21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)102 I
vom 1. Dezember 2025

Schriftliche Stellungnahme

von Kerstin Petretto, BDI Bundesverband der Deutschen Industrie e.V., Berlin vom 30. November 2025

Öffentliche Anhörung

zu dem

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen

BT-Drucksache 21/2510

Dem Ausschuss ist das vorliegende Dokument in nicht barrierefreier Form zugeleitet worden.

Stellungnahme

Schriftliche Stellungnahme zur Öffentlichen Anhörung zum Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen“ (BT-Drucksache 21/2510)

Bundesverband der Deutschen Industrie e.V.

Stand: 01.12.2025

Schriftliche Stellungnahme zur Öffentlichen Anhörung zum Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen“

Inhaltsverzeichnis

Vorbemerkung **3**

Stellungnahme **5**

1. Fehlende Harmonisierung mit NIS2UmsuCG **5**

2. Fehlende Rechtsverordnungen **5**

3. Ausnahme der Bundes- und Landesverwaltungen **6**

4. Unklare Zuständigkeiten **6**

5. Zentrale Meldestelle begrüßenswert, Austausch defizitär **7**

6. Zuverlässigkeitsprüfungen unzureichend geregelt **8**

7. Drohnenabwehr bleibt ungeregelt **9**

8. Keine Aussagen zum Erfüllungsaufwand **9**

9. Evaluierung mit Defiziten **10**

Über den BDI **11**

Impressum **11**

Vorbemerkung

Der Bundesverband der Deutschen Industrie (BDI) begrüßt die Möglichkeit, in der öffentlichen Anhörung am Montag, 1. Dezember 2025, Stellung zum Referentenentwurf des KRITIS-Dachgesetzes (BT-Drucksache 21/2510) nehmen zu können.

Die unten eingefügte Stellungnahme entspricht – abgesehen von geringfügigen Anpassungen bei Paragraphenangaben – der am 4. September eingereichten Stellungnahme.

Wie schon in den schriftlichen Anhörungen 2023 und 2024 haben wir uns auch darin kritisch geäußert, dass die Frist zur Abgabe einer schriftlichen Stellungnahme erneut sehr knapp bemessen war. Dies erschwert es Unternehmen und Verbänden, die Tragweite des Entwurfs angemessen zu prüfen und abgestimmte Beiträge einzubringen. Angesichts der hohen sicherheitspolitischen Relevanz des Themas halten wir ein solches Verfahren für unangemessen.

Zugleich war bereits für den 10. September 2025 – nur vier Werktage nach Ablauf der Verbändeanhörung – die Kabinettsbefassung vorgesehen. Eine ernsthafte inhaltliche Berücksichtigung der Beiträge aus Wirtschaft und Gesellschaft war unter diesen Rahmenbedingungen kaum möglich.

Angesichts des im Koalitionsvertrag festgehaltenen Vorhabens, Experten und Betroffene frühzeitig mit angemessenen Fristen (in der Regel vier Wochen) zu beteiligen, ist dieses Vorgehen nicht nachvollziehbar.

Hinzu kommt: Trotz der aktuellen Bedrohungslage und der bereits 2022 erlassenen CER-Richtlinie (EU 2022/2557) wurde das Gesetz nicht rechtzeitig auf den Weg gebracht bzw. finalisiert. Nun drohen Vertragsverletzungsverfahren und Strafzahlungen weshalb das Gesetz nun so rasch wie möglich verabschiedet werden soll. Umso schwerer wiegt, dass der aktuelle Entwurf in wesentlichen Punkten unklar bleibt und der sicherheitspolitischen Lage nach wie vor nicht gerecht wird. Denn der Schutz kritischer Infrastrukturen ist bei weitem nicht nur eine technische oder administrative Frage von Standards und Meldepflichten, sondern hat eine strategische sicherheitspolitische Dimension im Sinne der Gesamtverteidigung.

Für eine wehrhafte Sicherheitsarchitektur sind militärische Fähigkeiten ebenso essenziell wie eine leistungsfähige, innovationsstarke und resiliente Industrie, eingebettet in eine widerstandsfähige Zivilgesellschaft. Unternehmen sind ein zentraler Pfeiler der zivilen und militärischen Verteidigungsfähigkeit. Mit technologischer Stärke, industrieller Innovationskraft und Fertigungskompetenzen liefern sie Lösungen, die Bundeswehr,

Nachrichtendienste und unsere Partner für Abschreckung, Schutz und Einsatzfähigkeit benötigen. Gleichzeitig sind viele Unternehmen selbst Ziel sicherheitsrelevanter Bedrohungen – insbesondere dort, wo sie zur Einsatzfähigkeit von Streitkräften und Sicherheitsbehörden und zur Grundversorgung der Bevölkerung beitragen. Ziel solcher Angriffe ist es, Verunsicherung zu schüren, staatliche Handlungsfähigkeit zu testen und zu untergraben und gesellschaftlichen Zusammenhalt zu schwächen.

