21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)069
vom 10. Oktober 2025

Schriftliche Stellungnahme

des Bundesamtes für Sicherheit in der Informationstechnik vom 10. 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

Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 13.10.2025

Das **Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung** hat aus Sicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) höchste Priorität und sollte zeitnah beschlossen werden. Es ist grundsätzlich dazu geeignet, das Cybersicherheitsniveau in Deutschland deutlich anzuheben und wird ein klares Signal an die Verantwortlichen für die betroffenen Organisationen senden. Gleichwohl ist davon auszugehen, dass Cyberangriffe, insbesondere auf Wirtschaftsunternehmen und Einrichtungen der Bundesverwaltung, zunehmen werden. Der bisherige Gesetzentwurf wird dieser Bedrohungslage noch nicht vollumfänglich gerecht.

Das BSI erachtet eine schnellstmögliche Umsetzung des Gesetzesvorhabens als unerlässlich und räumt dieser auch höchste Priorität ein. Vor diesem Hintergrund werden durch das BSI derzeit nur die absolut dringendsten Anpassungsbedarfe geltend gemacht, um die zeitnahe Umsetzung der NIS-2-Richtlinie nicht zu gefährden. Weitere wichtige Rechtsänderungen sind als Anlage beigefügt. Diese sollten nach Abschluss dieses Rechtsetzungsverfahrens unverzüglich angegangen werden.

Im Einzelnen und nach Priorität geordnet:

1. Regelungsbedarf in Bezug auf die in der NIS-2-Richtlinie festgelegten Pflichten der Organisationen

1.1 Regelungen für die Bundesverwaltung

Aufgrund der aktuellen Bedrohungslage sieht es das BSI als zwingend erforderlich an, dass schnellstmöglich ein einheitliches Cyber-Sicherheitsniveau für die gesamte Bundesverwaltung geschaffen wird und alle Institutionen des Bundes ein hinreichendes Resilienzniveau erreichen. Nicht zuletzt hat neben dem BSI auch der Bundrechnungshof hier dringenden Handlungsbedarf identifiziert.

Hierzu werden zwei Regelungen empfohlen:

- Grundsätzliche Anwendung des Gesetzes auf die gesamte Bundesverwaltung ohne Unterscheidung zwischen BKAmt / Bundesministerien und der restlichen Bundesverwaltung.
- Schaffung eines CISO Bund beim BSI mit den entsprechenden Befugnissen, um die notwendigen Resilienzmaßnahmen mit den Institutionen des Bundes operativ umzusetzen.

Hier ist hervorzuheben, dass insbesondere das Zusammenspiel beider Regelungen die Cybersicherheit in der Bundesverwaltung spürbar erhöhen wird. Die dringend gebotene Verbesserung der Situation in der Bundesverwaltung kann ferner nur gelingen, wenn Mandat, Fähigkeiten und Ressourcen für eine operative Umsetzung an der richtigen Stelle gebündelt und stringent eingesetzt werden. Hierfür wird die Ansiedlung des CISO Bund beim BSI empfohlen, der zusammen mit den Institutionen des Bundes die Umsetzung vollzieht. Dies sollte bezüglich des Auftrags für die Umsetzung und die Überwachung der erreichten Ergebnisse auf Ministerebene flankiert werden.

Die Einrichtungen des Bundes nutzen in Teilen die gleichen Netz- und Lieferstrukturen, wodurch eine einheitliche Behandlung aller Einrichtungen des Bundes zum Schutze der Bundesverwaltung geboten ist; einzelne nicht hinreichend geschützte Einrichtungen können sonst zu einem Einfallstor werden. Hinzu kommen das Argument und der Ruf nach der Gleichbehandlung mit der Wirtschaft bzgl. der dort geltenden Anforderungen.

