NOTĂ DE FUNDAMENTARE

Secţiunea 1 **Titlul proiectului de act normativ** **Hotărâre a Guvernului** **privind aprobarea Strategiei de Securitate Cibernetică a României şi a Planului de Acţiune 2021-2026**	
Secţiunea a 2-a **Motivul emiterii actului normativ**	
1. Descrierea situaţiei actuale	Creşterea gradului de digitalizare şi conectivitate atât la nivelul României, al Uniunii Europene, dar şi la nivel global, duce la o serie de beneficii majore dar şi la o agravare a riscurilor de securitate cibernetică, societatea şi economia devenind astfel mai vulnerabile la ameninţările cibernetice. Se amplifică ameninţările cibernetice persistente orchestrate de actori statali şi non-statali ce vizează instituţii ale statului, operatori economici şi infrastructuri cibernetice naţionale din transport, sănătate, energie, sectorul financiar-bancar, apă potabilă, servicii poştale şi de curierat, termoficare, infrastructurile digitale, industria chimică şi farmaceutică, administraţia publică centrală şi locală, cât şi persoane private, riscând, prin toate acestea, să pună în pericol buna funcţionare a societăţii româneşti în ansamblul său, precum şi din perspectiva apartenenţei României la structurile Uniunii Europene. La nivel naţional, ameninţarea cibernetică se situează în prezent pe un trend ascendent şi susţinut, principala provocare la adresa securităţii cibernetice fiind reprezentată de atacurile cibernetice derulate de entităţi asociate unor actori statali, de grupări de criminalitate cibernetică, precum şi de grupări de hackeri cu motivaţie ideologică, politică sau extremist-teroristă. Amploarea, frecvenţa, complexitatea şi impactul incidentelor de securitate cibernetică sunt într-o creştere constantă şi reprezintă o ameninţare gravă pentru funcţionarea infrastructurilor, a reţelelor şi a sistemelor informatice, atât la nivelul României cât şi la nivelul Uniunii Europene, cu impact major la adresa securităţii naţionale, societăţii şi economiei. Toate aceste ameninţări de natură cibernetică necesită un răspuns determinat, decisiv, coordonat şi coerent la nivelul instituţiilor competente ale statului român. Mai mult, în ultima perioadă, numărul şi amploarea incidentelor de securitate cibernetică observate la nivelul ţării au crescut continuu, iar situaţia de criză generată de răspândirea virusului SARS-COV-2 a scos în evidenţă şi mai mult acest lucru. Consecinţele atacurilor şi incidentelor cibernetice se reflectă asupra tuturor sectoarelor importante pentru statul român şi pot genera pierderi majore ori chiar pot conduce la materializarea unor riscuri severe la adresa securităţii naţionale. În aceste condiţii, securitatea şi reziliența infrastructurilor, a reţelelor şi a sistemelor informatice trebuie incluse în priorităţile statului român,