In diesem Spannungsfeld kommt den Betreibern kritischer Infrastrukturen, den Beschäftigten in Industrie und Wirtschaft eine zentrale Rolle zu: Sie halten kritische Produktionsprozesse am Laufen und sichern Stabilität und Versorgung im Innern – selbst unter schwierigen Bedingungen. Damit leisten sie einen wesentlichen Beitrag zur Resilienz. Sie sichern Grundversorgung, schützen Kritische Infrastrukturen und engagieren sich zivilgesellschaftlich in Krisenzeiten. Eine starke und innovative Wirtschaft ist daher nicht nur eine Voraussetzung für Verteidigungsfähigkeit, sondern auch für gesamtgesellschaftliche Resilienz. Resilienz und Verteidigungsfähigkeit entstehen nur in enger Partnerschaft.

Stellungnahme

Der aktuelle Entwurf unterscheidet sich inhaltlich kaum von der Kabinettsfassung vom 5. November 2024, der zwar bedauerlicherweise keiner Verbändeanhörung zugeführt wurde. Darin wurden jedoch bereits zentrale Anliegen der Industrie berücksichtigt, was ausdrücklich positiv hervorzuheben ist. Dazu zählen die Harmonisierung des Melde- und Registrierungswesens sowie die vorgesehene Gleichwertigkeit von Nachweisen, die unnötige Doppelregulierung vermeidet.

In der seit dem 29. August 2025 vorliegenden Fassung ist zudem positiv hervorzuheben, dass branchenspezifische Resilienzstandards künftig öffentlich beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) abrufbar sein werden. Dies stärkt Transparenz und Praxistauglichkeit.

Gleichwohl sind zentrale Kritikpunkte weiterhin ungelöst. Viele unserer in den vorherigen Stellungnahmen aus den Jahren 2023 und 2024 bereits dargelegten Kritikpunkte und Verbesserungsvorschläge behalten daher Gültigkeit.

Besonders hervorzuheben sind folgende Punkte:

1. Fehlende Harmonisierung mit NIS2UmsuCG

Die notwendige Harmonisierung der Gesetzesvorlagen zur NIS2-Richtlinie (NIS2UmsuCG) und zur CER-Richtlinie (KRITIS-Dachgesetz) ist weiterhin nicht erfolgt. Es bestehen Ungleichheiten, die zu Herausforderungen in der einheitlichen Betroffenheitsprüfung im Rahmen der noch ausstehenden (gemeinsamen) Rechtsverordnung führen können. Teils fallen auch doppelte, aber unterschiedlich ausgestaltete Regelungen auf, etwa im Bereich personelle Sicherheit / Sicherheitsüberprüfung oder alternative Lieferketten. Erforderlich ist eine konsequente Harmonisierung und auch eine gemeinsame Rechtsverordnung.

2. Fehlende Rechtsverordnungen

Der vorliegende Entwurf legt lediglich fest, welche staatlichen Strukturen künftig per Verordnung Mindestverpflichtungen erlassen, prüfen und weiterentwickeln dürfen. Solange die in § 4 angekündigten sektorenübergreifenden und sektorspezifischen Rechtsverordnungen nicht vorliegen, besteht jedoch erhebliche Rechtsunsicherheit – etwa bei der Zuordnung kritischer Dienstleistungen zu den Sektoren. § 4 Abs. 5 schließt zudem den Zugang zu den Akten aus, die die Bestimmung kritischer Dienstleistungen betreffen. Damit

fehlt jede Möglichkeit, die Kriterien und Abwägungen der Einstufung nachzuvollziehen. Angesichts dieser offenen Fragen ist die Einbindung von Experten aus der Praxis in der weiteren Gesetzesausarbeitung mit hoher Priorität erforderlich. Dies gilt insbesondere für die Entwicklung der sektorspezifischen wie auch der sektorenübergreifenden Rechtsverordnungen.