Konkrete Anpassungsempfehlungen:

- Einheitliche IT-Sicherheitsvorgaben für die gesamte Bundesverwaltung. Hierzu muss insbesondere die Unterscheidung zwischen Bundesverwaltung und Bundeskanzleramt / Bundesministerien in den §§ 29 und 44 BSIG-E gestrichen werden.
- Aufnahme des CISO Bund als zusätzliche Aufgabe des BSI und Vorschläge für die erforderlichen Befugnisse:
    - Die Leitung des BSI nimmt diese Aufgaben wahr.
    - Der CISO Bund muss über die erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich der Informationssicherheit verfügen.
    - Der CISO Bund koordiniert das operative Informationssicherheitsmanagement des Bundes. Im Benehmen mit den obersten Bundesbehörden entwickelt der CISO Bund Programme zur Gewährleistung der Informationssicherheit des Bundes und schreibt diese fort.
    - Der CISO Bund beaufsichtigt die Umsetzung der Programme zur Gewährleistung der Informationssicherheit des Bundes durch die Befugnisse des BSI.
    - Der CISO Bund unterrichtet kalenderjährlich dem Haushaltsausschuss des Deutschen Bundestages über den Umsetzungsstand der Programme.
    - Der CISO Bund ist direkt angebunden an den zuständigen Bundesminister.
    - Der CISO Bund wird bei allen Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben beteiligt, soweit sie Fragen der Informationssicherheit berühren.

1.2 Erweiterte Befugnis zur Messung der Resilienz deutscher IT-Systeme und Detektion von Angreifer-Infrastrukturen

Derzeit darf das BSI Messungen zu einer Verwundbarkeit aufgrund öffentlich bekannter Schwachstellen bei öffentlich erreichbaren IT-Systemen (Resilienz-Messungen) nur in einem sehr eingeschränkten Bereich durchführen (v.a. Einrichtungen des Bundes, kritische Infrastrukturen, große digitale Dienste und Unternehmen im öffentlichen Interesse).

Das BSI sollte analog zur Mehrheit der europäischen Staaten ebenfalls zu Resilienz-Messungen für alle im deutschen IP-Raum erreichbaren IP-Adressen befugt sein. Ziel ist die Warnung der Betroffenen, damit diese möglichst zeitnah Schutzmaßnahmen ergreifen können. Die Warnung der Betroffenen sollte dadurch erfolgen, dass das BSI befugt ist, Provider zur entsprechenden Information ihrer Kundinnen und Kunden anzuweisen. Angreifer scannen den kompletten IP-Raum regelmäßig auf Verwundbarkeiten. Ziel muss es sein, ihnen zuvorzukommen.

Ergänzend dazu sollte das BSI Befugnisse zur Detektion von Angreifer-Infrastrukturen erhalten. Die Dunkelziffer von Systemen, die durch staatliche Angreifer kompromittiert werden, ist hoch. Eine besondere Bedrohung sind Prepositioning-Angriffe. Hierbei wird Schadsoftware installiert, aber nicht aktiv genutzt, sondern für den Einsatz in einem eskalierenden Krisenfall zu Sabotagezwecken vorgehalten. Da die Schadsoftware bis zum Eintritt des Krisenfalls nicht aktiv ist, ist sie schwieriger zu

erkennen. Das BSI hat aktuell keine Möglichkeit, seine Kenntnis über Angreifer und deren Werkzeuge außerhalb der Regierungsnetze einzusetzen.

Technisch ist es möglich, Angreiferserver zu identifizieren. Dies geschieht anhand bestimmter Indikatoren, etwa anhand eines bestimmten Kommunikationsverhaltens bei C2-Servern. Auf diese Weise könnte das BSI Prepositioning-Schadsoftware finden, bevor sie zum Einsatz kommt. Das BSI sollte daher in die Lage versetzt werden, im Internet nach Systemen zu suchen, die aktiv für Angriffe genutzt werden.

1.3 Ausweitung der Befugnisse gegenüber Diensteanbietern und verbesserter Schutz vor Phishing-Angriffen

Die in § 16 des neuen BSIG geregelten Befugnisse des BSI reichen insgesamt nicht aus, um einen flächendeckenden Schutz vor Cyberkriminellen zu ermöglichen.

Danach dürfen – wie auch schon nach der aktuellen Rechtslage – weiterhin nur Telekommunikations-Anbieter mit mehr als 100.000 Kunden adressiert werden; regionale Internet Service Provider, Universitäten, Content-Anbieter und DNS-Anbieter sind nicht einbezogen. Weiterhin erfasst die Regelung Phishing- und andere schädliche Webseiten, von denen für Wirtschaft und Gesellschaft erhebliche Gefahren im Alltag ausgehen, nicht hinreichend.

