21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)085 D
vom 31. Oktober 2025

Gemeinsame Stellungnahme

des Bundesverbands der Deutschen Industrie e.V.(BDI), des Bundesverbands der Deutschen Sicherheits- und Verteidigungsindustrie e.V. (BDSV), des Bundesverbands der Luft- und Raumfahrt (BDLI), des Branchenverbands der deutschen Informations- und Telekommunikationsbranche e.V. (Bitkom), des Bundesverbands und Bundesarbeitskreises der Sicherheitsbevollmächtigten für den Geheimschutz in der Wirtschaft (BAK SiBe) und des Verbands für Sicherheit in der Wirtschaft –VSW-Bundesverband e.V.
vom 29. September 2025

übermittelt von Günther Schotten (VSW-Bundesverband e.V.)

Öffentliche Anhörung

zu dem Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Modernisierung des Sicherheitsüberprüfungsgesetzes und zur Änderung beamtenrechtlicher Vorschriften

BT-Drucksache 21/1926

Stellungnahme zum Referentenentwurf des Bundesministeriums des Innern für ein Gesetz zur Änderung sicherheitsüberprüfungsrechtlicher und beamtenrechtlicher Vorschriften vom 17.06.2025

Gemeinsame Stellungnahme des Bundesverbands der Deutschen Industrie e.V. (BDI), des Bundesverbands der Deutschen Sicherheits- und Verteidigungsindustrie e.V. (BDSV), des Bundesverbands der Luft- und Raumfahrt (BDLI), des Branchenverbands der deutschen Informations- und Telekommunikationsbranche e.V. (Bitkom), des Bundesverbands und Bundesarbeitskreis der Sicherheitsbevollmächtigten für den Geheimschutz in der Wirtschaft (BAK SiBe) und dem Verband für Sicherheit in der Wirtschaft – VSW-Bundesverband e.V. zum o.g. Referentenentwurf.

Erweiterte Fassung vom 29. September 2025

Vorbemerkung

Wir begrüßen grundsätzlich das Anliegen des Bundesministeriums des Innern (BMI), die Sicherheitsüberprüfungen angesichts der veränderten sicherheitspolitischen Lage weiterzuentwickeln und das Verfahren an die Bedürfnisse einer modernen Sicherheitsarchitektur anzupassen.

Die zunehmenden Bedrohungen durch Ausspähung, Sabotage und Einflussnahme auf Unternehmen, insbesondere im Bereich kritischer Infrastrukturen und sicherheits- und verteidigungsrelevanter Industrien, machen eine robuste, verlässliche und zugleich beschleunigte Sicherheitsüberprüfung notwendig.

Sicherheitsüberprüfungen sind ein grundlegender Baustein unserer Verteidigungsfähigkeit, zivil *und* militärisch: Sie sind essenzielle Voraussetzung für die von der Bundesregierung angestrebte Härtung Kritischer Infrastrukturen sowie für Produktionshochlauf und Kapazitätsausbau der Sicherheits- und Verteidigungsindustrie. Nur wenn (potenzielle) Mitarbeiterinnen und Mitarbeiter zeitnah überprüft und eingesetzt werden können, lassen sich Anlagen kritischer Infrastrukturen verlässlich absichern, neue Fertigungslinien hochfahren, Zulieferketten stabilisieren – gerade auch dort, wo bislang branchenfremde Unternehmen als neue Partner einsteigen (z. B. Automobil-, Maschinenbau-, Elektro- oder chemische Industrie). Bereits bestehende Engpässe in laufenden Verfahren drohen, sich mit dem politisch gewollten Ausbau der zivilen und militärischen Verteidigungsfähigkeit weiter zu verschärfen. Unternehmen der Sicherheits- und Verteidigungsindustrie sowie KRITIS-Betreiber sind auf effiziente, planbare und rechtssichere Verfahren angewiesen; Verzögerungen wirken unmittelbar auf Personalplanung, Betriebsabläufe und Einsatzbereitschaft.

