VDV Die Verkehrsunternehmen

Lobbyregister-Nr. bei Bundestag und Bundesregierung: R001242
EU-Transparenzregisternummer: 50254292140-86

VDV
04. Juli 2025

VDV-Stellungnahme zum „Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung" (NIS2UmsCG) des Bundesministeriums des Inneren vom 23.06.2025

Sehr geehrte Damen und Herren,

wir bedanken uns für die Gelegenheit zur Stellungnahme zum vorbezeichneten Referentenentwurf. Der Verband deutscher Verkehrsunternehmen e.V. ist mit über 650 Mitgliedsunternehmen der führende Branchenverband für den öffentlichen Verkehr. Neben der politischen Interessensvertretung wirkt der VDV auch intensiv über die Facharbeit in Ausschüsse und Gremien mit dem Ziel, Normen, Spezifikationen und Empfehlungen zu erarbeiten, die branchenweit von den Verkehrsunternehmen zur Ausschreibung und zur Abnahme von technischen Systemen werden, sowie deren Aufsichtsbehörden genutzt und hierbei kontinuierlich weiterentwickelt und systematisch aktualisiert werden. Wir begrüßen grundsätzlich das im Gesetz adressierte Vorhaben den Ordnungsrahmen zum Schutz informationstechnischer Systeme von kritischen Infrastrukturen weiterzuentwickeln und die europäischen Vorgaben umzusetzen. Denn auch die Anlagen und Einrichtungen sowie technischen Systeme im Nah- und Fernverkehr gehören zu den „Kritischen Infrastrukturen" (KRITIS) und sind für die Sicherung der Mobilitätsangebote von zentraler Bedeutung.

Der VDV schließt sich als Mitglied der UP KRITIS bei der Beurteilung des Referentenentwurfs inhaltlich den Positionen der UP KRITIS-TAK Regulierung voll an. Wir möchten an dieser Stelle folgende Punkte aus Sicht der VDV-Mitgliedsunternehmen besonders hervorheben und erweitern unsere Position wie folgt:

I. Position des VDV im Überblick

1. Resilienz physischer und informationstechnischer kritischer Infrastrukturen gemeinsam denken: NIS2UmsCG und KRITIS-DachG sollten stärker miteinander abgestimmt und verankert werden.
2. Stärkerer Fokus von kritischer Infrastruktur im öffentlichen Raum: Um einen effizienten Support der Sicherheitsbehörden bei der Ausübung von hoheitlichen Tätigkeiten zu ermöglichen, sind diese weiter zu ertüchtigen, um die betroffenen Unternehmen bestmöglich zu unterstützen.
3. Finanzierungsbedarf: Die hohen zusätzlichen Kosten, welche durch die Einführung und die Anpassung von digitalen Prozessabläufen sowie durch die Erfüllung zusätzlicher Informations- und Dokumentationspflichten entstehen, stellen für viele Unternehmen eine erhebliche Belastung dar.
4. Adäquate und rechtssichere Begriffsbestimmungen in § 2 BSIG-E: Erheblichkeitskriterium in § 2 Nr. 11a einfügen und immatierellen Schadensersatz in § 2 Nr. 11b BSIG-E ausschließen.
5. Die Zuordnung zu einer besonders wichtigen oder wichtigen Einrichtung nach § 28 Abs. 3 BSIG-E ist dahingehend zu konkretisieren, dass nur die von der NIS2-RL adressierte konkrete Geschäftstätigkeit umfasst ist.

6. Die Formulierung in § 30 Abs. 1 BSIG-E „die sie für die Erbringung ihrer Dienste zu nutzen" ist zu weit gefasst und die „Verhältnismäßigkeit" zu konkretisieren. Insbesondere für wichtige Einrichtungen entsteht sonst Rechtsunsicherheit bzgl. des umzusetzenden Schutzniveaus.
7. Beschaffungsengpässe und Oligopolbildung vermeiden durch Gestaltungsräume und Vertrauen bei der Wahl von Komponenten und Prozessen – § 30 Abs. 2 BSIG-E maßvoll anwenden.
8. Übergangsfristen in § 39 BSIG-E für Betreiber kritischer Infrastrukturen einführen, die sich bereits aktuell in einer KRITIS-Prüfung nach § 8a III BSIG befinden oder bereits beauftragt haben.
9. Die in § 39 Abs. 2 beschriebene Ermächtigung des BSI zur Ausgestaltung des Verfahrens von Prüfungen und der Erbringung von Nachweisen für Betreiber kritischer Anlagen, darf nicht dazu führen, dass international anerkannte Normen und Verfahren sowie auch national etablierte Prüfverfahren nach dem Stand der Technik nicht mehr möglich sind oder es zu ungerechtfertigten Herabstufungen von Prüfergebnissen kommt.
10. Bzgl. § 41 BSIG-E verweisen wir auf die Stellungnahme des UP-KRITIS (die dortige Ziff. 3). Da bei den Unternehmen des Verkehrssektors sehr lange Nutzungszeiten der kritischen Komponenten und Anlagen bestehen, ist dies für uns ein zentraler Punkt.

