21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)071
vom 13. Oktober 2025

Schriftliche Stellungnahme

der Gesellschaft für Informatik e. V., Berlin vom 12. Oktober 2025

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

BT-Drucksache 21/1501

GESELLSCHAFT
FÜR INFORMATIK

Berlin, 12. Oktober 2025

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

Zum Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

Stand: 08.09.2025 (Drucksache 21/1501)

Ansprechpartner:

- **Nina Locher**, Senior Referentin Cybersicherheitspolitik, Gesellschaft für Informatik, Geschäftsstelle Berlin, Mail: nina.locher@gi.de
- **Aleksandra Sowa**, GI-Fachgruppe Datenschutzfördernde Technik (PET), Mail: a_sowa@web.de
- **Bernhard C. Witt**, Fachexperte für Governance im GI-Fachbereich Sicherheit, Mail: bernhard.witt@sits.com

Die Gesellschaft für Informatik e.V. (GI) begrüßt eine rasche Umsetzung der NIS-2-Richtlinie in deutsches Recht und die damit verbundene deutlich erkennbare Steigerung hinsichtlich des angestrebten Niveaus zur generellen Cybersicherheit (besonders) wichtiger Einrichtungen als auch zur Informationssicherheit in der Bundesverwaltung. Aktiv haben wir im Entwurfsprozess bereits Stellung bezogen, abrufbar unter:

- https://gi.de/meldung/gi-sieht-baustellen-im-nis2-umsetzungsgesetz
- https://gi.de/meldung/neue-nis-2-version-gi-fordert-konsequenz-statt-ausnahmen
- https://gi.de/meldung/nis2-gi-fordert-klare-definitionen

Weiterhin stellen wir jedoch erheblichen Nachbesserungsbedarf fest, damit die NIS-2-Richtlinie EU-rechtskonform umgesetzt werden kann und tatsächlich überhaupt die beabsichtigte Wirkung entfalten kann. Aus fachlicher Sicht der GI sind vor allem folgende Punkte im Gesetz nachzubessern:

1. Wichtige Begriffe normenübergreifend einheitlich und klarer definieren,
2. Einfachheit bei der Meldungen von Sicherheitsvorfällen durchsetzen,
3. Entschlossenheit bei der Meldung von Schwachstellen zeigen sowie
4. Authentizität als eigenes Sicherheitsziel anerkennen.

1) Wichtige Begriffe normenübergreifend einheitlich und klarer definieren

Um spätere Auslegungsschwierigkeiten zu vermeiden, sollten die im Kontext der Cybersicherheit relevanten Begriffsdefinitionen noch klarer und über alle Gesetze hinweg einheitlich gefasst werden.

Zu Art. 1, § 2 Nr. 11 BSIG-E:

In der Durchführungsverordnung (EU) 2024/2690 der Kommission vom 17. Oktober 2024 wurde für einen maßgeblichen Teil der NIS-2-Verpflichteten verbindlich festgelegt, wann ein „**erheblicher Sicherheitsvorfall**“ vorliegt. Die Regelungen aus Art. 3 und 4 der NIS2-DVO 2024/2690 sind auch für weitere Einrichtungen anwendbar und konkretisieren wesentlich zielgenauer als die bestehende Formulierung in Art. 1, § 2 Nr. 11 BSIG-E, wann ein Sicherheitsvorfall im Sinne von ErwG 101 der NIS-2-Richtlinie erheblich ist.

> Empfehlung:
> Ersetzen der Legaldefinition in Art. 1, § 2 Nr. 11 BSIG-E durch die Formulierung aus Art. 3 Abs. 1 lit. a – e und Art. 4 NIS2-DVO 2024/2690 als neuen Buchstabe f.

Um eine gesetzesübergreifende Einheitlichkeit zu erreichen, könnte hierbei zusätzlich ein Bezug auf den Terminus „schwerwiegender IKT-bezogener Vorfall“ aus der DORA-

VO mit Verweis auf die Delegierte Verordnung (EU) 2024/1772 der Kommission aufgenommen werden, welche in Art. 8 & 9 analoge Schwellen für die Wesentlichkeit verbindlich für den Finanzsektor festlegt.

Zu Art. 1, § 28 BSIG-E:

Die Verwendung des Begriffs „**besonders wichtige Einrichtungen**“ in Art. 1, § 28ff BSIG-E für „**wesentliche Einrichtungen**“ gemäß der NIS-2-Richtlinie ist nicht nachvollziehbar und dient allenfalls einer Verwirrung der betroffenen Einrichtungen. Im Umsetzungsgesetz sollte daher der Begriff aus der NIS-2-Richtlinie unverändert übernommen werden.

