Deutscher Bundestag **Drucksache 18/4096**
18. Wahlperiode 25.02.2015

Gesetzentwurf
der Bundesregierung

Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

A. Problem und Ziel

Die Nutzung informationstechnischer Systeme (IT-Systeme) und des Internets mit seinen vielfältigen Angeboten durchdringen Staat, Wirtschaft und Gesellschaft in immer größerem Maße. Bedeutende Teilbereiche des privaten und öffentlichen Lebens werden zunehmend ins Netz verlagert oder von diesem beeinflusst. Quer durch alle Branchen ist schon heute mehr als die Hälfte aller Unternehmen in Deutschland vom Internet abhängig. Mit der digitalen Durchdringung der Gesellschaft entstehen in nahezu allen Lebensbereichen neue Potentiale, Freiräume und Synergien. Gleichzeitig wächst die Abhängigkeit von IT-Systemen im wirtschaftlichen, gesellschaftlichen und individuellen Bereich und damit die Bedeutung der Verfügbarkeit und Sicherheit der IT-Systeme sowie des Cyberraums insgesamt.

Die IT-Sicherheitslage in Deutschland ist weiterhin angespannt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erhält und analysiert − u.a. im CERT-Bund, dem IT-Lagezentrum sowie in besonderen Einzelfällen auch in dem 2011 gegründeten Cyberabwehrzentrum − kontinuierlich eine Vielzahl von Informationen zur aktuellen Bedrohungssituation im Cyberraum. Die Angriffe erfolgen zunehmend zielgerichtet und sind technologisch immer ausgereifter und komplexer.

Mit dem Gesetz soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland erreicht werden. Die vorgesehenen Neuregelungen dienen dazu, den Schutz der Systeme im Hinblick auf die Schutzgüter der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität) zu verbessern, um den aktuellen und zukünftigen Gefährdungen der IT-Sicherheit wirksam begegnen zu können. Ziel des Gesetzes ist die Verbesserung der IT-Sicherheit von Unternehmen, der verstärkte Schutz der Bürgerinnen und Bürger im Internet und in diesem Zusammenhang auch die Stärkung von BSI und Bundeskriminalamt (BKA).

Besondere Bedeutung kommt im Bereich der IT-Sicherheit denjenigen Infrastrukturen zu, die für das Funktionieren unseres Gemeinwesens zentral sind. Der Schutz der IT-Systeme von solchen Kritischen Infrastrukturen und der für den Infrastrukturbetrieb nötigen Netze ist daher von größter Wichtigkeit. Das IT-Sicherheitsniveau bei Kritischen Infrastrukturen ist derzeit sehr unterschiedlich: In manchen Infrastrukturbereichen existieren detaillierte gesetzliche Vorgaben auch zur IT-Sicherheit, in anderen Bereichen fehlen solche vollständig. Manche Bereiche verfügen über ein ausgeprägtes Risikomanagement und übergreifende Sicherheitskonzepte, führen Audits durch, beteiligen sich am Informationsaustausch und an Übungen. In anderen Bereichen sind diese Maßnahmen noch nicht oder nur rudimentär entwickelt. Auf Grund des hohen Grades der Vernetzung und der daraus resultierenden Interdependenzen zwischen den unterschiedlichen Bereichen Kritischer Infrastrukturen ist dieser Zustand nicht hinnehmbar.

B. Lösung

Defizite im Bereich der IT-Sicherheit sind abzubauen. Insbesondere Betreiber Kritischer Infrastrukturen sind wegen der weitreichenden gesellschaftlichen Folgen, die ein Ausfall oder eine Beeinträchtigung ihrer Infrastrukturen nach sich ziehen kann, und ihrer insoweit besonderen Verantwortung für das Gemeinwohl zu verpflichten, ein Mindestniveau an IT-Sicherheit einzuhalten und dem BSI IT-Sicherheitsvorfälle zu melden. Die beim BSI zusammenlaufenden Informationen werden ausgewertet und den Betreibern Kritischer Infrastrukturen zur Verbesserung des Schutzes ihrer Infrastrukturen schnellstmöglich zur Verfügung gestellt. Die Betreiber leisten insoweit durch die Meldepflicht einen eigenen Beitrag zur IT-Sicherheit und bekommen dafür, da sie auch von den Meldungen der anderen Betreiber und der Auswertung dieser Meldungen durch das BSI profitieren, im Gegenzug ein Mehrfaches an Informationen und Know-how zurück. Gleichzeitig wird die Beratungsfunktion des BSI in diesem Bereich gestärkt.

Um den Schutz der Bürgerinnen und Bürger zu verbessern, werden die Telekommunikationsanbieter, die eine Schlüsselrolle für die Sicherheit des Cyberraums haben, verpflichtet, IT-Sicherheit nach dem Stand der Technik nicht nur zum Schutz des Fernmeldegeheimnisses und zum Schutz personenbezogener Daten, sondern auch im Hinblick auf die Verfügbarkeit ihrer Telekommunikations- und Datenverarbeitungssysteme zu gewährleisten. Die Umsetzung der zugrunde liegenden IT-Sicherheitskonzepte in den Unternehmen wird von der Bundesnetzagentur regelmäßig überprüft. Damit wird die Widerstandsfähigkeit der Kommunikationsinfrastruktur insgesamt verbessert und die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit datenverarbeitender Systeme

sowie der dort vorgehaltenen Daten gesichert. Mittelbar steigt so auch die Verantwortung der Hersteller zum Angebot entsprechender Produkte.

Telekommunikationsanbieter sollen zudem IT-Sicherheitsvorfälle, die zu einem unerlaubten Zugriff auf die Systeme der Nutzerinnen und Nutzer oder einer Beeinträchtigung der Verfügbarkeit führen können, unverzüglich über die Bundesnetzagentur an das BSI melden und betroffene Nutzerinnen und Nutzer über bekannte Störungen informieren, die durch Schadprogramme auf den datenverarbeitenden Systemen der Nutzerinnen und Nutzer hervorgerufen werden.

Da eine Vielzahl von IT-Angriffen bereits durch die Umsetzung von Standardsicherheitsmaßnahmen abgewehrt werden könnte, leistet eine verstärkte Sensibilisierung der Nutzerinnen und Nutzer durch die im Gesetz vorgesehene Aufklärung der Öffentlichkeit durch einen jährlichen Bericht einen wichtigen Beitrag zur Verbesserung der IT-Sicherheit. Die gewachsene Rolle des BSI als nationale zentrale Stelle für IT-Sicherheit gegenüber ausländischen Staaten wird festgeschrieben, der Anteil des BSI an der Erstellung des Sicherheitskatalogs für Telekommunikationsnetzbetreiber ausgebaut. Begleitend dazu wird das BKA im Bereich Cyberkriminalität angesichts der zunehmenden Zahl von IT-Angriffen gegen Bundeseinrichtungen und gegen bundesweite Kritische Infrastrukturen in seinen Rechten gestärkt.

Die Regelungen für Betreiber Kritischer Infrastrukturen, die branchenspezifische Sicherheitsanforderungen sowie die Meldepflicht erheblicher IT-Sicherheitsvorfälle betreffen, entsprechen im Grundsatz dem Vorschlag der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union.

C. Alternativen

Beibehalten des bisherigen Rechtszustandes.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Hinsichtlich des Erfüllungsaufwands für die Wirtschaft ist zu unterscheiden zwischen Genehmigungsinhabern nach dem Atomgesetz, Betreibern von Energieversorgungsnetzen und Energieanlagen, bestimmten Telekommunikationsanbietern, sonstigen Betreibern Kritischer Infrastrukturen sowie bestimmten Telemediendiensteanbietern:
Betreibern Kritischer Infrastrukturen entsteht Erfüllungsaufwand für

- die Einhaltung eines Mindestniveaus an IT-Sicherheit,
- den Nachweis der Erfüllung durch Sicherheitsaudits,
- die Einrichtung und Aufrechterhaltung von Verfahren für die Meldung erheblicher IT-Sicherheitsvorfälle an das BSI sowie
- das Betreiben einer Kontaktstelle.

Genehmigungsinhabern nach dem Atomgesetz entsteht Erfüllungsaufwand für

- die Einrichtung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an das BSI.

Betreibern von Energieversorgungsnetzen und Energieanlagen, die als Kritische Infrastruktur im Sinne des BSI-Gesetzes eingestuft wurden, entsteht Erfüllungsaufwand für

- die Einrichtung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an das BSI .

Betreibern von Energieanlagen (einschließlich der Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes), die als Kritische Infrastruktur im Sinne des BSI-Gesetzes eingestuft wurden, entsteht darüber hinaus Erfüllungsaufwand

- für die Einhaltung zusätzlicher IT-Sicherheitsanforderungen sowie
- die Überprüfung der Einhaltung dieser Sicherheitsanforderungen.

Telemediendiensteanbietern entsteht Erfüllungsaufwand für

- die Sicherung ihrer technischen Einrichtungen durch Maßnahmen nach dem Stand der Technik.

Betreibern öffentlicher Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste entsteht Erfüllungsaufwand für

- die Sicherung ihrer technischen Einrichtungen durch Maßnahmen nach dem Stand der Technik,
- die Aufrechterhaltung und Erweiterung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an die Bundesnetzagentur sowie
- die Benachrichtigung der Nutzerinnen und Nutzer, wenn erkannt wird, dass von deren Datenverarbeitungssystemen Störungen ausgehen.

Die Verpflichtung zur Einhaltung eines Mindestniveaus an IT-Sicherheit wird dort zu Mehrkosten führen, wo kein hinreichendes IT-Sicherheitsniveau vorhanden ist. Der entstehende Aufwand hängt einerseits vom erforderlichen Sicherheitsniveau und andererseits vom jeweiligen Status quo des Normadressaten ab. Der hierfür anfallende Aufwand kann im Voraus nicht quantifiziert werden. Entsprechendes gilt für den durch die Überprüfung der Einhaltung dieses Sicherheitsniveaus entstehenden Aufwand für Sicherheitsaudits. Der Aufwand und damit die Kosten für eine Zertifizierung oder für ein Audit hängen stark von dem gewählten Zertifizierungsverfahren sowie von den jeweiligen Gegebenheiten im Unternehmen ab. Auch dieser Aufwand kann daher im Voraus nicht quantifiziert werden. Auch die Verpflichtung zum Betreiben einer Kontaktstelle wird dort zu einem Mehraufwand führen, wo noch keine entsprechende Kontaktstelle vorhanden ist. Die Kosten hierfür hängen von der konkreten Ausgestaltung der Erreichbarkeit durch den Betreiber der Kritischen Infrastruktur ab. Kostensenkend kann sich insoweit die Einrichtung einer gemeinsamen übergeordneten Ansprechstelle auswirken.

Der jährliche Erfüllungsaufwand der Wirtschaft für das Meldeverfahren ergibt sich aus

- der Anzahl der meldepflichtigen Unternehmen,
- der Anzahl der meldepflichtigen Vorfälle pro Jahr und pro Unternehmen sowie
- dem Aufwand pro Meldung.

Die konkrete Berechnung der Gesamtkosten kann erst mit Erlass der Rechtsverordnung nach § 10 des BSI-Gesetzes auf der Grundlage des im Zweiten Teils der Begründung dargestellten Verfahrens erfolgen, da erst durch die Rechtsverordnung der Adressatenkreis der entsprechenden Verpflichtungen hinreichend konkret eingegrenzt und eine entsprechende Zahl meldepflichtiger Betreiber Kritischer Infrastrukturen benannt werden kann.

Nach aktuellen Schätzungen wird die Zahl der meldepflichtigen Betreiber Kritischer Infrastrukturen bei maximal 2.000 Betreibern liegen. Weiterhin wird geschätzt, dass pro Betreiber maximal sieben Meldungen von IT-Sicherheitsvorfällen pro Jahr erfolgen. Da relevante IT-Sicherheitsvorfälle von den Betreibern auch ohne die im Gesetz vorgesehene Meldepflicht untersucht, bewältigt und dokumentiert werden müssen, fällt bei den Bürokratiekosten nur insoweit ein Mehraufwand an, als die Bearbeitung über die ohnehin im Rahmen einer systematischen Bearbeitung relevanten Vorfälle hinausgeht. Auf Grund von Angaben aus der Wirtschaft auf der Grundlage von Berechnungen nach dem Standardkostenmodell werden die Kosten für die Bearbeitung einer Meldung derzeit mit 660 Euro pro Meldung (11 Stunden Zeitaufwand bei einem Stundensatz von 60 Euro) beziffert. Zum Teil werden solche Vorfälle schon heute dem BSI gemeldet.

Legt man den Berechnungen eine Anzahl von 2.000 Betreibern Kritischer Infrastrukturen zugrunde, die jeweils sieben IT-Sicherheitsvorfälle pro Jahr melden, für deren Bearbeitung jeweils ein zusätzlicher Aufwand von 660 Euro pro Meldung entsteht, so entsteht den Betreibern Kritischer Infrastrukturen für die Erfüllung der Meldepflicht ein jährlicher Erfüllungsaufwand von insgesamt 9,24 Millionen Euro.

Hinzu kommt der Erfüllungsaufwand für die Betreiber öffentlicher Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste für die Aufrechterhaltung und Erweiterung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an die Bundesnetzagentur. Da es in diesem Bereich bereits ein etabliertes Verfahren zur Meldung von IT-Sicherheitsvorfällen an die Bundesnetzagentur gibt, das durch das Gesetz lediglich erweitert wird, lässt sich der hierdurch entstehende Mehraufwand nicht quantifizieren. Auf Grund von Angaben aus der Wirtschaft werden die Kosten für die Bearbeitung einer Meldung derzeit auch für diesen Bereich mit 660 Euro pro Meldung (11 Stunden Zeitaufwand bei einem Stundensatz von 60 Euro) beziffert. Von entsprechenden Kosten je Meldung wird auch für die Genehmigungsinhaber nach dem Atomgesetz ausgegangen.

E.3 Erfüllungsaufwand für die Verwaltung

Schon heute werden den zuständigen Behörden IT-Sicherheitsvorfälle gemeldet.

Beim BSI entsteht für die Erfüllung der im Gesetz vorgesehenen Aufgabe − in Abhängigkeit von der Zahl der Betreiber Kritischer Infrastrukturen und der Anzahl der eingehenden Meldungen − ein Aufwand von insgesamt zwischen 115 bis zu maximal 216,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich zwischen rund 8,95 und bis zu maximal 15,867 Millionen Euro sowie Sachkosten in Höhe von einmalig rund 5 bis 7 Millionen Euro.

Beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) führen die neuen Mitwirkungsaufgaben zu einem Bedarf von zwischen 9 und bis zu maximal 13 Planstellen/Stellen mit jährlichen Personalkosten zwischen 711 000 und bis zu maximal 1,011 Millionen Euro.

Bei der Bundesnetzagentur (BNetzA) führen die neuen Aufgaben zu einem Bedarf von bis zu maximal 28 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von rund bis zu maximal 3,202 Millionen Euro. Des Weiteren entstehen Kosten für Sachmittel in Höhe von einmalig 150 000 Euro im ersten Jahr für die Aufgaben nach § 109 Absatz 4 Satz 7 und 8 sowie Absatz 5 des Telekommunikationsgesetzes.

In den Fachabteilungen des BKA entsteht ein Ressourcenaufwand von zwischen 48 und bis zu maximal 78 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von jährlich zwischen rund 3,226 und bis zu maximal 5,310 Millionen Euro. Des Weiteren entstehen Kosten für Sachmittel in Höhe von jährlich bis zu maximal 630 000 Euro.
In den Fachabteilungen des Bundesamtes für Verfassungsschutz (BfV) entsteht durch die Zuständigkeit gemäß § 8b Absatz 2 Nummer 4 des BSI-Gesetzes ein Bedarf von zwischen 26,5 und maximal 48,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich zwischen 1,836 und maximal 3,253 Millionen Euro. Des Weiteren entstehen Kosten für Sachmittel in Höhe von maximal 610 000 Euro jährlich.

In den Fachabteilungen des Bundesnachrichtendienstes (BND) entsteht durch die Zuständigkeit gemäß § 8b Absatz 2 Nummer 4 des BSI-Gesetzes im Zusammenhang mit der Prüfung ausländischer Datenstrecken auf Schadsoftware-Signaturen und Rückverfolgung von Schadsoftware im Ausland ein Bedarf von maximal 30 Planstellen/Stellen mit Personalkosten in Höhe von jährlich maximal 2,153 Millionen Euro. Des Weiteren ein jährlicher Bedarf an Sachkosten in Höhe von maximal 688 000 Euro.

In der Fachabteilung des für die nukleare Sicherheit und die Sicherung zuständigen Bundesministeriums für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB) führen die neuen Mitwirkungspflichten für das zentrale IT-Meldesystem an das BSI nach § 44b des Atomgesetzes (neu) und bei der Erarbeitung der Sicherheitsanforderungen für Energieanlagen nach § 11 Absatz 1b des Energiewirtschaftsgesetzes zu einem Bedarf von bis zu maximal 4 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von maximal rund 240 000 Euro.

Bei der Bundesbeauftragten für Datenschutz und Informationsfreiheit entsteht ein Bedarf von zwischen 2,4 und bis zu maximal 7 Planstellen/Stellen.

Im Ressort des Bundesministeriums für Arbeit und Soziales wird für das Bundesversicherungsamt vor Erlass der Rechtsverordnung nach § 10 Absatz 1 des BSI-Gesetzes noch nicht quantifizierbarer Aufwand im Hinblick auf die Rechtsaufsicht als zuständige Aufsichtsbehörde über die bundesunmittelbaren Träger der Sozialversicherung erwartet. Das Gleiche gilt für die fachlichen Aufsichtsbehörden (Bundesamt für Güterverkehr, Eisenbahn-Bundesamt, Luftfahrt-Bundesamt, Bundesaufsichtsamt für Flugsicherung, Generaldirektion Wasserstraßen und Schifffahrt, Bundesamt für Seeschifffahrt und Hydrografie) im Ressort des Bundesministeriums für Verkehr und Digitale Infrastruktur im Hinblick auf den Sektor Transport und Verkehr.

Darüber hinaus können Verträge des Bundes mit Dritten, die Kommunikationstechnik im Auftrag des Bundes betreiben sollen und hierzu Leistungen von Unternehmen in An-

spruch nehmen, die dem Gesetz unterliegen, zu Ausgaben führen, die aus heutiger Sicht noch nicht bezifferbar sind.

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

Der Erfüllungsaufwand für die Länder und Kommunen ist derzeit noch nicht bezifferbar.

F. Weitere Kosten

Infolge der von den Betreibern Kritischer Infrastrukturen umzusetzenden Maßnahmen entstehen geringe, aber noch nicht quantifizierbare Kosten für die fallweise Anpassung der IT-Verfahren, die von den Bundesbehörden bereitgestellt werden.

BUNDESREPUBLIK DEUTSCHLAND Berlin, 25. Februar 2015

DIE BUNDESKANZLERIN

An den
Präsidenten des
Deutschen Bundestages
Herrn Prof. Dr. Norbert Lammert
Platz der Republik 1
11011 Berlin

Sehr geehrter Herr Präsident,

hiermit übersende ich den von der Bundesregierung beschlossenen

> Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

mit Begründung und Vorblatt (Anlage 1).

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium des Innern.

Die Stellungnahme des Nationalen Normenkontrollrates gemäß § 6 Absatz 1 NKRG ist als Anlage 2 beigefügt.

Der Bundesrat hat in seiner 930. Sitzung am 6. Februar 2015 gemäß Artikel 76 Absatz 2 des Grundgesetzes beschlossen, zu dem Gesetzentwurf wie aus Anlage 3 ersichtlich Stellung zu nehmen.

Die Auffassung der Bundesregierung zu der Stellungnahme des Bundesrates ist in der als Anlage 4 beigefügten Gegenäußerung dargelegt.

Mit freundlichen Grüßen
Dr. Angela Merkel

Anlage 1

Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Vom …

Notifiziert gemäß der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 204 vom 21.07.1998, S. 37), zuletzt geändert durch Artikel 26 Absatz 2 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 (ABl. L 316 vom 14.11.2012, S. 12).

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1
Änderung des BSI-Gesetzes

Das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 3 Absatz 7 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist, wird wie folgt geändert:

1. § 1 wird wie folgt gefasst:

   „§ 1 Bundesamt für Sicherheit in der Informationstechnik

   Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) als Bundesoberbehörde. Das Bundesamt ist zuständig für die Informationssicherheit auf nationaler Ebene. Es untersteht dem Bundesministerium des Innern.“

2. Dem § 2 wird folgender Absatz 10 angefügt:

   „(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und

2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.

3. § 3 wird wie folgt geändert:

a) Absatz 1 Satz 2 wird wie folgt geändert:

aa) In Nummer 2 werden die Wörter „zur Wahrung ihrer Sicherheitsinteressen erforderlich ist“ durch die Wörter „erforderlich ist, sowie für Dritte, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist;“ ersetzt.

bb) In Nummer 15 werden die Wörter „kritischen Informationsinfrastrukturen“ durch die Wörter „Sicherheit in der Informationstechnik Kritischer Infrastrukturen“ und der Punkt am Ende durch ein Semikolon ersetzt.

cc) Die folgenden Nummern 16 und 17 werden angefügt:

„16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland, unbeschadet besonderer Zuständigkeiten anderer Stellen;

17. Aufgaben nach den §§ 8a und 8b als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen.“

b) Folgender Absatz 3 wird angefügt:

„(3) Das Bundesamt kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen.“

4. Die Überschrift von § 4 wird wie folgt gefasst:

„§ 4

Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes“.

5. § 7 Absatz 1 Satz 1 wird durch die folgenden Sätze ersetzt:

„Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 kann das Bundesamt

1. die folgenden Warnungen an die Öffentlichkeit oder an die betroffenen Kreise richten:

a) Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten,

b) Warnungen vor Schadprogrammen und

c) Warnungen im Falle eines Verlustes von oder eines unerlaubten Zugriffs auf Daten;

2. Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen.

Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist.“

6. Nach § 7 wird folgender § 7a eingefügt:

„§ 7a

Untersuchung der Sicherheit in der Informationstechnik

„(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14 und 17 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Es kann sich hierbei der Unterstützung Dritter bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen.

(2) Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zu den in Absatz 1 Satz 1 genannten Zwecken genutzt werden. Soweit erforderlich darf das Bundesamt seine Erkenntnisse weitergeben und veröffentlichen. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben.“

7. Nach § 8 werden die folgenden §§ 8a bis 8d eingefügt:

„§ 8a

Sicherheit in der Informationstechnik
Kritischer Infrastrukturen

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei ist der Stand der Technik zu berücksichtigen. 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.

(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt

1. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,

2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde.

