Entwurf eines Bundesgesetzes über die Informationssicherheit (ISG)

Erläuternder Bericht

---

vom 26. März 2014

Übersicht

Information ist die Währung der Informationsgesellschaft. Die Bundesbehörden tragen die Verantwortung für den sicheren Umgang mit den Informationen, die sie oder ihre unterstellten Organisationen im Auftrag und im Namen der Schweiz bearbeiten. Um diese Verantwortung wahrnehmen zu können, müssen sie über zeitgemässe Instrumente verfügen. Die Gefahren und Bedrohungen für Informationen sind mit der Entwicklung zu einer Informationsgesellschaft komplexer und dynamischer geworden. Mehrere Angriffe auf Informationssysteme des Bundes haben aufgezeigt, dass der Schutz von Informationen Lücken aufweist. Diese Lücken, insbesondere im organisatorischen Bereich, sind auch auf unzeitgemässe oder inkohärente Rechtsgrundlagen zurückzuführen.

Der vorliegende Gesetzesentwurf schafft - basierend auf international anerkannten Standards - einheitliche formell-gesetzliche Grundlagen für das Management der Informationssicherheit im Zuständigkeitsbereich des Bundes. Dabei strebt er an, den Schutz der Informationen und die Sicherheit beim Einsatz von Informations- und Kommunikationstechnologien (IKT) an die Anforderungen einer modernen, vernetzten Informationsgesellschaft anzupassen sowie Lücken und Schwachstellen des geltenden Rechts zu beheben.

Kernpunkte des Entwurfs

Informationssicherheit

Der Begriff "Informationssicherheit" erfasst "sämtliche Anforderungen und Massnahmen, die zum Schutz der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Informationen dienen, und zwar unabhängig davon, ob die Informationen elektronisch, mündlich oder in Papierform bearbeitet werden".

Die bestehenden Rechtsgrundlagen für die Festlegung solcher Anforderungen und die Umsetzung von Massnahmen sind beim Bund sehr sektoriell ausgelegt, kaum aufeinander abgestimmt und oft lückenhaft. Dasselbe gilt für die organisatorischen Zuständigkeiten. So betreibt der Bund heute sowohl rechtlich also auch organisatorisch parallele Organisationen für den Datenschutz, den Informationsschutz (Schutz klassifizierter Informationen), die Informatiksicherheit, die Personensicherheit, die physische Sicherheit und das Risikomanagement. Die Praxis hat gezeigt, dass diese sektorielle Ausrichtung nicht effizient ist. Der Entwurf fasst deshalb die wichtigsten Massnahmen für den Schutz von Informationen in einer einzigen, einheitlichen Regelung zusammen. Er sieht ferner eine einzige Struktur vor, um die Belange der Informationssicherheit rechtlich und organisatorisch integral zu steuern und zu überprüfen.

Institutioneller Geltungsbereich

Der Umfang des zunehmend elektronischen Informationsaustauschs unter Behörden sowie zwischen Behörden und Privaten (inkl. Wirtschaft) hat stark zugenommen. Die Schutzwürdigkeit einer Information hängt aber nicht davon ab, welche Stelle oder Person sie bearbeitet. IKT-Infrastrukturen und Systeme werden zudem vermehrt untereinander vernetzt. Dadurch wird das Risiko erhöht, dass sich Angriffe sowie Bedrohungen gegen eine Behörde auf die Zuständigkeitsbereiche anderer beteiligten Behörden ausbreiten können. Es ist daher notwendig, ein einheitliches, behördenübergreifendes Sicherheitsniveau festzulegen, um einerseits das gegenseitige Vertrauen der Bundesbehörden bei der Informationsbearbeitung zu gewährleisten, andererseits aber auch, um das Risiko für alle beteiligten Behörden zu reduzieren.

Vom primären Geltungsbereich des Entwurfs werden deshalb alle Bundesbehörden (die Bundesversammlung, die eidgenössischen Gerichte, der Bundesrat, die Bundesanwaltschaft, die Aufsichtsbehörde über die Bundesanwaltschaft und die Nationalbank) sowie die ihnen unterstellten Organisationen (die Parlamentsdienste, die Verwaltungen der eidgenössischen Gerichte, die Bundesverwaltung und die Armee) erfasst werden. Soweit die Kantone oder Dritte mit der Bearbeitung von Informationen des Bundes betraut werden oder Zugang zu seinen IKT-Mitteln erhalten, müssen die Vorgaben des Bundes für sie ebenfalls verbindlich sein.

Risikomanagement

Die Komplexität und Dynamik der Bedrohungen erfordert von den Bundesbehörden, dass sie den Fokus vermehrt auf die systematische Bewertung des Schutzbedarfs von Informationen und auf die Beurteilung der entsprechenden Risiken setzen. Dies setzt ein wirksames Risikomanagement im Bereich der Informationssicherheit sowie eine regelmässige Überprüfung der Umsetzung von risikomindernden Massnahmen voraus. Beides fehlt heute weitgehend. Deshalb initialisiert der Entwurf auch einen Prozess zur nachhaltigen und wirtschaftlichen Aufrechterhaltung der Informationssicherheit.

Klassifizierung von Informationen

Aufgrund der höhten Erwartungen der Bürgerinnen und Bürger an die Transparenz der Bundesbehörden legt die Vorlage die Kriterien für die Klassifizierung von Informationen des Bundes transparent fest und erhöht zudem die Schwellenwerte für die Klassifizierung. Das Öffentlichkeitsprinzip der Bundesverwaltung wird durch die Bestimmungen zur Klassifizierung in keinerlei Weise eingeschränkt.

Sicherheit beim Einsatz von IKT

Der Entwurf trägt der Erkenntnis Rechnung, dass die Gewährleistung der Informationssicherheit beim Einsatz der IKT seit einigen Jahren stark an Bedeutung gewonnen hat. Er legt einen Mechanismus zur Beurteilung der Kritikalität von IKT-Mitteln fest und verknüpft diese Beurteilung mit der Umsetzung entsprechender Sicherheitsmassnahmen. Der Fokus soll dabei hauptsächlich auf die Sicherheit der kritischsten IKT-Systeme und Mittel gesetzt werden. Die Vorlage verstärkt die strategische und operationelle Rolle der Behörden bei der Umsetzung von Massnahmen sowie das Auditwesen.

Personensicherheitsprüfungen (PSP)

Die PSP stellen in erster Linie eine Massnahme der Informationssicherheit dar. Sie werden deshalb vom BWIS in das neue Informationssicherheitsgesetz übertragen. Gleichzeitig werden bestehende Mängel der heutigen Regelung behoben und es wird eine Straffung der PSP angestrebt. Die Prüfgründe werden angepasst an die heutigen Bedürfnisse der Informationssicherheit. Es wird von drei auf zwei Prüfstufen reduziert. Die Datenerhebung wird für beide Prüfstufen angepasst. Inskünftig sollen weniger, aber risikogerechtere Prüfungen durchgeführt werden.

Betriebssicherheitsverfahren (BSV)

Das BSV ist anwendbar auf Unternehmen, die im Rahmen einer öffentlichen Beschaffung des Bundes mit der Ausübung sicherheitsempflindlicher Tätigkeiten beauftragt werden sollen. Es dient einerseits der Prüfung der Vertrauenswürdigkeit dieser Unternehmen und ermöglicht es andererseits, die Wahrung der Informationssicherheit während der Ausführung des Auftrags zu kontrollieren und durchzusetzen. Der Anwendungsbereich des heutigen Geheimschutzverfahrens ist auf klassifizierte Aufträge aus dem militärischen Bereich beschränkt. Mit der Vorlage wird ein einheitliches BSV eingeführt. Gleichzeitig wird eine Grundlage für die Abgabe behördlicher Sicherheitserklärungen zu Gunsten von Schweizer Unternehmen geschaffen, die sich für ausländische oder internationale Aufträge bewerben und hierfür eine nationale Sicherheitserklärung benötigen. Dadurch wird die Wettbewerbsfähigkeit dieser Unternehmen gestärkt.

Unterstützung der kritischen Infrastrukturen (KI)

In seiner Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken vom 27. Juni 2012 (BBl 2013 563) hat der Bundesrat den Grundsatz der Unterstützung der KI-Betreiber durch den Bund im Bereich der Informationssicherheit festgelegt. Im Rahmen der Zusammenarbeit zwischen den KI-Betreibern und dem Bund müssen die zuständigen Stellen Personendaten (Adressierungselemente im Fernmeldebereich) austauschen können, die eventuell im Zusammenhang mit administrativen und strafrechtlichen Verfolgungen und Sanktionen stehen. Der Entwurf schafft die formell-gesetzliche Grundlage, die für die Bearbeitung solcher Personendaten erforderlich ist.

Vollzug

Der Vollzug dieses Gesetzes soll einerseits möglichst einheitlich erfolgen; andererseits müssen die Unabhängigkeit und Organisationsautonomie der jeweiligen Bundesbehörden gewahrt werden. Der Vorentwurf berücksichtigt diese an sich widersprüchlichen Anforderungen mit drei Mechanismen:

- *"Opting-out"-Regelung für den Vollzug: Jede Behörde vollzieht den Erlass in ihrem Bereich selbständig und erlässt entsprechendes Verordnungsrecht. Das Vollzugsrecht des Bundesrates gilt jedoch für die übrigen Bundesbehörden sinngemäss, solange und soweit sie keine eigenen Regelungen erlassen.*
- *Standardanforderungen und -massnahmen: Der Bundesrat wird ermächtigt, standardisierte Anforderungen und Massnahmen nach dem Stand der Lehre und der Technik festzulegen. Diese gelten für die anderen Bundesbehörden als Empfehlungen.*
- *Schaffung eines behördenübergreifenden Koordinationsorgans: Dieses Organ (Konferenz der Informationssicherheitsbeauftragten) dient hauptsächlich dem einheitlichen, behördenübergreifenden und risikobasierten Vollzug des Gesetzes. Es wird auch bei der Festlegung der Standardanforderungen und -massnahmen berücksichtigt.*

Mit der vorgeschlagenen Lösung wird die Unabhängigkeit der Bundesbehörden beim Vollzug bewahrt. Da die Bundesbehörden den Ausführungsbestimmungen des Bundesrats nicht unterstellt werden dürfen, müssen alle minimalen Anforderungen und Massnahmen, die zwingend für alle Behörden gelten sollen, im Gesetz selbst verankert werden. In der Folge enthält das Gesetz viele Bestimmungen, die von der Normenhierarchie her normalerweise auf Verordnungsebene hätten verankert werden können. Die Vorlage bewahrt auch eine hinreichende Vollzugsautonomie für die Kantone und bestimmte Organisationen, die dem Gesetz und dem Ausführungsrecht des Bundesrats unterstellt werden. Schliesslich schafft der Entwurf die heute fehlende formell-gesetzliche Grundlage für den Abschluss von internationalen Vereinbarungen im Bereich der Informationssicherheit durch den Bundesrat.

Organisation der Informationssicherheit

Der Entwurf passt die Fachorganisation der Informationssicherheit an diese neue komplexe und dynamische Realität an. Dies geschieht auf zwei Organisationsebenen:

- *Interne Organisation:*
  - *Management der Informationssicherheit: Die Bundesbehörden sollen sich beim Management der Informationssicherheit nach international anerkannten, in der Praxis erprobten Fachnormen richten (z.B. DIN ISO/IEC Normen 27'001 und 27'002).*
  - *Informationssicherheitsbeauftragte: Die Bundesbehörden sollen eine/n Informationssicherheitsbeauftragte/n sowie eine Stellvertretung bezeichnen, die oder der für die Steuerung aller Belange der Informationssicherheit zuständig sein wird.*
- *Übergreifende Organisation:*
  - *Fachstelle des Bundes für Informationssicherheit: Bestimmte bestehende Organe sollen in einer neuen Fachstelle zusammengeführt werden, um erkannte Zuständigkeitsprobleme systemisch zu lösen und das interdisziplinäre Fachwissen zu erhöhen. Dieser Fachstelle, die unterstützend und beratend agieren soll, kommen aufgrund der Unabhängigkeit der jeweiligen Bundesbehörden im behördenübergreifenden Rahmen keine Weisungsbefugnisse zu. Das Ausführungsrecht des Bundesrats wird die Ansiedelung und die detaillierten Aufgaben der Fachstelle regeln.*
  - *Konferenz der Informationssicherheitsbeauftragten: Dieses Organ dient hauptsächlich dem einheitlichen und behördenübergreifenden Vollzug des Gesetzes. Bei Bedarf sollen auch Experten aus den Kantonen, der Wissenschaft oder der Privatwirtschaft einbezogen werden.*
  - *Fachstellen für Personensicherheitsprüfungen: Der Bundesrat wird zur Sicherstellung unabhängiger Prüfungen wie bis anhin mindestens zwei Fachstellen einsetzen.*
  - *Fachstelle für Betriebssicherheit: Zur Durchführung des BSV muss der Bundesrat eine Fachstelle einsetzen.*

<u>Auswirkungen</u>

Das Gesetz wird eine wesentliche Verbesserung des Managements der Informationssicherheit im Bund bewirken. Somit werden die entsprechenden Risiken, die teilweise auch finanzieller Art sind, reduziert. Die Praxis hat gezeigt, dass ein effizientes Management der Informationssicherheit mittelfristig sogar zu Kosteneinsparungen führen kann. Das Gesetz wird für den Bund aber auch direkte finanzielle und personelle Auswirkungen nach sich ziehen. Der Mehrbedarf kann zurzeit noch nicht sachgemäss abgeschätzt werden. Er wird in der Botschaft transparent ausgelegt. Nachfolgend sind die Hauptkostentreiber aufgeführt:

- *die Organisation, Steuerung und Überprüfung der Informationssicherheit*
- *das verstärkte Kontroll- und Auditwesen*
- *die Personensicherheitsprüfungen*
- *das Betriebssicherheitsverfahren*
- *die Schaffung der Fachstelle des Bundes für Informationssicherheit und die Aufgaben derselben*

Zu beachten ist, dass das Gesetz selbst fast keine detaillierten Massnahmen festlegt und deshalb nicht direkt umsetzbar ist: Die jeweiligen Bundesbehörden müssen ihre eigenen Ausführungsbestimmungen erlassen. Massgebend für die Beurteilung der Vollzugskosten werden deshalb das von ihnen festzulegende Sicherheitsniveau sein sowie die daraus abzuleitenden organisatorischen, personellen, technischen und baulichen Massnahmen, welche sie nach sachgerechten "Kosten-Nutzen"-Analysen auf Verordnungs-, Weisungs- oder Projektebene beschliessen werden.

Die Auswirkungen auf die Kantone werden gering ausfallen. Volkswirtschaft und Gesellschaft sind vom Entwurf kaum betroffen.

Inhaltsverzeichnis

Erlasse, die mit Abkürzung zitiert werden

AnlageschutzG	Bundesgesetz vom 23. Juni 1950 über den Schutz militärischer Anlagen; SR **510.518**
BGA	Archivierungsgesetz vom 26. Juni 1998; SR **152.1**
BGÖ	Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeitsprinzip der Verwaltung; SR **152.3**
BinfV	Bundesinformatikverordnung vom 9. Dezember 2011; SR **172.010.58**
BöB	Bundesgesetz vom 16. Dezember 1994 über das öffentliche Beschaffungswesen; SR **172.056.1**
BPG	Bundespersonalgesetz vom 24. März 2000; SR **172.220.1**
BPI	Bundesgesetz vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes; SR **361**
BGG	Bundesgerichtsgesetz vom 17. Juni 2005; SR **173.110**
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999; SR **101**
BWIS	Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit; SR **120**
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz; SR **235.1**
FHG	Bundesgesetz vom 7. Oktober 2005 über den eidgenössischen Finanzhaushalt; SR **611.0**
GeheimschutzVO	Geheimschutzverordnung vom 29. August 1990 des VBS; SR **510.413**
HMG	Bundesgesetz vom 15. Dezember 2000 über Arzneimittel und Medizinprodukte; Heilmittelgesetz; SR **812.21**
ISA CH-EU	Abkommen vom 28. April 2008 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Union über die Sicherheitsverfahren für den Austausch von Verschlusssachen; SR **0.514.126.81**
ISchV	Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes; SR **510.411**
KEG	Kernenergiegesetz vom 21. März 2003; SR **732.1**
MG	Militärgesetz vom 3. Februar 1995; SR **510.10**
MStG	Militärstrafgesetz vom 13. Juni 1927; SR **321.0**
MIG	Bundesgesetz vom 3. Oktober 2008 über die militärischen Informationssysteme; SR **510.91**
MStP	Militärstrafprozess vom 23. März 1979; SR **322.1**
NBG	Bundesgesetz vom 3. Oktober 2003 über die Schweizerische Nationalbank; Nationalbankgesetz, SR **951.11**
StGB	Schweizerisches Strafgesetzbuch vom 13. Juni 1937; SR **311.0**
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007; SR **321.0**
StromVG	Bundesgesetz vom 23. März 2007 über die Stromversorgung; Stromversorgungsgesetz; SR **734.7**
ParlG	Parlamentsgesetz vom 13. Dezember 2002171.10; SR **171.10**
PSPV	Verordnung vom 19. Dezember 2001 über die Personensicherheitsprüfungen; SR **120.4**
PSPVK	Verordnung vom 9. Juni 2006 über die Personensicherheitsprüfungen im Bereich Kernanlagen; SR **732.143.3**
RVOG	Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997; SR **172.010**
VGG	Bundesgesetz vom 17. Juni 2005 über das Bundesverwaltungsgericht; SR **173.32**
VSDG	Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz; SR **235.11**
VwVG	Bundesgesetz vom 20. Dezember 1968 über das Verwaltungsverfahren; SR **172.021**
ZNDG	Bundesgesetz vom 3. Oktober 2008 über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes; SR **121**

1 Allgemeiner Teil

1.1 Ausgangslage

1.1.1 Entwicklung der Schweiz zu einer Informationsgesellschaft

Die Welt erlebt seit einigen Jahrzehnten einen fundamentalen gesellschaftlichen Wandel, der durch die sich noch laufend beschleunigenden Entwicklungen der Informations- und Kommunikationstechnologien (IKT) gefördert wird. Von den neuen Möglichkeiten, jederzeit und überall auf Informationen zugreifen und diese austauschen zu können, sind alle Bereiche der Gesellschaft betroffen: Kultur, Wirtschaft, Bildung und Forschung, Gesundheit, Verkehr und Energie, Verteidigung, usw. Diese Entwicklungen sind zugleich unvermeidliche Begleiterscheinung und unentbehrliche Bedingung für die laufende Globalisierung. Alle Gesellschaften werden vernetzter, mobiler und mehrheitlich transparenter als je zuvor. Unsere Lebensweise hat sich innert - historisch betrachtet - kürzester Zeit grundlegend verändert.

