13.05.2025

Propuneri de modificare ale AmCham România privind
Ordinul pentru aprobarea criteriilor și pragurilor de determinare a gradului de perturbare a unui serviciu și metodologia de evaluare a nivelului de risc al entităților

Observații generale:
În urma unei interpretări coroborate a prevederilor legale privind clasificarea entităților ca esențiale sau importante, înțelegerea noastră este că, în funcție de rezultatul evaluării nivelului de risc, o entitate clasificată inițial ca importantă poate fi reîncadrată drept esențială, în cazul în care perturbarea serviciilor furnizate de aceasta ar avea un impact semnificativ. Totuși, inversul nu ar fi posibil — respectiv, o entitate desemnată inițial ca esențială nu ar putea fi ulterior reclasificată ca importantă. Vă rugăm să ne confirmați dacă această interpretare este corectă sau, în caz contrar, să ne indicați dacă este permisă o abordare alternativă, potrivit căreia o entitate încadrată inițial ca esențială ar putea fi ulterior reclasificată ca importantă, de exemplu, în considerarea măsurilor robuste de securitate cibernetică pe care le are implementate.

Nr. articol	Forma din proiect	Forma propusă	Motivare
Art.4 alin. (3)	(3) În vederea determinării nivelului de risc al entității, Directoratul Național de Securitate Cibernetică, în continuare DNSC, stabilește un scor de bază pentru fiecare sector din fiecare anexă la Ordonanța de urgență a Guvernului nr. 155/2024. Scorul final obținut de către entitate determină nivelul de complexitate a măsurilor de securitate, aferent standardului Cyber Fundamentals.	Completare Ordin cu definiție/detalii privind standardul Cyber Fundamentals referit (ex. emitent, modalitate de accesare, versiune)	Formularea actuală poate genera confuzie, întrucât „standardul Cyber Fundamentals" nu este definit în mod explicit/nu poate fi identificat. Prin corelarea nivelelor prevăzute la Anexa nr.2, Art. 3, pct. 5 presupunem că cel mai probabil intenția legiuitorului a fost de a referi CyberFundamentals Framework (https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework), dar este necesară clarificarea privind necesitatea utilizării acestui framework sau intenția legiuitorului de a dezvolta un astfel de standard aplicabil în corelare cu prezentul ordin.
Anexa nr.2 – Art. 4 alin. (2)	(2) DNSC recomandă tuturor entităților cărora nu li se aplică prevederile Ordonanței de urgență a Guvernului nr. 155/2024 să implementeze cerințele standardului Cyber Fundamentals, nivel „Basic".		
Art. 1 (1)	Entitățile, astfel cum acestea sunt definite la art. 4 lit. f) din Ordonanța de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil,	**Art. 1** – (1) Entitățile, astfel cum acestea sunt definite la art. 4 lit. f) din Ordonanța de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național	Nu este clar cui se aplică acest ordin, pentru că, conform OUG 155, entitățile de la Art. 5 (2) sunt deja incluse la Art. 5 (1) b)

	care nu au fost calificate drept entități esențiale sau entități importante conform art. 5 alin. (1) lit. a), c) - f), alin. (2)-(4), art. 6 alin. (1) și alin. (2) lit. b) și c) și nici conform art. 9 lit. a) și d) din același act normativ, realizează evaluarea gradului de perturbare a serviciilor în vederea completării informațiilor solicitate conform ordinului directorului Directoratului Național de Securitate Cibernetică pentru aprobarea cerințelor privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor.	civil, care ~~nu~~ au fost calificate drept entități esențiale sau entități importante conform art. 5 alin. (1) lit. b....	
Art. 2	Rezultatele autoanalizei privind faptul că entitatea este singurul furnizor al unui serviciu care este esențial pentru susținerea unor activități societale și economice critice, conform dispozițiilor art. 9 lit. a) din Ordonanța de urgență a Guvernului nr. 155/2024, astfel cum acestea au fost transmise în aplicarea ordinului pentru aprobarea cerințelor privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor emis în temeiul dispozițiilor art. 18 din același act normativ, se interpretează în conformitate cu prevederile art. 5 alin. (1) lit. b), respectiv conform prevederilor art. 6 alin. (2) lit. a) din actul normativ menționat anterior, astfel:	Rezultatele autoanalizei privind faptul că entitatea este singurul furnizor al unui serviciu care este esențial pentru susținerea unor activități societale și economice critice, conform dispozițiilor art. 9 lit. a) din Ordonanța de urgență a Guvernului nr. 155/2024~~, astfel cum acestea au fost transmise în aplicarea ordinului pentru aprobarea cerințelor privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor emis în temeiul dispozițiilor art. 18 din același act normativ~~, se interpretează în conformitate cu prevederile art. 5 alin. (1) lit. b), respectiv conform prevederilor art. 6 alin. (2) lit. a) din actul normativ menționat anterior, astfel: .... Rezultatele autoanalizei privind faptul că entitatea este singurul furnizor al unui serviciu care este esențial pentru susținerea unor activități societale și economice critice sunt transmise de către entitate prin intermediul "Formularului de notificare", așa cum este specificat în "Ordinul pentru aprobarea cerințelor privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor" emis în temeiul dispozițiilor art. 18 al OUG 155/ 2024.	Propunem reformularea acestei fraze astfel încât să fie evitată confuzia : „actul normativ menționat anterior" este OUG 155/ 2024 nu OUG pentru aprobarea cerințelor privind procesul de notificare (care ar fi util să aibă și număr în momentul publicării prezentului Proiect de OUG). Modul de transmitere a rezultatelor autoanalizei este specificat la finalul articolului, pentru claritate.