II. Hinweise im Detail

1. Zu Punkten 1 & 2 - Allgemeines:

Der VDV unterstützt das Gesetzesvorhaben grundsätzlich als wichtigen Baustein der Erreichung eines hohen Schutzniveaus der Sicherheit informationstechnischer Systeme und der Stärkung der Resilienz kritischer Infrastrukturen. Eine kohärente Umsetzung der NIS2- und CER-Richtlinie verlangt jedoch eine größtmögliche Verzahnung der nationalen Umsetzungsgesetze. Um Redundanzen und Mehraufwände zu vermeiden, ist es erforderlich, dass einheitliche Begriffsbestimmungen (wie z.B. zu kritischen Anlagen) zu Grundlage liegen, Regelungsinhalte eng abgestimmt werden und die Sicherheit kritischer Anlagen im Sinne eines All-Gefahren-Ansatzes betrachtet werden und somit der physische Raum und der Cyberraum gemeinsam gedacht werden.

Bei der Bewertung sollten bewährte Methoden zur Bestimmung von Schwellenwerten kritischer Anlagen herangezogen und vor allem sektorspezifisch und in enger Abstimmung mit der zuständigen Regulierungsbehörde – und insbesondere unter Einbezug der Wirtschaft – erfolgen. Eine frühzeitige und umfassende Beteiligung der sektorspezifischen Branchen, Verbände und Wirtschaftsvertreter ist sinnvoll, zweckmäßig und erforderlich. Insbesondere vor dem Hintergrund haushälterischer Rahmenbedingungen haben Parlament und Gesellschaft nur so die Möglichkeit die Auswirkungen auf Staat und Gesellschaft abzuschätzen und Ziele zu setzen.

Ohne hoheitliche Unterstützung ist es den Wirtschaftsunternehmen nicht möglich auch militärischen Bedrohungsszenarien gerecht zu werden. Die Gefahrenabwehr, ist sowohl im physischen Raum, als auch im Cyberraum eine hoheitliche Tätigkeit. Dies können die betroffenen Wirtschaftsunternehmen weder wirtschaftlich leisten noch sind diese rechtlich dazu befugt. Um dieser Resilienz-Lücke zu begegnen, muss der Bund ausreichende Mittel für Landes- und Bundesbehörden zur Unterstützung der Betreiber kritischer Infrastrukturen bereitstellen und eine erweiterte Zuständigkeit der Sicherheitsbehörden beim Schutz kritischer Infrastrukturen anordnen. Eine ausreichende finanzielle, materielle und personelle Unterstützung der Betreiber kritischer Anlagen ist auch durch die zugrundeliegenden EU-Richtlinien vorgesehen - dies gilt es auch national umzusetzen.

Gleichzeitig ist bei der nationalen Umsetzung darauf zu achten, dass das zugrundeliegende Ziel – die Erreichung eines internationalen bzw. europäischen hohen Cybersicherheitsniveaus -nicht durch die Bestimmung abweichender Schutzziele oder der Neuregelung der Prüfung von Konformitätsbewertungsprogrammen konterkariert wird. Aufgrund steigender Harmonisierungsanforderungen sind

nationale Alleingänge zu vermeiden und die NIS2-Regelungen ohne wesentliche Verschärfungen und Erweiterungen in deutsches Recht zu übernehmen.