Der Einsatz der IKT eröffnet der Schweiz bei ihrer Entwicklung zu einer Informationsgesellschaft vielfältige Chancen. Mit den neuen technischen Möglichkeiten und Vernetzungen sind aber auch Risiken verbunden, die nicht ignoriert werden dürfen. Informationen kann - als Währung der Informationsgesellschaft - ein hoher Wert zukommen. Der Verlust, der Diebstahl, die Preisgabe und der Missbrauch von Informationen oder die Störung der Mittel zu deren Bearbeitung können wesentliche öffentliche Interessen oder die Rechte Dritter schwerwiegend beeinträchtigen, erhebliche finanzielle Folgen nach sich ziehen und sogar die Erfüllung kritischer gesetzlicher Aufgaben des Bundes gefährden. Deuten schwere oder wiederholte Vorfälle darauf hin, dass der Bund seine Informationen nicht sorgfältig schützt, kann darunter überdies das Vertrauen der Bevölkerung und der ausländischen Partner der Schweiz in die Bundesbehörden dauerhaft leiden.

1.1.1.1 Strategie für eine Informationsgesellschaft in der Schweiz

Der Bundesrat ist sich der grundlegenden Bedeutung der IKT für den Wirtschaftsstandort und den Lebensraum Schweiz bewusst. Bereits 1998 hat er eine Strategie für die Informationsgesellschaft in der Schweiz verabschiedet, die 2006 und 2012 aktualisiert wurde (BBl 2012 3765). Er will die Chancen nutzen, welche die Anwendung von IKT bietet. Er hält aus diesem Grund fest, dass die IKT so eingesetzt werden sollen, dass sie zur Stärkung der gemeinsamen Wohlfahrt, der nachhaltigen Entwicklung, des inneren Zusammenhalts und der kulturellen Vielfalt des Landes beitragen. Die Strategie nennt die Handlungsfelder, in welchen das Innovationspotenzial der IKT besonders grosse Wirkung erzielen kann und definiert schwerpunktmässig den Handlungsbedarf für den Bund.

Der Bundesrat verfolgt damit zwei übergeordnete strategische Ziele:

- Der Wirtschaftsstandort Schweiz wird durch den Einsatz der IKT innovativ und international wettbewerbsfähig gestaltet.
- Die IKT werden zum Nutzen aller Menschen eingesetzt und gestalten den Lebensraum Schweiz.

Er gab im Zusammenhang mit diesem gesellschaftlichen Wandel zahlreiche Projekte in Auftrag (z.B. E-Government, E-Justice, E-Health, elektronische Geschäftsverwaltung (GEVER), usw.). Zudem erteilte er dem EJPD mehrere Aufträge zur Sicherstellung der Rechtsgrundlagen der Informationsgesellschaftsstrategie Schweiz. Aus diesen Projekten ergibt sich eine laufend komplexer und dynamischer werdende Vernetzung des Informationsaustauschs und der Systeme von Bürgern und Behörden einerseits sowie von Behörden untereinander andererseits.

1.1.1.2 Öffentlichkeitsprinzip der Bundesverwaltung

Der Bundesrat erkannte in seiner Botschaft vom 12. Februar 2003 zum BGÖ (BGÖ-Botschaft; BBl 2003 1963), dass der damals in der Verwaltung geltende Geheimhaltungsgrundsatz den Anforderungen einer effektiven demokratischen Kontrolle der Verwaltungstätigkeit durch die Bürgerinnen und Bürger nicht mehr gerecht wurde. Am 17. Dezember 2004 wurde in der Folge das Öffentlichkeitsgesetz verabschiedet. Es berechtigt jede Person, ohne besonderen Interessennachweis amtliche Dokumente einzusehen und von den Verwaltungseinheiten Auskünfte über den Inhalt amtlicher Dokumente zu erhalten.

Der Grundsatz der Öffentlichkeit hat eine Tragweite, die über den rein rechtlichen Rahmen hinausgeht. Er bedeutet, dass der Staat seine Informationen im Auftrag und im Namen des schweizerischen Volkes bearbeitet. Dieses ist jederzeit berechtigt, seine Kontrolle auszuüben. Ausnahmen vom Öffentlichkeitsprinzip sind zwar möglich, werden im Gesetz aber abschliessend aufgezählt. Wird der Zugang zu einem Dokument zum Schutz von überwiegenden öffentlichen oder privaten Interessen ausnahmsweise eingeschränkt, aufgeschoben oder verweigert, muss das entsprechende Dokument aber in der Folge auch gemäss seinem tatsächlichen Schutzbedarf geschützt werden.

1.1.1.3 Open Government Data (OGD)

OGD ist ein Konzept, das eng mit dem Öffentlichkeitsprinzip verbunden ist und das auf die Zugänglichkeit und Wiederverwendung von Daten zielt, die im Rahmen der Verwaltungstätigkeit produziert werden. Die Veröffentlichung und freie Sekundärnutzung von Behördendaten kann wirtschaftlichen, politischen und verwaltungsinternen Nutzen stiften.

In seinem Bericht vom 13. September 2013 in Erfüllung des Postulats Wasserfallen 11.3884 vom 29. September 2011 ("OGD als strategischer Schwerpunkt im E-Government") hielt der Bundesrat fest, dass die Abwägung von Chancen und Risiken von OGD zeigt, dass ein attraktives Potenzial für eine transparente, effiziente Verwaltungsführung und die wirtschaftliche Wertschöpfung besteht. Er beauftragte das Informatiksteuerungsorgan des Bundes (ISB) in Zusammenarbeit mit dem Bundesarchiv (BAR), die Federführung und Koordination bei der Weiterentwicklung von OGD zu übernehmen und eine schweizerische OGD-Strategie zu formulieren.

1.1.2 Risiken der Informationsgesellschaft

Der Bundesrat will das Risiko reduzieren, dass der gesellschaftliche Wandel zu Nachteilen für die Bevölkerung und die Wirtschaft oder zur Verletzung von Persönlichkeitsrechten führt. Es bestehen insbesondere Risiken, die nicht primär die Auswirkungen des gesellschaftlichen Wandels (z.B. sogenannte "Digitale Gräben"), sondern die Informationen selbst sowie die vernetzte Informations- und Kommunikationsinfrastruktur betreffen. Der wahre Wert von Informationen wird bedauerlicherweise oft erst nach einem Vorfall und beim Eintreten negativer Auswirkungen erkannt. Sowohl für öffentliche Stellen als auch für Unternehmen und Privatpersonen kann der Verlust, der Diebstahl, die unberechtigte Preisgabe oder der Missbrauch von Informationen äusserst unliebsame Folgen zeitigen.

Auch die Informations- und Kommunikationsinfrastruktur sowie die einzelnen IKT-Mittel, die Behörden und Unternehmen zur Unterstützung ihrer Geschäftsprozesse einsetzen, sind verwundbar. So kann der Ausfall eines Informatiksystems je nach Geschäftskritikalität erhebliche finanzielle Folgen nach sich ziehen. Wenn ein solcher Ausfall den Betreiber einer Infrastruktur betrifft, die Dienste erbringt, die für das Funktionieren der Gesellschaft, der Wirtschaft oder des Bundes unerlässlich sind (kritische Infrastruktur, KI), kann dies schlimmstenfalls katastrophale Auswirkungen, inkl. den Verlust von Menschenleben, zu Folge haben.

1.1.2.1 Gefahren für Informationen und IKT-Mittel

Die Medien berichten fast täglich über Spionage, Angriffe, Ausfälle von IKT-Diensten und sonstige Ereignisse im Bereich der Informationssicherheit. Diese Gefahren werden auch in der Nationalen Strategie vom 27. Juni 2012 zum Schutz der Schweiz vor Cyber-Risiken (NCS; BBL 2013 563, s. Ziff. 1.1.2.2) beschrieben. Für eine realistische Wahrnehmung in diesem Bereich sind drei Punkte zu beachten.

Die Gefahren müssen ernst genommen werden. Fachspezialisten haben zwar oft die Tendenz, die Gefahren und ihre potenziellen Auswirkungen zu dramatisieren. Umgekehrt dürfen die Risiken aber auch nicht unterschätzt werden. Die Geldmittel und das technische Know-how, die von der organisierten Kriminalität eingesetzt werden, um online-Kundendaten (insbesondere Bank- und Kreditdaten) zu stehlen oder Privatpersonen zu erpressen, mögen gross sein. Sie sind jedoch bloss winzig im Vergleich zu den finanziellen und personellen Mitteln, die von bestimmten staatlichen Akteuren eingesetzt werden, um politische, diplomatische, wissenschaftliche und wirtschaftliche Spionage zu betreiben. Gewisse Staaten verfolgen als prioritäre Massnahme gezielt Wirtschafts- und Industriespionage zur Industrialisierung und Weiterentwicklung ihrer Wirtschaft oder zur Modernisierung ihrer Streitkräfte.

Ernstzunehmende Gefahren bestehen überdies nicht nur in Bezug auf den Schutz der Vertraulichkeit von Informationen. Auch die Verfügbarkeit von öffentlichen oder privaten Infrastrukturen und Diensten ist wegen deren Abhängigkeit von den IKT gefährdet. Sabotageangriffe wie der im Juni 2010 entdeckte Angriff auf iranische Urananreicherungsanlagen mittels des Schadprogramms *Stuxnet* mögen die meist zitierten Gefährdungsannahmen darstellen. Betriebsstörungen wegen technischen Versagens, Fehlmanipulationen oder Elementarereignissen, wie beispielsweise einem Stromausfall oder einem Brand, kommen aber deutlich öfter vor und können ebenso gravierende Auswirkungen zur Folge haben.

Schliesslich darf die massenhafte Überwachung des Internetverkehrs, insbesondere durch die Kompromittierung von breit benutzten IKT-Diensten und Anwendungen sowie die systematische Korruption von Verschlüsselungsstandards nicht vergessen werden. Die jüngsten Enthüllungen über derartige Handlungen belegen, dass die Grundannahmen über die Integrität des Internets und der Basisdienste, von denen viele in Bezug auf die sichere Bearbeitung von Informationen ausgegangen waren, nicht zutreffen.

Es findet ein "digitales Wettrüsten" statt. Die meisten entwickelten Länder sind sich ihrer Abhängigkeit von der Informations- und Kommunikationsinfrastruktur und der damit verbundenen Bedrohungen bewusst. Sie

setzen entsprechende Schutzvorkehrungen um. Bei weitem nicht alle Staaten verfolgen aber bloss *defensive* Strategien. Viele sind daran, auch *offensive* militärische und nachrichtendienstliche Fähigkeiten aufzubauen. Auch in der Schweiz werden nun Stimmen laut, die den Ausbau solcher offensiven Fähigkeiten fordern. Im Gegensatz zum klassischen Wettrüsten nehmen aber nicht nur staatliche oder staatlich finanzierte Akteure daran teil. Da dies nicht immer besonders kompliziert und kostspielig ist oder grössere Anlagen verlangt, arbeiten zahlreiche Informatiker, Mathematiker und sonstige technologisch versierte Personen unermüdlich an der Entwicklung neuer technischer Schutz- oder Schadprogramme. Angesichts der eingesetzten Mittel und der Heterogenität der Akteure scheint das digitale Wettrüsten erst begonnen zu haben. Diese Dynamik einzudämmen, wird eine riesige Herausforderung sein, auf die es zurzeit keine Antwort gibt, ausser dass kein Land sie allein bewältigen kann.

Die enge Fokussierung auf den Bereich "Cyber" ist gefährlich. Durch die Elektronisierung der Informationsbearbeitung und die Vernetzung der Systeme zur Informationsbearbeitung, insbesondere über das Internet, sind neue Bedrohungsarten entstanden. Es ist deshalb verständlich, dass momentan der Schutz vor diesen neuen Bedrohungen im Zentrum der Aufmerksamkeit und des Handelns steht. Dies darf aber nicht dazu führen, dass der Schutz von Informationen und IKT-Mitteln auf den Schutz vor Cyber-Angriffen reduziert wird. Wesentliche Gefahren haben nämlich wenig oder nur indirekt mit dem Internet oder elektronischen Schadprogrammen zu tun. Spionage wird beispielweise immer noch mit *alten* Methoden ausgeübt. Zwar ist der Einsatz elektronischer Spionagemittel verhältnismässig günstiger und weniger riskant als der Einsatz von eigentlichen Spionen. Die menschliche Komponente ist jedoch für die Beschaffung hochqualitativer Informationen weiterhin unentbehrlich. Informationen werden auch heute noch zwischen Menschen mündlich ausgetauscht oder auf Papier bearbeitet. Die Risiken, die damit verbunden sind, dürfen bei den Bestrebungen zur Schaffung von Informationssicherheit nicht ignoriert werden.

1.1.2.2 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

Der Bundesrat will in Zusammenarbeit mit Behörden, Wirtschaft und den Betreibern von kritischen Infrastrukturen (KI) die Cyber-Risiken, welchen diese täglich ausgesetzt sind, minimieren. Die NCS identifiziert Cyber-Risiken als Ausprägung bestehender Prozesse und Verantwortlichkeiten. Entsprechend sollen sie in bereits bestehenden Risikomanagementprozessen berücksichtigt werden.

Der Bundesrat verfolgt folgende Ziele:

- Frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich;
- Erhöhung der Widerstandsfähigkeit der KI;
- Wirksame Reduktion der Cyber-Risiken, insbesondere der Cyber-Kriminalität, der Cyber-Spionage und der Cyber-Sabotage.

Er will die Zusammenarbeit zwischen Behörden und Wirtschaft im Cyber-Bereich vertiefen und das bereits gelegte Fundament weiter stärken. Er setzt somit auf bestehende Strukturen und verzichtet auf ein zentrales nationales Steuerungs- und Koordinationsorgan, wie es derzeit in andern Ländern aufgebaut wird. Die NCS führt die Handlungsfelder und Massnahmen auf, die zur Reduktion der Cyber-Risiken auf nationaler Ebene führen sollen. Die bestehende Melde- und Analysestelle Informationssicherung (MELANI), welche diese Aufgabe in Form von Public Private Partnerships schon bis anhin wahrnahm, wurde zu diesem Zweck gestärkt. Der Bundesrat erteilte den Departementen überdies den Auftrag, auf ihrer Ebene sowie im Dialog mit den kantonalen Behörden und der Wirtschaft die Umsetzung verschiedener Massnahmen an die Hand zu nehmen. Diese reichen von Risikoanalysen zu kritischen IKT-Infrastrukturen bis hin zur stärkeren Einbringung der Schweizer Interessen auf internationaler Ebene. Für die Koordination der Umsetzung der NCS wurde im EFD eine Koordinationsstelle geschaffen.

Zur Nationalen Strategie zum Schutz kritischer Infrastrukturen s. Ziff. 3.5.3.

1.1.2.3 Risiken für die Bundesbehörden

Die Bundesbehörden sind den in der NCS aufgeführten Gefahren ebenfalls ausgesetzt. Sie betreiben nämlich auch Informations- und Kommunikationsinfrastrukturen, deren Störung, Ausfall oder Zerstörung die Erfüllung kritischer gesetzlicher Aufgaben gefährden und somit gravierende Auswirkungen auf die Gesellschaft, die Wirtschaft oder den Staat haben kann. Der Bund bearbeitet zur Erfüllung seiner Aufgaben zudem täglich grosse Mengen von Informationen. Unter diesen Informationen befinden sich auch solche, die für die innere oder äussere Sicherheit, die internationalen Beziehungen oder die wirtschaftspolitischen Interessen der Schweiz besonders empfindlich sind und deshalb mittels Klassifizierung geschützt werden müssen.

Klassifizierte Informationen sind aber nicht die einzigen Informationen, die einen erhöhten Schutzbedarf aufweisen. Spionage richtete sich zwar in der Vergangenheit hauptsächlich auf die Beschaffung von militäri-

schen und aussenpolitischen Informationen. Sie ist heute aber vermehrt wirtschaftsorientiert. Im harten globalen Wettbewerb schafft sich derjenige einen entscheidenden Vorteil, welcher sich das Wissen (Forschungs- und Entwicklungsergebnisse, Knowhow) seiner Konkurrenten verschaffen kann. Entsprechend hat Spionage in der Wirtschaft und in der Industrie, insbesondere im hochtechnologischen Bereich, seit einigen Jahren zugenommen. Gerade in diesem Zusammenhang aber stellt die Bundesverwaltung ein hochsensibles Nervenzentrum dar: Sie reguliert die Privatwirtschaft; sie prüft bestimmte Produkte und entscheidet über deren Zulassung; sie kontrolliert gewisse Unternehmen; sie beschafft selber hochwertige Produkte und Dienstleistungen, usw. Die Bundesverwaltung steht dabei in einem ständigen Dialog mit ihren öffentlichen und privaten Partnern im In- und im Ausland. Bei diesen Tätigkeiten bearbeitet sie sehr viele Informationen, die Geschäfts- und Fabrikationsgeheimnisse Dritter beinhalten. Sie kann in der Folge ins Visier derjenigen geraten, die solche Informationen beschaffen wollen. Dritte, die ihre Informationen aufgrund einer gesetzlichen Pflicht oder eines Vertrags den Bundesbehörden anvertrauen, erwarten zu Recht, dass diese auch dort zuverlässig geschützt werden.

Der Bund bearbeitet überdies in grossem Umfang Personendaten. Diese dürfen nach den Vorschriften der Datenschutzgesetzgebung nur rechtmässig, zweckkonform sowie in verhältnismässigem Rahmen bearbeitet werden. Sie müssen sowohl mit organisatorischen als auch mit technischen Massnahmen geschützt werden. Bei einem Datenmissbrauch können die Persönlichkeitsrechte der Personen, deren Daten bearbeitet werden, schwerwiegend verletzt werden. Gewisse Personendaten sind ebenso gefragt wie Technologieinformationen der Industrie. Ihr finanzieller Wert sollte nicht unterschätzt werden. Es gibt einen blühenden Markt für die Beschaffung und die Bekanntgabe personenbezogener Daten.