Art. 5 – (1)	Entitățile își calculează scorul prevăzut la art. 3 utilizând formulele de calcul prevăzute în Anexa nr. 2, pornind de la valorile de bază aferente sectorului din care fac parte, prevăzute în cadrul anexei la Metodologia privind evaluarea nivelului de risc al entităților, și în conformitate cu dimensiunea acestora.	Entitățile își calculează scorul prevăzut la Art. 4 (3) utilizând metodologia de calcul prevăzută în Anexa nr. 2, Metodologia privind evaluarea nivelului de risc al entităților. Entitățile transmit rezultatul acestei autoanalize prin intermediul "Formularului de notificare", așa cum este specificat în "Ordinul pentru aprobarea cerințelor privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor" emis în temeiul dispozițiilor art. 18 al OUG 155/ 2024.	Pentru corecție și claritate în referire
Anexa nr. 1	**Anexa nr. 1** **Criterii și praguri de determinare a gradului de perturbare a unui serviciu**		
Art. 2 (2)	În vederea determinării impactului generat de perturbarea serviciului furnizat de entitate conform dispozițiilor art. 9 lit. b) din Ordonanța de urgență a Guvernului nr. 155/2024, se evaluează nivelul impactului în conformitate cu art. 10 alin. (1) lit. a) - d).	În vederea determinării impactului generat de perturbarea serviciului furnizat de entitate conform dispozițiilor art. 9 lit. b) din Ordonanța de urgență a Guvernului nr. 155/2024, se evaluează nivelul impactului în conformitate cu art. 10 alin. (1) lit. a) - d) din acelasi act normativ.	Pentru claritate în referire
Art. 2 (3)	În vederea determinării impactului generat de perturbarea serviciului furnizat de entitate conform art. 9 lit. c) din Ordonanța de urgență a Guvernului nr. 155/2024, se evaluează nivelul impactului în conformitate cu art. 10 alin. (1) lit. f).	În vederea determinării impactului generat de perturbarea serviciului furnizat de entitate conform art. 9 lit. c) din Ordonanța de urgență a Guvernului nr. 155/2024, se evaluează nivelul impactului în conformitate cu art. 10 alin. (1) lit. f), din acelasi act normativ	Pentru claritate în referire
Anexa nr. 2	**Anexa nr. 2** **Metodologie privind evaluarea nivelului de risc al entităților**		
Art. 3 (3)	Valoarea riscului se determină prin înmulțirea următorilor parametri: dimensiunea entității, astfel cum aceasta este determinată la dispozițiile alin. (1) lit. b), natura atacului, astfel cum aceasta este determinată la dispozițiile alin. (1) lit. a) pct. ii, impactul, astfel cum acesta este determinat la	Valoarea riscului se determină prin înmulțirea următorilor parametri: dimensiunea entității, astfel cum aceasta este determinată la dispozițiile alin. (1) lit. b), natura atacului, astfel cum aceasta este determinată la dispozițiile alin. (1) lit. a) pct. ii, impactul, astfel cum acesta este determinat la	Pentru claritate în referire

	dispozițiile alin. (1) lit. c) pct. i și probabilitatea, astfel cum aceasta este determinată la dispozițiile alin. (2) lit. c) pct. ii).	dispozițiile alin. (1) lit. c) pct. i și probabilitatea, astfel cum aceasta este determinată la dispozițiile alin. (2) lit. c) pct. ii), din prezentul articol.	
Art. 3 (5)	Scorul general al entității va determina nivelul de risc al acesteia în funcție de care se stabilește categoria de cerințe de securitate cibernetică aplicabilă, după cum urmează: a) entitățile care au obținut un scor între ”0” și ”99” de puncte vor implementa nivelul „Basic”; b) entitățile care au obținut un scor între ”100” și ”199” de puncte vor implementa nivelul „Important”; c) entitățile care au obținut un scor între ”200” și ”1.500” de puncte vor implementa nivelul „Esențial”.	Scorul general al entității va determina nivelul de risc al acesteia în funcție de care se stabilește categoria de cerințe de securitate cibernetică aplicabilă, după cum urmează: a) entitățile care au obținut un scor între ”0” și ”99” de puncte vor implementa nivelul „Basic”, conform metodologiei/ standardului...; b) entitățile care au obținut un scor între ”100” și ”199” de puncte vor implementa nivelul „Important” , conform metodologiei/ standardului...; c) entitățile care au obținut un scor între ”200” și ”1.500” de puncte vor implementa nivelul „Esențial” , conform metodologiei/ standardului....	De clarificat ce anume înseamnă nivel „Basic”, „Important”, respectiv „Esențial” în relația cu „categoria de cerințe de securitate cibernetică aplicabilă”
Art. 4 – (1)	În cazul în care o entitate nu a utilizat Platforma NIS2@RO în cadrul procesului de evaluare a nivelului de risc din cauza indisponibilității acesteia, entitatea va avea obligația de a completa și încărca raportul și documentele justificative, după caz, într-un termen de cel mult 20 de zile de la data la care aceasta devine disponibilă. Validarea și confirmarea acestor acțiuni va fi efectuată de către DNSC.	În cazul în care o entitate nu a utilizat Platforma NIS2@RO în cadrul procesului de evaluare a nivelului de risc din cauza indisponibilității acesteia, entitatea va avea obligația de a completa și încărca raportul și documentele justificative, după caz, într-un termen de cel mult 20 de zile de la data la care aceasta devine disponibilă. Validarea și confirmarea acestor acțiuni va fi efectuată de către DNSC în termen de 30 zile calendaristice de la .	Adăugarea unui termen de răspuns pentru activitatea DNSC