Zum anderen sollte zur Verbesserung des Schutzes vor Phishing-Angriffen eine explizite Befugnis des BSI ergänzt werden, Informationen über Phishing-Domains zu sammeln, zu verifizieren und bereitzustellen. Telekommunikations-Anbieter sollten verpflichtet werden, eigene Erkenntnisse in diese Datenbank einzubringen, selbst Informationen abzurufen und ihren Kunden zumindest optional einen DNS-basierten Schutz zur Verfügung zu stellen.

Ferner sollte es dem BSI für einen schnellen und effektiven Schutz der Betroffenen erlaubt werden, mit Unterstützung der Provider Bereinigungsbefehle selbst an kompromittierte IT-Systeme zu senden. Aktuell dürfen dies nach § 7 c Absatz 1 Satz 1 Nummer 2 BSIG nur die Telekommunikations-Provider selbst. In der Regel erfolgt aber zuvor schon eine Umleitung des Datenverkehrs auf Server des BSI nach § 7 c Absatz 3, um den Datenverkehr analysieren zu können. Während der Umleitung können Diensteanbieter keine Bereinigungsbefehle mehr versenden.

Darüber hinaus bestehen außerdem noch Regelungslücken bei der Bekämpfung von Botnetzen, die eine der größten Gefahren für die Cybersicherheit darstellen. Botnetze werden von Cyber-Kriminellen etwa zur Verbreitung von Schadprogrammen, für Informationsdiebstahl, zum Versand von Spam-Nachrichten oder zur Durchführung von DDoS-Angriffen eingesetzt. Das BSI setzt seit mehreren Jahren erfolgreich Maßnahmen zur Abwehr von Botnetzen um, darunter auch die Umleitung von Domainnamen durch Internetprovider. Dies muss auf Domainregistrare ausgeweitet werden, um zu ermöglichen, dass die Botnetze nicht nur teilweise, sondern vollständig entschärft werden.

1.4 Regelungen für den Energiesektor

Für den Energiesektor sind einzelne Besonderheiten im Vergleich zu anderen Sektoren im Gesetzentwurf vorgesehen, u.a. dass das BSI bei der Erstellung der IT-Sicherheitskataloge im Energiesektor im Einvernehmen beteiligt wird. Die vorgesehene Überprüfung auf Aktualität der Kataloge alle zwei Jahre ist dagegen alleinig der Bundesnetzagentur (BNetzA) vorbehalten. Eine Beteiligung des BSI an der Überprüfung ist nicht vorgesehen. Dem BSI sollte dringend ein Initiativrecht zur Aktualisierung von IT-Sicherheitskatalogen eingeräumt werden, um aktuellste Erkenntnisse und

Expertise unmittelbar einbringen zu können. Nur wenn sowohl BNetzA als auch BSI gleichermaßen eine Aktualisierung der Kataloge anstoßen dürfen, kann die Aktualität derselben gewährleistet und damit ein ausreichend hohes Cybersicherheitsniveau adäquat sichergestellt werden.

Zudem sollte dem BSI die Möglichkeit zur stichprobenhaften Überprüfung der Absicherung von Betreibern im Energiesektor gegeben werden; ähnlich wie es dem BSI bereits im Telekommunikationssektor erlaubt ist. Hierbei könnten auch gemeinsame Prüfungen durch BSI und BNetzA vorgesehen werden.

Bei gefundenen Mängeln benötigt das BSI außerdem dringend eine Anordnungsbefugnis im Energiewirtschaftsgesetz (EnWG), um eine schnellstmögliche Behebung durchsetzen zu können. Die Erfahrungen aus der Praxis zeigen, dass solche Durchsetzungs- und Sanktionsmöglichkeiten ein wichtiger Faktor für eine zeitnahe Mängelbeseitigung durch KRITIS-Betreiber sind.