Bei schweren oder wiederholten Vorfällen, kann das Vertrauen in die Bundesbehörden ernsthaft gestört werden. Dies kann sogar soweit gehen, dass dem Bund wichtige Informationen vorenthalten werden, solange er deren zuverlässigen Schutz nicht nachweislich gewährleistet.

Diese Risiken für den Bund sind nicht abstrakte, unwahrscheinliche Hypothesen. So wurde im Oktober 2009 beim EDA ein Schadprogramm entdeckt, das Spionageaktivitäten ausführte. Es gelangte via E-Mail in das Netzwerk und blieb lange unentdeckt. Auf ähnliche Weise wurden in den Jahren zuvor das bundesnahe Rüstungsunternehmen RUAG und die Firma Mowag angegriffen. Nicht vergessen werden dürfen die Bedrohungen durch Mitarbeitende des Bundes. So wurde im Mai 2012 beim Nachrichtendienst des Bundes (NDB) ein schwerwiegender Datendiebstahl entdeckt. Ein Mitarbeiter des NDB speicherte grosse Mengen an sensiblen Informationen, die ihm mit seinen Berechtigungen zugänglich waren, auf entfernbare Datenträger und schmuggelte sie aus den Räumlichkeiten des Dienstes. Vor seiner Verhaftung traf der Mitarbeiter erste Vorkehrungen, um die entwendeten Daten zu verkaufen.

Häufig werden auch weniger gravierende Vorkommnisse festgestellt. Diese Ereignisse reichen über Diebstahl oder Verlust von Laptops oder Smartphones, Verlust von klassifizierten Informationsträgern oder unberechtigte, meistens politisch motivierte Preisgabe von schutzwürdigen Informationen hin bis zu Betriebsstörungen wegen Server-Ausfällen, Netzwerk-Überlastungen oder fehlerhaften Software-Konfigurationen. Da die Mehrheit solcher Vorfälle entweder nicht systematisch erfasst oder mindestens nicht an die Fachorgane zur Bewertung kommuniziert wird, ist es schwierig, den Gesamtschaden für den Bund einzuschätzen.

1.1.3 Aufträge des Bundesrats

Im Rahmen der Ausarbeitung des Entwurfs waren zahlreiche Aufträge, die der Bundesrat in Bezug auf die Informationssicherheit erteilt hatte, zu berücksichtigen. Nachfolgend werden nur diejenigen Aufträge aufgeführt, die einen wesentlichen Einfluss auf die Gesetzesvorlage hatten.

1.1.3.1 Verabschiedung der Informationsschutzverordnung und Prüfauftrag des Bundesrats

Mitte 2007 verabschiedete der Bundesrat die neue Informationsschutzverordnung (ISchV). Diese ersetzte die beiden bisherigen Verordnungen aus dem zivilen und dem militärischen Bereich und verzichtete auf die ohnehin kaum mehr mögliche Unterscheidung zwischen zivilen und militärischen Informationen. Mit den darin geregelten Klassifizierungs- und Bearbeitungsvorschriften wurde zudem erstmals ein einheitliches Schutzniveau innerhalb der Bundesverwaltung festgelegt. Die mit der ISchV neu eingeführte dritte Klassifizierungsstufe INTERN ermöglichte es zudem, fortan einen Grossteil der klassifizierten Informationen einfacher zu bearbeiten. Aus dem gleichen Grund vereinfachte sich auch die internationale Zusammenarbeit, insbesondere mit der Europäischen Union.

Die ISchV wurde als Übergangserlass konzipiert und ihre Geltungsdauer entsprechend befristet. Gleichzeitig mit ihrer Verabschiedung beauftragte der Bundesrat das VBS, ihm bis Ende 2009 einen Bericht über den Vollzug, die Wirksamkeit und die Wirtschaftlichkeit der ISchV zu erstatten und Antrag zur Schaffung formell-gesetzlicher Grundlagen zu stellen.

1.1.3.2 Bundesratsbeschluss über Massnahmen zur Erhöhung der Informationssicherheit in der Bundesverwaltung

Der Bundesrat beschloss in der Folge des Angriffs auf die Systeme des EDA am 16. Dezember 2009 und am 4. Juni 2010 Massnahmen zur Erhöhung der Informationssicherheit in der Bundesverwaltung. Er legte dabei eine Reihe von organisatorischen und technischen Massnahmen fest, die kurz- und mittelfristig den Schutz der Informationen bei deren Bearbeitung mit Informatikmitteln der Bundesverwaltung verbessern sollen.

Der Bundesrat beantragte zudem der Eidgenössischen Finanzkontrolle (EFK), den Stand der Umsetzung dieser Massnahmen zu überprüfen. Der erste Revisionsbericht der EFK wurde den Mitgliedern des Bundesrates am 2. Dezember 2011 zur Kenntnis gebracht.[1]

1.1.3.3 Bundesratsauftrag zur Schaffung formell-gesetzlicher Grundlagen für den Informationsschutz bzw. für die Informationssicherheit

Der vom Bundesrat bei der Verabschiedung der ISchV verlangte Bericht über den Vollzug, die Wirksamkeit und die Wirtschaftlichkeit zeigte auf, dass die von der ISchV vorgesehene Übergangsfrist bis Ende 2009 für technische Anpassungen zur Gewährleistung des Schutzes von Informationen mehrheitlich nicht eingehalten wurde. Damit bestanden erhebliche Lücken insbesondere beim elektronischen Schutz von klassifizierten Informationen. Nach Kenntnisnahme des Berichts des VBS sowie in Anbetracht der Lehren aus dem Hacker-Angriff gegen das EDA erteilte der Bundesrat am 12. Mai 2010 dem VBS den Auftrag, formell-gesetzliche Grundlagen für den Informationsschutz des Bundes auszuarbeiten. Die neue Regelung sollte insbesondere:

- den Geltungsbereich der Informationsschutzregelungen auf alle Personen erstrecken, die vom Bund mit der Bearbeitung geschützter Informationen betraut werden;
- einheitliche formell-gesetzliche Grundlagen für die Durchführung von Geheimschutzverfahren im militärischen und zivilen Bereich schaffen;
- eine einheitliche Vertragsschlusskompetenz des Bundesrats für internationale Vereinbarungen im Bereich des Informationsschutzes schaffen.

Der Bundesrat beauftragte ferner das VBS, bei der Erarbeitung des Entwurfs zu prüfen, ob und inwieweit weitere materielle Probleme im Bereich des Informationsschutzes einer formell-gesetzlichen Regelung zuzuführen sind sowie ob die Zuständigkeiten und Verantwortlichkeiten im Bereiche der Informationssicherheit den heutigen Anforderungen genügen.

1.1.3.4 Bundesratsbeschluss zur Empfehlung 12 der Geschäftsprüfungskommission des Ständerats (GPK-S) im Zusammenhang mit der Libyen-Krise

Die GPK-S stellte im Rahmen ihrer Prüfung des Verhaltens der Bundesbehörden in der diplomatischen Krise zwischen der Schweiz und Libyen eine Reihe von Informationsschutzproblemen fest. In ihrem Bericht vom 3. Dezember 2010 hielt sie fest, dass "*derartige Ereignisse belegen, dass in Sachen Informationsschutz und Schutz von technischen Geräten in der Bundesverwaltung ein grosser Handlungsbedarf besteht, weshalb es zwingend ist, dass eine rasche Abhilfe erfolgt*". Sie empfahl dem Bundesrat, "*in seinem Kompetenzbereich die nötigen Massnahmen zu treffen, um inskünftig die Geheimhaltung auch auf höchster Stufe innerhalb der Bundesverwaltung gewährleisten zu können. Dabei ist auch den technischen Aspekten der den Mitarbeitenden abgegebenen Geräte eine gebührende Aufmerksamkeit zu schenken*".[2]

Der Bundesrat beschloss in der Folge Massnahmen, um den erkannten organisatorischen und technischen Mängeln beizukommen.[3]

1.1.3.5 Ergänzung des Bundesratsauftrags

Am 14. Januar 2011 setzte der Chef VBS eine Expertengruppe unter der Leitung von Prof. Dr. iur. Markus Müller, Ordinarius für Staats- und Verwaltungsrecht an der Universität Bern, ein. Er erteilte ihr den Auftrag, ein Normkonzept und darauf gestützt einen vernehmlassungsreifen Gesetzesentwurf auszuarbeiten. Die Expertengruppe unterbreitete ihr Normkonzept dem Chef VBS am 29. Juni 2011. Dieser unterrichtete den Bundesrat über die Erkenntnisse der Expertengruppe. Der Bundesrat dehnte daraufhin mit Beschluss vom 30. November 2011 den künftigen Regelungsbereich vom engen Informationsschutz auf die Informationssicher-

---

1 www.efk.admin.ch/images/stories/efk_dokumente/publikationen/querschnittspruefungen/QP%20%2816%29/11387BE_Publikation.pdf

2 Bericht der GPK-S vom 3. Dezember 2010 über das Verhalten der Bundesbehörden in der diplomatischen Krise zwischen der Schweiz und Libyen, BBl **2011** 4304-05.

3 Bericht der GPK-S vom 3. Dezember 2010 über das Verhalten der Bundesbehörden in der diplomatischen Krise zwischen der Schweiz und Libyen: Stellungnahme des Bundesrat vom 20. April 2011, BBl **2011** 4388-90.

heit aus. Er beauftragte zudem das VBS, die Gesetzgebungsarbeiten mit den Aufträgen zur Erarbeitung einer Cyber-Defense-Strategie sowie zur Informationsgesellschaft Schweiz zu koordinieren.

Die Ausdehnung des Regelungsbereichs sowie die geforderte Koordination mit den erwähnten Projekten führten zu einer Erweiterung der Expertengruppe. Vertreten waren nun: Die BK, das EDA, das EJPD (GS, BJ, Fedpol), das VBS (GS, Armeestab), das EFD (GS, ISB, BIT), das UVEK (BAKOM), der EDÖB, die Parlamentsdienste, die eidgenössischen Gerichte und die Kantone (SIK). Der NDB wurde punktuell beigezogen.

1.1.3.6 Bundesratsauftrag zur Harmonisierung und Straffung der Personensicherheitsprüfungen

Am 1. Februar 2012 beauftragte der Bundesrat das VBS, eine Harmonisierung und Straffung der zu überprüfenden Funktionen und der ihnen zugeordneten Prüfstufen sowie weitere Optimierungsmassnahmen mit Auswirkungen auf den Ressourcenbereich zu prüfen. Nach Kenntnisnahme des Berichts der hierfür eingesetzten IDAG PSP beauftragte der Bundesrat am 29. November 2013 unter anderem die IDAG ISG, bei ihren Arbeiten die Empfehlungen des Berichts zu berücksichtigen und soweit angemessen in den Gesetzesentwurf einzuarbeiten (s. Ziff. 1.2.4).

1.1.3.7 Zusatzauftrag und Erweiterung zu einer interdepartementalen Arbeitsgruppe (IDAG ISG)

Nach Bekanntwerden eines Vorfalls im NDB erhielt die Expertengruppe am 24. Oktober 2012 vom Bundesrat den Zusatzauftrag, einen Bericht über die Gefahren und Lücken in der Informationssicherheit in der Bundesverwaltung zu erstellen sowie Vorschläge für Sofortmassnahmen zu unterbreiten. Die Expertengruppe wurde hierauf noch einmal erweitert. Sie bildete nun, mit Vertretungen des EDI und WBF, eine IDAG.

Die IDAG ISG überreichte ihren Bericht samt Empfehlungen am 29. Januar 2013 dem VBS. Daraufhin beschloss der Bundesrat am 15. März 2013, das Führungskader der Bundesverwaltung schulen zu lassen. Für die Durchführung der Ausbildungsmassnahmen ist das Eidgenössische Personalamt (EPA) federführend.

1.2 Kernpunkte der beantragten Neuregelung

Nachfolgend werden der Regelungsbedarf und die vorgeschlagenen Lösungen für die Kernpunkte der beantragten Neuregelung dargestellt. Die vorgeschlagene Neurregelung der Organisation der Informationssicherheit wird getrennt erläutert (Ziff. 1.3).

Zwei Bemerkungen sind eingangs erforderlich:

- Der Regelungsbedarf ergibt sich aus den materiellen und rechtlichen Lücken und Schwachstellen im Bereich der Informationssicherheit. Die Fokussierung auf diese Lücken könnte den Eindruck erwecken, dass alle bisherigen Vorgaben, Prozesse und Massnahmen schlecht sind. Dem ist aber keinesfalls so.
- Detaillierte Berichte über Lücken und Schwachstellen im Bereich der Informationssicherheit werden in der Regel klassifiziert. Aus diesem Grund kann im vorliegenden Bericht nicht auf alle Lücken und Schwachstellen näher eingegangen werden.

1.2.1 Informationssicherheit

Informationen werden heute mehrheitlich in elektronischer Form bearbeitet. Ihr Schutz hängt deshalb immer mehr von den elektronischen Verfahren und Mitteln ab, mit welchen sie bearbeitet werden. Zurzeit sind bei der elektronischen Bearbeitung von Informationen aller Art wesentliche Sicherheitslücken vorhanden.

1.2.1.1 Technische Lücken

Das VBS hat in einem Bericht zur Umsetzung, Wirksamkeit und Wirtschaftlichkeit der Informationsschutzverordnung (s. Ziff. 1.1.3.3) dem Bundesrat belegt, dass die im internationalen Vergleich eher wenig ambitiösen Vorgaben der ISchV für die elektronische Bearbeitung von klassifizierten Informationen mehrheitlich nicht eingehalten werden können, weil die dafür erforderlichen Sicherheitslösungen und -dienste heute entweder fehlen oder aus verschiedenen, insbesondere finanziellen Gründen nicht verwendet oder angeboten werden. Dies führt zu einer etwas skurrilen Situation: Mitarbeitende des Bundes, die im Privatleben ohne die erforderlichen Produkte und Verfahren, die dem aktuellen Stand der Sicherheitstechnik entsprechen, nie E-Banking betreiben würden, haben manchmal wenig Bedenken, VERTRAULICH oder sogar GEHEIM klassifizierte Informationen in ihrem Arbeitsumfeld unverschlüsselt zu speichern oder zu übermitteln.

Diese Erkenntnis betrifft nicht nur klassifizierte Informationen, die bereits heute nur einen kleinen Bruchteil aller schurzwürdigen Informationen des Bundes darstellen. Ähnliche Lücken sind beim Schutz von Personendaten, von Berufs-, Geschäfts- und Fabrikationsgeheimnissen sowie von anderen Informationen, die in Bezug auf die Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit geschützt werden müssen, vorhanden. Bei erhöhten Schutzanforderungen müssen besondere technische Sicherheitsmassnahmen getroffen werden. Diese setzen die vorgängige Umsetzung eines Grundschutzes der Informatiksicherheit voraus.

Ohne ein solches Fundament sind die zusätzlichen technischen Vorkehrungen leicht zu umgehen. Überprüfungen des BIT zeigen aber, dass die entsprechenden Mindestmassnahmen oft mangelhaft umgesetzt werden.

Vor dem Hintergrund wesentlicher Lücken beim elektronischen Schutz von Informationen muss aber auch festgehalten werden, dass die Aufgaben derjenigen Stellen, die für die Vorgaben der Informatiksicherheit oder für deren Umsetzung zuständig sind, innert kürzester Zeit wesentlich komplexer geworden sind. Gründe dafür sind die laufenden technologischen Innovationen, die damit verbundenen neuen Gefahren und Schwachstellen sowie die zu knappen finanziellen und personellen Ressourcen.

1.2.1.2 Organisatorische Mängel

Angesichts der Herausforderungen im technischen Bereich kündigte die Melde- und Analysestelle Informationssicherung (MELANI) bereits 2008 in ihrem Halbjahresbericht an, dass eine Neuausrichtung notwendig sei:

> "Aktuelle gezielte IT-Angriffe lassen sich auch mit Hilfe technischer Sicherheitsvorkehrungen sowie einer gesunden Portion Menschenverstand nicht immer erfolgreich abwehren. Deshalb ist eine Neufokussierung nötig, welche den Schutz der Information ins Zentrum rückt und nicht nur den Schutz der Computer und Netzwerke berücksichtigt. [...] Dies wird ein verstärktes Informations- und Datenmanagement, Informationsklassifizierung und dergleichen nach sich ziehen."[4]

Diese Aussage ist für das Verständnis der beantragten Neuregelung zentral. Die technische IKT-Sicherheit alleine genügt nicht mehr. Bedeutend wichtiger für einen wirksamen Schutz der Informationen sind die organisatorischen Massnahmen. Organisatorische Mängel bestehen beim Bund insbesondere beim Management der Informationssicherheit sowie bei den Rechtsgrundlagen.

Dass Sicherheit Chefsache ist und sich wirtschaftlich lohnt, wird in der Privatwirtschaft spätestens dann wahrgenommen, wenn ein Schadenfall eintritt und Schadenbegrenzung betrieben wird. Bei öffentlichen Verwaltungen wird Sicherheit aber häufig lediglich als Kostentreiber und Hindernis betrachtet. Grund dafür ist insbesondere die Tatsache, dass der öffentlichen Hand bei Vorfällen kein wettbewerblicher Schaden entstehen *kann*. Demzufolge wird in der Regel auch der Produktivitätsverlust, der z.B. durch den Ausfall von IKT-Diensten verursacht wird, weder eruiert noch mit den Kosten zur Umsetzung risikomindernder Massnahmen abgewogen.

Beim Bund ist die Lage beim Schutz von Informationen nicht anders. So wird beispielweise die IKT-Sicherheit oft als rein technische Angelegenheit betrachtet und nicht als Führungsaufgabe wahrgenommen. Demzufolge hat die Führungslinie in der Regel nur wenig Verständnis für ihre Rolle im Sicherheitsprozess und die geschäftsüblichen Führungstätigkeiten (z.B. Setzung von Zielen, Kontrolle der Umsetzung oder Prüfung der Wirksamkeit von Massnahmen) finden nur selten auf den Sicherheitsbereich Anwendung. Auch die Kosten der Sicherheit können nicht transparent dargelegt werden, was eine Beurteilung der Wirtschaftlichkeit der Massnahmen (Kosten-Nutzen-Analyse) verunmöglicht. Schliesslich werden bei Vorfällen oder Verstössen gegen die Vorschriften die Verantwortlichen nur selten zur Rechenschaft gezogen.

