VSW

Bundesverband

Whitepaper

Staatlicher Geheimschutz 2030

Strategischer Enabler für Deutschlands Verteidigungs-, Technologie- und Wettbewerbsfähigkeit

Stand: 13. August 2026

Modernisierungsimpuls an die Bundesregierung und das Bundesministerium für Wirtschaft und Energie (BMWE)

Leitthese
Ein leistungsfähiger amtlicher Geheim- und Sabotageschutz ist keine administrative Nebenfunktion. Er ist eine kritische Infrastruktur der nationalen Sicherheit: Er entscheidet mit darüber, ob Deutschland sicherheitsrelevante Technologien entwickeln, industrielle Kapazitäten hochfahren, kritische Infrastrukturen schützen und internationale Verpflichtungen verlässlich erfüllen kann.

Executive Summary

Deutschland steht vor einer Richtungsentscheidung. Die sicherheits- und industriepolitischen Ziele der Bundesregierung verlangen einen staatlichen Geheimschutz, der schnell, digital, skalierbar und international anschlussfähig arbeitet. Die heutige Architektur erreicht dieses Leistungsniveau nur teilweise. Ihre Funktionsfähigkeit beruht in erheblichem Maße auf der Erfahrung und dem persönlichen Einsatz weniger hochqualifizierter Fachkräfte, während Organisation, Ressourcen, Verfahren und technische Ausstattung mit der wachsenden Komplexität nicht Schritt gehalten haben.

1 **Strategische Bedeutung**: Geheimschutz bestimmt zunehmend die Innovations-, Liefer- und Kooperationsfähigkeit der Sicherheits- und Verteidigungswirtschaft sowie weiterer sicherheitsrelevanter Branchen.

2 **Strukturelle Überlastung**: Komplexere Anforderungen an den Geheimschutz in der Informationstechnik (IT), IT-Systeme zur Verarbeitung von Verschlusssachen (Classified Information Systems, CIS), materielle Sicherheit, Transporte von Verschlusssachen (VS) und internationale Programme treffen auf begrenzte personelle Kapazitäten, papiergebundene Abläufe und fragmentierte Zuständigkeiten.

3 **Akutes Reformrisiko**: Die derzeit geprüfte Verlagerung von Teilaufgaben auf eine weitere Bundesbehörde birgt die Gefahr zusätzlicher Schnittstellen, divergierender Auslegungen, längerer Verfahren und eines Verlusts der ganzheitlichen Unternehmensbetreuung.

4 **Erforderliche Richtung**: Nicht die Verteilung bestehender Knappheit, sondern die politische Aufwertung, Bündelung, Digitalisierung und nachhaltige Befähigung des Systems muss das Ziel sein.

Die zentrale Entscheidung lautet daher nicht, wo einzelne Teilaufgaben administrativ verortet werden. Entscheidend ist, ob Deutschland eine kohärente Gesamtarchitektur erhält, die Sicherheit und Geschwindigkeit verbindet, ohne das Schutzniveau abzusenken.

Verband für Sicherheit in der Wirtschaft, Bundesverband e.V.
VSW-Bundesverband | Bayerischer Platz 6 | 10779 Berlin
Telefon +49 (0)30 246 37 175 | Telefax +49 (0)30 200 77 056
info@vsw-bundesverband.de | www.vsw-bundesverband.de

1. Lagebild: Hohe Leistung in nicht mehr skalierbaren Strukturen

Das vorhandene Personal arbeitet hochprofessionell. Langjährige Erfahrung, tiefes Fachwissen und belastbare nationale wie internationale Netzwerke kompensieren heute wesentliche strukturelle Defizite. Gerade deshalb ist die Lage kritisch: Mehrere Leistungsträger stehen vor dem Ruhestand oder erwägen einen Wechsel. Geht dieses Erfahrungswissen verloren, kann die bereits angespannte Funktionsfähigkeit kurzfristig weiter abnehmen.