Zudem erfordert das absehbar steigende Volumen an Sicherheitsüberprüfungen einen gezielten Kapazitätsaufbau bei den zuständigen behördlichen Stellen. Nur so lassen sich planbare Fristen, transparente Verfahren und belastbare Service-Level gewährleisten. Die derzeit mehrmonatigen Bearbeitungszeiten bei Sicherheitsüberprüfungen sind nicht akzeptabel und stehen dem Ziel einer raschen Stärkung der nationalen Sicherheit entgegen.

Vor diesem Hintergrund bleibt aus Sicht der deutschen Industrie weiterhin unbefriedigend, dass die Weiterentwicklung des Geheim- und Sabotageschutzes bislang nur punktuell erfolgt und grundlegende strukturelle Reformen ausbleiben. Obwohl das Sicherheitsüberprüfungsgesetz (SÜG) die Erhöhung der Sicherheit zum Ziel hat, behandelt der Entwurf die Herausforderungen der nationalen Sicherheit weitgehend als reinen Verwaltungsakt. Der bestehenden Zersplitterung des Geheim- und Sabotageschutzes vermag der Entwurf nicht entgegenzuwirken. Notwendig ist ein ganzheitlicher Ansatz, der die Sicherheitsarchitektur in Deutschland neu denkt: mit klar gebündelten Zuständigkeiten, effizienten Prozessen, einer besseren Verzahnung von Bund und Ländern sowie einheitlichen Standards für Sicherheitsüberprüfungen. Idealerweise geht die bevorstehende Modernisierung über den klassischen Verwaltungsrahmen hinaus. Auch sicherheitsrelevante Wirtschaftsbereiche ohne unmittelbaren VS-Bezug – etwa in der Cyberabwehr oder bei Dual-Use-Technologien – benötigen rechtssichere und praxistaugliche Verfahren, um Personal auf Vertrauenswürdigkeit zu prüfen. Der Schutz geheimhaltungsbedürftiger Informationen ist niemals Selbstzweck, sondern zentraler Pfeiler unserer freiheitlichen Ordnung, der Handlungsfähigkeit unseres Staates und der Resilienz unserer Wirtschaft — er verlangt konsequente Modernisierung und effektive Steuerung.

Gesetzlich vorgeschriebene Sicherheitsüberprüfungen müssen deutlich zügiger erfolgen. Wartezeiten von bis zu einem Jahr und mehr sind weder für staatliche noch für wirtschaftliche Akteure zumutbar.

Vor diesem Hintergrund nehmen wir wie folgt zum vorliegenden Gesetzentwurf Stellung.

Wir begrüßen folgende Punkte:

- Die ausdrückliche Einbeziehung der Betreiber lebens- oder verteidigungswichtiger Einrichtungen in die Meldepflicht für sicherheitsempfindliche Stellen gemäß dem neu formulierten § 25a SÜG. Damit wird die Beteiligung der privatwirtschaftlichen Betreiber an den staatlichen Sicherheitsüberprüfungsverfahren formal ausgeweitet; allerdings geht dies für die betroffenen Unternehmen mit einem nicht unerheblichen zusätzlichen administrativen Aufwand einher, da Meldeprozesse und Schnittstellen zu den Behörden neu aufgebaut und dauerhaft vorgehalten werden müssen.
- Die Stärkung des vorbeugenden personellen Sabotageschutzes durch die Angleichung an die Anforderungen des Geheimschutzes schafft mehr Klarheit und Verlässlichkeit für die Unternehmen (§ 1 Abs. 2 und § 2 Abs. 1 SÜG).
- Die Erweiterung der Datenverarbeitungsbefugnisse zur Nutzung moderner digitaler Instrumente, insbesondere bei Internetrecherchen und der Einbeziehung sozialer Netzwerke, berücksichtigt die veränderten Kommunikations- und Bedrohungsmuster (§ 12 Abs. 1 Nr. 5 SÜG neu). In der Praxis sind OSINT-gestützte Prüfungen längst ein Teil moderner Risikoanalysen. Ihre gesetzliche Verankerung ist notwendig – allerdings sollten diese Verfahren auch automatisiert und risikobasiert möglich sein, z. B. im Rahmen eines gestaffelten Vorprüfsystems.
- Der Ausbau der Datenverarbeitungskompetenz und die Einführung einer durchgängigen elektronischen Aktenführung gemäß § 20 SÜG neu sowie § 18 Abs. 6 SÜG ermöglicht wichtige Digitalisierungsschritte.
- Die im Entwurf vorgesehene personelle Verstärkung bei den mitwirkenden Behörden (BfV, BAMAD, BND) durch Schaffung zusätzlicher Planstellen greift eine zentrale Forderung der Industrie zur Beschleunigung der Verfahren auf.