Mängel bestehen auch bei den rechtlichen Rahmenbedingungen. Die Rechtsgrundlagen für den Schutz von Informationen sind beim Bund sehr sektoriell ausgelegt, kaum aufeinander abgestimmt und oft lückenhaft. So betreibt der Bund heute sowohl rechtlich also auch organisatorisch parallele Systeme für den Datenschutz, den Informationsschutz (Schutz klassifizierter Informationen), die Informatiksicherheit, die physische Sicherheit und das Risikomanagement. Ferner ist heute die Durchführung von Personensicherheitsprüfungen (s. Ziff. 1.2.4) und von Betriebssicherheitsverfahren (s. Ziff. 1.2.5) hauptsächlich bei Personen bzw. Unternehmen vorgesehen, die klassifizierte Informationen des Bundes bearbeiten, nicht aber bei Personen, die seine kritischen IKT-Mitteln verwalten oder betreiben.

Darüber hinaus sind die Rechtsgrundlagen nicht immer auf die praktischen Bedürfnisse der elektronischen Bearbeitung von Informationen abgestimmt. Beispiele:

- Geschäfts- und Fabrikationsgeheimnisse werden hauptsächlich durch eine Schweigepflicht (Amtsgeheimnis) für die Personen, die sie bearbeiten müssen, geschützt. Die Wahrung des Amtsgeheimnisses erfordert jedoch in einer Informationsgesellschaft mehr als nur eine persönliche Schweigeflicht. Werden Geschäfts- und Fabrikationsgeheimnisse elektronisch erfasst, müssen sie ihrem Schutzbedarf entsprechend zusätzlich organisatorisch und technisch geschützt werden. Vorgaben, wie dieser Schutz erhoben, gestaltet, umgesetzt und überprüft werden muss, fehlen aber grösstenteils.
- Beim Schutz von Personendaten besteht hingegen eine hohe Regelungsdichte. Das Schwergewicht liegt dabei für die Bundesbehörden aber eher auf dem Vorliegen der notwendigen Rechtsgrundlagen für die

4 MELANI Halbjahresbericht 2008/1, http://www.melani.admin.ch/dokumentation/00123/00124/index.html

rechtmässige, zweckmässige und verhältnismässige Bearbeitung von Personendaten als auf dem tatsächlichen, praktischen Umgang der Mitarbeitenden mit Personendaten (z.B. Übermittlung, Aufbewahrung, Vernichtung, Verschlüsselung, usw.).

- Die Vorgaben zum Schutz von klassifizierten Informationen enthalten zahlreiche Widersprüche zu den Informatikvorgaben. Dies betrifft z.B. die Zuständigkeitsregelungen sowie bestimmte Verfahren.

Informationen können aus verschiedenen Gründen schutzwürdig sein. Die organisatorischen und technischen Massnahmenpakete, die zur Umsetzung der jeweiligen Schutzbedürfnisse erforderlich sind, unterscheiden sich jedoch kaum. Wenn deren Umsetzung einheitlich geregelt, organisiert und geführt wird, können Synergien genutzt und gleichzeitig der Schutz von Informationen verbessert werden. Dafür muss die Führungslinie ihre Aufgaben klarer wahrnehmen und die Rechtsgrundlagen müssen zwingend auf die Bedürfnisse der elektronischen Bearbeitung abgestimmt werden.

1.2.1.3 Neue Ausrichtung auf eine integrale Informationssicherheit

Der Bundesrat ist sich der zunehmenden gegenseitigen Abhängigkeiten zwischen dem technischen und organisatorischen Schutz von Informationen sowie den aufgeführten organisatorischen Mängeln bewusst. Im Sinne einer Sofortmassnahme hat er beschlossen, das Kader der Bundesverwaltung in den Belangen der Informationssicherheit schulen zu lassen (s. Ziff. 1.1.3.7). Im Rahmen einer Aussprache am 30. November 2011 hat er zudem festgehalten, dass eine Beschränkung des materiellen Geltungsbereichs des vorliegenden Gesetzesentwurfs bloss auf den Schutz klassifizierter Informationen dem erkannten Regelungsbedarf nicht genügen würde. Er hat deshalb in der Folge das VBS beauftragt, die Rechtsetzungsarbeiten neu auszurichten: Es sei auf eine umfassende, die organisatorische und technische Seite berücksichtigende *Informationssicherheit* abzuzielen und die Neuregelung der Organisation habe sich nach *anerkannten internationalen Standards* zu richten.

Die vom Bundesrat verlangte Neuorientierung auf eine *integrale Informationssicherheit* entspricht dem, was in der Privatwirtschaft und in vielen öffentlichen Verwaltungen weltweit bereits seit einigen Jahren als *règle de l'art* gilt. Die Informationssicherheit wird durch einige internationale Standards, insbesondere durch die Normen ISO/IEC 27001/27002, formalisiert. Solche Standards haben wenig mit der Technik zu tun. Der Fokus wird fast ausschliesslich auf die Aufgaben des *Managements* zum Schutz seiner informationellen Werte sowie auf die entsprechenden organisatorischen Massnahmen gesetzt. Die Standards enthalten jedoch auch praxistaugliche und -erprobte *Best Practices* zur Umsetzung von personellen, technischen und baulichen Massnahmen.

Der vorliegende Entwurf schafft einheitliche formell-gesetzliche Grundlagen für das Management der Informationssicherheit im Bund. Er basiert im Aufbau und Inhalt grösstenteils auf den erwähnten Normen und beabsichtigt deren massgeschneiderte Umsetzung. Dabei wird die Informationssicherheit *nach einem integralen Ansatz* betrachtet, d.h. möglichst alle Belange der Informationssicherheit werden zusammen gesteuert, umgesetzt, überprüft und verbessert. Die Vorlage fasst dementsprechend die wichtigsten organisatorischen Massnahmen für den Schutz aller Informationen und zur Gewährleistung der Sicherheit beim Einsatz der IKT in einer einzigen Regelung zusammen. Gegenüber den heutigen sektoriell ausgerichteten rechtlichen und organisatorischen Strukturen im Bund entspricht der Ansatz der Informationssicherheit einer neuen, integralen Ausrichtung.

1.2.2 Geltungsbereich

1.2.2.1 Sachlicher Geltungsbereich

Der sachliche Geltungsbereich ergibt sich grundsätzlich aus dem Begriff der Informationssicherheit. Im Zentrum des Schutzes sollen alle Informationen stehen, für welche die Bundesbehörden zuständig sind. Das Gesetz gilt für Informationen jeglicher Art (also beispielsweise nicht bloss für Informationen in Textform, sondern auch für graphische Darstellungen) und in beliebiger Form, d.h. nicht bloss für elektronische Informationen sondern auch für Informationen in physischer Form (Papierdokumente). Es handelt sich hauptsächlich um Informationen, die sie selber erstellen. Erfasst werden aber auch Informationen, welche die Bundesbehörden von Dritten erhalten und für deren sichere und rechtmässige Bearbeitung sie deshalb zuständig sind. Weiter sind Informationen betroffen, mit deren Bearbeitung die Bundesbehörden Dritte beauftragen. Eine Einschränkung des impliziten sachlichen Geltungsbereichs auf sensitive Informationen wäre nicht sinnvoll. Die Beurteilung, ob eine Information sensitiv oder schutzwürdig ist, setzt Beurteilungskriterien und -mechanismen voraus, die *zwangsläufig* auf alle Informationen angewendet werden müssten.

Vom Entwurf werden sämtliche IKT-Mittel erfasst, die von den Bundesbehörden eingesetzt werden oder deren Betrieb sie in Auftrag geben. Richtigbesehen müssen zwar die technischen Mittel zur Verarbeitung von Informationen nicht um ihrer selbst willen geschützt werden, sondern vielmehr selbst den Schutz der

damit verarbeiteten Informationen und der damit unterstützten Geschäftsprozesse gewährleisten. Da die Praxis aber die IKT-Mittel als *Schutzobjekte* betrachtet, werden diese im ISG auch ausdrücklich erfasst.

1.2.2.2 Institutioneller Geltungsbereich

Beim vorliegenden Erlass handelt es sich über weite Strecken um einen Organisationserlass. Das Gesetz soll aber von allen Bundesbehörden sowie den ihnen unterstellten Organisationen in ihrem jeweiligen Zuständigkeitsbereich angewendet werden, da nur auf diese Weise eine wirksame Informationssicherheit erzielt werden kann. Weitere Organisationen des öffentlichen oder privaten Rechts sollen vom Gesetz erfasst werden, sofern sie sicherheitsempfindliche Tätigkeiten im Auftrag des Bundes ausüben. Dies entspricht dem Auftrag des Bundesrats, den Geltungsbereich der Informationsschutzregelungen auf alle Personen zu erstrecken, die vom Bund mit der Bearbeitung geschützter Informationen betraut werden.

Die Gründe, weshalb alle Bundesbehörden einschliesslich der gesetzgebenden und der rechtsprechenden Behörden vom Gesetz erfasst werden sollen, sind vielfältig. Zum einen tauschen die Bundesbehörden regelmässig zur Erfüllung ihrer verfassungsmässigen und gesetzlichen Aufgaben Informationen untereinander aus. Darunter fallen auch klassifizierte Informationen oder sonstige schutzwürdige Informationen. Die Bundesbehörden verwenden jedoch bis anhin kein einheitliches Klassifizierungssystem. Die Massnahmen, die von den jeweiligen Behörden getroffen werden, um solche Informationen zu schützen, sind überdies sehr unterschiedlich und kaum aufeinander abgestimmt. Es ist deshalb in der Vergangenheit oft vorgekommen, dass z.B. klassifizierte Informationen der Bundesverwaltung, die an andere Bundesbehörden abgegeben wurden, so bearbeitet wurden, dass dabei wesentliche Schutzvorschriften des Bundesrats verletzt wurden. Alle Bundesbehörden sollen die gleichen Klassifizierungsgrundsätze anwenden und äquivalente Schutzmassnahmen treffen. Nur so kann das beim Umgang mit solchen Informationen erforderliche gegenseitige Vertrauen gewährleistet werden.

Weiter nimmt die Vernetzung der Informatiksysteme der Bundesbehörden untereinander laufend zu. Es ist ein Ziel des Bundesrats, vermehrt und verstärkt auf den elektronischen Austausch von Informationen und auf elektronische Dienstleistungen zu setzen (E-Government). Damit steht fest, dass die Systeme der verschiedenen Bundesbehörden immer mehr gemeinsame Schnittstellen aufweisen werden. Dadurch wird das Risiko erhöht, dass sich Angriffe sowie Bedrohungen gegen eine Behörde auf die Zuständigkeitsbereiche anderer beteiligten Behörden ausbreiten können. Es ist deshalb unentbehrlich, dass die jeweiligen Bundesbehörden gleichwertige Risikobeurteilungskriterien und -methoden anwenden und dass ihre organisatorischen, personellen, technischen und physischen Sicherheitsmassnahmen beim Einsatz der IKT aufeinander abgestimmt werden.

Der institutionelle Geltungsbereich soll nicht zur Folge haben, dass die verfassungsmässige Unabhängigkeit der betroffenen Behörden eingeschränkt wird. Deshalb sollen diese Bundesbehörden das Gesetz eigenständig vollziehen. Auf ein behördenübergreifendes Steuerungsorgan mit Weisungsbefugnissen wird verzichtet. Der eigenständige Vollzug hat einen Nachteil: Die minimalen organisatorischen Anforderungen der Informationssicherheit, die von allen Bundesbehörden erfüllt werden sollen, müssen zwingend auf Gesetzesebene verankert werden. Demzufolge enthält die Vorlage auch zahlreiche Bestimmungen, die von der Normenhierarchie eher dem Verordnungsrecht entsprechen.

1.2.3 Allgemeine Massnahmen der Informationssicherheit

1.2.3.1 Management der Informationssicherheit

Informationssicherheit ist Chefsache. Die Verantwortung dafür liegt bei der Behördenleitung und kann nicht delegiert werden. Der Entwurf legt entsprechend bestimmte Pflichten fest, die nur von den jeweiligen Bundesbehörden erfüllt werden dürfen. So werden die obersten Behörden z.B.:

- die für den Vollzug des Gesetzes erforderlichen Ausführungsbestimmungen erlassen (s. Art. 87);
- die Informationssicherheit nach dem Stand der Lehre (z.B. nach ISO 27001) organisieren, steuern, umsetzen und überprüfen. Dazu gehört die Festlegung von klaren Aufgaben, Kompetenzen und Verantwortlichkeiten (s. Art. 5 Abs. 1 Bst. a und Abs. 2);
- ihre Ziele für die Informationssicherheit sowie das zu erreichende Sicherheitsniveau festlegen (s. Art. 5 Abs. 3 Bst. a);
- die Eckwerte für den Umgang mit Risiken festlegen (s. Art. 5 Abs. 3 Bst. b);
- die Folgen bei Missachtung der Vorschriften festlegen und erläutern (s. Art. 5 Abs. 3 Bst. c);
- die regelmässige Überprüfung der Umsetzung und Wirksamkeit der Massnahmen anordnen (s. Art. 11);
- eine Liste der mittels Personensicherheitsprüfung zu prüfenden Funktionen erlassen (s. Art. 33).

Der Entwurf verstärkt schliesslich die operationelle Rolle der Linie beim Einsatz von IKT (s. Art. 23-26).

1.2.3.2 Risikomanagement

Die Gefahren für und Bedrohungen von Informationen und IKT-Mittel sind mit der Entwicklung zu einer Informationsgesellschaft komplexer und dynamischer geworden. Diese Ausgangslage erfordert von den Bundesbehörden, dass sie den Fokus vermehrt auf die systematische Bewertung des Schutzbedarfs von Informationen sowie auf eine laufende Beurteilung der entsprechenden Risiken setzen. Dies wiederum setzt ein wirksames Risikomanagement im Bereich der Informationssicherheit sowie eine regelmässige Überprüfung der Umsetzung von risikomindernden Massnahmen voraus. Beides fehlt heute weitgehend. Deshalb wird auch ein Prozess zur nachhaltigen und wirtschaftlichen Aufrechterhaltung der Informationssicherheit initialisiert.

Risikomanagement ist für die Bundesbehörden sowohl ein politisches als auch ein wirtschaftliches Anliegen. Die verpflichteten Behörden werden im Entwurf aufgefordert, das Niveau festzulegen, das sie in Bezug auf die Informationssicherheit erreichen wollen (Ziele für die Informationssicherheit). Dieses Niveau ist für die Gestaltung der Sicherheitsmassnahmen sowie für die Beurteilung von deren Wirksamkeit massgebend. Die verpflichteten Behörden müssen in Bezug auf den Umgang mit Risiken auch bestimmen, wer welche Risiken tragen darf und was geschieht, wenn die Restrisiken zu hoch sind.

Das Risikomanagement im Bereiche der Informationssicherheit ist fachspezifisch. Es muss aber bei allen verpflichteten Behörden in den allgemeinen Risikomanagementprozess integriert werden, weil die Risiken der Informationssicherheit selbstverständlich auch zu den allgemeinen Geschäftsrisiken gehören.

Im Rahmen des Risikomanagements wird der Schutzbedarf der Informationen (bezüglich Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit) beurteilt. Die Gefahren, die von Menschen, Technik und Elementarereignissen ausgehen sowie die entsprechenden Schwachstellen werden analysiert. Die Risikobewertung muss möglichst objektiv und systematisch erfolgen. Die zur Erreichung des massgebenden Sicherheitsniveaus erforderlichen Massnahmen müssen durch die Linie festgelegt werden. Schliesslich müssen die identifizierten Risiken überwacht werden.

Eng mit dem Risikomanagement verbunden ist auch das sogenannte Business Continuity Management (BCM). Das BCM soll sicherstellen, dass die Behörden ihre Kernaufgaben selbst in ausserordentlichen Situationen termingerecht erfüllen können. Aufgrund der zunehmenden Abhängigkeit der Auftragserfüllung vom Einsatz der IKT können die Risiken im Bereich der Informationssicherheit die Erfüllung kritischer gesetzlicher Aufgaben des Bundes gefährden (s. auch Art. 6 Abs. 3 RVOG). Entsprechend werden die Bundesbehörden aufgefordert, für Vorfälle der Informationssicherheit, welche die Erfüllung unverzichtbarer Aufgaben gefährden können, Vorsorgeplanungen zu erstellen und entsprechende Übungen durchzuführen.

1.2.3.3 Kontroll- und Auditwesen

Jede einzelne Massnahme im Bereich der Informationssicherheit, die angeordnet wird, muss überprüfbar sein und überprüft werden. Nur mit angemessenen Kontrollen können die Behörden und Organisationen wissen, in welchem Zustand sich ihre Informationssicherheit befindet, welche Risiken bestehen und welche Korrekturmassnahmen allenfalls erforderlich sind. Das Kontrollwesen stellt heute eine der wesentlichsten Schwächen im Bereich der Informationssicherheit des Bundes dar: Es wird nur in Einzelfällen oder erst nach einem Vorfall überprüft. Da zurzeit fast keine Kontrollen durchgeführt werden, fehlen grösstenteils das entsprechende Know-how und die personellen Mittel. Es muss deshalb davon ausgegangen werden, dass die verpflichteten Behörden und Organisationen für die Wahrnehmung dieser Aufgabe nicht darum herumkommen werden, zusätzliche Ressourcen einzusetzen.

Die Kontrollmechanismen und -instrumente müssen zwingend für alle Bereiche der Informationssicherheit verstärkt werden. Die Vorlage sieht deshalb eine allgemeine Kontrollpflicht vor (Art. 11). Dort wo gezielte Kontrollen, Audits oder Überprüfungen erforderlich sind, werden diese ausdrücklich verlangt (für die IKT: s. Ziff. 1.2.3.5). Die Verantwortung für die Kontrollen und Audits im Rahmen des Tagesgeschäfts soll nach wie vor grundsätzlich bei der Führungslinie bleiben. Es gehört zu den Kernaufgaben der Führung, die Umsetzung der angeordneten Massnahmen zu überprüfen. Die Vorlage verstärkt aber auch die Instrumente, die der Führungslinie für Audits und Kontrollen im Bereich der Informationssicherheit zur Verfügung stehen. So sollen die Informationssicherheitsbeauftragten Kontrollen im Auftrag ihrer Behörde durchführen können. Für schwierigere Audits oder für unabhängige Kontrollen sollen die Behörden die vorgesehene Fachstelle des Bundes für Informationssicherheit oder die EFK beauftragen können.