Organisation und Ressourcen

Die personelle Kapazität wurde trotz deutlich gestiegener fachlicher Anforderungen nicht entsprechend ausgebaut. Mitarbeitende betreuen teilweise mehrere Großdelegationen parallel; die Teilnahme an internationalen Gremien und spezialisierte Qualifizierungen sind nur eingeschränkt möglich. Zugleich erschwert die organisatorische Einbettung in ein breites, fachlich heterogenes Umfeld eine sichtbare Priorisierung und strategische Steuerung.

Wachsende technische Komplexität

Nicht die Zahl klassischer Sicherheitsbescheide ist das Kernproblem, sondern die steigende Komplexität der Projekte. IT-Geheimschutzanweisungen für moderne Datenverarbeitung und Abstrahlschutz, CIS, materielle Sicherheitsmaßnahmen, internationale Freigaben und VS-Transporte erfordern hochspezialisierte und zeitkritische Bewertungen.

Veraltete Prozesse

Zentrale Verfahrensschritte sind weiterhin papiergebunden oder von Medienbrüchen geprägt. Fehlende durchgängige digitale Aktenführung, eingeschränkte Remote-Fähigkeit und nicht harmonisierte Kommunikationswege verlängern Bearbeitungszeiten, reduzieren Transparenz und erschweren die internationale Zusammenarbeit.

Governance und Akkreditierung

Das BMWE verfügt über keine eigene Stelle für die Sicherheitsakkreditierung von VS-IT-Systemen (Security Accreditation Authority, SAA) und ist bei wesentlichen Bewertungen auf das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie die Deutsche militärische Security Accreditation Authority (DeuMilSAA) angewiesen. Die ressortübergreifenden Prozesse sind fachlich notwendig, aber häufig langwierig und nicht vollständig harmonisiert. Hinzu kommen unterschiedliche Auslegungen bei Verschlusssachen - Nur für den Dienstgebrauch (VS-NfD) sowie unklare Verantwortungsgrenzen bei Cloud, Künstlicher Intelligenz (KI) und multinationalen Datenräumen.

Marktzugang und Skalierung

Neue Anbieter können sich häufig nicht frühzeitig auf die Geheimschutzbetreuung vorbereiten. Lange Aufnahme- und Überprüfungsverfahren erschweren die Teilnahme an eingestuften Ausschreibungen, verzögern den Einsatz qualifizierten Personals und begrenzen den schnellen Eintritt innovativer Unternehmen in sicherheitsrelevante Lieferketten.

> **Systemisches Risiko**
> Die heutige Architektur funktioniert, aber sie ist nicht ausreichend resilient und nicht skalierbar. Sie hängt zu stark von Einzelpersonen, informellen Netzwerken und manuellen Verfahren ab. Genau in dem Moment, in dem Deutschland mehr Tempo, mehr Projekte und mehr internationale Kooperation benötigt, droht der staatliche Geheimschutz zum Engpass des politisch gewollten Hochlaufs zu werden.

Verband für Sicherheit in der Wirtschaft, Bundesverband e.V.
VSW-Bundesverband | Bayerischer Platz 6 | 10779 Berlin
Telefon +49 (0)30 246 37 175 | Telefax +49 (0)30 200 77 056
info@vsw-bundesverband.de | www.vsw-bundesverband.de

2. Aktuelle Neuordnung: Fragmentierung würde die Kernprobleme verschärfen

Nach vorliegenden Informationen wird geprüft, operative Teilaufgaben des amtlichen Geheim- und Sabotageschutzes aus dem BMWE in die Bundesnetzagentur zu verlagern und weitere Aufgaben auf bestehende Sicherheitsbehörden zu verteilen. Eine solche Aufteilung kann punktuell Entlastung versprechen, birgt jedoch erhebliche strukturelle Nebenwirkungen: zusätzliche Schnittstellen, mehr Abstimmungsbedarf, potenziell unterschiedliche Bewertungsmaßstäbe und den Verlust einer ganzheitlichen Unternehmensbetreuung.