(3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.

§ 8b

Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Das Bundesamt ist die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.

(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe

1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen zu sammeln und auszuwerten, insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise,

2. deren potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungs- und Katastrophenschutz zu analysieren,

3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen kontinuierlich zu aktualisieren und

4. unverzüglich

   a) die Betreiber Kritischer Infrastrukturen über sie betreffende Informationen nach den Nummern 1 bis 3,

   b) die zuständigen Aufsichtsbehörden und die sonst zuständigen Behörden des Bundes über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen nach den Nummern 1 bis 3 sowie

   c) die zuständigen Aufsichtsbehörden der Länder oder die zu diesem Zweck dem Bundesamt von den Ländern als zentrale Kontaktstellen benannten Behörden über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen nach den Nummern 1 bis 3

zu unterrichten.

(3) Die Betreiber Kritischer Infrastrukturen haben dem Bundesamt binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 eine Kontaktstelle für die Kommunikationsstrukturen nach § 3 Absatz 1 Satz 2 Nummer 15 zu benennen. Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit er-

reichbar sind. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.

(4) Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder bereits geführt haben, über die Kontaktstelle unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und zur Branche des Betreibers enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

(5) Zusätzlich zu ihrer Kontaktstelle nach Absatz 3 können Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, eine gemeinsame übergeordnete Ansprechstelle benennen. Wurde eine solche benannt, erfolgt der Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt in der Regel über die gemeinsame Ansprechstelle.

(6) Soweit im Rahmen dieser Vorschrift personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ist eine über die vorstehenden Absätze hinausgehende Verarbeitung und Nutzung zu anderen Zwecken unzulässig. § 5 Absatz 7 Satz 3 bis 8 ist entsprechend anzuwenden. Im Übrigen sind die Regelungen des Bundesdatenschutzgesetzes anzuwenden.

§ 8c

Anwendungsbereich

(1) Die §§ 8a und 8b sind nicht anzuwenden auf Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36). Artikel 3 Absatz 4 der Empfehlung ist nicht anzuwenden.

(2) § 8a ist nicht anzuwenden auf

1. Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,

2. Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 3 des Gesetzes vom … [einsetzen: Ausfertigungsdatum dieses Gesetzes und Fundstelle] geändert worden ist, in der jeweils geltenden Fassung,

3. Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 2 des Gesetzes vom … [einsetzen: Ausfertigungsdatum dieses Gesetzes und Fundstelle] geändert worden ist, in der jeweils geltenden Fassung für den Geltungsbereich der Genehmigung sowie

4. sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8a vergleichbar oder weitergehend sind.

(3) § 8b Absatz 3 bis 5 ist nicht anzuwenden auf

1. Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,

2. Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes,

3. Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes für den Geltungsbereich der Genehmigung sowie

4. sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8b Absatz 3 bis 5 vergleichbar oder weitergehend sind.

§ 8d

Auskunftsverlangen

(1) Das Bundesamt kann Dritten auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3 erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4 nur erteilen, wenn schutzwürdigen Interessen des betroffenen Betreibers Kritischer Infrastrukturen dem nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen zu erwarten ist. Zugang zu personenbezogenen Daten wird nicht gewährt.

(2) Zugang zu den Akten des Bundesamtes in Angelegenheiten nach den §§ 8a und 8b wird nur Verfahrensbeteiligten gewährt und dies nach Maßgabe von § 29 des Verwaltungsverfahrensgesetzes.“

8. § 10 wird wie folgt geändert:

a) Dem Absatz 1 wird folgender Absatz 1 vorangestellt:

„(1) Das Bundesministerium des Innern bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit unter Festlegung der in den jeweiligen Sektoren im Hinblick auf § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.“

b) Der bisherige Absatz 1 wird Absatz 2 und die Wörter „Wirtschaft und Technologie durch Rechtsverordnung“ werden durch die Wörter „Wirtschaft und Energie durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf,“ ersetzt.

c) Der bisherige Absatz 2 wird Absatz 3 und in Satz 3 werden nach dem Wort „Rechtsverordnung“ ein Komma und die Wörter „die nicht der Zustimmung des Bundesrates bedarf,“ eingefügt.

9. Folgender § 13 wird angefügt:

„§ 13

Berichtspflichten

(1) Das Bundesamt unterrichtet das Bundesministerium des Innern über seine Tätigkeit.

(2) Die Unterrichtung nach Absatz 1 dient auch der Aufklärung der Öffentlichkeit durch das Bundesministerium des Innern über Gefahren für die Sicherheit in der Informationstechnik, die mindestens einmal jährlich in einem zusammenfassenden Bericht erfolgt. § 7 Absatz 1 Satz 3 und 4 ist entsprechend anzuwenden.“

Artikel 2
Änderung des Atomgesetzes

Nach § 40 des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 5 des Gesetzes vom 28. August 2013 (BGBl. I S. 3313) geändert worden ist, wird folgender § 44b eingefügt:

„§ 44b

Meldewesen für die Sicherheit in der Informationstechnik

Genehmigungsinhaber nach den §§ 6, 7 und 9 haben Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer Gefährdung oder Störung der nuklearen Sicherheit der betroffenen kerntechnischen Anlage oder Tätigkeit führen können oder bereits geführt haben, unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik als zentrale Meldestelle zu melden. § 8b Absatz 1, 2 und 6 des BSI-Gesetzes sind entsprechend anzuwenden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, und der betroffenen Informationstechnik enthalten. Das Bundesamt für Sicherheit in der Informationstechnik leitet diese Meldungen unverzüglich an die für die nukleare Sicherheit und Sicherung zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder weiter.“

Artikel 3
Änderung des Energiewirtschaftsgesetzes

Das Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 6 des Gesetzes vom 21. Juli 2014 (BGBl. I S. 1066) geändert worden ist, wird wie folgt geändert:

1. § 11 wird wie folgt geändert:

a) Absatz 1a wird wie folgt geändert:

aa) In Satz 1 werden nach dem Wort „Datenverarbeitungssysteme“ die Wörter „die der Netzsteuerung dienen“ durch die Wörter „die für einen sicheren Netzbetrieb notwendig sind“ ersetzt.

bb) Nach Satz 2 wird folgender Satz eingefügt:

„Der Katalog der Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen.“

cc) In dem neuen Satz 4 werden die Wörter „wird vermutet“ durch die Wörter „liegt vor“ ersetzt.

dd) Der neue Satz 6 wird wie folgt gefasst:

„Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 4 treffen.“

b) Nach Absatz 1a werden die folgenden Absätze 1b und 1c eingefügt:

„(1b) Betreiber von Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 8 des Gesetzes vom … [einsetzen: Ausfertigungsdatum dieses Gesetzes und Fundstelle] geändert worden ist, in der jeweils geltenden Fassung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, haben binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicher-

heitsanforderungen und veröffentlicht diesen. Für Telekommunikations- und elektronische Datenverarbeitungssysteme von Anlagen nach § 7 Absatz 1 des Atomgesetzes haben Vorgaben auf Grund des Atomgesetzes Vorrang. Die für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder sind bei der Erarbeitung des Katalogs von Sicherheitsanforderungen zu beteiligen. Der Katalog von Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen. Ein angemessener Schutz des Betriebs von Energieanlagen im Sinne von Satz 1 liegt vor, wenn dieser Katalog eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Bundesnetzagentur überprüft werden. Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 6 treffen.

(1c) Betreiber von Energieversorgungsnetzen und Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben dem Bundesamt für Sicherheit in der Informationstechnik unverzüglich erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu melden, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können oder bereits geführt haben. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und der betroffenen Informationstechnik enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Das Bundesamt für Sicherheit in der Informationstechnik hat die Meldungen unverzüglich an die Bundesnetzagentur weiterzuleiten. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung, der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird. Zugang zu den Akten des Bundesamtes für Sicherheit in der Informationstechnik sowie zu den Akten der Bundesnetzagentur in Angelegenheiten nach den §§ 11a bis 11c wird nicht gewährt. § 29 des Verwaltungsverfahrensgesetzes bleibt unberührt. § 8d Absatz 1 des BSI-Gesetzes ist entsprechend anzuwenden."

2. § 21e Absatz 5 wird wie folgt geändert:

a) In Satz 1 in dem Satzteil vor Nummer 1 werden nach den Wörtern „dürfen noch“ die Wörter „bis zum Zeitpunkt, den eine Rechtsverordnung nach § 21i Absatz 1 Nummer 11 bestimmt, mindestens jedoch“ eingefügt und wird die Angabe „2014“ durch die Angabe „2015“ ersetzt.

b) Satz 3 wird aufgehoben.

3. § 21f Absatz 2 wird wie folgt geändert:

a) In Satz 1 werden nach den Wörtern „können noch“ die Wörter „bis zum Zeitpunkt, den eine Rechtsverordnung nach § 21i Absatz 1 Nummer 11 bestimmt, mindestens jedoch“ eingefügt und wird die Angabe „2014“ durch die Angabe „2015“ ersetzt.

b) Satz 2 wird aufgehoben.

4. In § 21i Absatz 1 Nummer 11 werden die Wörter „und eine Verlängerung der genannten Frist“ gestrichen.

5. In § 59 Absatz 1 Satz 2 werden nach dem Wort „Erstellung“ die Wörter „und Überprüfung“ eingefügt und nach der Angabe „§ 11 Absatz 1a“ die Angabe „Satz 2“ durch die Angabe „und 1b“ ersetzt.

Artikel 4
Änderung des Telemediengesetzes

Das Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692) geändert worden ist, wird wie folgt geändert:

1. § 13 wird wie folgt geändert:

a) Nach Absatz 6 wird folgender Absatz 7 eingefügt:

„(7) Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und

2. diese

a) gegen Verletzungen des Schutzes personenbezogener Daten und

b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind,

gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.“

b) Der bisherige Absatz 7 wird Absatz 8.

2. In § 16 Absatz 2 Nummer 3 werden nach der Angabe „§ 13 Absatz 4 Satz 1 Nummer 1 bis 4 oder 5“ die Wörter „oder Absatz 7 Satz 1 Nummer 1 oder Nummer 2 Buchstabe a“ eingefügt.

Artikel 5
Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 22 des Gesetzes vom 25. Juli 2014 (BGBl. I S. 1266) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 109a wie folgt gefasst:

„§ 109a Daten- und Informationssicherheit“.

2. § 100 Absatz 1 wird wie folgt gefasst:

„(1) Soweit erforderlich, darf der Diensteanbieter die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können.“

3. § 109 wird wie folgt geändert:

a) Nach Absatz 2 Satz 2 wird folgender Satz eingefügt:

„Bei Maßnahmen nach Satz 2 ist der Stand der Technik zu berücksichtigen.“

b) Absatz 4 Satz 7 wird durch die folgenden Sätze ersetzt:

„Die Bundesnetzagentur überprüft regelmäßig die Umsetzung des Sicherheitskonzepts. Die Überprüfung soll mindestens alle zwei Jahre erfolgen.“

c) Absatz 5 wird wie folgt gefasst:

„(5) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat der Bundesnetzagentur unverzüglich Beeinträchtigungen von Telekommunikationsnetzen und -diensten mitzuteilen, die

1. zu beträchtlichen Sicherheitsverletzungen führen oder

2. zu beträchtlichen Sicherheitsverletzungen führen können.

Dies schließt Störungen ein, die zu einer Einschränkung der Verfügbarkeit der über diese Netze erbrachten Dienste oder einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und zu der betroffenen Informationstechnik enthalten. Kommt es zu einer beträchtlichen Sicherheitsverletzung, kann die Bundesnetzagentur einen detaillierten Bericht über die Sicherheitsverletzung und die ergriffenen Abhilfemaßnahmen verlangen. Soweit es sich um Sicherheitsverletzungen handelt, die die Informationstechnik betreffen, leitet die Bundesnetzagentur die eingegangenen Meldungen sowie die Informationen zu den ergriffenen Abhilfemaßnahmen unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik weiter. Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Europäische Agentur für Netz- und Informationssicherheit über die Sicherheitsverletzungen. Die Bundesnetzagentur kann die Öffentlichkeit unterrichten oder die nach Satz 1 Verpflichteten zu dieser Unterrichtung auffordern, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt. § 8d des BSI-Gesetzes gilt entsprechend. Die Bundesnetzagentur legt der Europäischen Kommission, der Europäischen Agentur für Netz- und Informationssicherheit und dem Bundesamt für Sicherheit in der Informationstechnik einmal pro Jahr einen zusammenfassenden Bericht über die eingegangenen Meldungen und die ergriffenen Abhilfemaßnahmen vor.“

d) In Absatz 6 Satz 1 wird das Wort „Benehmen“ durch das Wort „Einvernehmen“ ersetzt.

e) Folgender Absatz 8 wird eingefügt:

„Über aufgedeckte Mängel bei der Erfüllung der Sicherheitsanforderungen in der Informationstechnik sowie die in diesem Zusammenhang von der Bundesnetzagentur geforderten Abhilfemaßnahmen unterrichtet die Bundesnetzagentur unverzüglich das Bundesamt für Sicherheit in der Informationstechnik.“

4. § 109a wird wie folgt geändert:

a) Die Überschrift wird wie folgt gefasst:

„§109a
Daten- und Informationssicherheit“.

b) Nach Absatz 3 wird folgender Absatz 4 eingefügt:

„(4) Werden dem Diensteanbieter nach Absatz 1 Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, so hat er die Nutzer, soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können.“

c) Der bisherige Absatz 4 wird Absatz 5.

5. § 149 Nummer 21a wird wie folgt gefasst:

„entgegen § 109 Absatz 5 Satz 1 Nummer 1 eine Beeinträchtigung von Telekommunikationsnetzen oder -diensten, die zu einer beträchtlichen Sicherheitsverletzung führt, nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig mitteilt,“

Artikel 6
Änderung des Bundesbesoldungsgesetzes

Die Anlage I des Bundesbesoldungsgesetzes in der Fassung der Bekanntmachung vom 19. Juni 2009 (BGBl. I S. 1434), das zuletzt durch Artikel 2 des Gesetzes vom 25. November 2014 (BGBl. I S. 1772) geändert worden ist, wird wie folgt geändert:

1. In der Gliederungseinheit „Besoldungsgruppe B 6“ wird die Angabe „Präsident des Bundesamtes für Sicherheit in der Informationstechnik“ gestrichen.

2. In der Gliederungseinheit „Besoldungsgruppe B 7“ wird nach der Angabe „Präsident des Bildungszentrums der Bundeswehr“ folgende Angabe eingefügt: „Präsident des Bundesamtes für Sicherheit in der Informationstechnik“

Artikel 7
Änderung des Bundeskriminalamtgesetzes

§ 4 Absatz 1 Satz 1 Nummer 5 des Bundeskriminalamtgesetzes vom 7. Juli 1997 (BGBl. I S. 1650), das zuletzt durch Artikel 3 des Gesetzes vom 20. Juni 2013 (BGBl. I S. 1602) geändert worden ist, wird wie folgt geändert:

1. In dem Satzteil vor Buchstabe a wird die Angabe „§ 303b“ durch die Wörter „den §§ 202a, 202b, 202c, 263a, 303a und 303b“ ersetzt,
2. In Buchstabe b werden vor dem Wort „sicherheitsempfindliche“ die Wörter „Behörden oder Einrichtungen des Bundes oder“ eingefügt.

Artikel 8
Weitere Änderung des BSI-Gesetzes

§ 10 Absatz 3 des BSI-Gesetzes, das zuletzt durch Artikel 1 dieses Gesetzes geändert worden ist, wird aufgehoben.

Artikel 9
Änderung des Gesetzes zur Strukturreform des Gebührenrechts des Bundes

Artikel 3 Absatz 7 des Gesetzes zur Strukturreform des Gebührenrechts des Bundes vom 7. August 2013 (BGBl. I S. 3154) wird aufgehoben.

Artikel 10
Inkrafttreten

Dieses Gesetz tritt vorbehaltlich des Satzes 2 am Tag nach der Verkündung in Kraft. Artikel 8 tritt am 14. August 2016 in Kraft.

Begründung
A. Allgemeiner Teil

I. Zweck und Inhalt des Gesetzes

Mit dem Gesetz soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland erreicht werden. Die vorgesehenen Neuregelungen dienen dazu, den Schutz der Systeme im Hinblick auf die Schutzgüter der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität) zu verbessern und die Systeme der IT-Sicherheitslage anzupassen. Ziel des Gesetzes ist eine Verbesserung der IT-Sicherheit bei Unternehmen, ein verstärkter Schutz der Bürgerinnen und Bürger im Internet und in diesem Zusammenhang auch eine Stärkung des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Bundeskriminalamts (BKA).

Der Entwurf sieht für Betreiber Kritischer Infrastrukturen zum einen die Pflicht zur Einhaltung eines Mindestniveaus an IT-Sicherheit und zum anderen die Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle vor. Zum Schutz der Bürgerinnen und Bürger kommen weitere Pflichten für Telekommunikations- und Telemediendiensteanbieter bei ihren Angeboten und den damit einhergehenden Datenverarbeitungsprozessen hinzu.

II. Gesetzgebungskompetenz des Bundes

Für die Änderungen des BSI-Gesetzes (Artikel 1), die den Schutz der Informationstechnik Kritischer Infrastrukturen betreffen, folgt die Gesetzgebungskompetenz des Bundes teilweise aus speziellen Kompetenztiteln (Luftverkehr: Artikel 73 Absatz 1 Nummer 6 GG, Eisenbahnen: Artikel 73 Absatz 1 Nummer 6a, Artikel 74 Absatz 1 Nummer 23 GG, Schifffahrt: Artikel 74 Absatz 1 Nummer 21 GG, Gesundheit: Artikel 74 Absatz 1 Nummer 19 GG oder Telekommunikation: Artikel 73 Absatz 1 Nummer 7 GG) und im Übrigen aus der konkurrierenden Gesetzgebungskompetenz für das Recht der Wirtschaft (Artikel 74 Absatz 1 Nummer 11 GG). Für die Änderung des Atomgesetzes (Artikel 2) ergibt sich die Gesetzgebungskompetenz des Bundes aus Artikel 73 Absatz 1 Nummer 14 GG. Die Gesetzgebungskompetenz für die Änderung des Energiewirtschaftsgesetzes (Artikel 3) und des Telemediengesetzes (Artikel 4) ergibt sich aus der konkurrierenden Gesetzgebungskompetenz für das Recht der Wirtschaft (Artikel 74 Absatz 1 Nummer 11 GG). Die Berechtigung des Bundes zur Inanspruchnahme dieser Gesetzgebungskompetenz ergibt sich aus Artikel 72 Absatz 2 GG.

Eine bundesgesetzliche Regelung dieser Materie ist zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich. Eine Regelung durch den Landesgesetzgeber würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die sowohl im Interesse des Bundes als auch im Interesse der Länder nicht hingenommen werden können. Insbesondere wäre zu befürchten, dass unterschiedliche landesrechtliche Behandlungen gleicher Lebenssachverhalte (zum Beispiel unterschiedliche Anforderungen an die von den Betreibern Kritischer Infrastrukturen zu treffenden Sicherheitsvorkehrungen) erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten.

Die Änderungen im Telekommunikationsgesetz (Artikel 5) können auf die ausschließliche Gesetzgebungskompetenz des Bundes nach Artikel 73 Absatz 1 Nummer 7 GG gestützt werden. Der Bund hat darüber hinaus die ausschließliche Gesetzgebungskompetenz nach Artikel 73 Absatz 1 Nummer 8 GG für die Rechtsverhältnisse der im Dienst des Bundes und der bundesunmittelbaren Körperschaften des öffentlichen Rechts stehenden Personen (Artikel 6). Die Änderung des BKA-Gesetzes (Artikel 7) beruht auf der Gesetzgebungskompetenz nach Artikel 73 Absatz 1 Nummer 10 GG.

III. Erfüllungsaufwand

1. Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

2. Erfüllungsaufwand für die Wirtschaft

Hinsichtlich des Erfüllungsaufwands für die Wirtschaft ist zu unterscheiden zwischen Genehmigungsinhabern nach dem Atomgesetz, Betreibern von Energieversorgungsnetzen und Energieanlagen, bestimmten Telekommunikationsanbietern, sonstigen Betreibern Kritischer Infrastrukturen sowie bestimmten Telemediendiensteanbietern:

Betreibern Kritischer Infrastrukturen entsteht Erfüllungsaufwand für

- die Einhaltung eines Mindestniveaus an IT-Sicherheit,
- den Nachweis der Erfüllung durch Sicherheitsaudits,
- die Einrichtung und Aufrechterhaltung von Verfahren für die Meldung erheblicher IT-Sicherheitsvorfälle an das BSI sowie
- das Betreiben einer Kontaktstelle.

Genehmigungsinhabern nach dem Atomgesetz entsteht Erfüllungsaufwand für

- die Einrichtung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an das BSI.

Betreibern von Energieversorgungsnetzen und Energieanlagen, die als Kritische Infrastruktur im Sinne des BSI-Gesetzes eingestuft wurden, entsteht Erfüllungsaufwand für

- die Einrichtung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an das BSI.

Betreibern von Energieanlagen (einschließlich der Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes), die als Kritische Infrastruktur im Sinne des BSI-Gesetzes eingestuft wurden, entsteht darüber hinaus Erfüllungsaufwand

- für die Einhaltung zusätzlicher IT-Sicherheitsanforderungen sowie
- die Überprüfung der Einhaltung dieser Sicherheitsanforderungen.

Telemediendiensteanbietern entsteht Erfüllungsaufwand für

- die Sicherung ihrer technischen Einrichtungen durch Maßnahmen nach dem Stand der Technik.

Betreibern öffentlicher Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste entsteht Erfüllungsaufwand für

- die Sicherung ihrer technischen Einrichtungen durch Maßnahmen nach dem Stand der Technik,
- die Aufrechterhaltung und Erweiterung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an die Bundesnetzagentur sowie
- die Benachrichtigung der Nutzerinnen und Nutzer, wenn erkannt wird, dass von deren Datenverarbeitungssystemen Störungen ausgehen.

Die Verpflichtung zur Einhaltung eines Mindestniveaus an IT-Sicherheit wird dort zu Mehrkosten führen, wo kein hinreichendes IT-Sicherheitsniveau vorhanden ist. Der entstehende Aufwand hängt einerseits vom erforderlichen Sicherheitsniveau und andererseits vom jeweiligen Status quo des Normadressaten ab. Der hierfür anfallende Aufwand kann im Voraus nicht quantifiziert werden. Entsprechendes gilt für den durch die Überprüfung der Einhaltung dieses Sicherheitsniveaus entstehenden Aufwand für Sicherheitsaudits. Der Aufwand und damit die Kosten für eine Zertifizierung oder für ein Audit hängen stark von dem gewählten Zertifizierungsverfahren sowie von den jeweiligen Gegebenheiten im Unternehmen ab. Auch dieser Aufwand kann daher im Voraus

nicht quantifiziert werden. Auch die Verpflichtung zum Betreiben einer Kontaktstelle wird dort zu einem Mehraufwand führen, wo noch keine entsprechende Kontaktstelle vorhanden ist. Die Kosten hierfür hängen von der konkreten Ausgestaltung der Erreichbarkeit durch den Betreiber der Kritischen Infrastruktur ab. Kostensenkend kann sich insoweit die Einrichtung einer gemeinsamen übergeordneten Ansprechstelle auswirken.