1.2.3.4 Klassifizierung von Informationen

Die Klassifizierung ist eine seit jeher angewandte Massnahme zum Schutz von organisationseigenen Informationen, deren unberechtigte Kenntnisnahme die Organisationsziele beeinträchtigen oder der Organisation

selbst Schaden zufügen kann. Die Klassifizierung von Informationen wird heute durch die ISchV nur für die Bundesverwaltung und die Armee geregelt. Eines der Ziele des vorliegenden Entwurfs ist ein Klassifizierungssystem, das behördenübergreifend gelten und nach möglichst einheitlichen Grundsätzen umgesetzt werden soll. Dabei sollen die erhöhten Erwartungen der Bürgerinnen und Bürger an die Transparenz des Handelns der Bundesbehörden berücksichtigt werden. Die Klassifizierung soll deshalb als eine zu begründende Ausnahme konzipiert werden. Zudem sollen gegenüber heute die Schwellenwerte für die Klassifizierung teilweise erhöht werden.

Das dreistufiges System erlaubt einen risikogerechten Schutz von Informationen. Je grösster das Risiko für die zu schützenden öffentlichen Interessen, desto aufwändiger und kostspieliger die Sicherheitsmassnahmen. Die Klassifizierungsstufe INTERN erlaubt eine einfache, aufwandarme Bearbeitung von Informationen, die zwar schutzwürdig sind, deren Schutzbedarf aber den Aufwand für die Bearbeitung von als VERTRAULICH klassifizierten Informationen nicht rechtfertigen kann. Damit soll auch im internationalen Verhältnis ein einheitliches Sicherheitsniveau erreicht werden. Die meisten Staaten verwenden ein vierstufiges System (z.B. für die EU: RESTRICTED, CONFIDENTIAL, SECRET und TOP SECRET).

1.2.3.5 Sicherheit beim Einsatz von IKT

Heute befinden sich die Bestimmungen über die Sicherheit beim Einsatz von IKT entweder auf Verordnungsebene oder, in den meisten Fällen, auf Weisungsstufe. Aufgrund der zunehmenden Vernetzung der IKT-Systeme sowie der stets ansteigenden Abhängigkeit der Bundesbehörden von diesen Mitteln für die Erfüllung ihrer gesetzlichen Aufgaben, hat die Sicherheit der IKT-Mittel seit einigen Jahren stark an Bedeutung gewonnen. Zahlreiche Vorfälle weltweit oder in der Schweiz belegen die Verwundbarkeit der IKT-Mittel und zeigen die potentiellen Konsequenzen solcher Vorfälle. Eine Übernahme bestimmter Eckwerte der IKT-Sicherheit auf die formell-gesetzliche Ebene ist heute insbesondere deshalb unerlässlich, weil die behördenübergreifende Vernetzung der IKT-Mittel und der elektronische Informationsaustausch weiterhin zunehmen werden. Deshalb werden vermehrt behördenübergreifende Lösungen und Prozesse angestrebt werden müssen. Die meisten konkreten Schutzmassnahmen werden aber aufgrund des raschen Fortschritts der technologischen Entwicklung weiterhin auf Verordnungs- oder sogar auf Weisungsstufe umschrieben und verankert werden müssen.

Berichte über detaillierte Lücken und Schwachstellen im Bereich der IKT werden in der Regel klassifiziert. Der erste Revisionsbericht der EFK nach dem Bundesratsbeschluss vom 16. Dezember 2009 über Massnahmen zur Erhöhung der Informationssicherheit in der Bundesverwaltung gibt trotz eingeschränktem Prüfumfang einen guten Überblick über den Handlungsbedarf, der beim Einsatz der IKT besteht (s. Ziff. 1.1.3.2).

Die Sicherheit von Informationen beim Einsatz der IKT wird oft als technische Angelegenheit betrachtet. Dies trifft nur am Rande zu: Die überwiegende Mehrheit der Sicherheitsvorkehrungen in Bezug auf die IKT sind organisatorischer Natur. Dafür sind hauptsächlich die Behörden und Organisationen zuständig, die den Einsatz von IKT beschliessen (Leistungsbezüger), und nicht die Organisationen, welche im Auftrag dieser Behörden und Organisationen die entsprechenden Mittel betreiben (Leistungserbringer). Es ist also der organisatorische Bereich, der den grössten Handlungsbedarf aufweist.

Die vorgeschlagene Regelung basiert auf bestehenden Prozessen und Verfahren, die entsprechend dem erkannten Bedarf angepasst werden. Dabei geht es, nebst der Verstärkung des Risikomanagements (s. Ziff. 1.2.3.2), hauptsächlich um vier wesentliche Aspekte:

- *Eine klare Regelung der Zuständigkeiten und Verantwortlichkeiten zwischen den IKT-Leistungsbezügern und den IKT-Leistungserbringern*. Die Hauptverantwortung für die Sicherheit beim Einsatz von IKT-Mitteln liegt bei den Leistungsbezügern. Sie sind für die Durchführung des Sicherheitsverfahrens zuständig. Die Leistungserbringer sind hingegen dafür zuständig, die Sicherheit der IKT-Mittel beim Betrieb zu gewährleisten. Sie müssen die Anforderungen und Massnahmen nach diesem Gesetz sowie die vereinbarten zusätzlichen Anforderungen der Leistungsbezüger berücksichtigen und umsetzen.
- *Die Beurteilung der Kritikalität der einzusetzenden IKT-Mittel in Bezug auf die Informationen, die damit bearbeitet werden sollen, sowie auf die Aufgabenerfüllung der betroffenen Behörde oder Organisation (Sicherheitseinstufung).* Die Sicherheitseinstufung eines IKT-Mittels dient einerseits dazu, dass die Behörden sich der Kritikalität ihrer Informationen und IKT-Mittel bewusst werden und in der Folge bei der Festlegung der Sicherheitsmassnahmen den Fokus auf ihre kritischsten Werte legen. Andererseits sollen zu jeder Sicherheitsstufe standardisierte minimale Sicherheitsanforderungen und -massnahmen bestimmt werden, die vor der Inbetriebnahme des IKT-Mittels umgesetzt werden sollen.
- *Eine verstärkte operationelle Rolle der Leitung der verpflichteten Behörde oder Organisation*. Die Leitung der Behörde oder Organisation muss im Sicherheitsverfahren einbezogen werden. Sie muss frühzeitig über die Risiken informiert werden und entsprechende Massnahmen beschliessen können. Deshalb

sieht der Entwurf vor, dass alle einzusetzenden IKT-Mittel von der Behörde und Organisation *sicherheitsmässig* zur Inbetriebnahme freigegeben werden müssen. Sofern aufgrund der Kritikalität eines IKT-Mittels die Erstellung eines Informationssicherheitskonzepts erforderlich ist, muss dieses Konzept von der Behörde oder Organisation genehmigt werden.

- *Verstärkte Kontrollen und Prüfungen*. Zusätzlich zu den allgemeinen Kontrollen (Art. 11) sieht der Vorentwurf im Bereich der IKT drei weitere Prüfungen vor.
  - *Eine Konformitätsprüfung*. Für jedes einzusetzende IKT-Mittel soll sichergestellt werden, dass das Sicherheitsverfahren rechtmässig durchgeführt wurde und die vorgesehenen Massnahmen umgesetzt worden sind. Es handelt sich hier also um eine Qualitätskontrolle.
  - *Eine Prüfung der Informationssicherheitskonzepte*. Die Informationssicherheitsbeauftragten sollen alle Informationssicherheitskonzepte prüfen, bevor diese der Geschäftsleitung zur Genehmigung unterbreitet werden.
  - *Eine Wirksamkeitsprüfung für die kritischsten IKT-Mittel*. Vor der Freigabe von IKT-Mitteln der höchsten Sicherheitsstufe («sehr hoher Schutz») soll die tatsächliche Wirksamkeit der umgesetzten Massnahmen geprüft werden. Für die Durchführung dieser Prüfungen können nur ausgewiesene und zertifizierte Auditoren in Frage kommen. Diese Wirksamkeitsprüfung ist die einzige Massnahme, welche Auskunft über die effektive Informationssicherheit geben kann.

1.2.3.6 Personelle Massnahmen

Die Mitarbeitenden sowie Dritte, die mit der Bearbeitung von Informationen des Bundes beauftragt werden, sind für die Einhaltung der Vorschriften beim Umgang mit Informationen und IKT-Mitteln verantwortlich. Die Wahrnehmung dieser Verantwortung setzt eine angemessene und stufengerechte Ausbildung voraus. In diesem Bereich ist der Handlungsbedarf besonders gross.

Entscheidend für die Wahrung der Informationssicherheit ist auch die restriktive Erteilung von Berechtigungen. Nach diesem Grundsatz sollen Personen nur über diejenigen Berechtigungen für die Bearbeitung von und den Zugriff auf Informationen sowie für den Zugang zu Räumlichkeiten und Bereichen verfügen, die sie tatsächlich für die Erfüllung ihrer Aufgaben benötigen. Zudem sollen die Berechtigungen regelmässig überprüft werden. Diese Regel, die insbesondere gegen die Gefahr einer Innentat gerichtet ist, wird zurzeit nicht überall eingesetzt und umgesetzt.

Der Entwurf legt deshalb beide Grundsätze (Ausbildung und restriktive Erteilung von Berechtigungen) als minimale personelle Anforderungen fest. Die verpflichteten Behörden und Organisationen werden im Rahmen ihres Vollzugsrechts detaillierte Vorgaben erlassen müssen.

1.2.3.7 Physischer Schutz von Informationen und IKT-Mitteln

Zu oft wird vergessen, wie wirksam Eingangskontrollen und sonstige physische Schutzmassnahmen für die Informationssicherheit sind. Die Vorlage legt in diesem Bereich die minimale Anforderung fest, diesen Schutz zu regeln.

Sie schafft zudem eine Grundlage für die Einrichtung von sogenannten Sicherheitszonen. Dabei handelt es sich um Räumlichkeiten und Bereiche, die besonders geschützt werden, weil in ihnen häufig klassifizierte Informationen der Stufe VERTRAULICH oder GEHEIM bearbeitet oder IKT-Mittel der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» betrieben werden. Solche Sicherheitszonen sind international üblich, beim Bund aber kaum bekannt. Die Einrichtung von Sicherheitszonen wird nicht als zwingende Massnahme, sondern als "Kann"-Vorschrift konzipiert. Für die Einrichtung ist eine formell-gesetzliche Grundlage erforderlich, weil Sicherheitszonen mit Massnahmen verbunden werden können, die einen relativ tiefen Eingriff in die Persönlichkeitsrechte darstellen (z.B. Verwendung von biometrischen Identifikationsmethoden oder ständige Videoüberwachung). Für den Zugang zu Sicherheitszonen kann auch die Durchführung einer vorgängigen Personensicherheitsprüfung erforderlich sein. In der Praxis werden solche Sicherheitszonen hauptsächlich für Server-, Führungs- oder Sicherheitsräume errichtet.

1.2.4 Personensicherheitsprüfungen

Eine der heikelsten und intensivsten Sicherheitsbedrohungen entsteht dann, wenn Personen, die über Zugang zu höher klassifizierten Informationen verfügen oder besonders kritische IKT-Mittel verwalten oder betreiben, Verrat oder Sabotage üben oder z.B. die staatlichen Institutionen auf rechtswidrige Art umgestalten wollen. Sensitive Funktionen sollen deshalb ausschliesslich Personen anvertraut werden, die möglichst weitgehend Gewähr dafür bieten, dass sie das ihnen entgegengebrachte Vertrauen nicht missbrauchen. Dies ist insbesondere dann nicht der Fall, wenn bei Personen Anzeichen auf Erpressbarkeit oder Bestechlichkeit bestehen. Diese beiden Eigenschaften haben erfahrungsgemäss häufig einen zeitlich zurück liegenden Aus-

gangspunkt, beispielweise persönliche oder finanzielle Schwierigkeiten. Eine Personensicherheitsprüfung (PSP) kann Linienvorgesetzten Risiken, die sich aus dem Vorleben oder dem Umfeld der geprüften Person ergeben, aufzeigen (s. auch: Botschaft vom 7. März 1994 zum BWIS und zur Volksinitiative «S.O.S. Schweiz ohne Schnüffelpolizei», BBl 1994 II 1127).

Die PSP stellt eine vorbeugende Massnahme zum Schutz vor Innentätern dar. Sie hat zum Ziel, das Risiko einer vorsätzlichen oder fahrlässigen Beeinträchtigung wesentlicher öffentlicher Interessen, das mit der Ausübung einer sicherheitsempfindlichen Tätigkeit durch eine bestimmte Person verbunden ist, zu *identifizieren*. Es liegt anschliessend alleine in der Verantwortung der auftraggebenden bzw. anstellenden Behörde oder Organisation, zu entscheiden, ob sie ein allfälliges erhöhtes Risiko tragen, ob sie es mit bestimmten Auflagen reduzieren oder ob sie es durch Nichtanstellung oder Kündigung vermeiden will. Auch eine positive Beurteilung des Sicherheitsrisikos durch die zuständige Fachstelle für Personensicherheitsprüfungen (Fachstelle PSP) entbindet die Linienvorgesetzten auf keinen Fall von ihrer Führungsverantwortung und von ihrer Pflicht, Personalrisiken zu identifizieren und zu bewältigen. Die PSP hat deshalb eine ähnliche Ausprägung wie ein Assessment, welches die Arbeitgeberinnen und Arbeitgeber vor der Anstellung von Führungs- oder Schlüsselpersonen oft in Auftrag geben.

1.2.4.1 Transfer der Regelung vom BWIS ins Informationssicherheitsgesetz

Die formell-gesetzlichen Grundlagen für die Durchführung von PSP befinden sich heute in zwei Gesetzen. Für den Bund sind sie zurzeit im BWIS geregelt. Für das Personal der Betreiberinnen von Kernkraftwerken sieht das KEG in seinem Art. 24 ebenfalls Zuverlässigkeitskontrollen vor. Für die Durchführung der Prüfungen setzte der Bundesrat zwei Fachstellen PSP ein: Die eine ist beim VBS angesiedelt. Sie ist für die Mehrheit der Prüfungen zuständig. Die andere ist der BK administrativ zugeordnet. Sie prüft das Top-Kader der Bundesverwaltung sowie die Angestellten der anderen Fachstelle PSP.

Mit dem geplanten Nachrichtendienstgesetz soll das BWIS fast vollständig aufgehoben werden. Übrig werden nur noch die PSP sowie diejenigen Aufgaben bleiben, für deren Erfüllung fedpol zuständig ist. Da die heutige Regelung der PSP im BWIS *ausschliesslich* dem Schutz von Informationen dient (s. Art. 19 Abs. 1 BWIS), ist es zweckmässig, diese Regelung in das vorliegende Gesetz zu verschieben. Geprüft wurde auch die Schaffung eines eigenständigen Gesetzes für die PSP (und für das Betriebssicherheitsverfahren; s. Ziff. 1.2.5). Angesichts des Zieles, alle Massnahmen der Informationssicherheit für den Bund in einem einzigen Erlass zusammenzuführen, wurde diese Variante aber verworfen.

1.2.4.2 Behebung rechtlicher Mängel

Mit dem Transfer der formell-gesetzlichen Bestimmungen über die PSP in den vorliegenden Entwurf sollen einige Mängel des geltenden Rechts behoben werden. Die PSP stellt einen schweren Eingriff in die Persönlichkeitsrechte der zu prüfenden Personen dar. Das verfassungsmässige Prinzip der Legalität verlangt für solche Eingriffe eine detaillierte formell-gesetzliche Grundlage. Die vorgeschlagene Regelung ist demnach wesentlich detaillierter als im heutigen BWIS. Sie erfüllt damit auch die Erwartungen des Parlaments an eine formell-gesetzliche Definition der Kriterien zur Risikobeurteilung (s. Art. 42).

Obschon die Regelung der PSP im BWIS ausschliesslich zum Schutz von Informationen dienen soll, wurden die Gründe für die Durchführung einer PSP in der PSPV in der Vergangenheit *contra legem* erweitert. Es wird deshalb vorgeschlagen, im künftigen Informationssicherheitsgesetz die Prüfgründe abschliessend festzulegen und diese auf die direkten Bedürfnisse der Informationssicherheit einzuschränken. Im Entwurf werden diese eng gefassten Prüfgründe unter dem Ausdruck "*sicherheitsempfindliche Tätigkeit*" subsumiert. Folgende Betätigungen stellen eine solche dar:

- die Bearbeitung von als VERTRAULICH oder GEHEIM klassifizierten Informationen oder der Umgang mit entsprechend klassifiziertem Material;
- die Verwaltung, den Betrieb, die Wartung oder die Überprüfung von IKT-Mitteln der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz»;
- den Zugang zu Sicherheitszonen, insbesondere zu Schutzzonen 2 oder 3 einer Anlage nach der Gesetzgebung über den Schutz militärischer Anlagen.

Bestimmte bisherige Prüfgründe werden also ersatzlos gestrichen. Dies betrifft insbesondere den bisherigen Grund des regelmässigen Zugangs zu besonders schützenswerten Personendaten, deren Offenbarung die Persönlichkeitsrechte der Betroffenen schwerwiegend beeinträchtigen könnte (s. Art. 19 Abs. 1 Bst. e BWIS). Es ist in der Praxis kaum möglich, die Informationen zu bestimmen, welche darunter fallen.

Sofern für weitere Tätigkeiten aus Sicherheitsgründen eine Prüfung erforderlich ist, sollen die Prüfgründe in der Spezialgesetzgebung geregelt werden. Um zwischen der PSP nach dem Informationssicherheitsgesetz

und nach den anderen Erlassen klar unterscheiden zu können, soll für letztere eine andere Terminologie verwendet werden: "*Prüfung der Vertrauenswürdigkeit*". Entsprechend wird im Anhang eine Änderung des BPG und des MG vorgeschlagen. So sollen Personen, welche regelmässig die Schweiz im Ausland vertreten oder Entscheidungskompetenzen bzw. Aufsichtsaufgaben in wesentlichen Finanzangelegenheiten erfüllen, einer Prüfung der Vertrauenswürdigkeit unterstellt werden können.