- Unternehmen benötigten künftig mehrere Ansprechpartner statt einer klaren Gesamtverantwortung.
- Materieller, personeller und IT-Geheimschutz könnten organisatorisch auseinanderfallen, obwohl sie in der Praxis eng verzahnt sind.
- Zivile Schlüsseltechnologien, kritische Infrastrukturen und industrielle Querschnittsprojekte drohten gegenüber klassischen Rüstungsvorhaben strukturell an Gewicht zu verlieren.
- Neue Übergaben, Doppelprüfungen und divergierende Auslegungen könnten Bearbeitungszeiten weiter verlängern und dem Ziel des Bürokratieabbaus entgegenwirken.

Die Reform darf daher nicht an Behördenzuständigkeiten beginnen, sondern an einem verbindlichen Zielbild. Erst wenn Gesamtverantwortung, Leistungsversprechen und Schnittstellen definiert sind, sollte über die institutionelle Verortung einzelner Aufgaben entschieden werden.

3. Zielbild 2030: Ein moderner staatlicher Geheimschutz

Eindeutige Gesamtverantwortung
Eine politisch sichtbare Stelle steuert Standards, Prioritäten, Ressourcen und internationale Vertretung.

Zentrale Anlaufstelle für die Wirtschaft
Unternehmen erhalten einen verantwortlichen Ansprechpartner und transparente digitale Verfahrensstände.

Integrierte Fachlichkeit
Personeller, materieller und IT-Geheimschutz sowie Sabotage- und Wirtschaftsschutz werden kohärent verzahnt.

Digitale Verfahren als Standard
Medienbruchfreie Akten, sichere Kollaboration, digitale Register und standardisierte Schnittstellen werden zum Regelfall.

Skalierbare Ressourcen
Personalaufbau, Fachlaufbahnen, Nachfolgeplanung und spezialisierte Qualifizierung sichern Wissen und Lieferfähigkeit.

Internationale Interoperabilität
Akkreditierungen, Anerkennungen und Standards werden ressortübergreifend und mit Partnerstaaten harmonisiert.

4. Fünf prioritäre Entscheidungen

1 **Zielbild vor Strukturentscheidung:** Vor einer Aufgabenverlagerung ist ein ressortübergreifendes Zielbetriebsmodell mit Wirkungs-, Schnittstellen- und Risikoanalyse festzulegen.

2 **Politische Aufwertung im BMWE:** Bündelung in einer leistungsfähigen Einheit „Strategischer Geheim- und Sabotageschutz & Wirtschaftssicherheit“ mit direkter Anbindung an die Staatssekretärsebene.

3 **Transformationsprogramm:** Mehrjähriger Personal- und Kompetenzaufbau, Nachfolgeplanung, vollständige Digitalisierung sowie grundlegende Modernisierung des Geheimschutzhandbuchs und der IT-/CIS-Regelwerke.

4 **Klare Akkreditierungs- und Servicearchitektur:** Eindeutige SAA-Verantwortung, verbindliche Schnittstellen zu BSI und DeuMilSAA, gegenseitige Anerkennung von Prüfungen sowie transparente Leistungszusagen und Fristen.

5 **Security Fast Track:** Beschleunigte, risikobasierte Verfahren für strategische Projekte, neue Marktteilnehmer und Unternehmen, die sich erstmals auf eingestufte Ausschreibungen bewerben - ohne Absenkung des Sicherheitsniveaus.

Schlussfolgerung: Die zentrale Aufgabe besteht nicht darin, bestehende Knappheit auf mehrere Behörden zu verteilen. Deutschland benötigt eine leistungsfähige Gesamtarchitektur, die Kompetenz bündelt, Verfahren beschleunigt und die Wirtschaft als Partner der nationalen Sicherheit versteht. Das BMWE hat die Chance, diese Modernisierung politisch zu führen und den Geheim- und Sabotageschutz von einem schwerfälligen Verwaltungsprozess zu einem strategischen Standort- und Fähigkeitsfaktor weiterzuentwickeln.[1]

[1] **Evidenzbasis**: Verdichtung verbändeübergreifender Stellungnahmen und Anhörungsunterlagen 2025/2026, aktueller Branchenpositionen sowie anonymisierter operativer Praxiserfahrungen aus Behörden und Wirtschaft. Das Papier benennt strukturelle Handlungsfelder; es bewertet keine individuellen Leistungen oder Verantwortlichkeiten.