1.5 Präzisierung des NIS-2 Ausnahmekriteriums „Vernachlässigbare Geschäftstätigkeit“

Grundsätzlich ist die Regelung in § 28 BSIG-E zur Präzisierung des Anwendungsbereichs bei den Einrichtungsarten zu begrüßen. Die nun neu eingefügte Regelung in § 28 Abs. 3 BSIG-E hinsichtlich „vernachlässigbarer Geschäftstätigkeiten“ wird jedoch sowohl im Gesetz als auch in der Gesetzesbegründung nicht ausreichend erläutert und bleibt damit unklar. Für das BSI als Aufsichtsbehörde lässt sich auf dieser Grundlage keine rechtssichere Identifizierung des Anwendungsbereichs vornehmen. Dadurch werden in der Praxis möglicherweise betroffene Unternehmen, insbesondere kleine und mittelständische, deutlich verunsichert sein, inwieweit sie vom Gesetz betroffen sind. Es sollte daher eine klare Definition hinsichtlich des Kriteriums „vernachlässigbar“ im Gesetz festgelegt werden, um Rechtsklarheit für alle Beteiligten zu schaffen.

(Anlage 1)

Erweiterter Regelungsbedarf in dieser Legislaturperiode zur Stärkung der Cybersicherheit

Das **Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung** hat aus Sicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) höchste Priorität und sollte zeitnah beschlossen werden. Vor diesem Hintergrund wurden durch das BSI für das aktuelle Gesetzgebungsverfahren nur die dringendsten Rechtsanpassungsbedarfe geltend gemacht.

Die in diesem Dokument aufgeführten Bedarfe wurden auch im Kontext des o.g. Gesetzesvorhabens diskutiert. Um das Verfahren jedoch nicht zu verzögern, können diese auch im Anschluss an das aktuelle Gesetzgebungsverfahren in dieser Legislaturperiode realisiert werden. Hierfür könnten die bevorstehenden Gesetzgebungsverfahren zum CRA (Cyber-Resilience-Act) und zur Schaffung weiterer Cyberabwehrbefugnisse genutzt werden.

Die nachfolgend aufgeführten Rechtsänderungsvorschläge sind für die Erhöhung der Cybersicherheit in Deutschland von elementarer Bedeutung.

Im Einzelnen:

1. Sensorik auch außerhalb des Regierungsnetzwerkes ermöglichen – Detektion stärken

Bislang beziehen sich die Detektionsmöglichkeiten des BSI ausschließlich auf die eigene Sensorik im Regierungsnetz. Da keine Sensorik außerhalb der Regierungsnetze existiert und Meldungen der Unternehmen an das BSI prozessbedingt erst verspätet (nach Entdecken und Bewerten des Vorfalls) und nicht flächendeckend erfolgen, gehen viele wichtige Informationen aus unternehmensbezogenen Angriffserkennungssystemen verloren. Manuelle Meldungen von Unternehmen müssen perspektivisch und zunehmend um automatisierte Datenströme ergänzt werden, um Lagebilder, Bewertungen und Maßnahmen in Echtzeit zu ermöglichen.

Es sollten daher die erforderlichen gesetzlichen Voraussetzungen geschaffen werden, dem BSI die automatisierte Entgegenahme und Verarbeitung von Informationen aus Angriffserkennungssystemen bei Unternehmen (z.B. KRITIS-Betreibern, besonders wichtigen und wichtigen Unternehmen) zu ermöglichen. Dies sollte durch BSI-eigene Sensorik bei ausgewählten Unternehmen ergänzt werden.

2. Registrierungsinformationen für Domänen und Betroffene kompromittierter Websites oder E-Mail-Konten

Das BSI benötigt einen schnellen Zugriff auf Domänennamen-Registrierungsdaten. Diese enthalten Informationen zum Inhaber einer Domain. Für das BSI sind diese Informationen von großer Bedeutung, insbesondere im Rahmen der Bewertung von Gefährdungspotentialen und zum Auffinden von Webseiten der Bundesverwaltung. Rund 50 Prozent der Webseiten des Bundes werden bei externen

Dienstleistern betrieben und sind deshalb oft nicht zentral erfasst. Nur bekannte Webseiten der Bundesverwaltung können in Schutzmaßnahmen des BSI einbezogen werden.