Umstritten war die Frage, ob für den Eintrag einer Funktion in die Liste der zu prüfenden Funktionen bei Bundesangestellten die einmalige Ausübung einer sicherheitsempfindlichen Tätigkeit genügen soll oder ob am Grundsatz der *Regelmässigkeit* gemäss heutigem System (s. Art. 19 Abs. 1 BWIS) festgehalten werden soll. Das Kriterium der Regelmässigkeit basiert unter anderem auf der Beurteilung des Nachrichtendienstes des Bundes, der die Gefährdung im Staatschutz insbesondere dort als hoch einschätzt, wo Mitarbeitende regelmässig und über einen längeren Zeitraum Zugang zu klassifizierten Informationen haben. Personen mit nur punktuellem und befristetem Zugang sind weniger stark gefährdet bzw. für Stellen, dies sich Informationen verschaffen wollen, weniger interessant. Mit dem Kriterium der Regelmässigkeit sind jedoch zwei Probleme verbunden. Nachrichtendienstliche Beschaffungsaktivitäten sind vorerst nur eine von vielen Bedrohungen für die Informationssicherheit. Bereits beim einmaligen Zugang zu einer als GEHEIM klassifizierten Information kann eine Person dem Bund schwerwiegenden Schaden zufügen. Dies kann z.B. der Fall sein, wenn diese Person Informationen über die Verhandlungsstrategie der Schweiz in besonders wichtigen Angelegenheiten der Öffentlichkeit preisgibt. Der Schaden selbst ergibt sich also nicht bloss aus der Regelmässigkeit des Zugangs, sondern auch aus dem Informationsinhalt. Des Weiteren ist der Begriff "*regelmässig*" selbst nicht eindeutig und hat im geltenden Recht oft zu uneinheitlichen Auslegungen geführt.

Die materiellen Voraussetzungen für den Eintrag einer Funktion in die Funktionsliste und damit für die Durchführung einer Personensicherheitsprüfung sind im Entwurf deshalb leicht anders als im heutigen System. Vom Kriterium der Regelmässigkeit, insbesondere bei der Bearbeitung von klassifizierten Informationen, soll formell-gesetzlich abgesehen werden. Wichtiger für die Unterstellung der Bundesangestellten unter die PSP ist nämlich die Frage, ob die Inhaberin oder der Inhaber einer bestimmten Funktion für ihre oder seine Aufgabenerfüllung klassifizierte Informationen der Stufen VERTRAULICH oder GEHEIM bearbeiten *muss*, IKT-Mittel der Stufe «hoher Schutz» oder «sehr hoher Schutz» verwalten, betreiben, warten oder überprüfen *muss* oder Zugang zu Sicherheitszonen haben *muss*. Wenn eine solche Tätigkeit für die funktionsbedingte Aufgabenerfüllung *erforderlich* ist, dann - und nur dann - muss die Funktion in die Liste der zu prüfenden Funktionen aufgenommen werden. Dieser Ansatz entspricht dem Grundsatz der restriktiven Erteilung von Berechtigungen (Art. 29) und dem Grundsatz des "*Need to know*", der für die Bearbeitung von klassifizierten Informationen gilt (Art. 15 Abs. 1).

Im Weiteren wurde die heutige Regelung insbesondere in folgenden Punkten geändert:

- *Rechtliche Natur der auszustellenden Erklärung*: Art. 22 PSPV sieht vor, dass die Fachstellen PSP nach Abschluss der PSP eine Verfügung nach Art. 5 VwVG erlassen. Die Beurteilung des allfälligen Sicherheitsrisikos durch die Fachstellen PSP entspricht aber nicht der rechtlichen Definition einer Verfügung, denn sie beeinflusst *im juristischen Sinne* die Rechte und Pflichten und den Status der betroffenen Person nicht unmittelbar. Die für die Übertragung der sicherheitsempfindlichen Tätigkeit zuständige Stelle ist nämlich nicht an die Erklärung der Fachstellen PSP gebunden (s. Art. 46) und die zu prüfende Person hat kein Recht auf eine Anstellung, die Übertragung einer bestimmten Funktion oder auf die Erteilung eines Auftrags. Die Beurteilungen der Fachstellen PSP bilden daher rechtlich gesehen Realakte nach Art. 25a VwVG (zum Rechtsmittelweg s. Art. 51).
- *Sicherheitserklärung mit Vorbehalt statt Auflagen*: Falls ein bedingtes Sicherheitsrisiko besteht, das durch bestimmte Massnahmen oder Auflagen hinreichend eingeschränkt werden kann, stellen die Fachstellen PSP neu eine Sicherheitserklärung mit Vorbehalt (anstatt wie bisher mit Auflagen) aus. Die Fachstellen PSP legen selbst keine Auflagen fest, empfehlen aber solche. Die neue Formulierung zeigt einerseits, dass die Fachstellen PSP einen Vorbehalt bezüglich der Sicherheitserklärung haben. Andererseits wird deutlich, dass ihr Vorbehalt bloss empfehlenden Charakter für die Behörde oder Organisation hat, die für die Übertragung der sicherheitsempfindlichen Tätigkeit bzw. Funktion zuständig ist. Diese Stelle legt allenfalls entsprechende Auflagen fest.
- *Streichung des Verbots nach Art. 20 Abs. 1 BWIS, Daten über die Ausübung verfassungsmässiger Rechte zu erheben*. Obwohl Sinn und Zweck dieser Bestimmung klar und zweckmässig sind, ist dieses Verbot nicht praxistauglich. Jede Person hat z.B. das verfassungsmässige Recht zu heiraten. Bei der Erhebung der Daten werden aber selbstverständlich auch Daten über den Zivilstand erhoben, was eigentlich aufgrund der erwähnten BWIS-Bestimmung verboten wäre. Die geltende Regelung will nur verhindern, dass Personen aufgrund ihrer politischen Ansichten sicherheitsmässig ausgeschlossen werden. Deshalb sieht der Entwurf neu vor, dass ein Sicherheitsrisiko immer durch die tatsächlichen Umstände der persönlichen

Verhältnisse der zu prüfenden Person begründet werden muss. Links- und rechtsextreme Ansichten sowie andere politische oder weltanschauliche Ansichten dürfen also die Annahme eines Sicherheitsrisikos nicht begründen, solange die betroffenen Personen *in diesem Zusammenhang* nicht rechtswidrig gehandelt haben (s. Art. 42).

- *Reduktion von drei auf zwei Prüfstufen*. Das heute geltende Recht (Art. 9-12 PSPV) sieht drei Prüfstufen vor: eine Grundsicherheitsprüfung, eine erweiterte PSP und eine erweiterte PSP mit Befragung. Während die beiden ersten Stufen nach PSPV einen nachvollziehbaren Prüfzweck haben, stellte sich die Frage, welche Informationen oder Aktivitäten nach Schweizer Recht besser zu schützen sein könnten als GEHEIM klassifizierte Informationen. Für den Zugang zu letzteren ist bereits eine erweiterte PSP nach Art. 11 PSPV erforderlich. Der Bund kennt aber keine Klassifizierungsstufe «STRENG GEHEIM», für welche die Prüfung nach Art. 12 PSPV allenfalls erforderlich sein könnte. Im Sinne einer Anpassung des geltenden Rechts an das Klassifizierungssystem des ISG sowie einer Vereinfachung der Prüfungsmodalitäten werden deshalb im vorliegenden Gesetz die Prüfstufen von drei auf zwei reduziert. Um die Wirksamkeit der PSP zu erhöhen, wird aber die Datenerhebung innerhalb der zwei verbleibenden Prüfstufen reorganisiert und wo nötig ergänzt (s. Art. 39).

Zu Diskussionen Anlass gab auch das heutige System einer durch Rechtssatz erlassenen Funktionenliste, das folgende Nachteile in sich birgt: Die Erstellung der Listen ist mit grossem Aufwand verbunden, sie sind unter den Departementen und der Bundeskanzlei kaum harmonisiert und müssen zudem aufgrund von Organisationsänderungen und Umbenennungen der Funktionen ständig angepasst werden. Auch aus Sicherheitsgründen sind sie nicht unproblematisch: die Listen geben nämlich den vollständigen Überblick über alle Funktionen der Behörden, die sicherheitsempfindliche Tätigkeiten beinhalten. Ihre Publikation macht sie weltweit jedermann zugänglich, auch fremden Nachrichtendiensten. Die Listen haben dennoch einen entscheidenden Vorteil gegenüber möglichen Varianten: Sie sorgen für Rechtssicherheit und schränken den zu prüfenden Personenkreis ein, so dass kein Wildwuchs an Prüfungen entstehen sollte. Vor dem Erlass seiner Ausführungsbestimmungen kann der Bundesrat allenfalls prüfen, ob die uneingeschränkte Veröffentlichung der Listen zweckmässig ist.

Im Rahmen der Revisionsarbeiten stellte sich schliesslich die Frage, ob nach Abschluss der PSP zukünftig automatisch ein Hinweis an die Fachstellen PSP ergehen soll, falls sich im Strafregister oder in anderen, für die PSP relevanten Datenbanken hinsichtlich der geprüften Personen neue Einträge ergeben. Technisch wäre eine solche automatische Information – entsprechende rechtliche Anpassungen vorausgesetzt – ohne weiteres realisierbar. Sie könnte die Sicherheit auch markant erhöhen, weil neue Sicherheitsrisiken rasch festgestellt werden könnten. Eine automatisierte Information der Fachstellen PSP würde aber auch bedeuten, dass die Fachstellen PSP die einleitende Stelle oder die für die Übertragung der sicherheitsempfindlichen Tätigkeit zuständige Stelle informieren müssten, damit diese eine neue PSP einleiten könnten. Die Funktion der PSP würde sich damit grundlegend ändern, indem sie sozusagen zu einer ständigen Überwachung der geprüften Person verpflichten würde. Aus diesen Gründen wurde auf eine Regelung zur automatischen Information der Fachstellen PSP verzichtet.

1.2.4.3 Straffung und Harmonisierung der PSP

Bei der Ausarbeitung der ersten Liste von Personen, die nach der Verordnung vom 15. April 1992 über die Sicherheitsprüfung in der Bundesverwaltung geprüft werden sollten, hatte sich der Bundesrat aus politischen Erwägungen entschieden, möglichst wenige Funktionen der Prüfung zu unterstellen. Er hatte für die Erstellung der Liste eine Planungsgrösse von 1200 Funktionen festgelegt (s. BWIS-Botschaft). Seit dem Inkrafttreten des BWIS im Jahre 1998 ist die Anzahl jährlich geprüfter Personen jedoch stetig angewachsen. So wurden im Jahre 2012 insgesamt über 75'000 Prüfungen durchgeführt. Über 60'000 solcher PSP wurden bei Stellungspflichtigen und Angehörigen der Armee durchgeführt, wobei diese Zahl auch die neu eingeführte Prüfung des Gewaltpotenzials nach Art. 113 MG einschliesst. Die Ressourcen der Fachstellen PSP mussten entsprechend regelmässig erhöht werden.

Der Gesetzesentwurf sieht mehrere Massnahmen vor, die in ihrer Gesamtheit dazu beitragen sollen, die Anzahl durchzuführender PSP zu reduzieren:

- Die Tätigkeiten, für welche die Durchführung der Prüfung erforderlich ist, werden klarer als im BWIS definiert. Die Prüfgründe werden auf die engen Bedürfnisse der Informationssicherheit reduziert.
- Die Reduktion auf zwei Prüfstufen soll auch bewirken, dass die erweiterte Prüfung nur noch bei Personen durchgeführt wird, die tatsächlich als GEHEIM klassifizierte Informationen bearbeiten oder Tätigkeiten einer entsprechenden Empfindlichkeit ausüben müssen. Im Jahr 2012 wurden über 28'000 erweiterte PSP durchgeführt. Somit sollten mehr als 28'000 Personen Zugang zu als GEHEIM klassifizierten Informatio-

nen haben. Dies kann keinesfalls zutreffen. Die Anzahl durchzuführender PSP dieser Stufe soll folglich deutlich geringer ausfallen.

- Zu den Kontrollaufgaben der Informationssicherheitsbeauftragten (s. Art. 84) gehört auch die Prüfung der Rechtmässigkeit des Eintrags einer Funktion auf der Liste der zu prüfenden Funktionen.

Die mit den aufgeführten Massnahmen angestrebte Erhöhung des Schwellenwertes für die Durchführung einer PSP wird dazu führen, dass bestimmte Sicherheitsbedürfnisse nicht mehr durch die PSP abgedeckt werden. Um die Schaffung eines Sicherheitsvakuums zu vermeiden sollen den Arbeitgeberinnen und Arbeitgebern andere, verhältnismässigere Mittel zur Verfügung gestellt werden, um ihren durchaus legitimen Sicherheitsbedürfnissen zu genügen. Die Arbeitgeberinnen und Arbeitgeber sollen ermächtigt werden, von Stellenbewerberinnen und Stellenbewerbern sowie den Angestellten zu verlangen, dass sie einen Auszug aus dem Strafregister und aus dem Betreibungsregister vorlegen, sofern dies für die Wahrung der Interessen des Arbeitgebers erforderlich ist. Es wird eine entsprechende Revision des BPG beantragt (s. Art. 20*a* BPG).

1.2.5 Betriebssicherheitsverfahren

Das Betriebssicherheitsverfahren (BSV; bis anhin "Geheimschutzverfahren" genannt) befasst sich mit der Wahrung der Informationssicherheit bei der Vergabe von Aufträgen der Behörden an Dritte (nachfolgend "Betriebe" genannt), die nicht ihrer unmittelbaren Aufsicht unterstehen. Die Behörden vergeben in vielen Sachbereichen Aufträge, die mit sicherheitsempfindlichen Tätigkeiten verbunden sind, an die Privatwirtschaft. Damit die Interessen nach Art. 1 Abs. 2 auch ausserhalb des unmittelbaren Anwendungsbereichs des Gesetzes geschützt werden, wird bei entsprechenden Auftragnehmern ein BSV durchgeführt. Das Verfahren dient einerseits der Prüfung der Vertrauenswürdigkeit der zu beauftragenden Betriebe, andererseits ermöglicht es, die notwendigen Massnahmen zur Wahrung der Informationssicherheit während der Ausführung des Auftrags zu kontrollieren und durchzusetzen. Das BSV dient nicht der Produktsicherheit: Dafür ist selbstverständlich einzig die auftraggebende Stelle zuständig.

Das BSV ist zweckmässig und international üblich (s. etwa Art. 11 des Beschlusses des Rates über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen vom 31. März 2011[5] resp. Abschnitt VII der Regeln und Vorschriften der Europäischen Weltraumorganisation vom 15. Dezember 2011[6]). Es wird in der Schweiz für Aufträge des Bundes mit militärisch klassifiziertem Inhalt seit Ende der siebziger Jahre gestützt auf die GeheimschutzVO durchgeführt. Aufgrund des begrenzten materiellen Geltungsbereichs dieser Verordnung werden zurzeit nur militärische klassifizierte Aufträge erfasst. Das Manko eines einheitlichen, d.h. auch für Aufträge aus dem zivilen Bereich durchzuführenden BSV wurde vom Bundesrat bereits vor längerer Zeit erkannt. Es führte einerseits dazu, dass für klassifizierte Aufträge des Bundes aus dem nicht-militärischen Bereich jeweils spezielle Sicherheitsvorkehrungen getroffen werden mussten. Andererseits hinderte es Schweizer Unternehmen mehrfach daran, sich erfolgreich um die Teilnahme an klassifizierten, nicht-militärischen Projekten des Auslandes zu bewerben. Als Beispiele können etwa die Herstellung von Ausweisen oder Zahlungsmitteln für Drittstaaten oder die Mitwirkung in bestimmten wissenschaftlichen Projekten erwähnt werden. Damit schadete es auch der Wettbewerbsfähigkeit der Schweizer Wirtschaft.

Das Verfahren läuft in groben Zügen wie folgt ab: Die auftragserteilende Stelle stellt der Fachstelle für Betriebssicherheit (Fachstelle BS) Antrag zur Durchführung des BSV. Nach der Einleitung desselben legt die Fachstelle BS in Absprache mit der Antragstellerin (Auftraggeberin) zunächst die Sicherheitsanforderungen fest. Hierauf prüft die Fachstelle BS die sicherheitsmässige Eignung der in Frage kommenden Firmen. Es soll insbesondere geprüft werden, ob die betroffenen Firmen von anderen Staaten kontrolliert oder beeinflusst werden und gegebenenfalls ob diese Kontrolle oder der Einfluss mit der Informationssicherheit des Bundes vereinbart werden kann. Die auftragserteilende Stelle vergibt anschliessend den Auftrag an eine Firma, welche als sicherheitsmässig geeignet beurteilt wurde. Die Fachstelle BS legt alsdann in einem Sicherheitskonzept fest, wie die Auftragnehmerin die Anforderungen an die Informationssicherheit umsetzen muss. Nachdem die erforderlichen Sicherheitsmassnahmen umgesetzt wurden, wird der Auftragnehmerin die Betriebssicherheitserklärung (BSE) ausgestellt. Sobald schliesslich nach der Durchführung der PSP auch die erforderlichen Sicherheitserklärungen vorliegen, darf die auftragserteilende Stelle dem Betrieb die für die Erledigung des sicherheitsempfindlichen Auftrags erforderlichen Mittel (z.B. Informationen, Daten etc.) zur Verfügung stellen. Die BSE hat besondere Wirkungen sowohl für den Betrieb als auch für die Fachstelle BS. Letztere erhält insbesondere das Recht, den Betrieb unangemeldet zu inspizieren sowie weitere Massnahmen zu treffen. Die Detailregelung des BSV wird der Bundesrat auf Verordnungsebene festlegen.

5 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32011D0292:DE:HTML

6 http://esamultimedia.esa.int/docs/eso/esa-reg-004d.pdf

Die Regelung steht zum Teil mit der PSP in relativ engem Zusammenhang, unterscheidet sich aber von dieser in wesentlichen Punkten des Verfahrensablaufs:

- Zwar wird im Grundsatz ebenfalls eine Prüfung der Vertrauenswürdigkeit des Betriebs vorgenommen. Je nach dem Ergebnis der Beurteilung wird dann eine BSE ausgestellt, welche die Vertrauenswürdigkeit des Betriebs bescheinigt und es ihm als Auftragnehmer ermöglicht, sicherheitsempfindliche Tätigkeiten des Bundes (oder einer ausländischen Behörde) auszuüben. Dabei geht es aber nicht nur um die eigentliche "Prüfung" des Betriebs, sondern auch um die Festlegung der umzusetzenden auftragsbezogenen Sicherheitsmassnahmen im Betrieb.
- Anders als die PSP ist das Verfahren mit der Erteilung der BSE auch nicht einfach abgeschlossen, sondern die Einhaltung der festgelegten Massnahmen muss jederzeit überprüft werden können.