Der jährliche Erfüllungsaufwand der Wirtschaft für das Meldeverfahren ergibt sich aus

- der Anzahl der meldepflichtigen Unternehmen,
- der Anzahl der meldepflichtigen Vorfälle pro Jahr und pro Unternehmen sowie
- dem Aufwand pro Meldung.

Die konkrete Berechnung der Gesamtkosten kann erst mit Erlass der Rechtsverordnung nach § 10 des BSI-Gesetzes auf der Grundlage des im Zweiten Teils der Begründung dargestellten Verfahrens erfolgen, da erst durch die Rechtsverordnung der Adressatenkreis der entsprechenden Verpflichtungen hinreichend konkret eingegrenzt und eine entsprechende Zahl meldepflichtiger Betreiber Kritischer Infrastrukturen benannt werden kann.

Nach aktuellen Schätzungen wird die Zahl der meldepflichtigen Betreiber Kritischer Infrastrukturen bei maximal 2.000 Betreibern liegen. Weiterhin wird geschätzt, dass pro Betreiber maximal sieben Meldungen von IT-Sicherheitsvorfällen pro Jahr erfolgen. Da relevante IT-Sicherheitsvorfälle von den Betreibern auch ohne die im Gesetz vorgesehene Meldepflicht untersucht, bewältigt und dokumentiert werden müssen, fällt bei den Bürokratiekosten nur insoweit ein Mehraufwand an, als die Bearbeitung über die ohnehin im Rahmen einer systematischen Bearbeitung relevanten Vorfälle hinausgeht. Auf Grund von Angaben aus der Wirtschaft auf der Grundlage von Berechnungen nach dem Standardkostenmodell werden die Kosten für die Bearbeitung einer Meldung derzeit mit 660 Euro pro Meldung (11 Stunden Zeitaufwand bei einem Stundensatz von 60 Euro) beziffert. Zum Teil werden solche Vorfälle schon heute dem BSI gemeldet.

Legt man den Berechnungen eine Anzahl von 2.000 Betreibern Kritischer Infrastrukturen zugrunde, die jeweils sieben IT-Sicherheitsvorfälle pro Jahr melden, für deren Bearbeitung jeweils ein zusätzlicher Aufwand von 660 Euro pro Meldung entsteht, so entsteht den Betreibern Kritischer Infrastrukturen für die Erfüllung der Meldepflicht ein jährlicher Erfüllungsaufwand von insgesamt 9,24 Millionen Euro.

Hinzu kommt der Erfüllungsaufwand für die Betreiber öffentlicher Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste für die Aufrechterhaltung und Erweiterung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an die Bundesnetzagentur. Da es in diesem Bereich bereits ein etabliertes Verfahren zur Meldung von IT-Sicherheitsvorfällen an die Bundesnetzagentur gibt, das durch das Gesetz lediglich erweitert wird, lässt sich der hierdurch entstehende Mehraufwand nicht seriös quantifizieren. Auf Grund von Angaben aus der Wirtschaft werden die Kosten für die Bearbeitung einer Meldung derzeit auch für diesen Bereich mit 660 Euro pro Meldung (11 Stunden Zeitaufwand bei einem Stundensatz von 60 Euro) beziffert. Von entsprechenden Kosten je Meldung wird auch für die Genehmigungsinhaber nach dem Atomgesetz ausgegangen.

3. Erfüllungsaufwand der Verwaltung

Schon heute werden den zuständigen Behörden IT-Sicherheitsvorfälle gemeldet.

Beim BSI entsteht für die Erfüllung der im Gesetz vorgesehenen Aufgaben − in Abhängigkeit von der Zahl der Betreiber Kritischer Infrastrukturen und der Anzahl der eingehenden Meldungen − ein Aufwand von insgesamt zwischen 115 bis zu maximal 216,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich zwischen rund 8,95 und bis zu maximal 15,867 Millionen Euro sowie Sachkosten in Höhe von einmalig rund 5 bis 7 Millionen Euro.

Der Personalbedarf des BSI begründet sich neben den erweiterten Verantwortlichkeiten insbesondere dadurch, dass Informationstechnik in den sieben relevanten KRITIS-Sektoren (KRITIS: Kritische Infrastrukturen) sehr unterschiedlich eingesetzt wird. Dies betrifft sowohl die genutzten Komponenten, Produkte, Systeme und externen IKT-Dienstleistungen (IKT: Informations- und Kommunikationstechnik) als auch die eingesetzte IT zur Sicherung der Funktionsfähigkeit der kritischen Prozesse selbst. Weiterhin ist zu berücksichtigen, dass im Vergleich zur klassischen Informationstechnik die Besonderheiten der sektorspezifischen Rahmenbedingungen für kritische Prozesse individuell betrachtet werden müssen. Dadurch ergibt sich auch die Notwendigkeit zur deutlichen Ausweitung der Grundlagenarbeit und Fachkompetenz im BSI, die bisher vordringlich auf die Sicherheit der Informationstechnik des Bundes fokussiert war. Die Beratung der KRITIS-Betreiber muss sich an der IKT-Sicherheit zur Gewährleistung der zu erbringenden Dienstleistung ausrichten. Hierzu sind umfangreiche Kenntnisse über die Funktionsweise und informationstechnische Abstützung der kritischen Prozesse der jeweiligen KRITIS-Sektoren und KRITIS-Branchen erforderlich. Der geforderte Personalbedarf

ermöglicht den Aufbau der notwendigen Fachexpertise und stellt die Basis für Grundlagenberatung und Unterstützung dar. Eine systematische, individuelle Einzelberatung für alle Betreiber Kritischer Infrastrukturen ist hingegen nicht möglich. Zur Ermittlung des Stands der Technik in den einzelnen KRITIS-Branchen und für die Anerkennung der von den Branchen erstellten Branchenstandards ist in hohem Maße Fachkompetenz und Ressourcenaufwand erforderlich. Dies gilt ebenfalls für die Identifizierung konkreter Sicherheitsmängel und für die Prüfung angeforderter Auditberichte. Auch zum Auswerten von in der Meldestelle eingehender Informationen, zum Fortschreiben des Lagebildes und bei der Vorhersage der potentiellen Auswirkungen einer Meldung bzw. Störung auf die betroffene Kritische Infrastruktur oder ihre Branche ist spezielles Know-how in Bezug auf die jeweiligen KRITIS-Sektoren und KRITIS-Branchen zwingend erforderlich. Darüber hinaus erfordert die Wahrnehmung der Aufgabe als zentrale Meldestelle für die Sicherheit in der Informationstechnik für die Betreiber Kritischer Infrastrukturen den Ausbau des BSI-Lagezentrums auf einen 24/7-Betrieb. Im Rahmen der neuen Aufgaben des BSI soll es auch zu weiteren Einnahmen von Gebühren kommen.

Beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) führen die neuen Mitwirkungsaufgaben zu einem Bedarf von zwischen 9 und bis zu maximal 13 Planstellen/Stellen mit jährlichen Personalkosten zwischen 711 000 und bis zu maximal 1,011 Millionen Euro.

Bei der Bundesnetzagentur (BNetzA) führen die neuen Aufgaben zu einem Bedarf von bis zu maximal 28 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von rund bis zu maximal 3,202 Millionen Euro. Des Weiteren entstehen Kosten für Sachmittel in Höhe von einmalig 150 000 Euro im ersten Jahr für die Aufgaben nach § 109 Absatz 4 Satz 7 und 8 sowie Absatz 5 des Telekommunikationsgesetzes.

In den Fachabteilungen des BKA entsteht ein Ressourcenaufwand von zwischen 48 und bis zu maximal 78 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von jährlich zwischen rund 3,226 und bis zu maximal 5,310 Millionen Euro. Des Weiteren entstehen Kosten für Sachmittel in Höhe von jährlich bis zu maximal 630 000 Euro.

In den Fachabteilungen des Bundesamtes für Verfassungsschutz (BfV) entsteht durch die Zuständigkeit gemäß § 8b Absatz 2 Nummer 4 des BSI-Gesetzes ein Bedarf von zwischen 26,5 und maximal 48,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich zwischen 1,836 und maximal 3,253 Millionen Euro. Des Weiteren entstehen Kosten für Sachmittel in Höhe von maximal 610 000 Euro jährlich.

In den Fachabteilungen des Bundesnachrichtendienstes (BND) entsteht durch die Zuständigkeit gemäß § 8b Absatz 2 Nummer 4 des BSI-Gesetzes im Zusammenhang mit der Prüfung ausländischer Datenstrecken auf Schadsoftware-Signaturen und Rückverfolgung von Schadsoftware im Ausland ein Bedarf von maximal 30 Planstellen/Stellen mit Personalkosten in Höhe von jährlich maximal 2,153 Millionen Euro. Des Weiteren ein jährlicher Bedarf an Sachkosten in Höhe von maximal 688 000 Euro.

In der Fachabteilung des für die nukleare Sicherheit und die Sicherung zuständigen Bundesministeriums für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB) führen die neuen Mitwirkungspflichten für das zentrale IT-Meldesystem an das BSI nach § 44b des Atomgesetzes (neu) und bei der Erarbeitung der Sicherheitsanforderungen für Energieanlagen nach § 11 Absatz 1b des Energiewirtschaftsgesetzes zu einem Bedarf von bis zu maximal 4 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von maximal rund 240 000 Euro.

Bei der Bundesbeauftragten für Datenschutz und Informationsfreiheit entsteht ein Bedarf von zwischen 2,4 und bis zu maximal 7 Planstellen/Stellen.

Im Ressort des Bundesministeriums für Arbeit und Soziales wird für das Bundesversicherungsamt vor Erlass der Rechtsverordnung nach § 10 Absatz 1 des BSI-Gesetzes noch nicht quantifizierbarer Aufwand im Hinblick auf die Rechtsaufsicht als zuständige Aufsichtsbehörde über die bundesunmittelbaren Träger der Sozialversicherung erwartet. Das Gleiche gilt für die fachlichen Aufsichtsbehörden (Bundesamt für Güterverkehr, Eisenbahn-Bundesamt, Luftfahrt-Bundesamt, Bundesaufsichtsamt für Flugsicherung, Generaldirektion Wasserstraßen und Schifffahrt, Bundesamt für Seeschifffahrt und Hydrografie) im Ressort des Bundesministeriums für Verkehr und Digitale Infrastruktur im Hinblick auf den Sektor Transport und Verkehr.

Darüber hinaus können Verträge des Bundes mit Dritten, die Kommunikationstechnik im Auftrag des Bundes betreiben sollen und hierzu Leistungen von Unternehmen in Anspruch nehmen, die dem Gesetz unterliegen, zu Ausgaben führen, die aus heutiger Sicht noch nicht bezifferbar sind.

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

Der Erfüllungsaufwand für die Länder und Kommunen ist derzeit noch nicht bezifferbar.

IV. Weitere Kosten

Geringe, aber noch nicht quantifizierbare Kosten für die fallweise Anpassung der von Bundesbehörden bereitgestellten IT-Verfahren infolge der von den Betreibern Kritischer Infrastrukturen umzusetzenden Maßnahmen.

V. Gleichstellungspolitische Relevanz

Die Regelungen sind inhaltlich geschlechtsneutral und damit ohne Gleichstellungsrelevanz. Die Stärkung der IT-Sicherheit betrifft sowohl mittelbar wie unmittelbar Frauen wie Männer gleichermaßen. § 1 Absatz 2 des Bundesgleichstellungsgesetzes, der verlangt, dass Rechts- und Verwaltungsvorschriften des Bundes die Gleichstellung von Frauen und Männern auch sprachlich zum Ausdruck bringen sollen, wurde in die Entwicklung der Gesetzesformulierung miteinbezogen. Gleichzeitig wurde aber auch die Diktion der jeweils zu ändernden Stammgesetze mitberücksichtigt.

VI. Nachhaltigkeit

Der Gesetzentwurf entspricht mit der Anhebung der Sicherheitsstandards in der deutschen IT-Sicherheitsarchitektur, die zunehmend alle Gesellschaftsbereiche durchdringt, dem Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der nationalen Nachhaltigkeitsstrategie.

VII. Demographie-Check

Von dem Vorhaben sind keine demographischen Auswirkungen − unter anderem auf die Geburtenentwicklung, Altersstruktur, Zuwanderung, regionale Verteilung der Bevölkerung oder das Generationenverhältnis − zu erwarten.

B. Besonderer Teil

Zu Artikel 1 (Änderung des BSI-Gesetzes)

Zu Nummer 1 (§ 1 Bundesamt für Sicherheit in der Informationstechnik)
Die neue Fassung von § 1 trägt der geänderten Rolle des BSI Rechnung. Die Aufgaben des BSI neben der Abwehr von Gefahren für die Sicherheit in der Informationstechnik des Bundes haben an Bedeutung gewonnen. Das BSI dient zunehmend Bürgerinnen und Bürgern, Unternehmen, Verwaltungen und der Politik als Ansprechpartner in Fragen der IT-Sicherheit. Auch auf EU-Ebene sowie international ist das BSI verstärkt der nationale Ansprechpartner in Fragen der IT- und Cybersicherheit in Deutschland. Die Entwicklung des BSI hin zur nationalen Informationssicherheitsbehörde wird mit der Änderung des § 1 nachvollzogen.

Zu Nummer 2 (§ 2 Begriffsbestimmungen)
§ 2 Absatz 10 Satz 1 definiert den Begriff der Kritischen Infrastrukturen im Sinne der Regelungen des BSI-Gesetzes. Da es bislang noch keine gesetzlich geregelte Definition der Kritischen Infrastrukturen in Deutschland gibt, ist die Begriffsbestimmung notwendig, um die Adressaten der §§ 8a und 8b des BSI-Gesetzes zu bestimmen.

Die Definition folgt im Grundsatz der innerhalb der Bundesregierung abgestimmten Einteilung Kritischer Infrastrukturen. Dazu gehören die Bereiche Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie das Finanz- und Versicherungswesen. Zur Umsetzung der in den §§ 8a und 8b des BSI-Gesetzes getroffenen Vorgaben sind innerhalb dieser Sektoren diejenigen Einrichtungen, Anlagen oder Teile davon zu identifizieren, die als Kritische Infrastrukturen im Sinne des BSI-Gesetzes einzustufen sind, weil sie für das Funktionieren des Gemeinwesens und die Sicherung der Grundbedürfnisse der Bevölkerung von hoher Bedeutung sind und deshalb besonders schutzwürdig sind.

Die weitere Konkretisierung bedarf der sektor- und branchenspezifischen Einbeziehung aller betroffenen Kreise (Verwaltung, Wirtschaft und Wissenschaft). Die jeweils anzulegenden Maßstäbe können nur in einem gemeinsamen Arbeitsprozess mit Vertretern der möglicherweise betroffenen Betreiber Kritischer Infrastrukturen und unter Einbeziehung der Expertise von externen Fachleuten in sachgerechter Weise erarbeitet werden. Hinzu kommt, dass der technische und gesellschaftliche Wandel sowie die im Rahmen der

Umsetzung der neuen gesetzlichen Vorgaben gemachten Erfahrungen in den Folgejahren gegebenenfalls Anpassungen erforderlich machen. Die nähere Bestimmung der Kritischen Infrastrukturen ist daher gemäß Satz 2 einer Rechtsverordnung vorbehalten. Diese ist auf der Grundlage von § 10 Absatz 1 des BSI-Gesetzes zu erlassen. Hierbei ist vorgesehen, die Einteilung der Kritischen Infrastrukturen nach den Kriterien Qualität und Quantität vorzunehmen. Zu Einzelheiten siehe die Ausführungen zu § 10 Absatz 1 des BSI-Gesetzes.

Nicht zu den vom BSI-Gesetz adressierten Kritischen Infrastrukturen gehören die Verwaltung von Regierung und Parlament sowie die öffentliche Bundesverwaltung und die von ihr eingesetzte Technik (einschließlich der Technik, die im Auftrag der Bundesverwaltung betrieben wird). Als Spezialregelung gelten hier unter anderem die §§ 4, 5 und 8 des BSI-Gesetzes. Entsprechendes gilt für die Verwaltungen der Länder und Kommunen, für die der Bund keine Gesetzgebungskompetenz besitzt. Das Gleiche gilt für den Sektor Kultur und Medien, da auch hier die Gesetzgebungskompetenz überwiegend bei den Ländern liegt.

Zu Nummer 3 (§ 3 Aufgaben des Bundesamtes)

Zu Buchstabe a (Änderungen der Aufgaben in Absatz 1 Satz 2)
Zu Doppelbuchstabe aa (Zurverfügungstellung gewonnener Erkenntnisse)
Die Änderung in Absatz 1 Satz 2 Nummer 2 dient der Klarstellung, dass durch das BSI bei der Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen gewonnene Erkenntnisse nicht nur Behörden, sondern auch anderen („Dritten“) zur Verfügung gestellt werden können, soweit dies zur Wahrung der Sicherheitsinteressen erforderlich ist. Hierdurch wird noch einmal der Mehrwert unterstrichen, den eine verbreitete Erkenntnisbasis und ein verbessertes Lagebild des BSI für Wirtschaft und Gesellschaft haben können. Dritte in diesem Sinne sind insbesondere auch die Betreiber Kritischer Infrastrukturen im Sinne des BSI-Gesetzes. Adressat sollen aber auch sonstige Einrichtungen oder Unternehmen sein, die zwar keine Betreiber Kritischer Infrastrukturen im Sinne des BSI-Gesetzes sind, dennoch aber anerkanntermaßen zum Bereich der Kritischen Infrastrukturen im weiteren Sinne gehören oder sonst ein berechtigtes Sicherheitsinteresse an den entsprechenden Informationen haben (zum Beispiel Einrichtungen aus dem nicht erfassten Sektor Kultur und Medien oder wissenschaftliche Einrichtungen).

Zu Doppelbuchstabe bb (IT-Sicherheit Kritischer Infrastrukturen)
Buchstabe b enthält redaktionelle Anpassungen.

Zu Doppelbuchstabe cc (Bundesamt als zentrale Stelle im internationalen Bereich)
Die ausdrückliche Festschreibung der Aufgabe als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland durch Aufnahme der neuen Nummer 16 trägt der gewachsenen Rolle des BSI als nationalem und internationalem Ansprechpartner in Fragen der IT- und Cybersicherheit in Deutschland Rechnung. Besondere Zuständigkeiten anderer Stellen im Bereich der Cybersicherheit (zum Beispiel des Auswärtiges Amtes, des Bundesministeriums der Verteidigung, des Bundesamtes für Verfassungsschutz oder des Bundesnachrichtendienstes) bleiben unberührt.

Bei Nummer 17 handelt es sich um eine notwendige Ergänzung um die vom BSI mit diesem Gesetz neu übernommene Aufgabe als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen, die in den §§ 8a bis 8c des BSI-Gesetzes konkretisiert wird.

Zu Buchstabe b (Aufgaben des Bundesamtes im Bereich der Sicherheit in der Informationstechnik Kritischer Infrastrukturen)
Absatz 3 ermöglicht es dem BSI, Betreiber Kritischer Infrastrukturen auf Ersuchen bei der Sicherung ihrer Informationstechnik, insbesondere im Hinblick auf die Erfüllung der Anforderungen nach den §§ 8a und 8b des BSI-Gesetzes, zu beraten und zu unterstützen. Dies soll (ebenso wie Feststellungen nach § 8a Absatz 2 Satz 2 des BSI-Gesetzes) als individuell zurechenbare öffentliche Leistung in der nach § 10 Absatz 3 des BSI-Gesetzes (neu) zu erlassenden Rechtsverordnung erfasst werden. Das BSI entscheidet nach pflichtgemäßem Ermessen, ob es einem entsprechenden Ersuchen des Betreibers einer Kritischen Infrastruktur nachkommt. In diesem Zusammenhang kann das BSI den Betreiber auch an einen qualifizierten Sicherheitsdienstleister verweisen.

Zu Nummer 4 (§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes)
Die Änderung der Überschrift dient klarstellend der Abgrenzung zur neuen Aufgabe des BSI nach § 8b des BSI-Gesetzes.

Zu Nummer 5 (§ 7 Absatz 1 Warnungen)

Die Neufassung von Absatz 1 Satz 1 strukturiert die bereits bestehenden Befugnisse des BSI neu und ergänzt diese um die Befugnis zu Warnungen bei Datenverlust oder bei einem unerlaubten Zugriff auf Daten (Nummer 1 Buchstabe c). Hierdurch wird klargestellt, dass das BSI nach § 7 auch in Fällen tätig werden kann, in denen nicht die Warnung vor einem Schadprogramm oder einer Sicherheitslücke im Vordergrund steht, sondern vielmehr die Bewältigung eines bereits erfolgten Verlustes von oder Zugriffs auf Daten. Zur Schadenseingrenzung wird das BSI im Regelfall frühzeitig eine Warnung aussprechen und die Bürgerinnen und Bürger informieren, es sei denn, dieses Vorgehen würde zu erheblichen Sicherheitsrisiken führen.

Satz 2 ermöglicht es dem BSI, auch zur Klarstellung unter Datenschutzgesichtspunkten, bei Warnungen Dritte als Informationsintermediäre einzubeziehen, sofern dies für eine wirksame und rechtzeitige Warnung erforderlich ist, insbesondere um Betroffene schnellstmöglich zu erreichen. Satz 2 eröffnet aber nicht die Möglichkeit, zusätzliche Daten bei den Dritten zu erheben. Informationsintermediäre sind insbesondere die von den Kundinnen und Kunden genutzten Provider und Diensteanbieter.

Oftmals wird das BSI abhandengekommene Daten nicht direkt einem Betroffenen zuordnen oder diesen nicht ohne weiteres selbst unterrichten können. Im Interesse einer effizienten Warnung der Betroffenen kann sich das BSI daher an sog. Informationsintermediäre mit der Bitte um Unterstützung wenden. Die Informationsintermediäre sind beispielsweise auf Grund der bei ihnen vorhandenen weiter gehenden Informationen oder aus technischen Gründen in der Lage, an einer möglichst schnellen Unterrichtung der Betroffenen mitzuwirken.