Die Zugangsgewährung nach § 50 BSIG-E ist jedoch unnötig bürokratisch sowohl für das BSI als auch für die Diensteanbieter. Es sollte vor allem die Darlegung eines berechtigten Interesses entfallen. Der hier umgesetzte Artikel 28 der NIS-2-Richtlinie verlangt lediglich, dass die Zugangsanfrager berechtigt sein müssen; ein berechtigtes Interesse schreibt die Richtlinie dagegen nicht vor. Daher sollte eine sachliche Begründung eines Zugriffsantrags ausreichend sein. Ferner sollte auch die Einschränkung „soweit dies für die Erfüllung von deren Aufgaben erforderlich ist“ entfallen. Private Diensteanbieter können und sollten nicht die Aufgabe übernehmen, die Erforderlichkeit einer Maßnahme für die Erfüllung öffentlicher Aufgaben einzuschätzen.

Darüber hinaus ist es für das BSI wichtig, Betroffene von kompromittierten Websites oder E-Mail-Konten informieren zu können. Das BSI erhält regelmäßig Daten zu kompromittierten Websites oder E-Mail-Konten. Es hat aber in diesen Fällen oft nicht die Möglichkeit, zu einem Domainnamen automatisiert einen Mailkontakt (Abuse-Kontakt) zu ermitteln, den es informieren kann. Insbesondere bietet die DENIC keine entsprechende Schnittstelle an.

Top-Level-Domain-Registries sollten daher verpflichtet werden, dem BSI zu Domainnamen automatisiert einen Mailkontakt zur Verfügung zu stellen.

3. Gesetzliche Grundlage für gemeinsame Daten zur Cyberabwehr

Für ein gesamtstaatliches Lagebild und eine behördenübergreifend koordinierte nationale Cyber-Abwehr bedarf es einer gemeinsamen Datengrundlage. Diese sollte Erkenntnisse der Behörden mit Cybersicherheitsaufgaben enthalten. Erst dann kann sie Ausgangspunkt für Lageeinschätzungen, Bedrohungsanalysen und schnelle Reaktionen auf Cyberangriffe sein. Für die Schaffung dieser Datengrundlage fehlen aktuell die entsprechenden rechtlichen Voraussetzungen.

4. Das BSI führt Schwachstellen immer der Schließung zu

Für das BSI sind Schwachstellenmeldungen von Sicherheitsforschenden und weiteren Privatpersonen von erheblicher Bedeutung. Meldungen setzen das Vertrauen in das BSI voraus. Derzeit haben Meldende oft Sorge, dass das BSI Schwachstellen zurückhalten könnte. Hinzu kommt die Angst vor einer möglichen Strafverfolgung. Aus fachlicher Sicht des BSI sollten Sicherheitslücken grundsätzlich an die betroffenen Hersteller gemeldet werden, damit diese möglichst schnell geschlossen werden.

Alle dem BSI gemeldeten Schwachstellen sollten in einen gesetzliche verankerten, transparenten Coordinated Vulnerability Disclosure-Prozess (CVD-Prozess) gehen. Um die Unabhängigkeit des BSI bei dieser Aufgabe sicherzustellen und den Anreiz zur Meldung von Schwachstellen an das BSI damit zu erhöhen, sollte gesetzlich konkretisiert werden, dass das BSI bei der Meldung von Sicherheitslücken an Hersteller keinen Weisungen durch die Fachaufsicht unterliegt.

Meldende sollten durch gesetzliche Klarstellungen im Computerstrafrecht von einer Sorge vor Strafverfolgung befreit werden („Hackerparagraph“). Ein transparentes, rechtssicheres Verfahren führt zu mehr Meldungen und damit zu mehr Cybersicherheit in Deutschland.

5. Verbesserung der Datenlage des BSI

Sogenannte Passive-DNS-Daten resultieren aus der Auflistung des angefragten DNS-Verkehrs. Sie helfen bei der Erkennung von Angriffen. Das BSI nutzt Passive-DNS-Daten bereits, bspw. für die Erstellung von zu scannenden Website-Listen. Sie sind außerdem unerlässlich bei der Bewertung von Domains und IP-Adressen (Ausschluss von Kollateralschäden) und bei BSI-Anordnungen gegenüber Diensteanbietern, bspw. zur Datenverkehrsumleitung von Schadsoftwareverbindungen. Das BSI muss diese Daten aktuell einkaufen. Dies ist teuer und ergibt ein lückenhaftes Bild.

