi anticipate eventuale măsuri administrative ori disciplinare.
În cazul în care autoritățile competente vor constata încălcări ale obligațiilor legale, profesionale sau contractuale, vor putea fi dispuse măsurile prevăzute de lege, cu respectarea competențelor instituționale și a dreptului la apărare.

Cu privire la **punctul opt**, *"Care este calendarul concret de repunere integrală în funcțiune a sistemului e-Terra și ce garanții tehnice suplimentare vor fi implementate pentru a preveni repetarea unui incident similar?"*, precizăm că Aplicația e-Terra este funcțională la nivelul tuturor oficiilor de cadastru și publicitate imobiliară și permite înregistrarea și procesarea cererilor. Infrastructura necesară funcționării acesteia a fost reconstruită și migrată în Cloudul Guvernamental, fiind supusă verificărilor tehnice și de securitate, precum și testelor funcționale și de performanță înainte de repunerea în exploatare. Procesul de restaurare privește însă un ansamblu mai larg de aplicații și servicii informatice interdependente. Celelalte platforme online gestionate de ANCPI sunt

repuse în funcțiune etapizat, numai după verificarea fiecărei componente, remedierea aspectelor identificate și confirmarea îndeplinirii condițiilor de stabilitate și securitate, neputând fi, astfel, indicată o dată unică pentru reactivarea simultană a tuturor serviciilor informatice.
În cadrul procesului de consolidare a securității au fost implementate sau sunt în curs de implementare următoarele măsuri:

- reconstruirea și migrarea etapizată a componentelor critice în Cloudul Guvernamental;
- extinderea utilizării autentificării multifactor;
- revizuirea politicilor de administrare a identităților și accesului;
- schimbarea credențialelor administrative și a cheilor de securitate;
- revizuirea și securizarea accesului la distanță;
- actualizarea echipamentelor și a mecanismelor de securitate;
- consolidarea infrastructurii de backup și de recuperare în caz de dezastru;
- realizarea unor copii suplimentare de siguranță și a unor puncte suplimentare de restaurare;
- introducerea unor măsuri suplimentare de monitorizare, detectare și răspuns;
- efectuarea testelor funcționale, de securitate și de performanță înaintea repunerii în exploatare;
- continuarea evaluărilor tehnice și a monitorizării împreună cu instituțiile abilitate.

În domeniul securității cibernetice nu poate fi oferită o garanție absolută privind imposibilitatea producerii unui nou incident. Măsurile adoptate urmăresc reducerea riscurilor, limitarea impactului unor eventuale evenimente și creșterea capacității de prevenire, detectare și răspuns. Prioritatea ANCPI o reprezintă restabilirea integrală a capacității operaționale, protejarea datelor administrate și reluarea tuturor serviciilor în cel mai scurt timp posibil, exclusiv în condiții de stabilitate și securitate.
Ministerul Dezvoltării, Lucrărilor Publice și Administrației își exprimă, și pe această cale, totala deschidere față de solicitările formulate de către membrii Parlamentului României, ca importantă resursă pentru optimizarea politicilor sale.

Cu deosebită considerație,

p. MINISTRUL DEZVOLTĂRII, LUCRĂRILOR PUBLICE ȘI ADMINISTRAȚIEI,
SUBSECRETAR DE STAT
GABRIEL TRAIAN GHILEA

Ghilea
Gabriel-Traian