Zu Nummer 6 (§ 7a Untersuchung der Sicherheit in der Informationstechnik)

Absatz 1 dient dazu, Rechtssicherheit für umfassende Untersuchungen von IT-Produkten (zum Beispiel mittels Reverse-Engineering) und IT-Systemen durch das BSI zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14 und 17 des BSI-Gesetzes herzustellen. Die gesetzliche Befugnis führt dazu, dass die Beschaffung von Daten und Informationen über den Aufbau und die Funktionsweise der Untersuchungsgegenstände durch das BSI nicht als unbefugt im Sinne von § 202a des Strafgesetzbuches (StGB) bzw. § 17 ff. des Gesetzes gegen den unlauteren Wettbewerb (UWG) anzusehen ist. Eine Strafbarkeit nach den §§ 17 ff. UWG würde im Übrigen ein Handeln zu

Zwecken des Wettbewerbs oder aus Eigennutz bzw. Schadenszufügungsabsicht voraussetzen.

Auf dem Markt bereitgestellte bzw. zur Bereitstellung auf dem Markt vorgesehene Untersuchungsgegenstände sind solche, die für einen Erwerb durch das BSI verfügbar sind. Die Formulierung „auf dem Markt bereitgestellte Produkte“ ist angelehnt an eine entsprechende Formulierung im Produktsicherheitsgesetz. Durch die Formulierung „zur Bereitstellung auf dem Markt vorgesehene“ Untersuchungsgegenstände wird klargestellt, dass die Untersuchungsbefugnis auch solche Produkte und Systeme erfasst, die zwar vom Hersteller bereits angekündigt wurden, aber noch nicht allgemein am Markt verfügbar sind.

Untersuchungsrechte des BSI bei Herstellern, Anbietern und sonstigen Einrichtungen werden durch Absatz 1 nicht begründet.

Bei der Auswahl der Dritten, die vom BSI nach Absatz 1 Satz 2 mit der Untersuchung beauftragt werden können, hat das BSI die schutzwürdigen Interessen des Herstellers zu berücksichtigen. Hierzu gehört auch, dass das BSI den beauftragten Dritten zur Wahrung einer entsprechenden Vertraulichkeit verpflichtet. Die Beauftragung eines direkten Konkurrenten des Herstellers ist in diesem Zusammenhang ausgeschlossen.

Absatz 2 enthält eine Zweckbindung für die aus der Untersuchung nach Absatz 1 gewonnenen Erkenntnisse. Soweit erforderlich, ist zudem eine Weitergabe und Veröffentlichung dieser Erkenntnisse durch das BSI zulässig. In diesem Fall ist dem Hersteller zuvor die Gelegenheit zu einer Stellungnahme einzuräumen. Wenn der Hersteller in diesem Rahmen − etwa bei einer festgestellten Sicherheitslücke − selbst an die Öffentlichkeit geht oder sonst Abhilfe schafft, ist eine zusätzliche Veröffentlichung der Erkenntnisse durch das BSI nicht erforderlich. Bei den Erkenntnissen nach diesem Absatz handelt es sich nicht um personenbezogene Daten.

Zu Nummer 7 (§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen, § 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen, § 8c Anwendungsbereich und § 8d Auskunftsverlangen)

Zu § 8a (Sicherheit in der Informationstechnik Kritischer Infrastrukturen)

Zweck von Absatz 1 ist der ordnungsgemäße Betrieb Kritischer Infrastrukturen im Sinne des BSI-Gesetzes und die fortlaufende Verfügbarkeit der jeweils angebotenen, in der Rechtsverordnung nach § 10 Absatz 1 des BSI-Gesetzes als kritisch eingestuften Dienstleistungen. Zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse (siehe § 2 Absatz 2 des BSI-Gesetzes), die für die Funktionsfähigkeit der Kritischen Infrastrukturen maßgeblich sind, sollen branchenspezifische Mindestanforderungen an die IT-Sicherheit zum Schutz der Kritischen Infrastrukturen nach § 2 Absatz 10 des BSI-Gesetzes erfüllt werden. Dies umfasst auch Maßnahmen zur Detektion und Behebung von Störungen.

Durch die Erfassung nicht nur der informationstechnischen Systeme, sondern auch der informationstechnischen Komponenten, die darin oder in sonstigen Systemen Verwendung finden, sowie durch die Erfassung der informationstechnischen Prozesse, also der Vorgänge der Informationsverarbeitung, wird sichergestellt, dass die Betreiber Kritischer Infrastrukturen überall dort Absicherungsmaßnahmen ergreifen müssen, wo Informationstechnik Einfluss auf die Erbringung ihrer kritischen Dienstleistungen hat. Hierfür sind angemessene organisatorische und technische Vorkehrungen zu treffen, zu denen auch infrastrukturelle und personelle Maßnahmen gehören können. Besonders kritische Prozesse bedürfen im Einzelfall besonderer Sicherheitsmaßnahmen durch Abschottung. Diese Prozesse sollten weder mit dem Internet oder öffentlichen Netzen verbunden noch von über das Internet angebotenen Diensten abhängig sein. Das Erfordernis, angemessene organisatorische und technische Vorkehrungen zu treffen, besteht auch dann, wenn der Betreiber der Kritischen Infrastruktur seine IT durch einen externen Dienstleister betreiben lässt.

Auf Grund der weitreichenden gesellschaftlichen Auswirkungen ist bei den technischen und organisatorischen Vorkehrungen der Stand der Technik zu berücksichtigen. Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten

oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden. Die Verpflichtung zur Berücksichtigung des Stands der Technik schließt die Möglichkeit zum Einsatz solcher Vorkehrungen nicht aus, die einen ebenso effektiven Schutz wie die anerkannten Vorkehrungen nach dem Stand der Technik bieten.

Bei der Frage der Angemessenheit ist der bei dem Betreiber erforderliche Aufwand, insbesondere die von ihm aufzuwendenden Kosten, zu berücksichtigen. Um die Umsetzung der Mindestanforderungen zu dokumentieren, ist es sachgerecht, dass diese von den Betreibern in entsprechende Sicherheits- und Notfallkonzepte aufgenommen werden.

Absatz 2 ermöglicht in Branchen, in denen es fachlich sinnvoll ist, die Erarbeitung branchenspezifischer Sicherheitsstandards und verankert damit den kooperativen Ansatz, wie er in der Nationalen Strategie zum Schutz Kritischer Infrastrukturen festgeschrieben wurde und im UP KRITIS und seinen Branchenarbeitskreisen realisiert wird. Ziel ist es, dass sich Betreiber Kritischer Infrastrukturen branchenintern zusammenfinden und branchenspezifische Sicherheitsstandards erarbeiten. Der UP KRITIS stellt dabei als etablierte Kooperationsplattform zwischen Betreibern und Staat bereits entsprechende Strukturen zur Verfügung. Darüber hinaus bietet das Deutsche Institut für Normung e. V. − als nationale Normungsorganisation und Mitglied der europäischen und internationalen Normungsorganisationen sowie als Kooperationsplattform zwischen Staat und Betreibern von Informations- und Sicherheitswirtschaft − entsprechende Strukturen und bewährte Prozesse. Auch die branchenspezifischen Sicherheitsstandards müssen regelmäßig dem sich weiterentwickelnden Stand der Technik angepasst werden.

Die Bewertung und Anerkennung der vorgetragenen Standards soll im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde erfolgen, um die Vereinbarkeit und Koordinierung mit anderen Belangen der Sicherheitsvorsorge zu gewährleisten. Die Differenzierung zwischen einem „Einvernehmen“ mit der zuständigen Aufsichtsbehörde des Bundes und einem „Benehmen“ mit der sonst zuständigen Aufsichtsbehörde berücksichtigt die Rechtspre-

chung des Bundesverfassungsgerichts, wonach Mitentscheidungsbefugnisse der einen föderalen Ebene bei Entscheidungen der anderen föderalen Ebene mit dem Grundgesetz nicht zu vereinbaren sind („Verbot der Mischverwaltung“). Unabhängig davon soll aber über das Benehmenserfordernis sichergestellt werden, dass die fachliche Expertise der sonstigen Aufsichtsbehörden einbezogen wird.

Auch dann, wenn branchenspezifische Sicherheitsstandards erarbeitet wurden, steht es dem einzelnen Betreiber frei, abweichend davon auch eigene den Stand der Technik berücksichtigende Maßnahmen umzusetzen.

Der Nachweis durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nach Absatz 3 dient der Kontrolle und Überprüfung der von den Betreibern nach Absatz 1 getroffenen Maßnahmen und damit der Einhaltung eines angemessenen Sicherheitsniveaus durch die Betreiber. Die Ausgestaltung der Sicherheitsaudits, Prüfungen und Zertifizierungen soll nicht im Detail gesetzlich vorgegeben werden, da die Ausgestaltung von den gegebenenfalls erarbeiteten branchenspezifischen Sicherheitsstandards, den in den Branchen vorhandenen technischen Gegebenheiten und bereits bestehenden Auditierungs- und Zertifizierungssystemen abhängt. Generell soll geprüft werden, ob der Betreiber die für seine Branche und Technologie geeigneten und wirksamen Maßnahmen und Empfehlungen befolgt, etwa ein Information Security Management (Sicherheitsorganisation, IT-Risikomanagement etc.) betreibt, kritische Cyber-Assets identifiziert hat und managt, Maßnahmen zur Angriffsprävention und -erkennung betreibt, ein Business Continuity Management (BCM) implementiert hat und darüber hinaus die branchenspezifischen Besonderheiten (zum Beispiel den jeweiligen branchenspezifischen Sicherheitsstandard, sofern ein solcher erstellt und anerkannt wurde) umsetzt.

Die Sicherheitsaudits, Prüfungen oder Zertifizierungen sollen von dazu nachweislich qualifizierten Prüfern bzw. Zertifizierern durchgeführt werden. Bei Zertifizierungen nach internationalen, europäischen oder nationalen Standards kann auf die bestehenden Zertifizierungsstrukturen zurückgegriffen werden. Ein Auditor gilt als qualifiziert, wenn er seine Qualifikation zur Überprüfung der Einhaltung der Sicherheitsstandards gegenüber dem BSI auf Verlangen formal glaubhaft machen kann. Denkbar ist in diesem Zusammenhang etwa die Anknüpfung an Zertifizierungen, die für die fachlich-technische Prüfung im jeweiligen Sektor angeboten werden (zum Beispiel zertifizierte Prüfer für bestimmte ISO-Normen oder Ähnliches). Eine Kontrolle der Einhaltung der Erfordernisse nach Absatz 1 kann zudem über etablierte Prüfmechanismen erfolgen. So prüfen Wirt-

schaftsprüfer bereits heute unter anderem im Rahmen der Jahresabschlussprüfung die für die Rechnungslegung relevanten IT-Systeme.

Bei Sicherheitsmängeln kann das BSI im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse verlangen und, soweit erforderlich, die Beseitigung der Sicherheitsmängel verlangen. Auch insoweit wird vom BSI im gesetzlich zulässigen Rahmen die fachliche Expertise der zuständigen Aufsichtsbehörden einbezogen (siehe hierzu die Begründung zu Absatz 2).

Zu § 8b (Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen)

§ 8b regelt die Meldungen an das BSI als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen. Die entsprechenden Meldungen sind Voraussetzung für die nationale Handlungsfähigkeit und Grundlage für bundesweit abgestimmte Reaktionen. Im Einzelnen:

Absatz 1 beschreibt die Aufgabe des BSI als zentraler Meldestelle für die Sicherheit in der Informationstechnik für Betreiber Kritischer Infrastrukturen.

Absatz 2 regelt die weiteren Aufgaben des BSI in diesem Zusammenhang. Das BSI sammelt alle eingehenden Meldungen und erstellt und aktualisiert − unter Einbeziehung seiner sonstigen Erkenntnisse − ein Lagebild. Des Weiteren stellt das BSI den Betreibern Kritischer Infrastrukturen, den zuständigen Aufsichtsbehörden und den sonst zuständigen Behörden des Bundes sowie den zuständigen Aufsichtsbehörden der Länder oder die zu diesem Zweck dem BSI von den Ländern benannten Behörden in angemessener Form (zum Beispiel konsolidiert, sanitarisiert oder als Rohdatenmaterial) die sie betreffenden bzw. die zur Erfüllung ihrer bestehenden Aufgaben erforderlichen Informationen zur Verfügung, soweit Quellen- und Geheimschutz sowie insbesondere die schutzwürdigen Interessen der Betreiber Kritischer Infrastrukturen dem nicht entgegenstehen. Die Betreiber leisten insoweit durch die Meldungen einen eigenen Beitrag und bekommen dafür, da sie auch von den Meldungen der anderen Betreiber an das BSI und der Bewertung dieser Meldungen durch das BSI profitieren, im Gegenzug ein Mehrfaches an Informationen und Know-how zurück.

Die Öffentlichkeit wird benachrichtigt, wenn das öffentliche Interesse dies erfordert. Auch hier dürfen insbesondere die schutzwürdigen Interessen der Betreiber Kritischer Infrastrukturen nicht entgegenstehen.

Absatz 3 stellt durch eine Anbindung der Betreiber Kritischer Infrastrukturen an die Warn- und Alarmierungsmechanismen nach § 3 Absatz 1 Nummer 15 sicher, dass bei erheblichen Störungen der informationstechnischen Systeme, Komponenten oder Prozesse Kritischer Infrastrukturen, die für die Verfügbarkeit der betriebenen Kritischen Infrastrukturen maßgeblich sind, ein schneller Informationsfluss gewährleistet ist und dass das Lagezentrum des BSI sowie andere Betreiber Kritischer Infrastrukturen unverzüglich informiert werden.

Absatz 4 regelt die Verpflichtung von Betreibern Kritischer Infrastrukturen, dem BSI unverzüglich erhebliche Störungen, die die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse betreffen, zu melden. Der Begriff der „Störung“ ist dabei entsprechend der höchstrichterlichen Rechtsprechung zu § 100 Absatz 1 des Telekommunikationsgesetzes funktional zu verstehen. Eine Störung im Sinne des BSI-Gesetzes liegt daher vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken. Dazu zählen insbesondere Fälle von Sicherheitslücken, Schadprogrammen und erfolgten, versuchten oder erfolgreich abgewehrten Angriffen auf die Sicherheit in der Informationstechnik sowie außergewöhnliche und unerwartete technische Defekte mit IT-Bezug (zum Beispiel nach Softwareupdates oder ein Ausfall der Serverkühlung).

Die Störungen sind dann meldepflichtig, wenn sie erheblich sind. Eine solche Störung liegt vor, wenn durch sie die Funktionsfähigkeit der erbrachten kritischen Dienstleistung bedroht ist. Nicht meldepflichtig sind Störungen, die zu keiner Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastrukturen führen können. Erheblich sind insbesondere solche IT-Störungen, die nicht bereits automatisiert oder mit wenig Aufwand mithilfe der nach § 8a als Stand der Technik beschriebenen Maßnahmen abgewehrt werden können. Dies ist beispielsweise der Fall bei neuartigen oder außergewöhnlichen IT-Vorfällen, bei gezielten Angriffen, für neue Modi Operandi sowie für unerwartete Vorkommnisse. Insbesondere gilt dies aber auch für Vorfälle, die nur mit deutlich erhöhtem Ressourcenaufwand bewältigt werden können (erhöhter Koordinierungsaufwand, Hinzuziehen zusätzlicher Experten, Nutzung einer besonderen Aufbauorganisation, Einberu-

fung eines Krisenstabs). IT-Störungen sind hingegen nicht erheblich, wenn es sich um tagtäglich vorkommende Ereignisse (Spam, übliche Schadsoftware, die standardmäßig im Virenscanner abgefangen wird, Hardwareausfälle im üblichen Rahmen) handelt und die mit den nach Stand der Technik nach § 8a des BSI-Gesetzes zu ergreifenden Maßnahmen ohne nennenswerte Probleme bewältigt werden.

Entsprechende Meldungen an das BSI − auch im Vorfeld konkreter Schadenseintritte − sind notwendig, um eine möglichst umfassende und frühzeitige Warnung möglicherweise ebenfalls betroffener Betreiber Kritischer Infrastrukturen zu gewährleisten und darüber hinaus fundierte Aussagen zur IT-Sicherheitslage in Deutschland treffen zu können. Im Sinne einer schnellen Information und Warnung potentiell betroffener Kreise ist es erforderlich, dass die Meldung stufenweise erfolgt. In einem ersten Schritt meldet der Betreiber schnellstmöglich die ihm ohne großen Rechercheaufwand zur Verfügung stehenden Informationen. Der Betreiber ergänzt die initiale Meldung dann nachträglich, im weiteren Verlauf der Vorfallsbearbeitung, um weitere, neu hinzukommende relevante Informationen.

Soweit die Störung nicht zu einem tatsächlichen Ausfall oder einer Beeinträchtigung führt, ist die namentliche Nennung des Betreibers nicht erforderlich. Die Meldung kann in diesem Fall pseudonymisiert erfolgen. Hierdurch wird der besonderen Sensibilität der Meldungen im Hinblick auf die wirtschaftlichen Auswirkungen eines möglichen Bekanntwerdens entsprechender Vorfälle Rechnung getragen. Auf die Nennung des Betreibers wird dementsprechend in den Fällen verzichtet, in denen die Meldung primär der Beratung und Warnung möglicher ebenfalls betroffener Kreise und der Erfassung der Cyberbedrohungslage dient. Gleichzeitig ermöglicht die Pseudonymisierung dem BSI, Rückfragen an den Meldenden zu stellen, ohne dass dessen Klarname dafür erforderlich ist.

Eine Nennung des Namens des Betreibers ist hingegen erforderlich bei bedeutenden Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die bereits konkret zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastruktur geführt haben. Denn im konkreten Schadensfall muss regelmäßig eine schnelle Krisenreaktion erfolgen, insbesondere um ähnliche Vorfälle bei anderen Betreibern noch abwenden zu können. Hierzu muss das BSI gegebenenfalls auch sofort auf den Meldenden zugehen können, um die dafür benötigten Informationen zu erhalten. Aufgrund der gebotenen Eile und der unmittelbaren Gefährdung der Versorgungssicherheit kann das Interesse der Meldenden,

anonym zu bleiben, in diesen Fällen nicht in gleicher Weise berücksichtigt werden wie bei den Fällen, bei denen es noch nicht zu einem konkreten Schadenseintritt gekommen ist.

Zur weiteren Konkretisierung der Meldepflicht wird das BSI − unter Einbeziehung der Betreiber Kritischer Infrastrukturen und der ansonsten im Bereich der Sicherheitsvorsorge zuständigen Aufsichtsbehörden − Kriterien für meldungsrelevante Sicherheitsvorfälle aufstellen und entsprechend der jeweils aktuellen IT-Sicherheitslage weiterentwickeln.

Absatz 5 eröffnet klarstellend die Möglichkeit für Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, ergänzend zu den Kontaktstellen nach Absatz 3 Satz 1 eine gemeinsame Ansprechstelle zu benennen, über die der Informationsaustausch zwischen den Kontaktstellen und dem BSI in der Regel erfolgen soll. Hierfür können bestehende Strukturen, beispielsweise über die ansonsten im Bereich der Sicherheitsvorsorge zuständigen Aufsichtsbehörden oder die eingerichteten Single Points of Contact (SPOCs) des UP KRITIS, genutzt und erweitert werden. Der gesamte Übermittlungsprozess muss vom Ablauf her nachvollziehbar und auch auditierbar sein.

Die im Rahmen von § 8b übermittelten Informationen sind üblicherweise rein technischer Natur. Sollte im Einzelfall doch ein Personenbezug gegeben sein, stellt Absatz 6 klar, dass personenbezogene Daten nur zu den in § 8b vorgesehenen Zwecken ausgewertet werden dürfen und die allgemeinen datenschutzrechtlichen Regelungen gelten. Für die nach § 8b erhaltenen Informationen gilt dementsprechend auch der allgemeine Grundsatz der Datensparsamkeit aus § 3a des Bundesdatenschutzgesetzes. Ergänzt wird dieses Datenschutzregime durch den Verweis auf § 5 Absatz 7 Satz 3 bis 8 des BSI-Gesetzes.

Zu § 8c (Anwendungsbereich)

Die Anwendung der §§ 8a und 8b des BSI-Gesetzes ist unabhängig von der Organisationsform des Betreibers Kritischer Infrastrukturen, so dass beispielsweise auch Einrichtungen des Bundes, die nicht Kommunikationstechnik im Sinne von § 2 Absatz 3 des BSI-Gesetzes sind, dem Anwendungsbereich unterfallen.

Nach Absatz 1 finden die §§ 8a und 8b des BSI-Gesetzes unter dem Gesichtspunkt der Verhältnismäßigkeit jedoch keine Anwendung auf solche Unternehmen, die als soge-

nannte Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36) Kritische Infrastrukturen betreiben. Kleinstunternehmen sind gemäß dieser Empfehlung Unternehmen, die weniger als 10 Personen beschäftigen und deren Jahresumsätze bzw. Jahresbilanzen 2 Millionen Euro nicht überschreiten. Die Ausnahme gilt auch für Unternehmen im Sinne von Artikel 3 Absatz 4 der Empfehlung, das heißt für Unternehmen, die an und für sich Kleinstunternehmen im Sinne der Empfehlung sind, von dieser aber ausgenommen wurden, weil 25 % oder mehr ihres Kapitals oder ihrer Stimmrechte direkt oder indirekt von einem oder mehreren öffentlichen Stellen oder Körperschaften des öffentlichen Rechts einzeln oder gemeinsam kontrolliert werden. Die entsprechenden Voraussetzungen müssen bei dem Betreiber der betreffenden Kritischen Infrastruktur selbst vorliegen und sind dem BSI auf dessen Verlangen hin auf geeignete Weise nachzuweisen. Dies kann beispielsweise durch die Vorlage einer Selbsterklärung des Unternehmens mit entsprechenden Nachweisen erfolgen. Organisatorische Maßnahmen des Betreibers, die zu einer (teilweisen) Auslagerung der Verantwortung für einzelne Bereiche der Kritischen Infrastrukturen führen, lassen die Verantwortung des Betreibers für die Kritische Infrastruktur als solche und die damit einhergehenden Verpflichtungen unberührt.