2. **Zu Punkt 3 – Finanzierungsbedarf**

Nach unserer Ansicht ist der Erfüllungsaufwand für die Wirtschaft und insbesondere für den öffentlichen Verkehrssektor nicht ausreichend berücksichtigt worden. Insbesondere wenn man im Sinne eines All-Gefahren-Ansatzes die erforderliche Ertüchtigung der physischen und der informationstechnischen Sicherheit von kritischer Infrastruktur – also die Umsetzung von NIS2-RL und CER-RL – gemeinsam betrachtet entsteht bei den betroffenen Unternehmen des Verkehrssektors ein erheblicher Mittelbedarf für die Umsetzung der Vorgaben. Eine aktuell laufende Abfrage bei den VDV-Mitgliedsunternehmen zeigt, dass sowohl bei den bisherigen KRITIS-Betreibern als auch bei den bisher nicht adressierten Unternehmen – die nunmehr als besonders wichtige und wichtige Einrichtungen bewerten werden würden – erhebliche Aufwände für die Einführung von ISMS, Zertifizierungen und Audits entstehen werden – neben der physischen Ertüchtigung kritischer Anlagen und damit verbundenen Objektschutzes durch mehr Personal und baulichen Maßnahmen.

3. **Zu Punkt 4 – Notwendige Begriffsbestimmung in § 2 Nr. 11 BSIG-E**

Die Begriffsbestimmungen in § 2 Nr. 11 BSIG-E sind missverständlich und könnten zu Überinterpretationen führen. Bereits im Gesetzestext sollte im Sinne der Rechtssicherheit und -klarheit hinreichend bestimmter ausformuliert werden. Wir beziehen uns auf den Vorschlag der UP KRITIS und regen an, in § 2 Nr. 11a BSIG-E ein Erheblichkeitskriterium einzufügen und immateriellen Schadensersatz auszuschließen. § 2 Nr. 11a BSIG-E ist folgendermaßen anzupassen:

11. „erheblicher Sicherheitsvorfall" ein Sicherheitsvorfall ***(siehe Ziff. 40),*** *der*

*a) schwerwiegende Betriebsstörungen der Dienste oder „**erhebliche**" finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder*

b) andere natürliche oder juristische Personen durch erhebliche materielle ~~oder immaterielle Schäden~~ beeinträchtigt hat oder beeinträchtigen kann,

sofern durch die Rechtsverordnung nach § 56 Absatz 5 keine konkretisierende Begriffsbestimmung erfolgt;

Das „Erheblichkeitskriterium" als unbestimmter Rechtsbegriff ist in der Rechtssetzung und Rechtsförmlichkeit bekannt und anerkannt. Dadurch wird einer zu weiten Auslegung begegnet und klargestellt, dass nicht jeder mögliche finanzielle Verlust einen erheblichen Sicherheitsvorfall darstellt.
Es sollte vielmehr stärker nach Art des Sicherheitsvorfalls ausdifferenziert werden.

Weiterhin sollte nicht jeder mögliche Datenschutzvorfall zusätzlich als „erheblicher Sicherheitsvorfall" betrachtet werden. In Anbetracht verschiedener Meldepflichten (NIS2 vs. DSGVO) und damit verbundener Mehraufwendungen, sollte deutlicher abgegrenzt werden, wann Ziff. 11b greifen soll. Darüber hinaus gewährt die DSGVO bereits immaterielle Schadensersatzansprüche bei Datenschutzverstößen (Art. 82 DSGVO), sodass es eines zusätzlichen Anspruchs aus dem BSIG-E nicht bedarf.

4. **Zu Punkt 5 – Zuordnung zu einer (besonders) wichtigen Einrichtung, § 28 Abs. 3 BSIG-E**

Durch § 28 Abs. 3 BSIG-E können künftig Geschäftstätigkeiten bei der Zuordnung zu einer der Einrichtungsarten nach den Anlagen 1 und 2 dann unberücksichtigt bleiben, wenn sie im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung als „vernachlässigbar" einzustufen sind. Eine weite Auslegung würde jedoch faktisch zu einer erheblichen Erweiterung des Anwendungsbereichs führen. Der Begriff „Vernachlässigbar" in Verbindung mit der gesamten Geschäftstätigkeit ist zu ungenau und kann sich zwischen Unternehmen der gleichen Branche unterscheiden.

In der Gesetzesbegründung wird zwar vage auf eine „nur geringfügige Nebentätigkeit" verwiesen. Diese Unschärfe führt jedoch zu Rechtsunsicherheit und bedarf einer Klarstellung.
Wir verweisen daher auf den Vorschlag der UP KRITIS (Ziff. 7).
Jedenfalls gilt es zu vermeiden, den Anwendungsbereich über die bisherige Regelung hinaus zu erweitern oder komplexe Anrechnungsregelungen einzuführen.