Vereinheitlichung der Vorgaben und der Zuständigkeit hinsichtlich der Betreuung für den materiellen Geheimschutz (insbes. im Hinblick auf IT) Nachbesserungsbedarf besteht aus unserer Sicht bei folgenden Punkten:

- Der Schaffung klar gebündelter Zuständigkeiten für Sicherheitsüberprüfungen in der Wirtschaft einerseits und die Vermeidung von Mehrfachüberprüfungen durch unterschiedliche Behörden auf Bundes- und Landesebene zur Reduzierung von Doppelstrukturen andererseits – eine zentrale Forderung der Industrie nach Zuständigkeitsbündelung – bleibt unberücksichtigt. Dies kann erreicht werden durch die Anerkennung bereits bestehender Zuverlässigkeitsüberprüfungen z.B. nach § 7 LuftSiG oder § 5 WaffG als gleichwertig zur einfachen Sicherheitsüberprüfung (§ 8 SÜG), sofern diese nicht älter als fünf Jahre sind. Hierdurch ließen sich Doppelüberprüfungen vermeiden und Behörden entlasten.

- Im Entwurf sollte sichergestellt werden, dass Sicherheitsüberprüfungen der Ressorts, Nachrichtendienste oder weiterer Behörden des Bundes und der Länder gegenseitig anerkannt werden. Nur so lassen sich für Unternehmen, die in Landes- und Bundeskontexten tätig sind, unnötige Mehrfachprüfungen und damit verbundene Aufwände vermeiden. Zudem sollte der Entwurf klarstellen, dass Vertrauenswürdigkeitsüberprüfungen ergänzend für exponierte Funktionen wie Mitglieder der Geschäftsführung, Mitarbeitende in der Unternehmenssicherheit, im ISMS, SOC, in der IT, Revision oder im Betrugsschutz einen zusätzlichen Sicherheitsgewinn darstellen. Hierzu unterbreiten wird den folgenden Formulierungsvorschlag für § 8, Abs. 2, SÜG:

  > *„Die zuständige Stelle kann von der Sicherheitsüberprüfung absehen, wenn die Zuverlässigkeit der betroffenen Person durch eine Überprüfung u.a. nach dem Luftsicherheitsgesetz (§ 7 LuftSiG) oder dem Waffengesetz (§ 5 WaffG) oder AtomG festgestellt wurde und diese nicht länger als fünf Jahre zurückliegt. Sicherheitsüberprüfungen auf Landes- und Bundesebene sind hierbei als gleichwertig zu betrachten.“*

- Einer expliziten gesetzlichen Verankerung verbindlicher Fristen für die Durchführung von Sicherheitsüberprüfungen (z. B. 3 Monate für einfache, 6 Monate für erweiterte Überprüfungen), um Unternehmen in ihren Planungen für Personal- und Projektentscheidungen mehr Verfahrenssicherheit zu geben. (Lediglich § 17 Abs. 3 SÜG neu sieht eine elektronische Erinnerungsfunktion vor, ohne jedoch verbindliche Fristen einzuführen). Dies könnte durch folgende Ergänzung des § 17 SÜG erreicht werden:

  > *„Die Sicherheitsüberprüfung ist innerhalb einer Frist von drei Monaten (einfache Überprüfung) bzw. sechs Monaten (erweiterte Überprüfung) nach Eingang der vollständigen Unterlagen abzuschließen. Bei Überschreitung ist die betroffene Person über den Stand des Verfahrens zu informieren.“*

- Der Einführung klarer und transparenter Ansprechstellen für Unternehmen (z.B. zentrale Koordinierungsstelle für Wirtschaftsakteure), um die Kommunikation im Prüfverfahren zu erleichtern, Bearbeitungszeiten zu verkürzen und eine einheitliche Zuständigkeit sicherzustellen. Die grundsätzliche Zuständigkeit für die Sicherheitsüberprüfung von Mitarbeitenden privater Wirtschaftsunternehmen sollte bei einer zentralen Stelle liegen, unabhängig vom konkreten Auftrag und Zuordnung des öffentlichen Auftraggebers zu einem Sektor (z.B. äußere Sicherheit, innere Sicherheit, KRITIS) oder der Ansiedlung auf Ebene Bund oder Länder. Entscheidend sollte der Arbeitgeber sein, nicht der projektbezogene Einsatz. § 24, Abs.2 widerspricht diesem Ansatz. Die hierdurch verursachte „Zersplitterung des Geheimschutzes“ konterkariert das Ziel einer gestärkten Nationalen Sicherheit. Ergänzend sollte § 3 SÜG wie folgt ergänzt werden:

„Zur Unterstützung nichtöffentlicher Stellen richtet das Bundesministerium des Innern eine zentrale Koordinierungsstelle für Sicherheitsüberprüfungen in der Wirtschaft ein."

- Einer vollständigen Digitalisierung des gesamten Antrags- und Prüfprozesses, inklusive elektronischer Antragstellung und durchgängiger digitaler Aktenführung, analog zu bestehenden Systemen wie ELSE (BAMAD) und ELEXI (BfV). Ansätze hierzu finden sich zwar in § 20 SÜG neu sowie § 18 Abs. 6 SÜG, eine vollständige Prozessdigitalisierung wird jedoch nicht realisiert. Wir schlagen folgende Anpassung des § 12 Abs. 1, Nr. 5 SÜG vor:

  „Die Sicherheitsakte und die Sicherheitsüberprüfungsakte sind vollständig digital zu führen. Die Antragstellung und Kommunikation erfolgen ausschließlich elektronisch über ein sicheres Behördenportal."

- Der Nutzung sicherer digitaler Kommunikationsverfahren (z. B. verschlüsselte E-Mail) anstelle des derzeit häufig noch papierbasierten Postweges, um Rückfragen schneller und effizienter zu klären.

- Einer ausdrücklichen Begrenzung des Umfangs der Datenabfragen, insbesondere bei Internetrecherchen und der Prüfung sozialer Netzwerke, um dem Grundsatz der Verhältnismäßigkeit und der Datensparsamkeit gerecht zu werden. (Der neue § 12 Abs. 1 Nr. 5 SÜG enthält hier eine erhebliche Ausweitung ohne klare Eingrenzung.). Daher erachten wir eine klare gesetzliche Eingrenzung der dieser Recherchen auf sicherheitsrelevante Aspekte inklusive einer Protokollierungspflicht für notwendig. Eine entsprechende Änderung könnte in § 12 Absatz 1 Nummer 5 SÜG erfolgen:

  „Recherchen auf öffentlich zugänglichen Internetplattformen einschließlich sozialer Netzwerke erfolgen nur in erforderlichem Maße und unter Beachtung des Grundsatzes der Verhältnismäßigkeit. Die Recherche ist zu dokumentieren und auf sicherheitsrelevante Inhalte zu beschränken."