Absatz 2 nimmt Betreiber Kritischer Infrastrukturen, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen (Ziffer 1), vom Anwendungsbereich des § 8a des BSI-Gesetzes aus. Grund hierfür ist, dass diese Betreiber mit § 109 des Telekommunikationsgesetzes (neu) bereits einer § 8a des BSI-Gesetzes gleichwertigen Regelung unterfallen. Entsprechendes gilt für Betreiber von Energieversorgungsnetzen und Energieanlagen im Sinne des Energiewirtschaftsgesetzes (Ziffer 2). Eine gleichwertige Regelung enthält auch das Atomgesetz einschließlich der darauf beruhenden Rechtsverordnungen sowie des untergesetzlichen Regelwerks für Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes hinsichtlich der nuklearen Sicherheit (Ziffer 3). Aufgrund der Genehmigungsvoraussetzung des § 7 Absatz 2 Nummer 5 des Atomgesetzes in Verbindung mit den konkretisierenden Regelungen sowie der Aufsicht nach § 19 des Atomgesetzes sind hier ebenfalls gleichwertige Regelungen hinsichtlich der nuklearen Sicherheit vorhanden. Im Falle einer Kollision zwischen den Zielen der nuklearen Sicherheit und Sicherung kerntechnischer Anlagen einerseits und der Versorgungssicherheit andererseits ist die nukleare Sicherheit und Sicherung kerntechnischer Anlagen in der Abwägung vorrangig zu berücksichtigen.

Ziffer 4 normiert einen allgemeinen Vorrang speziellerer Anforderungen und nimmt damit insbesondere den Fall in den Blick, dass nach Inkrafttreten des Gesetzes in anderen Regelungsbereichen mit § 8a des BSI-Gesetzes vergleichbare oder weitergehende Regelungen getroffen werden. So sollen zum Beispiel für die Telematikinfrastruktur im Gesundheitswesen künftig dem § 8a des BSI-Gesetzes vergleichbare Anforderungen gelten.

Absatz 3 nimmt Betreiber Kritischer Infrastrukturen, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen (Ziffer 1), vom Anwendungsbereich der Absätze 3 bis 5 von § 8b des BSI-Gesetzes aus. Grund hierfür ist, dass diese Betreiber mit § 109 Absatz 5 des Telekommunikationsgesetzes (neu) einer § 8b Absatz 3 bis 5 des BSI-Gesetzes gleichwertigen Regelung unterfallen. Das Gleiche gilt für Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes (Ziffer 2). Einer spezialgesetzlichen Meldepflicht unterfallen gemäß der neu geschaffenen Regelung des § 44b des Atomgesetzes auch Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes. Diese sind daher ebenfalls auszunehmen (Ziffer 3).

Ziffer 4 normiert einen allgemeinen Vorrang speziellerer Anforderungen und nimmt damit insbesondere den Fall in den Blick, dass nach Inkrafttreten des Gesetzes in anderen Regelungsbereichen mit § 8b des BSI-Gesetzes vergleichbare oder weitergehende Regelungen getroffen werden. So sollen zum Beispiel für die Telematikinfrastruktur im Gesundheitswesen künftig dem § 8b des BSI-Gesetzes vergleichbare Anforderungen gelten.

Zu § 8d (Auskunftsverlangen)

§ 8d regelt als Spezialregelung im Sinne von § 1 Absatz 3 des Informationsfreiheitsgesetzes abschließend die Auskunft an nicht am Meldeverfahren beteiligte Personen oder an nichtöffentliche Institutionen (Dritte) zu Informationen, die im Rahmen von § 8a Absatz 2 und 3 an das BSI übersandt wurden, sowie zu den Meldungen nach § 8b Absatz 4 des BSI-Gesetzes unter Berücksichtigung des besonderen schutzwürdigen Interesses der meldepflichtigen Betreiber Kritischer Infrastrukturen an einer vertraulichen Behandlung der von ihnen gemeldeten Informationen sowie wesentlicher Sicherheitsinteressen.

Auskunft kann demnach nur dann erteilt werden, wenn keine schutzwürdigen Interessen des betroffenen Betreibers Kritischer Infrastrukturen dem entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen zu erwarten ist. Dies gilt insbesondere in den Fällen der §§ 8a Absatz 3, 8b Absatz 4 Satz 3 des BSI-Gesetzes. Aber auch in den Fällen des § 8b Absatz 4 Satz 1 des BSI-Gesetzes sind Konstellationen denkbar, bei denen eine Auskunftserteilung die schutzwürdigen wirtschaftlichen Interessen einer ganzen Branche oder auch einzelner Betreiber erheblich beeinträchtigen kann, etwa dann, wenn eine entsprechende Zuordnung auch ohne Nennung des Betreibers möglich ist oder nahe zu liegen scheint. Zugang zu personenbezogenen Daten wird generell nicht gewährt. Für die Weitergabe von Informationen an Betreiber Kritischer Infrastrukturen als am Meldeverfahren Beteiligte gilt § 8b Absatz 2 Nummer 4 des BSI-Gesetzes.

Diese Spezialregelung ist erforderlich, da die Ausnahmevorschriften der §§ 3ff. des Informationsfreiheitsgesetzes die besondere Interessenlage eines Meldeverfahrens für Betreiber Kritischer Infrastrukturen nicht hinreichend berücksichtigen. Denn für die Funktionsfähigkeit eines solchen Meldeverfahrens ist der Schutz der übermittelten hochsensiblen Informationen von entscheidender Bedeutung. Dem öffentlichen Interesse an einem effektiven Schutz der Verfügbarkeit der Kritischen Infrastrukturen ist Vorrang einzuräumen, da sie von hoher Bedeutung für das Funktionieren des Gemeinwesens sind und durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Zudem ist der besonderen Sensibilität der im Rahmen von § 8b des BSI-Gesetzes ausgetauschten Informationen sowohl für die meldepflichtigen Betreiber Kritischer Infrastrukturen wie auch für die Gesellschaft Rechnung zu tragen. Wesentliche Sicherheitsinteressen können einer Auskunftserteilung auch dann entgegenstehen, wenn durch eine Veröffentlichung von Erkenntnissen das Vertrauen der Betreiber Kritischer Infrastrukturen in die Vertraulichkeit des Meldeverfahrens erschüttert und hierdurch die Effizienz des Meldeverfahrens insgesamt gefährdet würde.

Ein Zugang zu Akten des BSI in Angelegenheiten nach den §§ 8a und 8b des BSI-Gesetzes wird gemäß Absatz 2 ausschließlich Verfahrensbeteiligten gewährt. Bei den Informationen, die das BSI im Rahmen dieser Aufgabe sammelt und analysiert (etwa im Zusammenhang mit der Erstellung des Lagebildes), handelt es sich um hochsensible, kumulierte sicherheitskritische Informationen, die einem besonders hohen Schutzbedürfnis unterliegen. Die hohe Sicherheitsempfindlichkeit dieser Informationen und deren

Risikopotential schließen eine Zugänglichkeit von vornherein aus. Die Akteneinsicht der Verfahrensbeteiligten erfolgt nach Maßgabe des § 29 des Verwaltungsverfahrensgesetzes.

Zu Nummer 8 (§ 10 Ermächtigung zum Erlass von Rechtsverordnungen)
Zu Buchstabe a (Kriterien zur Bestimmung der Kritischen Infrastrukturen)

§ 10 Absatz 1 ermächtigt das Bundesministerium des Innern, in Konkretisierung der systemischen Definition Kritischer Infrastrukturen nach § 2 Absatz 10 des BSI-Gesetzes − nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit den genannten Bundesministerien − die Kriterien zur Bestimmung derjenigen Einrichtungen, Anlagen oder Teile davon festzulegen, die als Kritische Infrastruktur im Sinne des BSI-Gesetzes einzuordnen sind.

In die Rechtsverordnung bzw. in die Anhänge zu der Rechtsverordnung sollen in abstrakter Form die als Kritische Infrastrukturen einzuordnenden Einrichtungen, Anlagen oder Teile davon benannt werden. Methodisch ist vorgesehen, eine Konkretisierung nach den Kategorien Qualität und Quantität vorzunehmen. Bei der Festlegung der betroffenen Kritischen Infrastrukturen wird die Frage zu beantworten sein, ob erstens mittels der jeweiligen Einrichtungen, Anlagen oder Teile davon eine für die Gesellschaft kritische Dienstleistung erbracht wird (Qualität) und zweitens ein Ausfall oder eine Beeinträchtigung wesentliche Folgen für wichtige Schutzgüter und die Funktionsfähigkeit des Gemeinwesens hätte (Quantität):

Unter der Kategorie Qualität wird näher erfasst, welche Dienstleistungen innerhalb der genannten Sektoren in dem Sinne kritisch sind, dass sie von hoher Bedeutung für das Funktionieren des Gemeinwesens sind und durch ihren Ausfall oder ihre Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche Gefährdungen für die öffentliche Sicherheit eintreten würden. Die Kategorie Qualität sollte sich hierbei insbesondere auf die Sicherheit von Leib, Leben, Gesundheit und Eigentum der Teile der Bevölkerung beziehen, die von einem Ausfall unmittelbar oder mittelbar beeinträchtigt wären. Sie dient der Prüfung, ob ein bestimmter Teil einer Branche überhaupt kritisch ist. Eine Spezifizierung des Qualitätskriteriums soll anhand einer abstrakten Darstellung von solchen kritischen Dienstleistungen erfolgen, die für die Gewährleistung der genannten Werte notwendig sind.

Solche kritischen Dienstleistungen könnten jedenfalls sein:

1. SEKTOR ENERGIE
   - Stromversorgung (Branche: Elektrizität)
   - Versorgung mit Erdgas (Branche: Gas)
   - Versorgung mit Mineralöl (Branche: Mineralöl)
2. SEKTOR INFORMATIONSTECHNIK UND TELEKOMMUNIKATION
   - Sprach- und Datenkommunikation (Branchen: Telekommunikation, Informationstechnik)
   - Verarbeitung und Speicherung von Daten (Branche: Informationstechnik)
3. SEKTOR TRANSPORT UND VERKEHR
   - Transport von Gütern (Branchen: Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)
   - Transport von Personen im Nahbereich (Branchen: Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)
   - Transport von Personen im Fernbereich (Branchen: Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)
4. SEKTOR GESUNDHEIT
   - medizinische Versorgung (Branchen: medizinische Versorgung, Labore)
   - Versorgung mit Arzneimitteln und Medizinprodukten (Branchen: medizinische Versorgung, Labore, Arzneimittel und Impfstoffe)
5. SEKTOR WASSER
   - Trinkwasserversorgung (Branche: öffentliche Wasserversorgung)
   - Abwasserbeseitigung (Branche: öffentliche Abwasserbeseitigung)
6. SEKTOR ERNÄHRUNG
   - Versorgung mit Lebensmitteln (Branchen: Ernährungswirtschaft, Lebensmittelhandel)

7. SEKTOR FINANZ- UND VERSICHERUNGSWESEN

- Zahlungsverkehr Zahlungsdienstleistungen durch Überweisung, Zahlungskarten und E-Geld (Branchen: Banken, Finanzdienstleister)
- Bargeldversorgung (Branche: Banken)
- Kreditvergabe (Branche: Banken, Finanzdienstleister)
- Geld- und Devisenhandel (Branche: Börsen, Banken, Zahlungsdienstleister)
- Wertpapier- und Derivatehandel (Branche: Börsen, Banken, Zahlungsdienstleister)
- Versicherungsleistungen (Branche: Versicherungen)

Ausgehend von einer solchen in der Rechtsverordnung abschließend vorzunehmenden Einteilung soll die Kategorie Quantität den Versorgungsgrad der jeweiligen Einrichtungen, Anlagen oder Teile davon erfassen. Zu untersuchen ist in diesem Zusammenhang, ob die Auswirkungen eines Ausfalls bzw. einer Beeinträchtigung der jeweiligen Einrichtungen, Anlagen oder Teile davon für die Versorgung einer entsprechend großen Zahl an Personen (Schwellenwert) mit einer kritischen Dienstleistung unmittelbar oder mittelbar wesentlich sind, das heißt aus gesamtgesellschaftlicher Sicht eine stark negative Wirkung hätten. Zur konkreten Ausfüllung dieses Kriteriums sollen unter Einbeziehung von Verwaltung, Wirtschaft und Wissenschaft möglichst spezifische Schwellenwerte gebildet und in die Rechtsverordnung aufgenommen werden. Die jeweils maßgeblichen Schwellenwerte können dabei pro Sektor/Branche bzw. Dienstleistung variieren.

Mögliche Adressaten können so anhand der Rechtsverordnung feststellen, ob sie mit einer entsprechenden Anlage, Einrichtung oder eines Teils davon eine kritische Dienstleistung mit einem Versorgungsgrad über dem entsprechenden Schwellenwert erbringen und ob sie damit den Verpflichtungen nach den §§ 8a, 8b des BSI-Gesetzes unterliegen.

Zu den Buchstaben b und c (Zustimmungsbedürftigkeit)

Die Buchstaben c und d betreffen redaktionelle Klarstellungen in den bereits bestehenden Verordnungsermächtigungen des BSI-Gesetzes.

Zu Nummer 9 (§ 13 Berichtspflichten)

Über die Berichtspflicht nach Absatz 1 wird sichergestellt, dass das Bundesministerium des Innern als zuständige Aufsichtsbehörde vom BSI über dessen laufende Tätigkeit unterrichtet wird. Relevante Informationen können so unter anderemauch in die regelmäßigen Sitzungen des Nationalen Cyber-Sicherheitsrates einfließen.

Die gesetzliche Verankerung einer Berichtspflicht und die vorgesehene Veröffentlichung eines Jahresberichts nach Absatz 2 dienen der Sensibilisierung der Öffentlichkeit für das Thema IT-Sicherheit. Der Bericht ergänzt die bestehenden fachlichen Informationsangebote des BSI und trägt als Beitrag der Bundesregierung zur Diskussion im politischen Raum bei. Da eine Vielzahl von Cyberangriffen bereits durch Basismaßnahmen abgewehrt werden könnte, spielt die Aufklärung und Sensibilisierung der Öffentlichkeit eine zentrale Rolle für die Erhöhung der IT-Sicherheit in Deutschland.

Zu Artikel 2 (Änderung des Atomgesetzes)

Die Regelung in § 44b ordnet für alle Genehmigungsinhaber von kerntechnischen Anlagen bzw. Tätigkeiten nach den §§ 6, 7 und 9 des Atomgesetzes bei Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer Gefährdung oder Störung der nuklearen Sicherheit und Sicherung führen können oder bereits geführt haben, eine unverzügliche Meldepflicht an das BSI als zentraler Meldestelle in Angelegenheiten der Sicherheit der informationstechnischen Systeme, Komponenten oder Prozesse gemäß § 8b Absatz 1 des BSI-Gesetzes an.

Die dem BSI in § 8b Absatz 2 BSI-Gesetz eröffneten Aufgaben und Befugnisse sollen auch für Meldungen der Genehmigungsinhaber nach den §§ 6, 7 und 9 des Atomgesetzes gelten.

Die beim BSI eingegangenen Meldungen leitet das Bundesamt unverzüglich an die für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden der Länder und an das für die nukleare Sicherheit und den Strahlenschutz zuständige Bundesministerium weiter. § 8b Absätze 1, 2 und 6 des BSI-Gesetzes gelten hierbei entsprechend.

Zu Artikel 3 (Änderung des Energiewirtschaftsgesetzes)

Zu Nummer 1 (§ 11 Betrieb von Energieversorgungsnetzen)
Zu Buchstabe a (Redaktionelle Klarstellungen und Konkretisierungen)
Mit den Änderungen in Absatz 1a sollen in der Praxis aufgetretene Unklarheiten beseitigt und das Schutzniveau konkretisiert werden.

Zu Doppelbuchstabe aa (Schutz der Telekommunikations- und Datenverarbeitungssysteme)
Die Formulierung „die der Netzsteuerung dienen“ in Satz 1 hat in der Vergangenheit zu Diskussionen darüber geführt, wie weit die Verpflichtung reicht. Die nunmehr gewählte Formulierung stellt klar, dass die Telekommunikationssysteme und Datenverarbeitungssysteme der Netzbetreiber so zu schützen sind, dass ein sicherer Netzbetrieb garantiert ist.

Zu Doppelbuchstabe bb (Katalog der Sicherheitsanforderungen)
§ 11 Absatz 1a wurde mit der EnWG-Novelle 2011 in das Energiewirtschaftsgesetz aufgenommen. Ein erster Entwurf des Sicherheitskataloges der Bundesnetzagentur wurde erarbeitet und wird derzeit mit der Branche erörtert. Der vorgelegte Sicherheitskatalog enthält Vorschriften zu Zertifizierungen und regelmäßigen Überprüfungen der Schutzmaßnahmen in den Unternehmen. Mit dem nun ergänzten Satz 3 ist die Regulierungsbehörde verpflichtet, die Überprüfungen von den Betreibern zu fordern. Die Änderung trägt dem in § 8a Absatz 3 des BSI-Gesetzes etablierten Schutzniveau Rechnung und verhindert, dass der Sicherheitskatalog der Bundesnetzagentur hinter diesem Schutzniveau zurückfallen könnte. Für den vorgelegten Sicherheitskatalog hat dies keine praktischen Folgen, da dieser bereits entsprechende Anforderungen vorsieht.

Zu Doppelbuchstabe cc (Bedeutung des Sicherheitskataloges)
Bislang wird ein angemessener Schutz der Telekommunikations- und Datenverarbeitungssysteme vermutet, wenn die Netzbetreiber die Anforderungen des Sicherheitskataloges erfüllen. Soweit ein Betreiber nachweisen kann, dass seine Maßnahmen einen ebenfalls angemessenen Schutz gewähren, kann er von dem Sicherheitskatalog abweichen. Mit der Formulierung „liegt vor“ bekommen die Vorgaben des Sicherheitskataloges ein noch größeres Gewicht. Ein angemessener Schutz der Telekommunikations- und Datenverarbeitungssysteme liegt demnach nur dann vor, wenn die Anforderungen des Sicherheitskataloges erfüllt sind. Damit bleibt grundsätzlich kein Spielraum mehr für

die Betreiber, andere aus ihrer Sicht angemessene Schutzmaßnahmen zu erarbeiten. Der Sicherheitskatalog der Bundesnetzagentur stellt einen Mindeststandard dar, der von den Betreibern einzuhalten ist.

Zu Doppelbuchstabe dd (Konzentration auf der Fachebene)

Von der Festlegungskompetenz wurde bislang kein Gebrauch gemacht. Vielmehr wird der Inhalt und Anwendungsbereich des Sicherheitskataloges weiter ausgedehnt. Es ist sachgerecht, das gesamte Verfahren von der Erstellung des Sicherheitskataloges bis zur Überprüfung seiner Einhaltung bei der Fachabteilung zu bündeln.

Zu Buchstabe b (Sicherheitskatalog und Meldepflicht)

Mit Absatz 1b wird eine neue Vorschrift eingefügt, die sich an die Betreiber von Energieanlagen, die als Kritische Infrastruktur bestimmt wurden, richtet. Die Aufnahme von Schutzstandards für Energieanlagen, die in der Rechtsverordnung nach § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, ist notwendig, um einen umfassenden Schutz für den Netzbetrieb sicherstellen zu können. Energieanlagen, die mit dem öffentlichen Versorgungsnetz verbunden sind, werden verpflichtet, dort, wo eine Gefährdung für den Netzbetrieb möglich ist, ebenfalls Sicherheitsmaßnahmen zu ergreifen. Aufgrund der technischen Nähe ist es notwendig und sinnvoll, dass die Sicherheitsstandards für Netzbetreiber und für die betroffenen Energieanlagen aufeinander abgestimmt sind. Aus diesem Grund wird die Bundesnetzagentur als für die Sicherheitsstandards des Netzbetriebs zuständige Behörde beauftragt, auch die Sicherheitsstandards für die Energieanlagen zu erarbeiten und deren Einhaltung zu überwachen. Absatz 1b entspricht insoweit Absatz 1a. Darüber hinaus wird klargestellt, dass Vorgaben auf Grund des Atomgesetzes für Telekommunikations- und elektronische Datenverarbeitungssysteme von Anlagen nach § 7 Absatz 1 des Atomgesetzes Vorrang haben.

Mit Absatz 1c wird für Betreiber von Einrichtungen, Anlagen oder Teilen davon, die in der Rechtsverordnung nach gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur eingestuft wurden, eine Meldepflicht an das BSI eingeführt. Gemäß § 8b Absatz 1 des BSI-Gesetzes ist das BSI die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit der informationstechnischen Systeme, Komponenten oder Prozesse. Die Einrichtung einer solchen zentralen Stelle ist sinnvoll, um Wissen und Erfahrungen bestmöglich zu bündeln. Damit Sicherheitsprobleme aus dem Energiesektor ebenfalls in dieses „Kompetenzzentrum“ einfließen können, sieht Absatz 1c vor, dass erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und

Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können oder bereits geführt haben, unverzüglich an das BSI zu melden sind. Die Anforderungen an den Inhalt der Meldung entsprechen denen aus der allgemeinen Meldepflicht für die Betreiber Kritischer Infrastrukturen nach § 8b Absatz 4 Satz 2 des BSI-Gesetzes. Entsprechende Meldungen an das BSI − auch im Vorfeld konkreter Schadenseintritte − sind notwendig, um eine möglichst umfassende und frühzeitige Warnung möglicherweise ebenfalls betroffener Betreiber Kritischer Infrastrukturen zu gewährleisten und darüber hinaus fundierte Aussagen zur IT-Sicherheitslage in Deutschland treffen zu können. Umgekehrt ist das BSI nach § 8b Absatz 2 Nummer 4 des BSI-Gesetzes verpflichtet, auch die Betreiber von Netzen oder Energieanlagen im Sinne von Absatz 1a und 1b über Sicherheitsvorfälle zu informieren. Das besondere Interesse der Meldeverpflichteten an einer vertraulichen Behandlung der von ihnen gemeldeten Informationen wird berücksichtigt. Die hochsensiblen sicherheitskritischen Informationen unterliegen einem besonderen Schutzbedürfnis.

Zu den Nummern 2 bis 4 (Änderung von Übergangsvorschriften)

Die Übergangsvorschriften aus § 21e Absatz 5 und § 21f Absatz 2 sollen den fließenden Übergang hin zum BSI-konformen Intelligenten Messsystem ermöglichen. Zwar wurden seit der EnWG-Novelle 2011 die erforderlichen Schutzprofile und Technischen Richtlinien des BSI zügig fortentwickelt, allerdings sind zertifizierte Messsysteme, wie sie § 21e Absatz 4 des Energiewirtschaftsgesetzes fordert, Anfang 2015 voraussichtlich noch nicht am Markt verfügbar. Nichtsdestoweniger sollen insbesondere in Pilotprojekten bereits Messsysteme eingesetzt und getestet werden können, die zwar über einen hohen technischen Standard verfügen, jedoch noch nicht BSI-zertifiziert sind. Diese Pilotprojekte sind für das künftige Zusammenspiel aller Akteure im intelligenten Energienetz von großer Bedeutung. Dies erfordert eine Verlängerung der bestehenden Übergangsvorschriften und dient letztendlich dem reibungslosen Ablauf des technischen Übergangs.