3. Ausnahme der Bundes- und Landesverwaltungen

Ein erheblicher Teil der Bundesverwaltung wurde vom Gesetz ausgenommen, Landesverwaltungen wurden gar nicht erst adressiert - damit unterliegen diese Infrastrukturen im KRITIS Sektor „Staat und Verwaltung“ keinen Anforderungen. Sie sind jedoch weiterhin - genau wie Unternehmen - physischen Risiken ausgesetzt. Dies kann erhebliche Auswirkungen auch auf die Sicherheit von kritischen Infrastrukturen haben, denn Betreiber sind auf funktionierende staatliche Behörden angewiesen.

Wie bereits in unseren vorherigen Stellungnahmen dargelegt, gilt es, die öffentliche Verwaltung nach gleichen Maßstäben als KRITIS zu definieren. Neben Bundesbehörden sollten auch Behörden der Länder und Kommunen – insbesondere Genehmigungs- und Überwachungsbehörden, die sensible Daten verarbeiten und für besonders wichtige und wichtige Einrichtungen essenzielle Verwaltungsleistungen erbringen, nicht durch Ausnahmeverfahren von den Verpflichtungen des KRITIS-Dachgesetzes ausgenommen werden.

4. Unklare Zuständigkeiten

Unklar bleibt weiterhin die Abgrenzung der Zuständigkeiten zwischen den beteiligten Aufsichtsbehörden. Insbesondere die Rolle der Bundesländer bleibt auch im vorliegenden Referentenentwurf unklar. Da sie auch abseits des KRITIS-Dachgesetzes über Regelungskompetenzen verfügen, drohen Schnittstellenprobleme und Doppelstrukturen. Es bleibt offen, wie sich die beteiligten Bundesbehörden sinnvoll ergänzen können, ohne Unternehmen durch parallele Vorgaben unnötig zu belasten. Es sollte verbindlich geregelt sein, dass Festlegungen der zuständigen Bundesbehörde umfassend Vorrang vor einer Bestimmung einer Landesbehörde haben. Das betrifft u. a. § 3 Abs. 6 RefE und sollte auch für mögliche ergänzende Bestimmungen auf Länderebene gelten.

5. Zentrale Meldestelle begrüßenswert, Austausch defizitär

Der Entwurf des KRITIS-Dachgesetzes verpflichtet BBK und BSI, eine gemeinsame Meldestelle für Vorfälle einzurichten (§ 18). Dies ist begrüßenswert, um im Falle eines Vorfalls den Aufwand für Unternehmen zu reduzieren.

Entsprechend muss in allen Fällen sichergestellt sein, dass Betreiber kritischer Anlagen die erforderlichen Angaben pro Zeitperiode nur in einer Form gegenüber einer Behörde zu machen haben. Der behördenseitige Informationsaustausch obliegt allein den beteiligten Behörden. Die Einhaltung dieses Grundsatzes entspricht dem „once-only-Prinzip“ des neuen Ministers für Digitalisierung und Staatsmodernisierung. Die zentrale Funktion des BBK im Austausch mit den Betreibern kritischer Anlagen wird begrüßt.

Im Sinne einer Erhöhung der gesamtstaatlichen Sicherheit sollte es zudem ein klares Ziel sein, Informationen und Einschätzungen zu Risikolagen zwischen Staat und Wirtschaft systematisch in beide Richtungen auszutauschen. Nur so kann mit den unter das NIS2UmsuCG und das KRITIS-Dachgesetzes fallenden Unternehmen ein tagesaktuelles Lagebild zu digitalen und physischen Bedrohungen im Kontext der Gesamtverteidigung entstehen.

Der BDI schlägt daher erneut vor, einen zentralen Single Point Of Contact (SPOC) einzurichten, der die Behörden institutionalisiert einbindet, die für den Schutz von KRITIS (digital und physisch) Sorge tragen müssen. Der SPOC fungiert als Schnittstelle zwischen Unternehmen sowie Bundes- und Landesbehörden: Er verteilt Meldungen nach Zuständigkeit und stellt sicher, dass der „Need-to-know“-Ansatz umgesetzt wird. Auf unterschiedlichen Zugriffsebenen gilt es, beispielsweise im Rahmen einer durch den Bund bereitgestellten sicheren virtuellen Plattform, Betreibern von Kritischen Infrastrukturen und Sicherheitsbehörden des Bundes und der Länder Zugriff zu erteilen.