- Mehr Rechtssicherheit in Fällen, in denen die Dauer der Sicherheitsüberprüfung die Probezeit von Mitarbeitenden überschreitet. Arbeitgeber sollten hier mehr Transparenz erhalten, um fundierte Personalentscheidungen treffen zu können. Transparenz bedeutet dabei Informationen über den Bearbeitungsstand der Sicherheitsüberprüfung sowie Hinweise, ob sicherheitserhebliche Erkenntnisse den Fortgang des Verfahrens beeinflussen könnten, damit arbeitsrechtliche Entscheidungen rechtzeitig und verantwortungsvoll getroffen werden können. Belastbare arbeitsrechtliche Regelungen für den Umgang mit sicherheitserheblichen Erkenntnissen sind hierfür aus Unternehmenssicht unerlässlich. Transparente Verfahren ermöglichen es Unternehmen beispielsweise, die Möglichkeit einer Weiterbeschäftigung auch im Rahmen von maximal VS-NfD zu bewerten, falls Mitarbeitende keine Ü2 erhalten (z.B. aufgrund von Familienangehörigen aus bestimmten Herkunftsländern). In diesen Fällen sollte der Sicherheitsbevollmächtigte Auskunft über die Gründe erhalten.

- Einer Informationsmöglichkeit über den Bearbeitungsstand laufender Überprüfungen, insbesondere bei deutlicher Überschreitung üblicher Bearbeitungszeiten. Dies würde Unternehmen die Möglichkeit verschaffen, eine Abschätzung hinsichtlich der Sinnhaftigkeit einer weiteren Befassung vorzunehmen und die Gründe der langen Bearbeitungsdauer zu erfahren (vgl. hierzu auch die obigen Ausführungen).

- Der Gesetzentwurf greift den Bedarf der Wirtschaft an einer freiwilligen Vertrauenswürdigkeitsüberprüfung für Beschäftigte in besonders sensiblen Bereichen nicht auf.[1] Unternehmen, die weder dem Geheimschutz des Bundes unterliegen noch verpflichtet sind,

[1] Vgl. https://bdi.eu/publikation/news/vertrauenswuerdigkeitsueberpruefung

Sicherheitsüberprüfungen nach dem Sicherheitsüberprüfungsgesetz durchzuführen, sollten die Möglichkeit erhalten, für kritische Funktionen – etwa IT-Personal, Steuerungssysteme oder Werkschutz – freiwillig die persönliche Vertrauenswürdigkeit von Beschäftigten prüfen zu lassen. Angesichts dessen sollte die Bundesregierung im Rahmen der Gesetzgebungsverfahren zum NIS2UmsuCG sowie zur Umsetzung der Resilience-of-Critical-Entities-Richtlinie ((EU) 2022/2557) die in Artikel 14 vorgesehene Möglichkeit einer freiwilligen Zuverlässigkeits- und Vertrauenswürdigkeitsüberprüfung gesetzlich regeln und den Unternehmen damit ein rechtssicheres Instrument an die Hand geben. Eine Regelung hierzu kann durch die Einführung eines § 25 b SÜG Unternehmen die Möglichkeit geben, freiwillige Prüfungen für sensible Funktionen durchzuführen:

> *„Unternehmen, die nicht dem Geltungsbereich des § 1 Absatz 2 unterliegen, können für Beschäftigte in sicherheitsrelevanten Funktionen eine freiwillige Vertrauenswürdigkeitsüberprüfung nach Maßgabe der §§ 8 bis 10 beantragen. Die Durchführung erfolgt durch die zuständige Stelle nach § 3."*

- Eine regelmäßige gesetzlich vorgesehene Evaluierung der Sicherheitsüberprüfungsregelungen zusammen mit der Wirtschaft, wie sie politisch gefordert wird, enthält der Entwurf nicht. Lediglich eine allgemeine Evaluierung der Auswirkungen auf die Sicherheitslage wird im Entwurf erwähnt. Einer gesetzlich verankerten regelmäßigen Evaluierung der Wirksamkeit und Effizienz der Sicherheitsüberprüfungen unter Einbindung von Wirtschaftsverbänden kann durch Ergänzung des § 35 SÜG begegnet werden:

  > *„Die Bundesregierung evaluiert alle fünf Jahre gemeinsam mit Vertretern, Verbänden der Wirtschaft die Wirksamkeit und Effizienz der Sicherheitsüberprüfungen."*