Durch die Neufassung wird außerdem stärker herausgestellt, dass Rechtsverordnungen nach § 21i Absatz 1 Nummer 11 des Energiewirtschaftsgesetzes den maßgeblichen Zeitpunkt bestimmen oder differenziert ausgestalten können, ab dem der Einsatz nicht BSI-konformer Messsysteme nicht mehr zugelassen wird. Diese Flexibilität ist erforderlich, um auf unterschiedliche Entwicklungsstände verschiedenster technischer Modullösungen (zum Beispiel Modul zum Steuern unterbrechbarer Verbrauchsein-

richtungen, Modul zum Steuern von EE-Anlagen etc.) wie auch auf die in Pilotprojekten gemachten Erfahrungen reagieren zu können. Sie ist auch nötig, um einen Gleichklang mit möglichen nach § 21i Absatz 1 Nummer 8 des Energiewirtschaftsgesetzes verordneten Einbauverpflichtungen herzustellen.

Zu Nummer 5 (§ 59 Absatz 1 Organisation)

Es handelt sich um eine Folgeänderung zu den Änderungen in § 11 Absatz 1a des Energiewirtschaftsgesetzes. Mit der Änderung wird klargestellt, dass die Fachabteilung der Bundesnetzagentur für die Erstellung und Überprüfung des Sicherheitskataloges gemäß § 11 Absatz 1a und 1b zuständig ist.

Zu Artikel 4 (Änderung des Telemediengesetzes)

Zu Nummer 1 (§ 13 Pflichten des Diensteanbieters)

Zu Buchstabe a (Schutz der Telekommunikations- und Datenverarbeitungssysteme nach dem Stand der Technik)

Wegen der zunehmenden Verbreitung von Schadsoftware über Telemediendienste werden die bestehenden Pflichten für Telemediendiensteanbieter, die ihre Telemedien geschäftsmäßig anbieten, um technische und organisatorische Maßnahmen zum Schutz vor unerlaubten Zugriffen, der personenbezogenen Daten und vor Störungen ergänzt.

Geschäftsmäßig ist ein Angebot dann, wenn es auf einer nachhaltigen Tätigkeit beruht, es sich also um eine planmäßige und dauerhafte Tätigkeit handelt. Bei einem entgeltlichen Dienst liegt dies regelmäßig vor, so z.B. bei werbefinanzierten Webseiten. Das nicht-kommerzielle Angebot von Telemedien durch Private und Idealvereine wird demgegenüber nicht erfasst.

Die betreffenden Diensteanbieter haben im Rahmen ihrer jeweiligen Verantwortlichkeit durch technische und organisatorische Vorkehrungen, die den Stand der Technik berücksichtigen, sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und dass diese Einrichtungen gegen Verletzungen des Schutzes personenbezogener Daten und Störungen gesichert sind. Voraussetzung ist, dass die entsprechenden Vorkehrungen für den konkreten Diensteanbieter technisch möglich und wirtschaftlich zumutbar sind. Durch das Kriterium der Zumutbarkeit wird sichergestellt, dass von dem Diensteanbieter nur solche Vorkeh-

rungen zu treffen sind, deren Kosten in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Dies ermöglicht eine flexible Anpassung der jeweiligen Anforderungen im Einzelfall.

Ein wesentliches Ziel der Regelung ist es, einen der Hauptverbreitungswege von Schadsoftware einzudämmen: das unbemerkte Herunterladen allein durch das Aufrufen bzw. Nutzen einer dafür von Angreifern präparierten Website (sogenannte Drive-by-Downloads). Bereits durch eine regelmäßige Aktualisierung der für das Telemedienangebot verwendeten Software (Einspielen von Sicherheitspatches) seitens der Websitebetreiber könnten zahlreiche dieser Angriffe vermieden werden. Kompromittierungen können zudem auch durch Inhalte erfolgen, auf die der Diensteanbieter keinen unmittelbaren technischen Einfluss hat (zum Beispiel über kompromittierte Werbebanner, die auf der Webseite eingebunden sind). Dagegen sind organisatorische Vorkehrungen zu treffen. Hierzu zählt beispielsweise, Werbedienstleister, denen Werbefläche eingeräumt wird, vertraglich zu notwendigen Schutzmaßnahmen zu verpflichten. Die entsprechenden Maßnahmen sind im Rahmen der jeweiligen Verantwortlichkeit zu treffen.

Vorkehrungen nach Satz 1 können insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens sowie − bei personalisierten Telemedien − das Angebot eines sicheren und dem jeweiligen Schutzbedarf angemessenen Authentifizierungsverfahrens sein. Je nach Sensibilität und Umfang der verarbeiteten Daten kann das erforderliche Schutzniveau unterschiedlich sein. Authentifizierungsverfahren nach den entsprechenden aktuellen und veröffentlichten Technischen Richtlinien des BSI sind dabei jedenfalls als dem Stand der Technik gemäß hinreichend sicher anzusehen. Auf die Barrierefreiheit der Verfahren ist besonders zu achten.

Zu Buchstabe b (Folgeänderung)
Buchstabe b enthält eine notwendige Folgeänderung.

Zu Nummer 2 (§ 16 Bußgeldvorschriften)
Die Aufnahme eines Verstoßes gegen die in § 13 Absatz 7 Satz 1 Nummer 1 oder Nummer 2 Buchstabe a des Telemediengesetzes geregelte Pflicht des Diensteanbieters zum Einsatz technischer und organisatorischer Schutzmaßnahmen zur Gewährleistung von IT-Sicherheit der für Dritte angebotenen Inhalte in die Bußgeldvorschriften des § 16 Absatz 2 Nummer 3 entspricht der Bußgeldbewehrung eines Verstoßes gegen die weiteren in § 13 Absatz 4 geregelten Pflichten des Diensteanbieters. Bußgeldbewehrt ist

damit auch der Einsatz technischer und organisatorischer Maßnahmen durch den Diensteanbieter, die nicht den Stand der Technik berücksichtigen.

Zu Artikel 5 (Änderung des Telekommunikationsgesetzes)

Zu Nummer 1 (Änderung der Inhaltsangabe)
Nummer 1 enthält eine notwendige Folgeänderung.

Zu Nummer 2 (§ 100 Absatz 1 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten)
Die Änderung dient der Klarstellung, dass ein Diensteanbieter Bestands- und Verkehrsdaten auch zum Erkennen und Beseitigen von Störungen verwenden darf, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Möglich sind in diesem Zusammenhang beispielsweise Prüfungen des Netzwerkverkehrs, die Verwendung von sogenannten Honeypots (Fallen für Schadprogramme im Netz) oder Spamtraps (Blockieren der Versendung von Schadprogrammen).

Zu Nummer 3 (§ 109 Technische Schutzmaßnahmen)
Zu Buchstabe a (Berücksichtigung des Stands der Technik)
Die gesetzlichen Vorgaben zu technischen Schutzmaßnahmen enthalten nach derzeitiger Rechtslage erhöhte Anforderungen nur für Maßnahmen zum Schutz der Vertraulichkeit (Fernmeldegeheimnis) und für den Schutz personenbezogener Daten. Diese Maßnahmen müssen den Stand der Technik berücksichtigen. Zur Gewährleistung der IT-Sicherheit werden im Übrigen nur „angemessene technische Vorkehrungen und Maßnahmen“ verlangt, wobei die Angemessenheit einzelner Maßnahmen unbestimmt ist und daher insbesondere auch von allgemeinen Wirtschaftlichkeitserwägungen abhängig gemacht werden kann.

Auf Grund der hohen Bedeutung für die Kommunikation des Einzelnen und damit der gesamtgesellschaftlichen Relevanz müssen auch zum Schutz gegen unerlaubte Zugriffe auf die Telekommunikations- und Datenverarbeitungssysteme Maßnahmen getroffen werden, die den Stand der Technik berücksichtigen. Angriffe auf die Systeme erfolgen zunehmend auf höchstem technischen Niveau unter Ausnutzung öffentlich noch nicht bekannter Lücken in der Sicherheitsarchitektur von Hardware- und Softwareprodukten.

Durch diese Angriffe werden die Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität datenverarbeitender Systeme bedroht. Mit der Änderung werden entsprechende Mindestanforderungen für den Schutz gegen unerlaubte Zugriffe und die Auswirkungen von Sicherheitsverletzungen aufgestellt. Sie richten sich an Betreiber von öffentlichen Telekommunikationsnetzen und Anbieter von öffentlichen Telekommunikationsdiensten.

Zu Buchstabe b (Überprüfung der Sicherheitskonzepte)

Die bestehende Regelung im bisherigen Satz 7, wonach die Bundesnetzagentur die Umsetzung des Sicherheitskonzeptes überprüfen kann, wird ersetzt durch eine Verpflichtung zur regelmäßigen Überprüfung der Umsetzung des Sicherheitskonzeptes, die mindestens alle zwei Jahre stattfinden soll. Hierdurch soll erreicht werden, dass die technischen und organisatorischen Maßnahmen jederzeit den Stand der Technik berücksichtigen. Ferner wird den zunehmenden Bedrohungen Rechnung getragen, die dazu führen können, dass mit der Dienstleistungserbringung Angriffe auf die Vertraulichkeit, Integrität und Verfügbarkeit der übertragenen Kommunikation verbunden sind. Bei der Überprüfung kann sich die Bundesnetzagentur der Mittel nach § 115 Absatz 1 und Absatz 2 des Telekommunikationsgesetzes bedienen und mögliche Verstöße gemäß § 115 Absatz 3 des Telekommunikationsgesetzes ahnden.

Zu Buchstabe c (Meldepflichten)

Die bestehenden Meldepflichten gegenüber der Bundesnetzagentur in § 109 Absatz 5 des Telekommunikationsgesetzes werden um die Verpflichtung ergänzt, bekannt gewordene Vorfälle zu melden, die zu beträchtlichen Sicherheitsverletzungen von datenverarbeitenden Systemen der Endnutzer führen können (Nummer 2). Über die bestehenden Meldeverpflichtungen im Bereich des Datenschutzes und bei beträchtlichen Beeinträchtigungen grundlegender Telekommunikationsdienste hinaus wird so gewährleistet, dass die Unternehmen, die das Rückgrat unserer Informationsgesellschaft bilden, ebenfalls zu einem validen und vollständigen Lagebild der IT-Sicherheit beitragen. Ziel ist es, bereits in diesem Vorfeldbereich eine Verbesserung des Lagebildes zur IT-Sicherheit zu erreichen. Verletzungen der IT-Sicherheit (zum Beispiel Manipulationen der Internet-Infrastruktur und Missbrauch einzelner Server oder Anschlüsse, etwa zum Errichten und Betreiben eines Botnetzes) bergen ein großes Gefahrenpotential, das sich in diesem Stadium allerdings noch nicht gegen die Verfügbarkeit der Netze insgesamt, sondern gegen die Funktionsfähigkeit und Verlässlichkeit der IT einzelner Nutzerinnen und Nutzer richtet und gegebenenfalls spätere schwerwiegende Folgen nach sich zieht.

Das Telekommunikationsgesetz sieht eine solche Meldepflicht gegenüber der Bundesnetzagentur bislang nur für tatsächlich aufgetretene Störungen und außerdem nur dann vor, wenn die durch Sicherheitsverletzungen verursachten Auswirkungen auf den Betrieb der Telekommunikationsnetze oder das Erbringen von Telekommunikationsdiensten beträchtlich sind.

Die bei der Bundesnetzagentur hat die bei ihr eingegangenen Meldungen sowie Informationen zu den von dem betreffenden Unternehmen ergriffenen Abhilfemaßnahmen unverzüglich an das BSI weiterzuleiten. Dadurch wird das BSI in die Lage versetzt, seinen Aufgaben nach § 8b Absatz 2 des BSI-Gesetzes nachzukommen.

Zu Buchstabe d (Erstellung eines Sicherheitskataloges)
Die zunehmende Nutzung von Informationstechnik im Rahmen der Telekommunikationstechnik erfordert auch eine normative Stärkung der IT-Sicherheitsbelange bei der Erstellung des Sicherheitskataloges nach Absatz 6. Durch die stärkere Einbeziehung der fachlichen Kompetenz des BSI („Einvernehmen“ statt „Benehmen“) wird diesem Erfordernis Rechnung getragen. Zudem erfolgt eine entsprechende Anpassung für die Bundesbeauftragte bzw. den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Zu Buchstabe e (Übermittlung der Auditergebnisse an das BSI)

Über die im Rahmen von Audits aufgedeckten Mängel bei der Erfüllung der Sicherheitsanforderungen in der Informationstechnik sowie die in diesem Zusammenhang von der Bundesnetzagentur geforderten Abhilfemaßnahmen ist das BSI von der Bundesnetzagentur unverzüglich zu unterrichten.

Zu Nummer 4 (§ 109a Daten- und Informationssicherheit)
Zu Buchstabe a (Änderung der Überschrift)
Buchstabe a enthält eine redaktionelle Folgeänderung und trägt dem erweiterten Regelungsbereich Rechnung.

Zu Buchstabe b (Information der Nutzerinnen und Nutzer)
Die Neuregelung soll die Information der Nutzerinnen und Nutzer über Verletzungen der IT-Sicherheit gewährleisten, die von einem von ihnen betriebenen datenverarbeitenden System ausgehen. Derzeit wird eine entsprechende Information der Nutzerinnen und Nutzer bei den einzelnen Providern uneinheitlich gehandhabt. Die Information soll Nut-

zerinnen und Nutzer in die Lage versetzen, selbst Maßnahmen gegen die auf ihren Systemen vorhandene Schadsoftware zu ergreifen. Hierfür ist Voraussetzung, dass die Nutzerinnen und Nutzer über angemessene Werkzeuge verfügen, um entsprechende Schutzmaßnahmen ergreifen zu können. Ergänzend zur Informationspflicht werden die Anbieter von öffentlichen Telekommunikationsdiensten deshalb verpflichtet, soweit es technisch möglich und zumutbar ist, die Nutzerinnen und Nutzer auf einfach bedienbare Sicherheitswerkzeuge hinzuweisen, die sowohl vorbeugend als auch zur Beseitigung von Störungen bei einer bereits erfolgten Infizierung des Datenverarbeitungssystems mit Schadsoftware eingesetzt werden können.

Nicht erforderlich ist eine individuelle Untersuchung der Technik oder eine individuelle Beratung durch den Anbieter. Soweit eine Benachrichtigung der betroffenen Nutzerinnen und Nutzer innerhalb von wenigen Tagen technisch nicht möglich ist, werden die Anbieter nur ihre Teilnehmerinnen und Teilnehmer informieren und auf Hilfsmittel hinweisen können. Auf die Barrierefreiheit der angebotenen Sicherheitswerkzeuge ist besonders zu achten.

Durch den Einschub „soweit ihm diese bereits bekannt sind“ wird klargestellt, dass zur Ermittlung der Nutzerinnen und Nutzer nur auf solche Verkehrsdaten zugegriffen werden darf, die bereits aufgrund anderer Vorschriften erhoben und gespeichert wurden (etwa im Rahmen von § 100 Absatz 1 des Telekommunikationsgesetzes). Eine Erhebung weiterer Daten ausschließlich zum Zweck der Durchführung einer Benachrichtigung ist nicht zulässig.

Zu Buchstabe c (Folgeänderung)
Buchstabe c enthält eine notwendige Folgeänderung.

Zu Nummer 5 (Änderung der Bußgeldvorschriften)
Nummer 5 enthält eine notwendige Folgeänderung zu der Erweiterung der Meldepflichten in § 109 Absatz 5 des Telekommunikationsgesetzes.

Zu Artikel 6 (Änderung des Bundesbesoldungsgesetzes)

Zu den Nummern 1 und 2 (Anhebung der Besoldungsgruppe)

Mit der Anhebung der Besoldungsgruppe des Präsidenten des BSI auf die Besoldungsstufe B 7 wird der geänderten nationalen wie internationalen Rolle des Bundesamtes für Sicherheit in der Informationstechnik Rechnung getragen. Dem Bundesamt kommt in der Sicherheitsarchitektur der Bundesrepublik Deutschland mit der zunehmenden Digitalisierung aller Gesellschaftsbereiche und der steigenden Cyberbedrohungslage eine immer größere Bedeutung zu. Neben der mit diesem Gesetz einhergehenden Zuständigkeitserweiterung ist bereits nach geltender Rechtslage ein zunehmender Verantwortungs- und Aufgabenzuwachs verbunden. National wie international spielt das Bundesamt bei seinen Ansprechpartnern wie auch in der öffentlichen Wahrnehmung eine immer größere Rolle.

Zu Artikel 7 (Änderung des Bundeskriminalamtgesetzes)

Zu den Nummern 1 und 2 (Zuständigkeitserweiterung)

Durch die Vorschrift wird die Zuständigkeit des Bundeskriminalamts für die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung über die bereits bestehende Zuständigkeit für Straftaten nach § 303b des Strafgesetzbuchs (Computersabotage) hinaus auf Straftaten nach den §§ 202a, 202b, 202c, 263a und 303a des Strafgesetzbuchs ausgedehnt. Zusätzlich zu den Fällen, in denen sich die genannten Straftaten gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder gegen sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen richten, wird geregelt, dass die Zuständigkeit des BKA auch bei derartigen Straftaten gegen Bundeseinrichtungen gegeben ist. Bisher liegt die Zuständigkeit für die polizeilichen Aufgaben der Strafverfolgung in der Regel bei den Ländern, wobei die örtliche Zuständigkeit oftmals dem Zufall überlassen bleibt, abhängig davon, wo der Vorfall zuerst entdeckt wird. Gerade bei Angriffen auf bundesweite Einrichtungen ist eine klare Zuständigkeitsregelung notwendig. Die nachrichtendienstlichen Zuständigkeiten und Befugnisse bleiben unberührt.

Zu Artikel 8 (Weitere Änderung des BSI-Gesetzes)

Die Anpassung ist notwendig, da die schwebende Änderung in Artikel 3 Absatz 7 des Gesetzes zur Strukturreform des Gebührenrechts des Bundes vom 7. August 2013 (BGBl. I S. 3154) so nicht mehr ausführbar ist.

Zu Artikel 9 (Änderung des Gesetzes zur Strukturreform des Gebührenrechts des Bundes)

Siehe die Begründung zu Artikel 8.

Zu Artikel 10 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes. Zu Satz 2 siehe die Begründung zu Artikel 8.

Das Gesetz soll fünf Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 des BSI-Gesetzes anhand der Konzeption zur Evaluierung neuer Regelungsvorhaben gemäß dem Arbeitsprogramm bessere Rechtsetzung der Bundesregierung vom 28. März 2012, Ziffer II. 3., evaluiert werden.

Anlage 2

Stellungnahme des Nationalen Normenkontrollrates gem. § 6 Abs. 1 NKRG:

Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (NKR-Nr. 3044)

Der Nationale Normenkontrollrat hat den Entwurf des oben genannten Regelungsvorhabens geprüft.

I. Zusammenfassung

Bürgerinnen und Bürger Erfüllungsaufwand:	Keine Auswirkungen
Wirtschaft Jährlicher Erfüllungsaufwand:	Der bezifferbare Mehraufwand beläuft sich auf gut 9 Mio. Euro. Hinzu kommt der Aufwand für die erforderliche Anpassung der IT-Systeme, den Nachweis der Erfüllung der IT-Sicherheitsstandards und den Betrieb der Kontaktstellen.
Verwaltung Jährlicher Erfüllungsaufwand (Personalkosten):	Maximal 36 Mio. Euro (425 Stellen)
Jährlicher Erfüllungsaufwand (Sachkosten):	2 Mio. Euro
Einmaliger Erfüllungsaufwand:	6 Mio. Euro
Der mit dem Regelungsvorhaben verbundene Erfüllungsaufwand ist wesentlich von der Zahl der Unternehmen abhängig, die diesem Gesetz unterfallen sollen. Die Kriterien, nach welchen die Unternehmen bestimmt werden sollen, sollen jedoch erst zu einem späteren Zeitpunkt in einer Rechtsverordnung geregelt werden. Vor diesem Hintergrund ist die Annahme des Ressorts, dass 2.000 Unternehmen von dem Gesetz betroffen sein werden, mit nicht unerheblichen Unsicherheiten behaftet. Damit sind auch die Angaben zum Erfüllungsaufwand nur eingeschränkt belastbar.	

Legt man die oben genannte Zahl der Darstellung zugrunde, hat das Ressort den Aufwand der Wirtschaft, soweit dies ex ante möglich ist, nachvollziehbar dargestellt.

Vor diesem Hintergrund ist ebenfalls der Aufwand auf Seiten der Verwaltung (unter Einbeziehung der vom Ressort zur Verfügung gestellten weiteren Informationen) nachvollziehbar dargestellt. Gleichwohl ist aus Sicht des Nationalen Normenkontrollrats schwer zu beurteilen, inwieweit die ausgewiesenen Personalkapazitäten im Einzelnen tatsächlich erforderlich sind, um den zusätzlichen Aufgaben nachzukommen, die der Entwurf für die Verwaltung beinhaltet.

Auch deshalb begrüßt der Normenkontrollrat, dass das Ressort die Wirkungen des Regelungsvorhabens entsprechend dem Evaluierungsverfahren der Bundesregierung überprüfen wird. Dies soll fünf Jahre nach dem Inkrafttreten der Rechtsverordnung geschehen, mit welcher die Kriterien für die Bestimmung der betroffenen Unternehmen festgelegt werden sollen.

II. Im Einzelnen

Das Regelungsvorhaben hat den Schutz der IT-Systeme so genannter kritischer Infrastrukturen und weiterer Unternehmen, die für das Gemeinwesen von zentraler Bedeutung sind, zum Ziel. Geschützt werden sollen IT-Infrastrukturen von Unternehmen aus den Sektoren Energie, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. Die Kriterien für die Bestimmung der betroffenen Unternehmen sollen in einer Rechtsverordnung festgelegt werden. Auf Seiten der Verwaltung soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) zur zentralen Stelle und Ansprechpartner für IT-Sicherheit in Deutschland ausgebaut werden.

II.1 Erfüllungsaufwand der Wirtschaft

Das Ressort geht bei seiner Darstellung des Erfüllungsaufwands von 2.000 Unternehmen aus, die im Sinne des Regelungsvorhabens als systemrelevant einzustufen sind, das heißt, deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit mit sich bringen würden. Diese Annahme fußt auf einer Untersuchung des BSI und des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe. Zu berücksichtigen ist hierbei, dass die Zahl der Unternehmen wesentlich von der noch zu erstellenden Rechtsverordnung abhängt. Daher ist zum jetzigen Zeitpunkt lediglich eine sehr grobe Einschätzung der Zahl der Unternehmen möglich. Aus

diesem Grund sind die Darstellungen des Erfüllungsaufwands nur eingeschränkt belastbar.