Um einen derartigen SPOC zu ermöglichen – der zugleich einen wichtigen Beitrag zu einem gesamtstaatlichen Bedrohungslagebild im Rahmen des künftigen Nationalen Sicherheitsrates leisten könnte – ist eine Überprüfung der bestehenden Regeln zur Geheimhaltung erforderlich. Nur so können Sicherheitsbehörden für den Schutz von KRITIS relevante Informationen sowohl untereinander als auch mit Sicherheitsbeauftragten der Unternehmen direkt und zeitnah teilen.

6. Zuverlässigkeitsprüfungen unzureichend geregelt

Sicherheit wird nicht nur durch Regulierungen, durch technische Maßnahmen des Werk- oder des IT-Schutzes erreicht. Ebenso wichtig ist eine entsprechende Schulung der Mitarbeiterinnen und Mitarbeiter zu Präventionszwecken – und die Überprüfung der Vertrauenswürdigkeit von Beschäftigten, die in besonders sicherheitssensiblen Bereichen tätig sind.

Letzteres ist eine Leistung, die vorrangig durch staatliche Sicherheitsbehörden geleistet werden kann – im Rahmen des Geheimschutzes aber auch darüber hinaus, insbesondere in Bezug auf den Schutz von KRITIS. Das Dachgesetz muss dieser Anforderung Rechnung tragen. §13 (3) Nr. 5 enthält in der Auflistung potenzieller Maßnahmen lediglich eine Klarstellung, dass das von den Betreibern kritischer Anlagen zu berücksichtigende Sicherheitsmanagement im Hinblick auf Zuverlässigkeitsüberprüfungen der Mitarbeitenden unbeschadet der Vorschriften des Sicherheitsüberprüfungsgesetzes (SÜG) in Verbindung mit der Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV) sowie unbeschadet weiterer Fachgesetze wie dem Atomgesetz, dem Luftsicherheitsgesetz (LuftSiG), [dem Sicherheitsgewerbegesetz] und der Hafensicherheitsgesetze erfolgt.

Dies ist nicht ausreichend, um den notwendigen Schutzbedarf zu realisieren: Zurzeit sind personelle Sicherheitsüberprüfungen nur sehr eingeschränkt möglich (außer Telekommunikation / ÜNB / teilweise VNB), wobei zudem mehrmonatige Wartezeiten die Regel und nicht die Ausnahme sind. Dies hemmt die Wirtschaft und ist im Hinblick auf den Fachkräftemangel nicht tolerierbar.

Nur die Nutzung von Terrorlisten / Sanktionslisten bei Bestandspersonal und polizeiliche Führungszeugnisse bei Einstellung sind Optionen, die den Unternehmen zur Verfügung stehen. Der BDI fordert daher, Unternehmen, welche nicht ohnehin dazu verpflichtet sind, die Möglichkeit einzuräumen, Personal mit sicherheitskritischen Aufgaben zu überprüfen / überprüfen zu lassen bzw. in die Lage zu versetzen, sich mit Sicherheitsbehörden auszutauschen. Hierzu bedarf es einer gesetzlichen Grundlage mit justiziablen Mindeststandards und klaren Ausführungsbestimmungen unter Berücksichtigung der Widerspruchsfreiheit auf gesetzlicher und verordnungsrechtlicher Ebene zu schaffen. Ohne eine solche sind „Überprüfungsmaßnahmen“ nach DSGVO untersagt.

Von herausragender Bedeutung bei Überprüfungen von aktuellem oder künftigem Personal ist zudem der Zeitrahmen. Dieser sollte eng bemessen sein,

da der Fachkräftemangel in einem dynamischen Bewerbermarkt schnelle Entscheidungen erfordert. Denkbar wäre daher auch eine Regelung, die ähnlich dem Atomrecht oder dem LuftSiG eine Überprüfung der Zuverlässigkeit, ggfs. auch unter Entrichtung einer für den Anlagenbetreiber verhältnismäßigen Verwaltungsgebühr, zulässt.

Gleichzeitig unterstützen wir, dass entsprechende bereits existierende Vorschriften über Zuverlässigkeitsüberprüfungen unberührt bleiben.

Die deutsche Industrie würde es sehr begrüßen, wenn Verbände, Unternehmen und Experten eng in den Prozess zur Etablierung und Entwicklung von Überprüfungsverfahren einbezogen würden, um das Verfahren an den Bedarfen der Unternehmen auszurichten. Hierfür bieten die Wirtschaftsverbände ihre einschlägigen Gremien als Foren des Austauschs an.