- Personen, die aktuell oder in der Vergangenheit die Staatsangehörigkeit eines Staates gemäß § 13 Absatz 1 Nummer 17 besessen haben, dürfen Zugang zu Verschlusssachen der Geheimhaltungsgrade VS-VERTRAULICH, GEHEIM oder STRENG GEHEIM gemäß § 4 nur erhalten, wenn zuvor eine vertiefte sicherheitsmäßige Bewertung unter besonderer Berücksichtigung möglicher sicherheitserheblicher Risiken erfolgt ist. Für den Zugang zu Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH ist u.E. ebenfalls eine besondere Sensibilisierung geboten; die Verpflichtung durch die für VS-NUR FÜR DEN DIENSTGEBRAUCH verantwortliche Person in öffentlichen und nicht öffentlichen Stellen sollte daher in diesen Fällen um eine dokumentierte Risikobewertung ergänzt werden. Die Regelung dient der Berücksichtigung besonderer sicherheitsrelevanter Konstellationen bei Personen mit Bezug zu Staaten, die vom Bundesministerium des Innern als sicherheitskritisch eingestuft wurden. Ziel ist es, potenzielle Risiken durch nachrichtendienstliche Einflussnahme oder Loyalitätskonflikte frühzeitig zu erkennen und zu bewerten. In § 4 oder § 12 sollte u.E. daher ein neuer Absatz wie folgt ergänzt werden:

  > *„Bei Personen, die aktuell oder in der Vergangenheit die Staatsangehörigkeit eines Staates gemäß § 13 Absatz 1 Nummer 17 besessen haben, ist vor der Erteilung einer Ermächtigung zum Zugang zu Verschlusssachen der Geheimhaltungsgrade VS-VERTRAULICH, GEHEIM oder STRENG GEHEIM gemäß § 4 eine vertiefte sicherheitsmäßige Bewertung durchzuführen. Für den Zugang zu Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH ist ebenfalls eine besondere Sensibilisierung geboten; die Verpflichtung der Personen durch die für VS-NUR FÜR DEN DIENSTGEBRAUCH verantwortliche Person in öffentlichen und nicht öffentlichen Stellen ist in diesen Fällen um eine dokumentierte Risikobewertung zu ergänzen."*

- Im SÜG sollte die herausgehobene Stellung des Sicherheitsbevollmächtigten (SiBe) in ähnlicher Weise gewürdigt und die Position des SiBe durch einen Kündigungsschutz gestärkt werden, wie dies in § 6, Abs. 4 BDSG für den Datenschutzbeauftragten und in Art. 38, Abs. 3 DSGVO für den

Datenschutzbeauftragten in nicht öffentlichen Stellen erfolgt ist. Eine entsprechende Ergänzung könnte in § 25, Abs. 4 erfolgen.

- Weitere Vereinheitlichung der Regelwerke zum materiellen Geheimschutz, insbes. im Hinblick auf IT zur Nutzung im und für das militärische Umfeld und Wahrnehmung von Aufgaben im Kontext des geheimschutzrelevanten Behördenumfelds durch die Industrie. Nach wie vor unterliegt die Sicherheits- und Verteidigungsindustrie (SVI) hinsichtlich materiellem Geheimschutz unterschiedlichen Regelwerken. Materieller Geheimschutz und IT der SVI-Unternehmen fallen unter die Geheimschutzbetreuung des BMWE („Geheimschutzhandbuch"), Zuständigkeit für VS-Zulassung von z.B. Produkten obliegt dem BSI und in Verträgen mit dem Geschäftsbereich (GB) BMVg wird die Anwendung von Vorschriften und Erlassen des GB BMVg verbindlich vereinbart. Die Akkreditierung von materiellen/technischen Maßnahmen und – abhängig von der Nutzung durch Industrie, den GB BMVg oder weitere Stellen wie z.B. NATO – obliegt bisher unterschiedlichen Stellen. Aus Sicht der SVI sind die Regelwerke im Interesse von Wirksamkeit und Effizienz soweit zu vereinheitlichen, dass die Vorgaben unterschiedlicher Ressorts widerspruchsfrei umsetzbar sind und eine einheitliche Akkreditierung ermöglicht wird. Hierunter fällt insbesondere die weitere Vereinheitlichung der Zuständigkeit für Akkreditierungen und Einsatzfreigaben bzw. Zulassungen (z.B. Bündelung bei der zuständigen Stelle im GB BMVg).