> Empfehlung:
> Ersetze den Begriff „besonders wichtige Einrichtung“ durchgängig mit dem Begriff „wesentliche Einrichtung“ im gesamten BSIG-E.

Streng genommen ist es Ziel der NIS-2-Richtlinie, ausgehend vom betreffenden Sektor und den festgelegten Schwellen zur Mitarbeitendengröße als auch zum Umsatz- bzw. Bilanzvolumen die auswirkungsintensiven Einrichtungen zu ermitteln. Ergänzt wird dies durch national weitere Einrichtungen, die als wesentliche Einrichtungen eingestuft worden sind. Dies gilt damit konsequenterweise für **Betreiber einer kritischen Dienstleistung** im Sinne von § 2 Nr. 24 BSIG-E, die eine kritische Anlage im Sinne von § 2 Nr. 22 BSIG-E betreiben, selbst wenn diese nicht die EU-seitig vorgeschriebenen Schwellen überschreiten, dafür jedoch die bisherigen Schwellen zur Versorgungssicherheit. Dies würde soweit auch für Klarheit sorgen, wie die Ausnahmeklausel aus Art. 1, § 28 Abs. 3 BSIG-E zu interpretieren ist.

> Empfehlung:
> Füge in Art. 1, § 28 Abs. 3 BSIG-E hinter „solche Geschäftstätigkeiten“ ein: „außerhalb des Betriebs einer kritischen Anlage“

Zu Art. 1, § 37 BSIG-E:

Die Ausnahmeregelungen in Art. 1, § 37 Abs. 2 BSIG-E widerspricht dem Ziel eines einheitlichen und vollständigen Lagebildes zur Cybersicherheit. Gerade für betreffende Einrichtungen ist es aus Gründen der Cybersicherheit geboten, entsprechende Risikomanagementmaßnahmen nach Art. 1, § 30 BSIG-E als auch entsprechende Meldepflichten nach Art. 1, § 32 BSIG-E zu erfüllen, selbst wenn Art. 2 Abs. 8 der NIS-2-Richtlinie für diese Einrichtungen potenzielle Ausnahmeregelungen zulässt. Registrierungspflichten sind dagegen in der Tat entbehrlich.

> Empfehlung:
> Streiche Art. 1, § 37 Abs. 2 BSIG-E und Einfügen von Art. 1, § 37 Abs. 2 Nr. 1 BSIG-E anstelle von „in relevanten Bereichen“ in Art. 1, § 37 Abs. 3 BSIG-E

2) Einfachheit bei der Meldung von Sicherheitsvorfällen durchsetzen

Um die Komplexität und den Bürokratieaufwand bei der Meldung von Sicherheitsvorfällen möglichst zu reduzieren, ist es zweckmäßig, wenn das Bundesamt für Sicherheit in der Informationstechnik (BSI) tatsächlich als zentrale Stelle für Meldungen Dritten über Sicherheitsrisiken in der Informationstechnik fungieren würde. Zugleich würde dies die unabhängige Stellung des BSI unterstreichen. Zweckmäßigerweise sollte daher sektorübergreifend und damit auch konform zu Art. 19 DORA-VO das BSI als zuständige Behörde festgelegt werden, welche wiederum entsprechende Fachaufsichtsbehörden über entsprechend eingegangene Meldungen zu unterrichten hat.

> Empfehlung:
> In Art. 1, § 5 Abs. 1 BSIG-E folgenden Satz anfügen: Das Bundesamt fungiert sektorunabhängig als zuständige Behörde für Meldungen über Sicherheitsvorfälle und leitet eingehende Meldungen an weitere, für Cybersicherheit zuständige Behörden weiter.

Auf Bundesebene bilden neben dem BSI auch das BBK, die BaFin und die BNetzA wichtige Akteure der nationalen Cybersicherheitsarchitektur. Zurecht bemängelt der Bundesrechnungshof in seiner Stellungnahme daher die fehlende gemeinsame Datenbasis und einen hinsichtlich des Lagebildes einheitlich strukturierten Datenaustausch. Das BSI als zentrale Stelle für entsprechende Meldungen sollte folglich den Auftrag erhalten, hier für eine gemeinsame Datenbasis zu sorgen.