Das Regelungsvorhaben enthält für die Betreiber kritischer Infrastrukturen im Wesentlichen vier Vorgaben:

II.1.1 Einhaltung von Mindestanforderungen an die IT-Sicherheit

Betreiber kritischer Infrastrukturen sollen verpflichtet werden, spätestens zwei Jahre nach Erlass der oben genannten Rechtsverordnung organisatorische und technische Mindestanforderungen zur Vermeidung von Beeinträchtigungen ihrer informationstechnischen Systeme und Prozesse zu erfüllen, soweit diese für den Betrieb ihrer kritischen Infrastrukturen erforderlich sind.

Die Verpflichtung zur Sicherstellung dieses Mindeststandards an IT-Sicherheit wird dort zu Mehrkosten führen, wo kein hinreichendes IT-Sicherheitsniveau vorhanden ist. Der hierfür anfallende Aufwand ist ex ante nicht seriös bezifferbar, da er einerseits von den jeweiligen Sicherheitsanforderungen und andererseits davon abhängt, welche Maßnahmen die Unternehmen schon jetzt zur Sicherung ihrer Systeme ergriffen haben.

II.1.2 Meldung erheblicher IT-Sicherheitsvorfälle an das BSI

Ferner sollen Betreiber kritischer Infrastrukturen erhebliche Störungen ihrer informationstechnischen Systeme und Prozesse an das BSI melden, wenn diese Störungen zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastruktur führen können oder bereits geführt haben. Die Meldung soll Angaben zur Störung, zu den betroffenen IT-Systemen, zur vermuteten oder tatsächlichen Ursache etc. enthalten.

Das Ressort geht von sieben relevanten IT-Sicherheitsvorfällen pro Jahr und Unternehmen aus. Ausweislich einer Untersuchung von Seiten der Wirtschaft liegen die Kosten einer Meldung bei 660 Euro (bei rund 11 Stunden Zeitaufwand pro Meldung). Bei Zugrundelegung der oben genannten 2.000 Betreiber kritischer Infrastrukturen ist von einem jährlichen Erfüllungsaufwand von rund 9,2 Mio. Euro auszugehen.

II.1.3 Nachweis der Erfüllung der Mindestanforderungen durch Sicherheitsaudits

Darüber hinaus sollen die Betreiber kritischer Infrastrukturen künftig mindestens alle zwei Jahre nachweisen, dass sie die Mindestanforderungen erfüllen. Dies kann durch Sicherheitsaudits, Zertifizierungen oder auf sonstige geeignete Weise geschehen.

Da dieser Aufwand stark vom gewählten Prüfverfahren und von den Gegebenheiten im Unternehmen abhängig ist, ist dieser Aufwand ex ante kaum seriös quantifizierbar.

II.1.4 Betreiben einer Kontaktstelle

Betreiber kritischer Infrastrukturen sollen gegenüber dem BSI eine Kontaktstelle benennen, über die die Kommunikation zwischen dem BSI und dem Unternehmen abgewickelt werden kann. Diese Kontaktstelle soll jederzeit erreichbar sein.

Die Verpflichtung zum Betreiben einer Kontaktstelle wird dort zu Mehraufwand führen, wo noch keine Stelle existiert, die diese Aufgabe übernehmen kann. Um eventuelle Mehrkosten so gering wie möglich zu halten, ist im Regelungsvorhaben vorgesehen, dass Betreiber kritischer Infrastrukturen eine gemeinsame (übergeordnete) Kontaktstelle betreiben können. Dies dürfte auch die Umsetzung dieser Vorgabe für kleinere Unternehmen erleichtern, sofern solche nach der zu erlassenden Rechtsverordnung von dem vorliegenden Regelungsentwurf betroffen sind.

II.1.5 Weitere Adressaten aus dem Wirtschaftsbereich

Betreiber öffentlicher Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste sollen nur von einem Teil der oben genannten Vorgaben betroffen sein:

- Auch diese Betreiber sollen Maßnahmen zur Sicherung ihrer IT-technischen Einrichtungen vornehmen. Sie sollen dem Stand der Technik entsprechen. Die Ausführungen unter II.1.1 gelten entsprechend.
- Ferner sollen sie wie die Betreiber kritischer Infrastrukturen IT-Sicherheitsvorfälle an die Bundesnetzagentur (BNetzA) melden. Dabei ist zu berücksichtigen, dass es in diesem Bereich bereits ein Verfahren zur Meldung von IT-Sicherheitsvorfällen gibt. Danach ist eine Meldung an die BNetzA nur für tatsächlich aufgetretene Störungen und nur dann erforderlich, wenn die durch Sicherheitsverletzungen verursachten

Auswirkungen beträchtlich sind. Durch das vorliegende Regelungsvorhaben soll diese Verpflichtung insofern erweitert werden, als die Betreiber künftig auch Vorfälle melden sollen, die zu erheblichen Sicherheitsverletzungen von datenverarbeitenden Systemen der Endnutzer führen können. Insofern ist in diesem Bereich von einer Erhöhung der Zahl der Meldungen auszugehen.

II.2 Erfüllungsaufwand der Verwaltung

Nach Angaben des Ressorts führt das Regelungsvorhaben zu einem erheblichen Mehraufwand auf Seiten der betroffenen Behörden. Der Mehrbedarf liegt bei Zugrundelegung der oben genannten 2.000 Unternehmen bei maximal 425 Stellen (rund 36 Mio. Euro; auch bei den folgenden Angaben handelt es sich jeweils um Maximalwerte). Der Mehrbedarf soll in den jeweiligen Einzelplänen ausgeglichen werden:

- Der Großteil des oben genannten Mehraufwands entfällt mit knapp 220 Stellen (knapp 16 Mio. Euro) auf das BSI. Darüber hinaus ist mit Sachkosten von einmalig rund 6 Mio. Euro zu rechnen.
  Mit dem Regelungsentwurf soll das BSI zur nationalen Informationssicherheitsbehörde ausgebaut werden. Hierfür soll die Grundlagenarbeit im BSI deutlich ausgebaut werden, um insbesondere im Bereich der Beratung von Unternehmen (wie auch von Behörden) die erforderliche Fachkompetenz vorweisen zu können. Diese ist außerdem erforderlich, um konkrete Sicherheitsmängel identifizieren sowie die in den oben genannten Wirtschaftssektoren jeweils erforderlichen Sicherheitsstandards erarbeiten zu können.

  Aus Sicht des Ressorts wird außerdem aus der Auswertung der Meldungen von Seiten der Wirtschaft und der Beratung der Betreiber kritischer Infrastrukturen ein erheblicher Mehraufwand resultieren. Dieser ergibt sich unter anderem daraus, dass Informationstechnik in den sieben Sektoren sehr unterschiedlich eingesetzt wird. Dies betrifft sowohl die genutzten Komponenten, Systeme und externen Dienstleistungen als auch die eingesetzten Systeme zur Sicherung der Funktionsfähigkeit der kritischen Prozesse.

- Ausweislich des Entwurfs ist beim Bundeskriminalamt mit einem Mehraufwand von knapp 80 Stellen (gut 5 Mio. Euro) zu rechnen.
  Mit dem Entwurf soll die Zuständigkeit des Bundeskriminalamts für die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung ausgeweitet werden. So soll die Zu-

ständigkeit künftig auch die Straftatbestände des Ausspähens von Daten, des Abfangens von Daten, des Computerbetrugs etc. umfassen.

- Für das Bundesamt für Verfassungsschutz (BfV) geht der Entwurf von einem Mehraufwand von knapp 50 Stellen (3,3 Mio. Euro) aus.
  Dieser resultiert aus der Auswertung der vom BSI zur Verfügung gestellten Informationen und sich daraus für das BfV ergebenden Handlungserfordernissen.
- Der übrige Stellenmehrbedarf entfällt auf das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, die Bundesnetzagentur, den Bundesnachrichtendienst, das Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit sowie auf die Bundesbeauftragte für Datenschutz und Informationsfreiheit.
- Darüber hinaus dürfte auf Seiten der Aufsichtsbehörden ein gewisser Mehraufwand durch die Auswertung der Berichte des BSI für ihre Zwecke auftreten.

II.3 Evaluation

Das Ressort beabsichtigt, das Regelungsvorhaben fünf Jahre nach Inkrafttreten der Rechtsverordnung zu evaluieren, mit welcher die Kriterien für die Bestimmung der betroffenen Unternehmen festgelegt werden sollen.

Zusammenfassend ist festzustellen, dass die Darstellung des Erfüllungsaufwands mit nicht unerheblichen Unsicherheiten behaftet ist, da der Kreis der Adressaten derzeit nicht hinreichend einschätzbar ist. Damit sind die Angaben zum Erfüllungsaufwand nur eingeschränkt belastbar. Bei Zugrundelegung der Zahl von 2.000 Unternehmen ist der mit dem Regelungsvorhaben verbundene Aufwand, soweit dies ex ante möglich ist, nachvollziehbar dargestellt.

Hinsichtlich des Aufwands der Verwaltung ist es aus Sicht des Nationalen Normenkontrollrats schwer zu beurteilen, inwieweit die ausgewiesenen Personalkapazitäten im Einzelnen tatsächlich erforderlich sind, um den zusätzlichen Aufgaben nachzukommen, die der Entwurf für die Verwaltung beinhaltet. In diesem Zusammenhang wird bei der Umsetzung besonderes Augenmerk darauf zu legen sein, dass in den verschiedenen Behörden, die von dem Gesetz betroffen sind, dieselben Arbeiten – zum Beispiel die Analyse einer Schadsoftware – nicht mehrfach vorgenommen werden.

Im Hinblick auf die parallel zu diesem Gesetzgebungsverfahren laufenden Verhandlungen über die NIS-Richtlinie gilt es, ein Auseinanderfallen der Regelungen zu vermeiden, da eventuelle

spätere Änderungen infolge der Richtlinie zu unnötigem Mehraufwand bei den Adressaten führen würden.

Auch vor dem Hintergrund der Unsicherheiten im Hinblick auf die Folgekosten begrüßt der Normenkontrollrat, dass das Ressort die Wirkungen des Regelungsvorhabens entsprechend dem Evaluierungsverfahren der Bundesregierung überprüfen wird.

Dr. Ludewig	Prof. Kuhlmann
Vorsitzender	Berichterstatterin

Anlage 3

Stellungnahme
des Bundesrates

Der Bundesrat hat in seiner 930. Sitzung am 6. Februar 2015 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. Zum Gesetzentwurf allgemein:

a) Der Bundesrat begrüßt die Initiative der Bundesregierung zur Verbesserung der IT-Sicherheit von Unternehmen und zum verstärkten Schutz der Bürgerinnen und Bürger im Internet. Die Sicherheit der Informations- und Kommunikationsinfrastrukturen ist zentrale Grundlage für eine erfolgreiche Digitalisierung von Wirtschaft und Gesellschaft.

b) Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren dafür Sorge zu tragen, dass zur Schaffung von Planungs- und Rechtssicherheit eine weitere Konkretisierung von unbestimmten Rechtsbegriffen erfolgt. Dies betrifft vor allem die Präzisierung des Begriffs "Kritische Infrastrukturen" (§ 2 Absatz 10 BSIG-E), die Definition der Meldeschwelle für Telekommunikationsunternehmen bei auftretenden "beträchtlichen Sicherheitsverletzungen" (§ 109 Absatz 5 TKG-E), die Präzisierung des Begriffs "Stand der Technik" (§ 8a Absatz 1 Satz 2 BSIG-E) sowie die Definition einer "erheblichen Störung" (§ 8b Absatz 4 Satz 1 BSIG-E). Die Präzisierung des Begriffs "Kritische Infrastrukturen" sollte dabei in einem noch stärkeren Maße bereits im Gesetz selbst erfolgen.

c) Der Bundesrat bittet im weiteren Gesetzgebungsverfahren dafür Sorge zu tragen, dass eindeutige und transparente Regelungen getroffen werden, die einen angemessenen Schutz und eine sinnvolle Verwendung der umfangreichen Datenmengen sicherstellen, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) aufgrund der gesetzlichen Meldepflicht der Unternehmen erhält.

Begründung:

Der von der Bundesregierung vorgelegte Gesetzentwurf enthält sinnvolle Regelungen zur Verbesserung der IT-Sicherheit von Unternehmen und zum verstärkten Schutz der Bürgerinnen und Bürger im Internet. Zu nennen sind hier insbesondere die Etablierung von Mindeststandards an IT-Sicherheit nach dem Stand der Technik und die Meldepflicht von Betreibern kritischer Infrastrukturen bei schwerwiegenden Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse sowie die Information der Bürgerinnen und Bürger bei beträchtlichen Sicherheitsverletzungen und Störungen.

Der Gesetzentwurf enthält allerdings in zentralen Punkten unbestimmte Rechtsbegriffe, die zu einer erheblichen Rechts- und Planungsunsicherheit führen und deutlich höhere Mehrkosten bei den betroffenen Unternehmen als geplant verursachen könnten. So ist unter anderem der vom Gesetzentwurf betroffene Adressatenkreis nicht hinreichend konkret bezeichnet. Die Einstufung als kritische Infrastruktur kann gravierende wirtschaftliche Folgen für ein Unternehmen nach sich ziehen. Es sollte daher im Gesetz selbst eine weitergehende Klarstellung vorgenommen und dies nicht allein im Wege der Rechtsverordnung geregelt werden. Aufgrund dieser Unbestimmtheit bleibt die im Gesetzentwurf enthaltene Verpflichtung zu einem einzuhaltenden Mindeststandard an IT-Sicherheit ebenfalls zu vage.

Der Gesetzentwurf beantwortet außerdem nicht die Frage, wie das BSI mit den aufgrund der Meldepflicht künftig anfallenden riesigen Datenmengen umgehen will. Es ist daher zwingend erforderlich, dass zusammen mit den Standards für die Industrie auch die Standards und Arbeitsabläufe innerhalb des BSI hinsichtlich Klarheit, Effizienz und praktischem Nutzen dem Anspruch in der Zielsetzung des Gesetzentwurfs gerecht werden.

2. Zu Artikel 1 Nummer 1 (§ 1 Satz 2 BSIG)

In Artikel 1 Nummer 1 ist § 1 Satz 2 wie folgt zu fassen:

"Das Bundesamt ist zentraler Ansprechpartner für die Informationssicherheit in der Bundesrepublik Deutschland."

Begründung:

Mit dieser Formulierung wird das nationale Beratungsangebot des BSI zum Ausdruck gebracht, ohne die ebenfalls bestehenden Länderstrukturen zu übergehen.

3. Zu Artikel 1 Nummer 5 (§ 7 Absatz 1 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob die im geltenden § 7 Absatz 1 Satz 2 BSIG vorgesehene Verpflichtung zur rechtzeitigen Information von Herstellern betroffener Produkte auf Anbieter entsprechender informationstechnischer Dienstleistungen sowie betroffene Betreiber Kritischer Infrastrukturen ausgeweitet werden sollte.

Begründung:

§ 7 Absatz 1 Satz 1 BSIG-E sieht vor, dass das BSI Warnungen über Sicherheitslücken in informationstechnischen Produkten und Diensten an die Öffentlichkeit oder betroffene Kreise richten kann. § 7 Absatz 1 Satz 2 BSIG verpflichtet zur rechtzeitigen Information betroffener Hersteller von Produkten über die Warnungen. Eine Information an die Anbieter betroffener informationstechnischer Dienste ist bislang nicht explizit vorgesehen. Da informationstechnische Dienste oftmals über Telekommunikationsnetze angeboten werden, könnte darüber hinaus auch eine Information des entsprechenden Telekommunikationsnetzbetreibers als Betreiber einer betroffenen Kritischen Infrastruktur zielführend sein. Dies ist insbesondere auch von Bedeutung, da in der Novellierung die Nutzung unter anderem der Telekommunikationsnetzbetreiber als so genannte "Informationsintermediäre" zur Information an Dritte vorgesehen ist.

4. Zu Artikel 1 Nummer 6 (§ 7a Absatz 1 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob bezüglich der Untersuchung informationstechnischer Systeme der Telekommunikation das Einvernehmen mit der Bundesnetzagentur vorgesehen werden sollte.

Begründung:

Gemäß § 109 Absatz 7 TKG kann die Bundesnetzagentur bei Betreibern öffentlicher Telekommunikationsnetze oder bei Anbietern öffentlicher Telekommunikationsdienste eine Überprüfung bezüglich technischer Schutzmaßnahmen anordnen. Eine Kopie des Überprüfungsberichts ist an die Bundesnetzagentur zu übermitteln. Sofern informationstechnische Systeme der Telekommunikation gemäß § 7a Absatz 1 BSIG-E durch das BSI untersucht werden sollen, erscheint eine Verzahnung mit der Bundesnetzagentur bezüglich der dort bereits vorliegenden Informationen beziehungsweise geplanten Überprüfungsanordnungen sinnvoll. Es sollte geprüft werden, ob die verpflichtende Vorgabe einer diesbezüglichen engen Abstimmung zwischen BSI und Bundesnetzagentur durch Einvernehmensherstellung sinnvoll ist. Für weitere im Telekommunikationsgesetz geregelte Sachverhalte hat der Gesetzentwurf in der vorliegenden Fassung bereits weitgehend auf Doppelregulierung verzichtet (siehe auch § 8c Absatz 2 Nummer 1 BSIG-E).

5. Zu Artikel 1 Nummer 7 (§ 8b Absatz 2 Nummer 4 Buchstabe c BSIG)

In Artikel 1 Nummer 7 ist § 8b Absatz 2 Nummer 4 Buchstabe c wie folgt zu ändern:

a) Die Wörter "die zur Erfüllung ihrer Aufgaben erforderlichen" sind zu streichen.

b) Nach der Angabe "3" sind die Wörter ", insbesondere über Inhalte und Absender von Meldungen nach Absatz 4 mit möglichen Auswirkungen auf das jeweilige Land," einzufügen.

Begründung:

Mit dieser Formulierung werden die in § 8b Absatz 2 Nummer 4 Buchstabe c BSIG-E vorgesehenen Informationspflichten des BSI an die zuständigen Aufsichtsbehörden der Länder oder benannten Kontaktbehörden konkretisiert.

6. Zu Artikel 1 Nummer 7 (§ 8c Absatz 2 Nummer 3 BSIG),
Artikel 2 (§ 44b AtG),
Artikel 3 Nummer 1 Buchstabe b (§ 11 Absatz 1b Satz 3 und 4,
Absatz 1d - neu - EnWG)

a) In Artikel 1 Nummer 7 ist § 8c Absatz 2 Nummer 3 zu streichen.

b) In Artikel 2 ist § 44b wie folgt zu fassen:

"§ 44b

Sicherung der Informationstechnik

(1) Vorgaben zur Gewährleistung des erforderlichen Schutzes gegen Einwirkungen Dritter auf Telekommunikations- und elektronische Datenverarbeitungssysteme, die für diejenigen Anlagen nach § 7 Absatz 1 gelten, bei denen es sich um Energieanlagen im Sinne von § 3 Nummer 15 des Energiewirtschaftsgesetzes handelt und die durch Rechtsverordnung nach § 10 des BSI-Gesetzes als Kritische Infrastruktur eingestuft sind, werden auf Verlangen der Regulierungsbehörde nach § 54 Absatz 1 des Energiewirtschaftsgesetzes um Vorgaben ergänzt, die über die nukleare Sicherheit hinaus der Verfügbarkeit des Energieversorgungsnetzes oder der Energieanlage dienen, sofern dies nicht zu einer Verminderung der kerntechnischen Sicherheit führt.

(2) Inhaber von Anlagen im Sinne des Absatzes 1 haben der zuständigen Aufsichtsbehörde unverzüglich erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer Gefährdung der nuklearen Sicherheit der betroffenen Anlage oder zur Beeinträchtigung der Verfügbarkeit der Energieanlage führen können oder bereits geführt haben, zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, und der betroffenen Informationstechnik enthalten.

(3) Die Aufsichtsbehörde leitet Meldungen nach Absatz 2 verbunden mit einer sicherheitstechnischen Bewertung unverzüglich an die für die Informationssicherheit auf nationaler Ebene zuständige Bundesoberbehörde und an die Regulierungsbehörde nach § 54 Absatz 1 des Energiewirtschaftsgesetzes weiter. § 11 Absatz 1c Satz 5 bis 8 des Energiewirtschaftsgesetzes gilt entsprechend."

c) Artikel 3 Nummer 1 Buchstabe b ist wie folgt zu fassen:

'b) Nach Absatz 1a werden folgende Absätze 1b bis 1d eingefügt:

"(1b) Betreiber von Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 8 des Gesetzes vom […] [einsetzen: Ausfertigungsdatum dieses Gesetzes und Fundstelle] geändert worden ist, in der jeweils geltenden

Fassung als Kritische In-frastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, haben binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Der Katalog von Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen. Ein angemessener Schutz des Betriebs von Energieanlagen im Sinne von Satz 1 liegt vor, wenn dieser Katalog eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Bundesnetzagentur überprüft werden. Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 4 treffen.

(1c) Betreiber von Energieversorgungsnetzen und Energieanlagen, die ... <weiter wie Gesetzentwurf> ...

(1d) Die Absätze 1b und 1c gelten nicht für Betreiber von Energieanlagen, die einer Genehmigung nach § 7 Absatz 1 des Atomgesetzes bedürfen." '

Begründung:

Zu Buchstabe a:

Soweit es sich bei den in § 8c Absatz 2 Nummer 3 BSIG-E genannten Anlagen, die unter die Genehmigungspflicht nach § 7 Absatz 1 AtG fallen, um Kernkraftwerke handelt, unterfallen sie als Energieanlagen im Sinne des Energiewirtschaftsgesetzes bereits der Ausnahme nach § 8c Absatz 2 Nummer 2 BSIG-E. Denn der Begriff der Energieanlage umfasst nach § 3 Nummer 15, § 8c Absatz 2 Nummer 2 BSIG-E ausdrücklich auch "Anlagen zur Erzeugung […] von Energie". Hierunter fallen sämtliche Arten von Produktionsanlagen zur Erzeugung von Elektrizität, also auch Kernkraftwerke.

Sofern es sich bei den in § 8c Absatz 2 Nummer 3 BSIG-E genannten Anlagen, die unter die Genehmigungspflicht nach § 7 Absatz 1 AtG fallen, nicht um Kernkraftwerke handelt, würden sie gegebenenfalls von der Ausnahme des § 8c Absatz 2 Nummer 4 BSIG-E erfasst, wenn und soweit es sich überhaupt um Kritische Infrastrukturen handelt.