Fazit

Der Gesetzentwurf greift zentrale Elemente einer notwendigen Modernisierung des Sicherheitsüberprüfungsrechts auf. Die Einbeziehung privatwirtschaftlicher sicherheitsrelevanter Akteure wird gestärkt. Gleichzeitig entstehen neue Melde- und Verwaltungspflichten für Unternehmen, ohne dass die Komplexität der Verfahren insgesamt durch konsequent vereinfachte und verschlankte Prozesse spürbar reduziert wird.

Das verdeutlicht: Sicherheitsüberprüfungen werden im Entwurf weiterhin primär als Unternehmensregulierung adressiert – nicht als das, was sie sind: ein entscheidender Baustein der nationalen Sicherheit und Verteidigungsfähigkeit, der auch die staatliche Seite in die Pflicht nimmt. Dieser Zusammenhang – Sicherheitsüberprüfungen als essenzielle Voraussetzung für die Härtung Kritischer Infrastrukturen sowie für Produktionshochlauf und Kapazitätsausbau der Sicherheits- und Verteidigungsindustrie – findet in der Systemlogik des Entwurfs zu wenig Niederschlag.

Folgerichtig fehlen durchgängige Digitalisierung, klare Ansprechpartner, verbindliche Fristen und ein transparenter Informationsfluss. Wichtige industriepolitische Anliegen, die eine unmittelbaren Beschleunigungswirkung und eine Erhöhung der Sicherheit bewirken könnten, sind nicht hinreichend angelegt.-Aus unserer Sicht (BDI / BDSV / BDLI / Bitkom / BAK SiBe / VSW Bundesverband) ist eine grundsätzliche Vereinfachung und Effizienzsteigerung erforderlich, um diese Effekte zu erzielen: ein gestaffeltes, digitales, risikobasiertes und skalierbares Überprüfungssystem, das - ganz im Sinne unserer nationalen Sicherheit und Verteidigung - zwischen Nachrichtendiensten und wirtschaftlicher Realität vermittelt. Nur so lassen sich die in unserer Vorbemerkung benannten Zielmarken tatsächlich erreichen. Die Industrie steht für einen konstruktiven Dialog zur Weiterentwicklung des Sicherheitsüberprüfungsrechts jederzeit bereit.

Ansprechpartner:

Kerstin Petretto
Bundesverband der Deutschen Industrie (BDI)
Senior Managerin Sicherheit und Verteidigung
T: +49 30 2028-1710
k.petretto@bdi.eu

David Jansen
Referent für Cyber/IT
Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V. (BDSV)
Tel: +49 30 206 1899-15
d.jansen@bdsv.eu

Adrian Ahlers
Referent Verteidigung & Sicherheit
Bundesverband der Deutschen Luft- und Raumfahrtindustrie e. V. (BDLI)
Tel: +49 30 206140-59
ahlers@bdli.de

Felix Kuhlenkamp
Bereichsleiter Sicherheitspolitik
Branchenverband der deutschen Informations- und Telekommunikationsbranche (Bitkom)
Tel: +49 30 27576-279
f.Kuhlenkamp@bitkom.org

Sven Krippgans
Für den Vorstand des BAK SiBe
Sven Krippgans
Tel: +49 431 700 4301
sven.krippgans@tkmsgroup.com

Günther Schotten
Geschäftsführer
Verband für Sicherheit in der Wirtschaft – VSW-Bundesverband e.V.
Tel: +49 30 24 63 71 74