1.2.6 Informationssicherheit bei den kritischen Infrastrukturen (KI)

Mit Beschluss vom 30. November 2011 hat der Bundesrat das VBS beauftragt, soweit erforderlich die formell-gesetzlichen Bedürfnisse der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) in das vorliegende Gesetz zu integrieren. Der Bundesrat hat in der NCS am Grundsatz der dezentralen Regulierung der KI festgehalten (s. Ziff. 1.1.2.2). Die Prüfung des formell-gesetzlichen Regelungsbedarfs zur Erfüllung des dezentralen Vollzugs der NCS obliegt demnach denjenigen Departementen, die im Rahmen ihrer Aufgabenerfüllung gegenüber KI-Betreibern über Regulationsbefugnisse verfügen (z.B. das UVEK für die Sektoren der Kommunikationsinfrastruktur oder Energieversorgung). Soweit sektorspezifisch formell-gesetzlicher Handlungsbedarf besteht, muss die entsprechende Fachgesetzgebung angepasst werden.

Es gibt demgegenüber auch bestimmte Aufgaben, die sektorübergreifend angegangen werden müssen und nicht zuletzt aus Effizienz- und Kostengründen nicht durch die einzelnen dezentralen Regulatoren wahrgenommen werden können. Primär betroffen ist die Unterstützung der verschiedenen KI durch den gegenseitigen Austausch von Informationen über Bedrohungen im Bereich der Informationssicherheit, welche insbesondere der Früherkennung von Risiken und der Abwehr von Gefahren dient. In diesem Bereich hat sich in der Praxis gezeigt, dass die Verbindung zu einer einheitlichen Ansprechstelle auf der Seite des Bundes (in Form der Melde- und Analysestelle Informationssicherung MELANI) von den KI-Betreibern ausdrücklich erwünscht ist. Es hat sich weiter erwiesen, dass die im Rahmen von MELANI aufgebaute öffentlich-private Partnerschaft, insbesondere dank ihrem Zugang zu Informationen aus dem Nachrichtendienst des Bundes, sehr wirksam ist. Geschätzt werden neben den von MELANI bereitgestellten Informationen insbesondere der Verbleib der Informationsherrschaft beim Informationslieferanten bezüglich ausgetauschten Informationen über Vorfälle, die Freiwilligkeit der Zusammenarbeit sowie der Ansatz, durch Informationen und gegebenenfalls Empfehlungen den Informationssicherungs- und Risikomanagementprozess zu unterstützen, statt durch Regulierungen Massnahmen vorzuschreiben.

Diese bereichsübergreifende Aufgabe des Bundes zur Unterstützung der KI soll im vorliegenden "Querschnittgesetz" vorgesehen werden, soweit dafür eine formell-gesetzliche Grundlage nötig ist. Im Entwurf werden somit die zentralen Aufgaben von MELANI verankert. Zur Erfüllung dieser Aufgaben muss MELANI regelmässig Personendaten bearbeiten. Darunter können auch (selten) besonders schützenswerte Personendaten fallen. Der Entwurf schafft die erforderliche formell-gesetzliche Grundlage für die Bearbeitung solcher Daten.

1.2.7 Vollzug

1.2.7.1 Vollzug bei den Bundesbehörden

Die Regelung des Vollzugs dieses Gesetzes steht vor der Herausforderung, dass die Anwendung des Gesetzes nach möglichst einheitlichen Kriterien erfolgen soll. Die Vorgaben der Informationssicherheit sollen durchgehend zur Anwendung gelangen. Kann ein einheitlicher Vollzug (insbesondere bei der Handhabung klassifizierter Informationen oder beim Umgang mit IKT-Mitteln) nicht erreicht werden, sind im behördenübergreifenden Informationsaustausch zwangsläufig Lücken bei der Informationssicherheit die Folge. Die Organisations- und Vollzugsautonomie der betroffenen Behörden (Parlament, Bundesrat, Gerichte des Bundes, Bundesanwaltschaft, Nationalbank) muss aber gewahrt bleiben. Die verfassungsmässige Zuständigkeit der verschiedenen Behörden darf durch partielle behördenübergreifende Vollzugsvorgaben einer einzelnen Behörde (etwa des Bundesrats) nicht in Frage gestellt werden.

Der Vorentwurf berücksichtigt diese an sich widersprüchlichen Anforderungen mit drei Mechanismen:

- *Eine "Opting-out"-Regelung für den Vollzug:* Als Grundsatz wird festgelegt, dass jede Behörde in ihrem Bereich den Erlass selbständig vollzieht und entsprechendes Verordnungsrecht erlässt. Das Vollzugsrecht des Bundesrates soll jedoch für die übrigen Bundesbehörden sinngemäss gelten, solange und soweit sie keine eigenen Regelungen erlassen.

- *Standardanforderungen und -massnahmen*: Der Bundesrat soll ermächtigt werden, standardisierte Anforderungen und Massnahmen nach dem Stand von Lehre und Technik festzulegen, die für die anderen Bundesbehörden als Empfehlungen gelten sollen. Dabei handelt es sich nicht um grundsätzliche Organisationsfragen, sondern um untergeordnete Prozesse, Mittel und Dienstleistungen (z.B. Erhebung des Schutzbedarfs von Informationen, Methoden für die Risikobeurteilung, Verschlüsselung, Anforderungen an Sicherheitsbehältnisse). Damit soll ein einheitliches Sicherheitsniveau erreicht werden, es sollen aber auch die Projekt- und Umsetzungskosten reduziert werden. Der Bundesrat soll die Möglichkeit haben, die Festlegung an kompetente Fachorgane zu delegieren.
- *Die Schaffung eines fachspezifischen behördenübergreifenden Koordinationsorgans:* Die für die fachliche Steuerung der Umsetzung des Gesetzes zuständigen Informationssicherheitsbeauftragten werden aufgrund ihrer Stellung umfassende Kenntnisse der Situation und der Probleme der Informationssicherheit in ihrem Zuständigkeitsbereich, insbesondere bei der Umsetzbarkeit und Wirksamkeit der Vorschriften sowie der beschlossenen Massnahmen erhalten. Es bietet sich daher an, als Koordinationsorgan eine Konferenz dieser Beauftragten gesetzlich zu institutionalisieren. Die Konferenz dient hauptsächlich dem einheitlichen, behördenübergreifenden und risikobasierten Vollzug des Gesetzes. Sie soll hierzu auch bei der Festlegung der Standardanforderungen und -massnahmen einbezogen werden.

Mit der vorgeschlagenen Lösung wird die Unabhängigkeit der Bundesbehörden beim Vollzug bewahrt. Der Vollzug erfolgt dezentral. Das angestrebte einheitliche Sicherheitsniveau wird durch einheitliche Doktrin, durch die Erarbeitung von Standards sowie durch die professionelle Unterstützung und Beratung von Fachorganen erreicht. Zu den gesetzestechnischen Nachteilen der Lösung, s. Ziff. 1.2.2.2.

1.2.7.2 Vollzug in der Bundesverwaltung und bei weiteren verpflichteten Organisationen

Der Gesetzesentwurf regelt hauptsächlich den behördenübergreifenden Rahmen. Für den Vollzug in der Bundesverwaltung sowie bei Organisationen, welche Verwaltungsaufgaben im Sinne von Artikel 2 Absatz 4 RVOG erfüllen, ist der Bundesrat zuständig. Seine Vollzugsautonomie ist - unter Vorbehalt der Erfüllung der materiellen und organisatorischen Anforderungen des Gesetzes - kaum eingeschränkt. Die Vorlage sieht zwei Eingriffe in seine Autonomie vor:

- Der Bundesrat muss wie alle anderen Bundesbehörden die Informationssicherheit in seinem Zuständigkeitsbereich nach dem Stand von Lehre und Technik steuern, umsetzen und überprüfen (s. Art. 5 Abs. 1).
- Der Bundesrat sowie die Departemente und die BK müssen je eine/n Informationssicherheitsbeauftragte/n sowie eine Stellvertretung für ihren Bereich bezeichnen (s. Ziff. 1.3.2 sowie Art. 84).

Der Entwurf legt keine weiteren Vorgaben für den Vollzug in der Bundesverwaltung und das entsprechende Verordnungsrecht fest. Das Gesetz lässt hier dem Bundesrat viel Spielraum. So kann der Bundesrat z.B. den Organisationen des dritten Kreises oder Organisationen nach Art. 2 Abs. 4 RVOG eine grössere Vollzugsautonomie einräumen. In diesem Zusammenhang wird er auch beschliessen können, ob er am heutigen grösstenteils dezentralisierten Vollzug festhalten will oder ob bestimmte Kompetenzen und Zuständigkeiten zentralisiert werden sollen.

1.2.8 Bereiche, in denen auf eine Regelung verzichtet wird

Die Prüfung der Möglichkeiten und der Opportunität einer gesetzlichen Regelung der folgenden Problembereiche hat ergeben, dass sie die hier anvisierte Regelung eines Informationssicherheitsgesetzes materiell in verschiedener Hinsicht wesentlich ausdehnen und vermutlich auf wenig Akzeptanz stossen würde. Es wird daher auf entsprechende Regelungsvorschläge verzichtet.

1.2.8.1 Strafbestimmungen

Es wurde zwar festgestellt, dass die Bestimmungen im StGB und im MStG, die sich mit dem Schutz des Amtsgeheimnisses und dem Schutz klassifizierter bzw. schutzwürdiger Informationen des Bundes und der Kantone befassen, heute wenig kohärent und in verschiedensten Teilen revisionsbedürftig sind. Es handelt sich bei diesen Bestimmungen aber um eine Materie des Kernstrafrechts, die nicht annexweise im Rahmen eines Organisationserlasses, sondern durch eine selbständige Revision des StGB revidiert werden sollte. Der Bundesrat wird zu gegebener Zeit einen entsprechenden Auftrag erteilen.

1.2.8.2 Einschränkung des Zugangs zu klassifizierten Informationen aufgrund der Staatsbürgerschaft

In ersten Entwürfen der Expertengruppe war vorgesehen, den Zugang zu als GEHEIM klassifizierten Informationen des Bundes grundsätzlich Schweizer Bürgerinnen und Bürgern vorzubehalten. Personen, die das Bürgerrecht eines Staates besitzen, mit dem die Schweiz ein Informationsschutzabkommen geschlossen hat, hätte in Ausnahmefällen jedoch Zugang gewährt werden können. Auf Beschränkungen des Zugangs für aus-

ländische Staatsangehörige zu als GEHEIM klassifizierten Informationen des Bundes muss aber im Auftrag des Bundesrats verzichtet werden.

1.2.8.3 Rückgabe schutzwürdiger Informationen des Bundes im Besitz Privater

Es wurde geprüft, ob es für die rasche Durchsetzung des Informationsschutzes wesentlich wäre, dass Informationsträger mit schutzwürdigen Informationen, die ohne Zustimmung der zuständigen Behörde in den Besitz Dritter gelangt sind, durch direkte Verfügung sichergestellt werden könnten. Damit hätten die betroffenen Bundesbehörden im Rahmen des Verwaltungsverfahrensrechts (d.h. ohne vorgängiges Straf- oder Zivilverfahren) die Rückgabe oder Vernichtung entsprechender Informationsträger verfügen können. Da zu vermuten ist, dass eine solche Bestimmung insbesondere im Hinblick auf die Pressefreiheit ausserordentlich konfliktträchtig wäre und auf starken politischen Widerstand stossen würde, wird auf eine entsprechende Regelung verzichtet.

1.2.8.4 Gefährdung der Sicherheit durch die Verbreitung von Informationen durch Private

Ausserhalb eigentlicher Straftatbestände gibt es heute für die Behörden keine Grundlagen, um die Verbreitung von privaten Informationen zu verhindern, die für die Allgemeinheit und den Staat zu erheblichen Bedrohungen und Gefährdungen führen können. Gedacht wird dabei insbesondere an Baupläne bestimmter Waffen, Labordaten, Infrastrukturpläne etc. Es wurde geprüft, ob eine Kompetenz der vom Sachbereich her zuständigen Bundesstellen eingeführt werden sollte, solche Publikationen im Rahmen des Verwaltungsverfahrens im Einzelfall zu untersagen oder die Inhaber solcher Informationen zu Sicherheitsmassnahmen nach dem Gesetz zu verpflichten (Klassifizierung der Informationen, Durchführen von PSP oder eines BSV). Eine solche Regelung würde aber einen erheblichen Eingriff in grundrechtlich geschützte Positionen Dritter darstellen und es wäre mit erheblichem politischem Widerstand zu rechnen.

1.2.8.5 Integration bestehender gesetzlicher Regelungen im Bereich des Objektsschutzes

An sich ist unbestritten, dass die Informationssicherheit (einschliesslich des Schutzes der IKT-Mittel) und die PSP einen relativ engen Zusammenhang mit dem Objektschutz haben, d.h. mit dem Schutz der Gebäude und Einrichtungen des Bundes. Diese Materie wird derzeit durch verschiedene gesetzliche Bestimmungen mit relativ unterschiedlicher Ausgestaltung und in unterschiedlicher Weise erfasst (s. im militärischen Bereich das AnlageschutzG, im zivilen Bereich etwa Art. 22-24 BWIS, Art. 62f RVOG, Art. 69 ParlG und Art. 25a BGG). Die Prüfung hat ergeben, dass eine gewisse Harmonisierung dieser Bestimmungen bzw. die Schaffung einer einheitlichen gesetzlichen Grundlage zwar wünschbar wäre, von der materiellen und organisatorischen Tragweite her aber den Rahmen des vorliegenden Projektes sprengen würde. Die Vorlage enthält jedoch zwei Bestimmungen über den physischen Schutz von Informationen und IKT-Mitteln. Die heutigen Zuständigkeiten im Bereich des Objektschutzes werden damit nicht in Frage gestellt.

1.3 Organisation der Informationssicherheit im Bund

Der Bundesrat hat in seinem Beschluss vom 12.05.2010 das VBS beauftragt, bei der Erarbeitung des Entwurfs zu prüfen, ob und inwieweit die Zuständigkeiten und Verantwortlichkeiten im Bereiche der Informationssicherheit den heutigen Anforderungen genügen. Zu prüfen war insbesondere auch, ob eine Zusammenlegung der verschiedenen interdepartementalen Ausschüsse opportun erscheint. Dieser Prüfauftrag betrifft grundsätzlich nur die Bundesverwaltung. Die Prüfungsergebnisse liefern aber wichtige Erkenntnisse, die für die Organisation der behördenübergreifenden Informationssicherheit auch gelten.

1.3.1 Heutige Organisation der Informationssicherheit in der Bundesverwaltung

In der Bundesverwaltung werden die Zuständigkeiten und Verantwortlichkeiten für den Schutz von Informationen je nach Informationsart (z.B. klassifizierte Informationen oder Personendaten) oder Bearbeitungs- oder Schutzmassnahmenart (elektronisch oder physisch) durch verschiedene rechtliche Erlasse und Vorgabestellen geregelt. Der Bund betreibt in der Folge auch mehrere parallele Organisationen, die sich mit Haupt- oder Teilaufgaben der Informationssicherheit befassen (Informationsschutz, Datenschutz, Informatiksicherheit, Objektsicherheit und Risikomanagement). Nachfolgend werden die drei Bereiche, die vom Bundesrat explizit erwähnt wurden (Informationsschutz, Datenschutz und Informatiksicherheit), bezüglich Zuständigkeiten und Verantwortlichkeiten näher betrachtet.

1.3.1.1 Organisation des Informationsschutzes

Der Informationsschutz in der Bundesverwaltung ist zur Hauptsache in der ISchV geregelt. Ergänzende Regelungen befinden sich in den sogenannten Informationsschutzabkommen (ISA; s. auch Art. 90). Die Umsetzung des Informationsschutzes erfolgt dezentral, wird aber zentral durch Organe ohne Weisungsbefugnisse koordiniert.

- *Generalsekretärenkonferenz (GSK):* Nach Art. 8 und 18 ISchV ist die GSK für den Erlass der detaillierten Vorgaben (Klassifizierungskatalog und Bearbeitungsvorschriften) im Bereich des Informationsschutzes zuständig. Die Bearbeitungsvorschriften legen auch Verhaltensvorschriften für den elektronischen Umgang mit klassifizierten Informationen sowie Anforderungen an die Sicherheit von IKT-Mitteln fest.
- *Informationsschutzbeauftragte*: Alle Departemente und die Bundeskanzlei müssen nach Art. 19 ISchV eine/n Informationsschutzbeauftragte/n bezeichnen. Die Informationsschutzbeauftragten sorgen für die Umsetzung des Informationsschutzes in ihrem Zuständigkeitsbereich. Obschon die ISchV es nicht verlangt, haben alle Departemente auf Stufe Verwaltungseinheit weitere "Informationsschutzberater" bezeichnet.
- *Koordinationsausschuss für den Informationsschutz im Bund (KOAISchB)*: Die interdepartementale Koordination erfolgt im Rahmen des KOAISchB (Art. 20 ISchV). Er sorgt für einen einheitlichen Vollzug des Informationsschutzes im Bund, erarbeitet die Vorlagen zu Handen der GSK und erstattet ihr alle zwei Jahre Bericht. Er koordiniert seine Tätigkeiten mit dem Ausschuss Informatiksicherheit (A-IS) des ISB.
- *Koordinationsstelle für den Informationsschutz im Bund (KISchB)*: Der KOAISchB und die Informationsschutzbeauftragten werden nach Art. 20a ISchV von der bei der Informations- und Objektsicherheit (IOS) im VBS angesiedelten KISchB unterstützt. Sie erstellt die notwendigen Ausbildungshilfsmittel und nimmt die Rolle der Ansprechstelle für Kontakte mit in- und ausländischen sowie internationalen Stellen im Bereich des Informationsschutzes wahr. Sie kann auch die in völkerrechtlichen Verträgen vorgesehenen Sicherheitsinspektionen und im Einvernehmen mit den Departementen und der BK weitere Kontrollen durchführen.