7. Drohnenabwehr bleibt ungeregelt

Seit Beginn von Putins Angriffskrieg gegen die Ukraine hat sich die nationale Sicherheitslage deutlich verändert: Angriffe und Spionage mit Drohnen gehören inzwischen zum festen Instrumentarium staatlicher wie nichtstaatlicher Akteure. Auch in Deutschland wurden bereits zahlreiche Drohnen über Kritischen Infrastrukturen und Bundeswehrliegenschaften gesichtet. Der Entwurf enthält jedoch keinerlei konkrete Vorgaben zur Drohnenabwehr. Diese Leerstelle ist sicherheitspolitisch problematisch, da gerade Drohnenangriffe mit geringem Aufwand erheblichen Schaden anrichten können.

Vor diesem Hintergrund ist fraglich, ob § 13 ohne klare Anforderungen an den Schutz vor unbemannten Luftfahrtsystemen den heutigen Bedrohungen gerecht wird. Insgesamt fehlt ein klarer, bundesweit einheitlicher Rechtsrahmen. Unternehmen benötigen Rechtssicherheit für die Detektion, Störung und gegebenenfalls Abwehr unbemannter Luftfahrtsysteme – entweder durch die zuständigen Behörden oder, unter klar definierten Bedingungen, auch durch die Unternehmen selbst. Ergänzend ist eine zentrale Meldestelle nötig, um Vorfälle systematisch zu erfassen, Lageeinschätzungen zu bündeln und eine schnelle Koordination mit Polizei und Sicherheitsbehörden sicherzustellen.

8. Keine Aussagen zum Erfüllungsaufwand

Der Gesetzentwurf vermeidet jede klare Aussage zu den Kosten und zum Ressourcenbedarf für Kommunen, Länder und Betreiber. Stattdessen wird darauf verwiesen, eine belastbare Schätzung sei erst nach Festlegung der

branchenspezifischen Resilienzstandards möglich. Dies unterstreicht den erheblichen Nachholbedarf: Solange die Resilienzstandards nicht vorliegen, bleibt trotz bereits laufender Anstrengungen zur Härtung von Anlagen unklar, welche Investitionen künftig erforderlich sein werden. Umso wichtiger ist eine enge und frühzeitige Einbindung der Wirtschaft in die Entwicklung der Standards und in die Ausarbeitung der Rechtsverordnungen.

9. Evaluierung mit Defiziten

Obwohl die grundsätzliche Idee der Evaluierung in § 25 zu begrüßen ist, bleiben wesentliche Punkte offen. Der Evaluierungsbericht sollte zur Transparenz regelmäßig und durch Dritte einsehbar veröffentlicht werden. Zudem fehlt eine klare Festlegung, in welchem Zeitrahmen das Gesetz „regelmäßig“ überprüft wird. Die im Entwurf vorgesehene erste Evaluierung durch das BMI im Jahr 2029 liegt zu weit in der Zukunft. Ergänzend wären weitere Berichtspflichten der Bundesregierung sinnvoll, etwa ein regelmäßiger Bericht an den Deutschen Bundestag.

Bundesverband der Deutschen Industrie e.V.

Lobbyregisternummer
R000534

Hausanschrift
Breite Straße 29
10178 Berlin

Postanschrift
11053 Berlin

Ansprechpartner
Kerstin Petretto
T:+49 30 2028-1710

E-Mail:
k.petretto@bdi.eu

Internet
www.bdi.eu

Über den BDI

Der BDI transportiert die Interessen der deutschen Industrie an die politisch Verantwortlichen. Damit unterstützt er die Unternehmen im globalen Wettbewerb. Er verfügt über ein weit verzweigtes Netzwerk in Deutschland und Europa, auf allen wichtigen Märkten und in internationalen Organisationen. Der BDI sorgt für die politische Flankierung internationaler Markterschließung. Und er bietet Informationen und wirtschaftspolitische Beratung für alle industrierelevanten Themen. Der BDI ist die Spitzenorganisation der deutschen Industrie und der industrienahen Dienstleister. Er spricht für 39 Branchenverbände und mehr als 100.000 Unternehmen mit rund acht Mio. Beschäftigten. Die Mitgliedschaft ist freiwillig. 15 Landesvertretungen vertreten die Interessen der Wirtschaft auf regionaler Ebene.

Impressum

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Lobbyregisternummer: R000534

Ansprechpartner

Kerstin Petretto
Senior Manager Sicherheit und Verteidigung
T: +49 30 2028-1710
k.petretto@bdi.eu

BDI Dokumentennummer: D2204