> Empfehlung:
> In Art. 1, § 5 BSIG-E folgenden neuen Absatz einfügen: Das Bundesamt stellt für die weiteren, für Cybersicherheit zuständigen Behörden auf Basis der erhaltenen und ermittelten Sicherheitsrisiken eine gemeinsam nutzbare Datenbasis hinsichtlich des Lagebildes bezüglich der Sicherheit in der Informationstechnik bereit und unterrichtet diese nach § 40 Abs. 3 entsprechend.

Da ein meldepflichtiger Sicherheitsvorfall zugleich auch eine meldepflichtige Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO darstellen kann, wäre es für die Praxis hilfreich, wenn bei den Einzelheiten zur Ausgestaltung des Meldeverfahrens nach Art. 1, § 32 Abs. 4 BSIG-E eine verknüpfende Meldung möglich wäre. Dies würde zugleich die Vorgabe aus Art. 1, § 7 Abs. 8 BSIG-E unterstreichen.

> Empfehlung:
> In Art. 1, § 32 Abs. 4 BSIG-E folgenden Satz anfügen: Potenzielle Synergien mit einer Meldung nach Art. 33 DS-GVO werden dabei berücksichtigt.

3) **Entschlossenheit bei der Meldung von Schwachstellen zeigen**

Die Ausnahme aus Art. 1, § 5 Abs. 4 Nr. 2 BSIG-E, dass auf Grund von Vereinbarungen des Bundesamtes mit Dritten Informationen über Sicherheitsrisiken nicht übermittelt werden dürfen, ist zu unspezifisch und ermöglicht soweit u.U. ein Offenhalten von Schwachstellen und schwächt die Wirksamkeit von IT-Sicherheitsmaßnahmen unangemessen. Nachvollziehbar wären dagegen Auswirkungen auf die nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, da hierfür in Art. 2 Abs. 7 & 8 der NIS-2-Richtlinie ausdrücklich Ausnahmen zulässig sind.

Empfehlung:
– Ersetze Art. 1, § 5 Abs. 4 Nr. 2 BSIG-E mit: die nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung unangemessen beeinträchtigen
– Ersetze „Vereinbarungen mit Dritten“ in Art. 1, § 43 Abs. 5 Satz 2 BSIG-E mit „aufgrund von § 5 Abs. 4 Nr. 2“

4) **Authentizität als eigenes Sicherheitsziel anerkennen**

Integrität und Authentizität sind aus gutem Grund eigenständige Sicherheitsziele der IT-Sicherheit und erfordern jeweils unterschiedliche Sicherheitsstrategien. Im bisher geltenden BSI-Gesetz wird dies noch berücksichtigt, im vorgelegten Gesetzesentwurf dagegen überraschend und mit unzutreffender Begründung aufgegeben.

Authentizität sollte dagegen weiterhin als eigenes Sicherheitsziel festgeschrieben und nicht als Unterfall der Integrität betrachtet werden. Authentizität stellt die Echtheit von Daten und Identitäten fest. Dies ist beispielsweise wichtig, um Phishing-E-Mails zu erkennen. Authentizität ist daher für die Vertrauenswürdigkeit von digitalen Services von größter Wichtigkeit.

Ohne ausdrücklich vorgenommene Zielsetzung zur Authentizität läuft jegliche Digitalisierungsstrategie und Technikoffenheit ins Leere. Während die Integrität insbesondere die Vertrauenswürdigkeit von Datenbestand bzw. Systemzustand garantiert, wird die Vertrauenswürdigkeit des Auslösers eines digitalen Ereignisses nur durch die Authentizität gewährleistet. Authentizität flankiert dabei sogar alle drei klassischen Sicherheitsziele.

Empfehlung:
Authentizität als zusätzliches Sicherheitsziel aufnehmen in

– Art. 1, § 2 Nr. 1, 17, 23 lit. B, 39 und 40 BSIG-E
– Art. 1, § 8 Abs. 6 Nr. 3 BSIG-E
– Art. 1, § 16 Abs. 2 BSIG-E
– Art. 1, § 30 Abs. 1 BSIG-E
– Art. 1, § 41 Abs. 3 und 5 Nr. 5 & 6 BSIG-E

GESELLSCHAFT
FÜR INFORMATIK

Über die Gesellschaft für Informatik e.V. (GI)

Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Weitere Informationen finden Sie unter www.gi.de.