5. Zu Punkt 6 – Konkretisierung des § 30 Abs. 1 BSIG-E bzgl. des zu erreichenden Schutzniveaus und der erfassten Dienste

Die weite Auslegung in § 30 Abs. 1 BSIG-E begegnet ebenfalls der Rechtsunsicherheit. Wir beziehen uns auf den Vorschlag der UP KRITIS und regen an, § 30 Abs. 1 BSIG-E wie folgt anzupassen:

> *„Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die sie für die Erbringung ihrer Dienste im Rahmen der kritischen Dienstleistung entsprechend der Einrichtungsarten nach den Anlagen 1 und 2 nutzen. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind **angemessen**, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht."*

Das Verhältnismäßigkeitskriterium führt in Bezug auf die Umsetzung von Schutzmaßnahmen bei wichtigen Einrichtungen zu Rechtsunsicherheiten, da keine weiteren Angaben zum umzusetzenden Schutzniveau bzw. der „Maßnahmen" gemacht werden, sondern nur zur Erforderlichkeit.
Der Formulierungsvorschlag der UP KRITIS ist an den aktuellen § 8a BSIG angelehnt. Diese „Angemessenheitsprüfung" aus Unternehmenssicht in Verbindung mit der Aufwandsbewertung ist in der bisherigen Praxis bekannt und bewährt.

In § 31 BSIG-E ist in der Folge ebenfalls der Begriff der „Verhältnismäßigkeit" durch „Angemessenheit" aus Unternehmenssicht auszutauschen, um einen Gleichklang zu ermöglichen.

> § 31 Abs. 1 BSIG-E:
>
> *„Für Betreiber kritischer Anlagen gelten für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, im Vergleich zu anderen informationstechnischen Systemen, Komponenten und Prozessen besonders wichtiger Einrichtungen auch über das Schutzniveau dieser Einrichtungen hinausgehende Maßnahmen nach § 30 Absatz 1 Satz 1 als ~~verhältnismäßig~~ **angemessen**, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht."*

6. Zu Punkt 7 – Verpflichtung zur Nutzung zertifizierter Komponenten und Prozesse, § 30 Abs. 2 BSIG-E

Die in dem vorliegenden Entwurf bestimmte Verpflichtung zum Einsatz national zertifizierter Komponenten und Prozesse in § 30 Abs. 2 Nr. 5 & 6 iVm Abs. 6, 7 BSIG-E begegnet erheblichen Bedenken.

Die Erfahrungen etwa mit der Smart-Meter-Gateway-Infrastruktur haben gezeigt, dass insbesondere nationale Zertifizierungsframeworks die zügige Einführung sicherer digitaler Infrastrukturen in den KRITIS-Sektoren im Wege stehen und die Bildung von Oligopolen begünstigen können. Diese Oligopole sind aus einer systemischen Sicherheitsperspektive selbst als Cluster-Risiken zu bewerten. Auch im Sinne der internationalen Wettbewerbsfähigkeit deutscher Hersteller sollte der Stand der Technik nicht durch Dokumente und technische Richtlinien einer Bundesbehörde festgelegt, sondern

lediglich als Ergänzung zu öffentlich anerkannten Beschreibungen zum Stand der Technik aufgefasst werden.

Eine rein nationale Zertifizierung ist deshalb auch nicht im Sinne der NIS2-Richtlinie, da die NIS2-Richtlinie primär auf einen gemeinsamen europäischen Binnenmarkt ohne Zutrittsbarrieren für Unionsstaaten abzielt. Es kann nicht davon ausgegangen werden, dass Hersteller zwingend ein Interesse an den Aufwänden einer rein deutschen Zertifizierung haben. Zusätzlich ist der Einsatz von ausschließlich zertifizierten Komponenten für eine Aufrechterhaltung eines Regelbetrieb aufgrund Ersatzbeschaffung sehr problematisch und kann im worst-case zum Stillstand der KRITIS führen.

7. Zu Punkt 8 – Übergangsfristen für KRITIS-Betreiber einführen, § 39 BSIG-E

Wir begrüßen die Erweiterung des Nachweiszyklus für Betreiber kritischer Anlagen auf drei Jahre als einen wichtigen Schritt in Richtung Internationalisierung des nationalen Cybersicherheitsrecht entlang der einschlägigen europäischen und internationalen Normen im Bereich der Informationssicherheit. Allerdings bedarf es an Übergangsregelungen für KRITIS-Betreiber, die sich in einer Prüfung nach § 8a Abs. 3 BSIG befinden, bzw. eine solche beauftragt haben.