Im Übrigen ist die Ausnahme des § 8c Absatz 2 Nummer 3 BSIG-E durch die Beschränkung auf den "Geltungsbereich der Genehmigung" zu eng gefasst. Es ist nicht zweckmäßig, beim Schutz der Informationstechnik (IT) eines Kernkraftwerks zwischen dem kerntechnischen und dem konventionellen Bereich zu unterscheiden. Nach der für Kernkraftwerke geltenden Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorie I und II gegen Störmaßnahmen und sonstige Einwirkungen Dritter (SEWD-Richtlinie IT) sind ohnehin alle IT-Systeme zu erfassen, die vom Betreiber oder in seinem Auftrag betrieben werden und mit der Anlage in einem engen räumlichen, informationstechnischen oder betrieblichen Zusammenhang stehen.

Zu Buchstabe b:

Zu § 44b Absatz 1 - neu - AtG:

Die in § 11 EnWG-E vorgesehene Konstruktion führt für Kernkraftwerke zu einer nicht klar definierbaren Schnittstelle von Vorgaben nach dem Atomgesetz und Vorgaben nach dem Energiewirtschaftsgesetz. Vorgaben, die der kerntechnischen Sicherheit dienen, dienen in der Regel gleichzeitig auch der Verfügbarkeit und damit der Versorgungssicherheit, tun dies aber nicht vorrangig und zwangsläufig. Würden für Kernkraftwerke sowohl die SEWD-Richtlinie IT als auch der Katalog der Netzagentur gelten, müsste im Einzelfall geklärt werden, ob die Vorrangregelung des § 11 Absatz 1b Satz 3 EnWG-E greift. Außerdem müsste die Bundesnetzagentur bei der Erstellung ihres Katalogs mindestens sechs atomrechtliche Genehmigungs- und Aufsichtsbehörden beteiligen. Außerdem würde die im Gesetzentwurf vorgesehene Konstruktion zu sich überschneidenden Zuständigkeiten der Bundesnetzagentur und der atomrechtlichen Aufsichtsbehörden führen.

Der Gegenvorschlag zielt darauf ab, die Vorgaben für die IT-Sicherheit und die Aufsicht über deren Einhaltung ausschließlich dem Atomrecht zuzuordnen. Danach würde für Kernkraftwerke nur die SEWD-Richtlinie IT gelten, die vom Bundesministeriums für Umwelt, Naturschutz, Bau und Reaktorsicherheit mit der Bundesnetzagentur daraufhin abzustimmen wäre, ob auch die Bedürfnisse der Versorgungssicherheit abgedeckt werden. Die atomrechtlichen Vorgaben können auf Vorschlag der Bundesnetzagentur um allein der Versorgungs-sicherheit dienende Vorgaben ergänzt werden, sofern sie dem Schutzzweck des Atomgesetzes nicht zuwiderlaufen.

Die vorgeschlagene Regelung stellt sicher, dass – bei einem Konflikt zwischen Versorgungssicherheit und kerntechnischer Sicherheit – die kerntechnische Sicherheit Vorrang hat und dass hierüber die für die kerntechnische Sicherheit zuständige oberste Bundesbehörde (im üblichen Regelsetzungsverfahren unter Beteiligung der Länder) entscheidet.

Im Übrigen wurde der im Gesetzentwurf verwendete Begriff "Funktionsfähigkeit" durch "Verfügbarkeit" ersetzt, da es für die Versorgungssicherheit auf

die Verfügbarkeit ankommt. Eine Anlage kann durchaus voll funktionsfähig sein und trotzdem unverfügbar sein.

Zu § 44b Absatz 2 - neu - und Absatz 3 - neu - AtG:

§ 44b Absatz 2 - neu - und Absatz 3 - neu - AtG stellt sicher, dass Meldungen über Störungen der IT in Kernkraftwerken schnellstmöglich das BSI und die Bundesnetzagentur erreichen. Es erscheint jedoch unerlässlich, dass diese Meldungen mit einer sicherheitstechnischen Bewertung durch die zuständige atomrechtliche Aufsichtsbehörde versehen werden. Dies schließt nicht aus, dass sich Betreiber von Kernkraftwerken bei Bedarf auch direkt der Beratung und Hilfe durch das BSI bedienen.

Im Übrigen ist bei Bedarf eine schnelle Information anderer Kraftwerksbetreiber auch schon über die Quermeldungen der Kernkraftwerksbetreiber untereinander sichergestellt.

Durch die entsprechende Anwendung von § 11 Absatz 1c Satz 5 bis 8 EnWG-E wird das besondere Interesse der Meldeverpflichteten und der atomrechtlichen Genehmigungs- und Aufsichtsbehörden an einer vertraulichen Behandlung der von ihnen gemeldeten Informationen berücksichtigt. Die hochsensiblen sicherheitskritischen Informationen unterliegen insbesondere im Hinblick auf die öffentliche Sicherheit einem besonderen Schutzbedürfnis.

Zu Buchstabe c:

Es handelt sich um eine Folgeänderung zum Änderungsvorschlag in Buchstabe b.

7. Zu Artikel 1 Nummer 8 Buchstabe a (§ 10 Absatz 1 Satz 1 BSIG)

In Artikel 1 Nummer 8 Buchstabe a ist in § 10 Absatz 1 Satz 1 das Wort "Wirtschaftsverbände" durch das Wort "Branchenverbände" zu ersetzen.

Begründung:

Unter den Begriff "Branchenverband" fällt auch der im Gesetzentwurf an dieser Stelle bislang verwendete Begriff "Wirtschaftsverband" und umfasst zudem auch die technischen Regelsetzer. In Artikel 1 Nummer 7 (§ 8a Absatz 2 Satz 1 BSIG-E) wird der Begriff "Branchenverband" in einem ähnlichen Zusammenhang bereits verwendet.

8. Zu Artikel 1 Nummer 8 Buchstabe a (§ 10 Absatz 1 Satz 1 BSIG),

Buchstabe b (§ 10 Absatz 2 BSIG),

Buchstabe c (§ 10 Absatz 3 Satz 3 BSIG)

In Artikel 1 Nummer 8 Buchstabe a § 10 Absatz 1 Satz 1, Buchstabe b § 10 Absatz 2 und Buchstabe c § 10 Absatz 3 Satz 3 ist jeweils das Wort "nicht" zu streichen.

Begründung:

Mit der Streichung des Wortes "nicht" in § 10 Absatz 1 Satz 1, Absatz 2 und Absatz 3 Satz 3 BSIG-E werden föderale Aspekte bei der Bestimmung Kritischer Infrastrukturen durch Rechtsverordnung berücksichtigt, zumal das Gesetz bei den Ländern – zumindest mittelbar – bedeutenden Erfüllungsaufwand auslösen wird.

9. Zu Artikel 5 Nummer 2 (§ 100 Absatz 1 TKG)

Artikel 5 Nummer 2 ist zu streichen.

Begründung:

Grundsätzlich besteht kein Änderungsbedarf.

Gemäß § 100 Absatz 1 TKG-E sollen Telekommunikationsanbieter die erweiterten Befugnisse erhalten, Nutzungsdaten "zum Erkennen, Eingrenzen und Beseitigen von Störungen sowie von Missbrauch seiner für Zwecke seines Telemedienangebots genutzten technischen Einrichtungen" zu erheben und zu verwenden. Bei der damit eingeführten Speicherbefugnis handelt es sich im Kern um eine weitreichende Vorratsdatenspeicherung, für die unter anderem das Bundesverfassungsgericht und der Europäische Gerichtshof enge Grenzen gesetzt haben. Die im Gesetzentwurf vorgesehene Speicherung von Informationen führt im Kern zu keiner Verbesserung der Informationssicherheit, sondern könnte zu einer weiteren Gefahrenquelle werden.

10. Zum Gesetzentwurf allgemein

Der Bundesrat bittet die Bundesregierung, die finanziellen Auswirkungen des Gesetzgebungsvorhabens auf die Länder und Kommunen vor allem unter folgenden Gesichtspunkten näher zu prüfen und darzulegen:

a) Die Verwaltungen der Länder und Kommunen gehören nicht zu den vom BSI-Gesetz adressierten Kritischen Infrastrukturen, weil der Bund hierfür keine Gesetzgebungskompetenz besitzt. Gleichwohl können Länder und Kommunen von der Neuregelung betroffen sein, wenn sie als Teil der Wirtschaft agieren (zum Beispiel: kommunale Wasser- und Energieversorgung). Darüber hinaus werden voraussichtlich die Zuschussbedarfe für die von den Ländern mitfinanzierten Infrastrukturen steigen (zum Beispiel: Krankenhaus, Rettungsdienst, öffentlicher Personennahverkehr).

b) Es ist davon auszugehen, dass wie bei der Bundesverwaltung faktisch auch bei den Verwaltungen der Länder und Kommunen personeller und sachlicher Mehraufwand, zum Beispiel für die verstärkte Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik oder für die Auswertung der Berichte zu den kritischen Infrastrukturen entstehen wird.

Um eine Bewertung des Gesetzentwurfs vornehmen zu können, müssen die finanziellen Auswirkungen bekannt sein. Der Bundesrat bittet deshalb die Bundesregierung, gemeinsam mit den Ländern und Kommunen eine umfassende Kostenschätzung vorzunehmen.

Anlage 4

Gegenäußerung der Bundesregierung

Die Bundesregierung nimmt zur Stellungnahme des Bundesrates vom 6. Februar 2015 wie folgt Stellung:

Zu Nummer 1

Zu Buchstabe a

Die Bundesregierung begrüßt, dass der Gesetzentwurf vom Bundesrat grundsätzlich positiv bewertet wird.

Zu Buchstabe b

Die Verwendung unbestimmter Rechtsbegriffe im Gesetzentwurf der Bundesregierung ist verfassungsrechtlich nicht zu beanstanden und genügt nach der Rechtsprechung des Bundesverfassungsgerichts insbesondere dem Gebot hinreichender Bestimmtheit aus Artikel 20 Absatz 3 des Grundgesetzes („Rechtsstaatsprinzip“)

(BVerfGE 21, 73, 79). Im Hinblick auf die Vielschichtigkeit mancher Lebenssachverhalte ist die Verwendung wertausfüllungsbedürftiger Begriffe oftmals unvermeidbar (BVerfGE 78, 205.213). Durch eine weitergehende Konkretisierung der Rechtsbegriffe entstünde zudem die Gefahr, dass – in einem insgesamt sehr dynamischen Umfeld – konkrete künftige Entwicklungen nicht mehr erfasst werden könnten. Die Verwendung unbestimmter Rechtsbegriffe macht den Gesetzentwurf demgegenüber zukunfts- und technologieoffen. Soweit möglich, erfolgt eine weitergehende Konkretisierung der Rechtsbegriffe in der Gesetzesbegründung.

Die vom Bundesrat erbetene Präzisierung des Begriffs der „Kritischen Infrastrukturen“ im Sinne des BSI-Gesetzes (BSIG) bedarf der sektor- und branchenspezifischen Einbeziehung aller betroffenen Kreise und kann nur in einem gemeinsamen Arbeitsprozess mit Vertretern der möglicherweise betroffenen Betreiber Kritischer Infrastrukturen und unter Einbeziehung der Expertise von externen Fachleuten erarbeitet werden. Dieser Prozess wird in § 10 Absatz 1 BSIG-E ausdrücklich und vollumfänglich abgebildet. In der Gesetzesbegründung zu § 10 Absatz 1 des BSIG-E wird darüber hinaus bereits detailliert die Methodik beschrieben, nach der eine Bestim-

mung der Kritischen Infrastrukturen im Rahmen der Rechtsverordnung erfolgen soll. Da die von den Verpflichtungen des Gesetzentwurfs erfassten Betreiber Kritischer Infrastrukturen nach Inkrafttreten der Rechtsverordnung eine Frist von zwei Jahren zur Umsetzung von IT-Sicherheitsstandards haben, besteht auch keine Rechts- und Planungsunsicherheit.

Zu Buchstabe c

Aus § 8b Absatz 2 des BSIG-E ergibt sich im Einzelnen, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit den dort eingehenden Meldungen zu verfahren hat. Das BSI als Informationssicherheitsbehörde des Bundes legt bei der Sicherung seiner eigenen Datenverarbeitung höchste Standards an. Dies wird auch für die nach dem IT-Sicherheitsgesetz zu speichernden Daten der Fall sein. Entsprechende Standards können untergesetzlich festgeschrieben werden. Zusätzlichen Gesetzgebungsbedarf gibt es hierzu nicht.

Zu Nummer 2

Zu Buchstabe a

Das nationale Beratungsangebot des BSI - auch in Richtung Länder - ist als Aufgabe des BSI in § 3 Absatz 1 Nummer 14 BSIG bereits hinreichend festgeschrieben. § 1 Absatz 1 Satz 2 BSIG-E soll demgegenüber die gestiegene Bedeutung der Aufgaben des BSI jenseits der Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes in allgemeiner Form nachvollziehen.

Zu Nummer 3

§ 7 Absatz 1 Satz BSIG-E sieht die Möglichkeit einer Warnung „an die betroffenen Kreise“, zu dem auch die Betreiber Kritischer Infrastrukturen gehören können, vor. Eine entsprechende Information der Anbieter informationstechnischer Dienste entspricht im Übrigen der heutigen Praxis des BSI. Die Bundesregierung hält allerdings eine entsprechende klarstellende Ergänzung im Gesetzestext für wünschenswert.

Zu Nummer 4

Die in § 7a BSIG-E vorgesehenen Produktuntersuchungen überschneiden sich nicht mit den konkreten Untersuchungsbefugnissen der Bundesnetzagentur, da das BSI nicht die in einem

Unternehmen konkret eingesetzten, sondern nur im Rahmen seiner Zuständigkeit allgemein am Markt verfügbare Produkte auf ihre generelle Sicherheitstauglichkeit untersuchen kann.

Zu Nummer 5

Nach Auffassung der Bundesregierung trägt der Formulierungsvorschlag nicht zu einer Konkretisierung der Informationspflichten des BSI gegenüber den Ländern bei. Es ist zudem nicht ersichtlich, warum bei der Informationspflicht des BSI gegenüber Landesbehörden ein anderer Maßstab gelten soll, als dies gegenüber Bundesbehörden (§ 8b Absatz 2 Nummer 4 Buchstabe b BSIG-E) der Fall ist.

Zu Nummer 6

Zu Buchstabe a

Nach Auffassung der Bundesregierung dient die Aufnahme der „Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes“ in § 8c Absatz 2 Nummer 3 BSI-E der Regelungsklarheit.

Zu Buchstabe b

Nach Auffassung der Bundesregierung sollte eine Vermischung der Schutzziele „nukleare Sicherheit“ und „Versorgungssicherheit“ im Atomgesetz vermieden werden. Die Vorgaben zur Versorgungssicherheit decken sich nicht mit den Schutzzielen des Atomgesetzes und können daher auch nicht in den IT-Regelungen für kerntechnische Anlagen und Einrichtungen geregelt werden. Der Vorschlag des Bundesrates, „die Vorgaben für die IT-Sicherheit und die Aufsicht über deren Einhaltung ausschließlich dem Atomrecht zuzuordnen“, ist abzulehnen, da die atomrechtliche Aufsicht im Wege der Bundesauftragsverwaltung durch die Länder ausgeübt wird und die Zuständigkeit für die Aufsicht über die Versorgungssicherheit bei der Bundesnetzagentur liegt.

§ 44b des Atomgesetzes in der Fassung des Gesetzentwurfs stellt sicher, dass alle Inhaber von Genehmigungen nach den §§ 6, 7 und 9 des Atomgesetzes von der Meldepflicht erfasst werden. Die vom Bundesrat vorgeschlagene Beschränkung auf Anlagen nach § 7 Absatz 1 des Atomgesetzes, die als Kritische Infrastruktur eingestuft worden sind, wird abgelehnt. Um ein einheitlich geltendes effektives Meldewesen aufzubauen, sind von der Meldepflicht alle Inhaber von Ge-

nehmigungen nach den §§ 6, 7 und 9 des Atomgesetzes zu erfassen, und zwar unabhängig von der Frage ihrer Einstufung als Kritische Infrastruktur im Sinne des BSI-Gesetzes.

Der Gesetzentwurf sieht vor, dass die Meldungen zunächst unverzüglich an das BSI zu senden sind, das diese Meldungen wiederum unverzüglich an die für die nukleare Sicherheit und Sicherung zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder weiterleitet. Hierdurch wird gewährleistet, dass vergleichbare Vorfälle, die bei Betreibern verschiedener Anlagen auftreten, schnell erkannt werden können. Eine vorgeschaltete sicherheitstechnische Bewertung durch die jeweils zuständige atomrechtliche Aufsichtsbehörde des Landes würde das bundesweite Lagebild durch das BSI unnötig verzögern und kann im Nachgang erfolgen.

Aus Sicht der Bundesregierung ist aber denkbar, dass eine parallele Meldung durch den Betreiber an das BSI und die zuständigen atomrechtlichen Genehmigungs- und Aufsichtsbehörden der Länder erfolgt, um eine parallele Information der Aufsichtsbehörden zu gewährleisten.

§ 44b Satz 1 AtG würde dann wie folgt lauten:

„Genehmigungsinhaber nach den §§ 6, 7 und 9 haben Beeinträchtigungen ihrer

informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer Gefährdung oder Störung der nuklearen Sicherheit der betroffenen kerntechnischen

Anlage oder Tätigkeit führen können oder bereits geführt haben, unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik als zentrale Meldestelle sowie an die zuständigen Aufsichts- und Genehmigungsbehörden des Bundes und der Länder zu melden."

Zu Buchstabe c

Nummer 6 Buchstabe b) folgend ergibt sich nach Auffassung der Bundesregierung kein Änderungsbedarf.

Eine Vermischung der Schutzziele „nukleare Sicherheit" und „Versorgungssicherheit" im Atomgesetz soll vermieden werden. Durch das Atomgesetz bzw. durch Regelungen auf Grundlage des Atomgesetzes wird die Sicherstellung der Infrastrukturleistung von Kernkraftwerken für die Stromversorgung nicht abgedeckt. Regelungen, die für die Sicherstellung der Stromversorgung zu treffen sind, müssen daher vom EnWG getroffen werden und sollten auch die Kernkraftwerke

umfassen, sofern diese nicht eindeutig aus dem Bereich der kritischen Infrastrukturen für die Sicherstellung der Stromversorgung ausgenommen werden.

Für den aus Sicht der Bundesregierung denkbaren und nicht unwahrscheinlichen Fall, dass Anforderungen und Maßnahmen zur Versorgungssicherheit dem Schutzziel der nuklearen Sicherheit und Sicherung zuwider laufen, bedarf es einer materiellen Kollisionsnorm, die den Vorgaben auf Grund des Atomgesetzes Vorrang einräumt.

Eine Beteiligung der atomrechtlichen Genehmigungs- und Aufsichtsbehörden an der Erarbeitung des Katalogs der Sicherheitsanforderungen ist nach Auffassung der Bundesregierung erforderlich, um sicherzustellen, dass es keinen Konflikt zwischen den Anforderungen und Maßnahmen auf Grundlage dieses Sicherheitskatalogs und den Maßnahmen auf Grundlage des Atomgesetzes geben wird. Die Beurteilung, ob ein solcher Konflikt zu erwarten ist, wird für einzelne Anforderungen nur durch die Aufsichtsbehörden der vier Länder mit Kernkraftwerken im Leistungsbetrieb möglich sein, die die konkrete Situation in den Anlagen kennen. Das Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit ist im Hinblick auf seine Funktion innerhalb der Bundesauftragsverwaltung ebenfalls zu beteiligen.

Das Regelwerk der nuklearen Sicherung unterliegt den Bestimmungen des Geheimschutzes, so dass die dort getroffenen Anforderungen nur offengelegt werden können, soweit eine Kenntnis erforderlich ist. Ob dies erforderlich ist, wird sich im Rahmen der Beteiligung zeigen.

Zu Nummer 7

Die Bundesregierung stimmt im Interesse einer einheitlichen Gesetzesanwendung der Auffassung des Bundesrates zu. Sie hält eine Verwendung des Begriffes „Branchenverbände“ sowohl in § 8a Absatz 2 Satz 1 BSIG-E als auch in § 10 Absatz 1 Satz 1 BSIG-E für wünschenswert.

Zu Nummer 8

Es besteht keine Zustimmungsbedürftigkeit der Rechtsverordnung von Verfassungs wegen. Eine solche ist auch in der Sache nicht geboten, da es bei der Festlegung der Kritischen Infrastrukturen im Sinne des BSI-Gesetzes aus Bundesperspektive um die Frage geht, bei welchen

Infrastrukturen ein Ausfall der IT aus nationaler Sicht nicht hinnehmbar wäre. Die Bundesregierung weist aber darauf hin, dass sie der in

§ 62 Absatz 2 Satz 1 in Verbindung mit § 47 GGO vorgesehenen Einbeziehung der Länder in den Prozess der Erstellung der Rechtsverordnung aufgrund der für Bund und Länder in gleicher Weise relevanten Erreichung der Ziele, die mit dem IT-Sicher-heitsgesetz verfolgt werden, besondere Bedeutung beimisst.

Zu Nummer 9

Die Bundesregierung stimmt der Auffassung des Bundesrates nicht zu. § 100 Ab-satz 1 TKG in der derzeit geltenden Fassung enthält das Recht von Telekommunikationsdiensteanbietern, soweit erforderlich zum Erkennen, Eingrenzen und Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen Bestandsdaten und Verkehrsdaten zu erheben und zu verwenden. Die im Gesetzentwurf hierzu vorgesehene Ergänzung dient lediglich der Klarstellung, dass hiervon auch solche Störungen erfasst werden, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können.

Das in der Begründung des Bundesrates wiedergegebene Zitat findet sich im Übrigen nicht im Gesetzentwurf der Bundesregierung.

Zu Nummer 10

Zu den Buchstaben a und b

Soweit Länder und Kommunen als Teil der Wirtschaft agieren, gelten für sie die Ausführungen in dem Gesetzentwurf zum Erfüllungsaufwand für die Wirtschaft entsprechend. Weitergehende Aussagen zu möglichen finanziellen Auswirkungen auf die Länder und Kommunen können erst nach Abschluss der Arbeiten an der Rechtsverordnung nach § 10 Absatz 1 BSIG-E getroffen werden. Wie bereits in der Gegenäußerung zu Nummer 8 ausgeführt, misst die Bundesregierung der Einbeziehung der Länder in diesen Prozess besondere Bedeutung bei.