In Frankreich wurden Telekommunikations-Anbieter gesetzlich verpflichtet, der französischen Partnerbehörde Passive-DNS-Daten zur Verfügung zu stellen. Eine gesetzliche Verpflichtung der Anbieter nach französischem Vorbild würde die Datenlage erheblich verbessern.

(Anlage 2)

Kurzbeschreibung zum Resilienz-Programm: Cybersicherheit in der Bundesverwaltung

Die Cybersicherheit in der Bundesverwaltung weist erhebliche Defizite auf, die eine umgehende und effektive Antwort erfordern. Die zunehmende Digitalisierung mit nicht hinreichend geschützten Angriffsflächen und die steigende Komplexität der Bedrohungslage machen deutlich, dass Sicherheit und Resilienz der informationstechnischen Systeme nachhaltig gesteigert werden müssen. Um diesen Herausforderungen zu begegnen, wird ein sofortiges Resilienz-Programm „CyberGovSecure“ vorgeschlagen, das durch einen Kabinettsbeschluss mandatiert werden soll. Es umfasst die Beseitigung akuter Sicherheitsmängel sowie den systematischen Aufbau von Cybersicherheitsfähigkeiten in der Bundesverwaltung. Die strategische Ausrichtung wird durch einen Lenkungskreis unter dem Vorsitz des zuständigen Bundesministers festgelegt, während die operative Umsetzung durch das Programmteam „Cyber Bund“ koordiniert wird, in dem alle Chief Information Security Officers (CISOs) der Ressorts mit dem Vorsitz des Bundes-CISOs vereint werden.

Chief Information Security Officers steuern und überwachen Cybersicherheitsmaßnahmen innerhalb ihrer jeweiligen Organisation. Der Bundes-CISO fungiert als Vorsitzender des Programmteams „Cyber Bund“. Diese Rolle ist essenziell für das Programm „CyberGovSecure“, da der Bundes-CISO die Umsetzung und das Fortkommen der Maßnahmen überwacht, Risiken bewertet und sicherstellt, dass die Cybersicherheitsstandards eingehalten werden. Durch die zentrale Position des Bundes-CISOs wird eine ressortübergreifende Zusammenarbeit ermöglicht, die die Effizienz und Wirksamkeit der Maßnahmen steigert. Trotz der gemeinsamen Koordination von Planungen und Maßnahmen bleiben die Ressorts jedoch weiterhin eigenverantwortlich für die individuelle Cybersicherheit ihrer Häuser.

Das Programm zielt darauf ab, die Cyber-Resilienz der Bundesverwaltung nachhaltig zu steigern, beispielsweise durch die Sicherstellung von geschützten mobilen Arbeitsumgebungen (Arbeitsplätze und VPN-Verbindungen), Multi-Faktor-Authentifizierung (MFA) und Mobile Device Management (MDM) die die Sicherheit durch zusätzliche Schutzebenen erhöhen und unbefugten Zugriff erschweren. Regelmäßige Sicherheitsübungen sowie Backup- und Recovery-Systeme sichern die Handlungsfähigkeit der Verwaltung auch im Falle eines Angriffs und minimieren Datenverluste. Ergänzend tragen Firewalls und die Verschlüsselung von Daten dazu bei, sensible Informationen vor unbefugtem Zugriff zu schützen. Die Anzahl der Arbeitsfelder ist groß und es gilt, sie gemeinsam in die richtige Reihenfolge zu bringen und gezielt abzuarbeiten.

Die nächsten Schritte umfassen die Einrichtung der Programmorganisation, die Priorisierung erster Projekte und die Durchführung von Sensibilisierungsmaßnahmen. Dieses Programm ist ein dringend notwendiger Beitrag zur digitalen Wehrhaftigkeit Deutschlands und soll durch zusätzliche Haushaltsmittel aus dem Sondervermögen Infrastruktur unterstützt werden.