Aufgrund der sehr umfangreichen KRITIS-Prüfungen nach § 8a Abs. 3 BSIG (inklusive Planung, Beauftragung, Vorbereitung, Durchführung und Berichtserstellung ist mit bis zu 12 Monaten zu rechnen) müssen die Prüfungen frühzeitig geplant und beauftragt werden. Somit wird es vorkommen, dass einige Betreiber sich bei Inkrafttreten der neuen Regelungen nach § 39 BSIG-E noch in einer laufenden Prüfung nach § 8a BSIG befinden oder diese Prüfung kurz danach beginnen wird.

Aufgrund fehlender Regelungen im aktuellen Entwurf besteht für diese Unternehmen die Gefahr, dass nach Abschluss der Prüfung die Ergebnisse nicht anerkannt werden und hierdurch eine weitere Prüfung direkt im Jahr darauf erforderlich ist.

Generell sollten Nachweise aus bereits laufenden oder beauftragten KRITIS-Prüfungen auch nach Inkrafttreten des BSIG-E anerkannt werden.

Wir folgen daher auch hier dem Vorschlag der UP KRITIS (Ziff. 6).

8. Zu Punkt 9 – Konformitätsbewertung nach § 39 Abs. 2 BSIG-E

Die Ausgestaltung des Prüfverfahrens darf nicht dazu führen, dass die im Referentenentwurf formulierten Anforderungen, über denen von anerkannten Normen und Verfahren hinausgehen oder zu Verzerrungen der Prüfergebnisse führen. Schon in der jetzigen Praxis kommt es durch die Ausgestaltung des Prüfverfahrens (RUN, Gain) durch das BSI im Rahmen der derzeitigen gültigen Reifegradbewertung zu pauschalen Herabstufungen der Prüfungsergebnisse, ohne dass dies auf Basis einer durchgängigen Herleitung aus der Mängelliste erfolgt. Zwar ist eine Harmonisierung des Prüfungsvorgehens anzustreben, allerdings nicht mit der Folge von erhöhten nationalen Anforderungen oder der pauschalen Herabstufung von Prüfergebnissen. Die Anwendung von § 39 Abs. 2 ist daher zu überprüfen.

9. Zu Punkt 10 – Anpassung des Prüfprozesses bei kritischen Komponenten nach § 41 BSIG-E

Das angedachte nationale Prüfverfahren nach § 41 BSIG-E zur Untersagung zum Einsatz kritischer Komponenten mit einzelnen Prüfungen ist mit den vorgesehenen Prüffristen (bis zu vier Monate) nicht praktikabel. Außerdem erscheint eine EU-weite Abstimmung gegenüber einer nationalen Prüfung sinnvoller. Wir sprechen uns daher ebenfalls für die Empfehlung der UP KRITIS aus, dass in § 41 angedachte Verfahren durch EU-weit abgestimmte Blacklist(s) von Herstellern/Produkten/Technologien zu ergänzen. Dieses würde die Beschaffungsprozesse innerhalb der Unternehmen beschleunigen und weniger Verwaltungsaufwand seitens der Behörden erfordern.

Die ebenfalls vorgesehenen rückwirkenden Verbote (§ 41 Abs. 4 und 6), die ggf. den Ausbau von Komponenten zur Folge haben können, bergen auch aus Sicht des VDV mehr Risiken als Sicherheitsgewinne. Bezüglich der rückwirkenden Untersagung des Einsatzes kritischer Komponenten sollte eine Formulierung gefunden werden, die einen Austausch außerhalb des normalen Lebenszyklus einer Komponente nur dann vorsieht, wenn durch zusätzliche Mitigations-Maßnahmen das Risiko nicht auf ein akzeptables Maß gesenkt werden kann.

Zudem ist im Gesetzestext nicht klar geregelt, wie eine Kostenträgerschaft für entstehende Rückabwicklungsaufwände im Falle der Untersagung geregelt wäre. Gleichzeitig können rückwirkende Verbote im Widerspruch zu anderen europäischen Regelungen wie dem Vergaberecht stehen.
Wir regen Klärung und ggf. die Auflösung der möglichen Widersprüche zu anderen europäischen Regelungen wie z. B. dem Vergaberecht an. Darüber hinaus folgen wir der Empfehlung der UP KRITIS eine Kostenübernahme durch den Bund, mindestens jedoch eine klare gesetzliche Regelung aufzunehmen.

Wir bitten um Berücksichtigung unserer Stellungnahme, bedanken uns für die Möglichkeit der Stellungnahme und stehen für tiefergehende Arbeitsgespräche diesbezüglich gerne zur Verfügung.