1.3.1.2 Organisation des Datenschutzes

Die Rechtsgrundlagen für die Bearbeitung von Personendaten finden sich in den jeweiligen Spezialgesetzen. Die Organisation des Datenschutzes im Bund ist dagegen grundsätzlich im DSG und in der VDSG geregelt. Im Gegensatz zur ISchV gelten diese Erlasse auch für Private. Der Vollzug des Datenschutzes erfolgt dezentral. Er wird aber zentral durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) überwacht und durch die Gruppe Datenschutz, ein informelles Organ ohne Weisungsbefugnisse, koordiniert.

- *Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB):* Das DSG hat die Stelle des EDÖB geschaffen, mit dem Zweck, Privatpersonen und Bundesorgane im Hinblick auf die Einhaltung der Datenschutzbestimmungen zu beraten und zu beaufsichtigen. Der EDÖB überwacht die Einhaltung des DSG und der übrigen Datenschutzvorschriften des Bundes durch die Bundesorgane. Er ist administrativ der BK zugeordnet.
- *Datenschutzberater:* Die Bundeskanzlei und die Departemente müssen nach Art. 23 VDSG jeweils mindestens einen Berater für den Datenschutz bezeichnen. Diese Berater unterstützen die verantwortlichen Organe und Benutzer, fördern die Information und die Ausbildung der Mitarbeiter und wirken beim Vollzug der Datenschutzvorschriften mit. Der Verkehr der Bundesorgane mit dem EDÖB läuft über die Berater. Die meisten Verwaltungseinheiten haben auch auf ihrer Ebene eine/n Datenschutzberater/in bezeichnet.
- *Gruppe Datenschutz:* Die Datenschutzgesetzgebung sieht kein Organ für die departementsübergreifende Koordination des Datenschutzes im Bund vor. Deshalb wurde eine informelle Gruppe Datenschutz unter der Leitung des Datenschutzberaters der Bundeskanzlei geschaffen. Ihr gehören alle Datenschutzberater der Departemente, eine Vertretung des EDÖB und eine Vertretung der Parlamentsdienste an. Die Gruppe sorgt insbesondere für einen einheitlichen und koordinierten Vollzug des Datenschutzes im Bund, vertritt Praxisanliegen gegenüber dem EDÖB und sorgt für die Organisation von Ausbildungsveranstaltungen.

1.3.1.3 Fachorganisation der Informatiksicherheit

Die Organisation der Informatiksicherheit ist hauptsächlich in der Bundesinformatikverordnung (BinfV) geregelt, wobei zahlreiche andere Erlasse Einfluss auf die entsprechenden Zuständigkeiten und Verantwortlichkeiten haben (ISchV, Informationsschutzabkommen, VDSG, GEVER-Verordnung, usw.). Der Vollzug der Informatiksicherheit erfolgt dezentral. Die Departemente und die Bundeskanzlei sind für die Umsetzung in ihrem Bereich selbst verantwortlich. Der Vollzug wird aber zentral durch ein Organ mit Weisungsbefugnissen (ISB) gesteuert und durch ein Konsultativorgan (A-IS) begleitet.

- *Bundesrat:* Der Bundesrat übernimmt bei der IKT-Sicherheit eine strategische Rolle. Viele seiner Aufgaben im IKT-Sicherheitsbereich beziehen sich auf seine Verantwortung im allgemeinen IKT-Bereich nach Art. 14 BinfV: Er bestimmt die IKT-Strategie des Bundes; überwacht die Umsetzung der IKT-Strategie

und beschliesst bei Bedarf Massnahmen; legt die IKT-Standarddienste fest; erlässt Weisungen über die IKT-Sicherheit; und bewilligt Abweichungen von seinen Vorgaben.

- *ISB:* Das ISB entscheidet nach Art. 17 BinfV im Bereich der IKT-Sicherheit über Anträge der Departemente, der Bundeskanzlei und der Verwaltungseinheiten für Sonderregelungen bezüglich der Vergabe von sicherheitsrelevanten Rechten und Mandaten, insbesondere im Zusammenhang mit Firewalls, Zugriffsrechten und Privilegien. Bei Gefährdung der Bundesverwaltung entscheidet es über spezifische IKT-Sicherheitsmassnahmen. Es klärt als Sachverständigenorgan im Auftrag eines Departements oder der Bundeskanzlei vermutete oder erfolgte Sicherheitsvorfälle ab. Es stellt den Informatiksicherheitsbeauftragten des Bundes. Es führt die Melde- und Analysestelle Informationssicherung (MELANI) in Zusammenarbeit mit dem Nachrichtendienst des Bundes und leitet das Konsultativorgan Ausschuss Informatiksicherheit.
- *Informatiksicherheitsbeauftragte:* Für den dezentralen Vollzug müssen die Departemente und die Bundeskanzlei je eine/n Informatiksicherheitsbeauftragte/n bezeichnen (Art. 19 Abs. 1 BinfV). Diese koordinieren alle Informatiksicherheitsaspekte innerhalb des Departements sowie mit den überdepartementalen Stellen. Auch die Verwaltungseinheiten sind verpflichtet, eine/n Informatiksicherheitsbeauftragte/n zu bestimmen. Diese koordinieren alle Informatiksicherheitsaspekte innerhalb der Organisationseinheit sowie mit den departementalen Stellen.
- *Ausschuss Informatiksicherheit (A-IS):* Der A-IS ist das Konsultativorgan für das ISB zu allen IKT-Sicherheitsfragen (Art. 19 BinfV). Er dient auch der überdepartementalen Koordination. Er setzt sich aus den Informatiksicherheitsbeauftragten der Departemente und der Bundeskanzlei zusammen. Mit beratender Stimme können je ein Vertreter oder eine Vertreterin der EFK, des EDÖB sowie der Parlamentsdienste teilnehmen.
- *Informatikrat des Bundes (IRB*): Der IRB ist das Konsultativorgan für das ISB zu IKT-Geschäften (inkl. Geschäfte mit Bezug zur IKT-Sicherheit), die der Absprache mit den Departementen und der Bundeskanzlei bedürfen, insbesondere für den Erlass von Vorgaben und für die Genehmigung von Ausnahmen von denselben (Art. 18 BinfV). Er setzt sich aus dem oder der Delegierten für die IKT-Steuerung und je einem namentlich bezeichneten Vertreter oder einer namentlich bezeichneten Vertreterin jedes Departements und der Bundeskanzlei zusammen. Mit beratender Stimme können je ein Vertreter oder eine Vertreterin der Eidgenössischen Finanzverwaltung (EFV), des EDÖB, der internen Leistungserbringer sowie der Parlamentsdienste teilnehmen.
- *Eidgenössische Finanzkontrolle (EFK):* Die EFK nimmt seit dem 1. Januar 2012 die Informatikrevision in der Bundesverwaltung wahr (Art. 28 BinfV).

Neben dieser Grundorganisation gibt es viele Organe oder Stellen, die sich ebenfalls mit IKT-Sicherheit im Bund befassen. Nachfolgend werden nur diejenigen aufgeführt, die fachspezifische Zuständigkeiten und Verantwortungen haben, die für die IKT-Sicherheit der Bundesbehörden von Bedeutung sind. Nachrichtendienstliche, strafrechtliche oder sonstige Stellen werden nicht erwähnt.

- *Informations- und Objektsicherheit (IOS):* Die in der Gruppe Verteidigung angesiedelte IOS ist für die IKT-Sicherheitsvorgaben des VBS und der Armee und für die Prüfung von deren Umsetzung zuständig. Insoweit nimmt sie auf Stufe Armee und teilweise VBS sehr ähnliche Aufgaben wie das ISB wahr.
- *Melde- und Analysestelle Informationssicherung (MELANI):* MELANI wurde vom Bundesrat im Jahr 2004 definitiv eingesetzt und mit dem Schutz der kritischen Informationsinfrastrukturen in der Schweiz beauftragt. Die vom ISB geleitete Kooperation (Art. 17 Abs. 1 Bst. i BinfV) von EFD, VBS und Privatwirtschaft zum Schutz der KI basiert auf dem Modell der *Public Private Partnership*. Es handelt sich dabei um eine enge Zusammenarbeit zwischen Verwaltung und Privatunternehmen der verschiedenen Wirtschaftssektoren, die im Umfeld der Sicherheit von Computersystemen und des Internets sowie des Schutzes der schweizerischen KI tätig sind.
- *Sonderstab Informationssicherung (SONIA):* SONIA tritt in Krisen, die durch Störungen in der Informations- und Kommunikationsinfrastruktur ausgelöst wurden, zusammen. Er umfasst Entscheidträger aus Verwaltung, Kantonen und Wirtschaft (KI) und wird vom Delegierten für die Informatiksteuerung des Bundes (ISB) geleitet. Als Lagezentrum für SONIA fungiert MELANI.
- *Computer Security Incident Response Team (CSIRT):* Das beim EFD/BIT tätige CSIRT sorgt für die Sicherung der zivilen Bundesnetze durch Überwachung, Prävention und Reaktion. Es arbeitet eng mit anderen Bundespartnern wie MELANI oder fedpol zusammen und hat folgende Kernaufgaben: Beobachten aktueller Bedrohungen und analysieren von Logfiles; Erteilung von Handlungsempfehlungen zur Risikominimierung, zur raschen Eingrenzung des Schadens im Falle von IKT-Sicherheitsvorfällen und zum

Schutz der Daten, die dem BIT anvertraut wurden (operativer Schutz der zentralen IKT-Infrastrukturen des Bundes).

- *Militärisches Computer Emergency Response Team (MilCERT):* Das MilCERT sorgt als Pendant des CSIRT für die Sicherung der Netzwerke der Armee und des VBS. Es ist innerhalb der Führungsunterstützungsbasis der Armee (FUB) im Zentrum Elektronische Operationen (ZEO) integriert, um als unabhängige Einheit sicherheitsrelevante Vorfälle innerhalb des VBS und der Armee zu untersuchen.
- *Informationssicherheit und Kryptologie (IS Krypt):* Der Bereich IS Krypt ist ebenfalls bei der FUB/ZEO angesiedelt. Seine Kryptologen stellen die Kommunikationssicherheit von Armee, VBS und weiteren Einheiten der Bundesverwaltung sicher, indem sie kryptographische Verfahren und Systeme evaluieren und selber entwickeln. Seine Arbeit erstreckt sich von der Überprüfung von kryptologischen Grobkonzepten bis hin zur Analyse einzelner kryptologischer Funktionen, wofür profunde Kenntnisse der aktuellen kryptoanalytischen Forschung notwendig sind.
- *Armasuisse, Wissenschaft und Technologie (W+T):* Durch den Bereich Informatik und Cyberspace der W+T werden Risikoanalysen, Sicherheitsprüfungen und Audits im Bereich der organisatorischen und technischen Informationssicherheit durchgeführt. Die Dienste der W+T werden zunehmend auch von zivilen Stellen der Bundesverwaltung in Anspruch genommen, insbesondere für den Nachweis der Effektivität von Sicherheitskonzepten und der Schutzwirkung von Sicherheitsmassnahmen sowie für technische Verifikations- und Penetrationstests. W+T betreibt in diesem Bereich auch ein Monitoring der Technologie- und Bedrohungsentwicklung.

1.3.1.4 Vergleich der Zuständigkeiten und Verantwortlichkeiten

Die drei umschriebenen Fachorganisationen haben je einen beschränkten Auftrag im Bereich der Informationssicherheit zu erfüllen. In allen drei Bereichen sind die Departemente und die Bundeskanzlei für die Umsetzung der Vorgaben verantwortlich. Alle Bereiche haben darüber hinaus grundsätzlich den genau gleichen organisatorischen Aufbau:

- eine Vorgabestelle;
- Beauftragte auf den Stufen Departement / BK sowie Verwaltungseinheit; und
- ein überdepartementales Koordinationsgremium.

Die verschiedenen Funktionsinhaber nehmen in ihren Fachbereichen grundsätzlich auch dieselben Aufgaben wahr. Die einzige wichtige Ausnahme stellen die verschiedenen Vorgabestellen dar, deren Befugnisse sich zum Teil stark unterscheiden. Die nachfolgende Tabelle liefert eine Übersicht über diese Situation. Sie schliesst auch die zwei anderen Bereiche ein, die einen direkten Konnex zur Informationssicherheit haben: die Objektsicherheit und das Risikomanagement.

	Vorgaben	**Dep/BK**	**Verwaltungseinheit**	**Koordination**
Informationsschutz	GSK	Informationsschutz-beauftragte	Informationsschutz-beauftragte/-berater	KOAISchB / KISchB
Datenschutz	EDÖB	Datenschutzberater	Datenschutzberater	IDAG Datenschutz
IKT-Sicherheit	BR / ISB	Informatiksicherheits-beauftragte	Informatiksicherheits-beauftragte	ISB-Sec / A-IS
Objektsicherheit	fedpol / BSD	Sicherheitsbeauftragte	Sicherheitsbeauftragte	Koordinationsausschuss Sicherheit
Risikomanagement	BR / GSK	Risikomanager/in	Risikocoach	Koordinationsstelle EFV

1.3.1.5 Organisatorische Mängel

Die heutige Organisation weist viele Lücken und Schwachstellen auf:

- *Die Zuständigkeiten der verschiedenen Bereiche sind nicht immer klar und die Schnittstellen zwischen den einzelnen Fachgebieten der Informationssicherheit werden ungenügend gepflegt.*

  Die unklaren Zuständigkeiten sind auf alle Ebenen ersichtlich. Für die elektronische Bearbeitung von besonders schützenswerten Personendaten oder klassifizierten Informationen ab der Klassifizierungsstufe VERTRAULICH ist beispielweise ein Informationssicherheits- und Datenschutz-Konzept (ISDS-Konzept) erforderlich. Ist dies eine Frage des Datenschutzes, des Informationsschutzes oder der IKT-Sicherheit und wer ist für die korrekte Einstufung der Informationen und für die Kontrolle der Umsetzung der Massnahmen zuständig? Ist der Schutz von Netzwerkleitungen eine Frage der Informatiksicherheit oder des Objektschutzes? Ist die Aktenvernichtung eine Frage des Informationsschutzes, des Datenschut-

zes oder der physischen Sicherheit und wer definiert die Anforderungen? Wer setzt sie um? Ist ein USB-Stick ein Informationsträger im Sinne der ISchV oder ein IKT-Mittel im Sinne der BinfV?

Die erwähnten Probleme zeitigen auch im internationalen Bereich direkte Auswirkungen. Aufgrund unklarer Zuständigkeiten und Verantwortlichkeiten innerhalb der Bundesverwaltung konnte beispielsweise bisher keine Lösung für die elektronische Übermittlung klassifizierter Informationen mit der EU gefunden werden. Dementsprechend werden selbst Informationen der tiefsten EU-Klassifizierungsstufe bis heute ausschliesslich in Papierform ausgetauscht. Ähnliche Probleme sind auch bei der Zusammenarbeit mit der European Space Agency (ESA) vorhanden. Dabei stellt sich z.B. die Frage, wer für den Bereich Kommunikationssicherheit (COMSEC[7]) zuständig ist. Diese Frage hat grossen Einfluss auf die erfolgreiche Teilnahme der schweizerischen Institutionen und Unternehmen an ESA Aktivitäten. Sie blieb aber bis jetzt unbeantwortet.

Die Fachbereiche sind verpflichtet, Ausbildungs- und Sensibilisierungsmassnahmen durchzuführen. Häufig werden aber Sensibilisierungs- und Ausbildungsmassnahmen der verschiedenen Dienststellen nicht miteinander koordiniert, obschon sie ähnliche Inhalte enthalten.

- *Es gibt zu viele Akteure, die teilweise über ungenügendes Fachwissen oder ungenügende personelle Ressourcen verfügen. Bestehende Ressourcen werden teilweise schlecht genutzt. Die kritische Masse wird nirgends erreicht.*

  Die Pflichtenhefte der Beauftragten aus den aufgeführten Teilbereichen enthalten nebst den Aufgaben aus dem Bereich Informationssicherheit meistens weitere Pflichten. Für die Wahrnehmung der Informationssicherheitsaufgaben steht ihnen oft nur ein geringer Teil ihrer Arbeitszeit zur Verfügung. Sie können sich diesen Aufgaben deshalb nur beschränkt widmen. In der Folge verfügen sie auch nicht alle über das erforderliche Fachwissen. Hierunter leidet die Sicherheit stark. In den Bereichen Informations- und Datenschutz sind zudem hauptsächlich Juristen tätig, die in der Regel mit den Belangen der Informatiksicherheit nur marginal vertraut sind. Sie tendieren dazu, die Problematik hauptsächlich als rechtliche Angelegenheit zu betrachten und sind oft nicht in der Lage, die tatsächliche Umsetzung der Sicherheitsanforderungen in IKT-Projekten zu begleiten oder zu überprüfen. Bei den Spezialisten aus dem Bereich IKT-Sicherheit verhält es sich umgekehrt. Sie kennen sich häufig in Sachen Informations- oder Datenschutz zu wenig gut aus.

  Diese Feststellungen sind ebenfalls für die Fachstellen gültig. Fast alle Fachstellen sind im Vergleich mit den zu erledigenden Arbeiten personell unterdotiert. Die kritische Masse wird nirgends erreicht. Teilweise fehlt ihnen überdies genügendes Fachwissen aus den anderen Bereichen. Zudem sind insbesondere im Bereiche der Informatiksicherheit sehr viele Akteure vorhanden, die ergänzende Aufgaben wahrnehmen. Diese Aufgaben und Dienste werden aber teilweise nicht koordiniert oder überhaupt nicht in Anspruch genommen (z.B. die Dienste der Kryptologen des VBS).

  Spezialisten der Informationssicherheit, sowohl im technischen Bereich als auch im Management, sind heute gefragter als je zuvor. Der Bund verfügt über solche Spezialisten. Vielfach nehmen diese aber nicht vollzeitlich Aufgaben aus dem Bereich der Informationssicherheit wahr. Es ist daher fraglich, ob diese knappen Ressourcen richtig eingesetzt werden.

- *Die Befugnisse der verschiedenen Akteure sind häufig ungenügend.*

  Gravierend erscheint die Erkenntnis, dass die Umsetzung beschlossener Massnahmen der Informationssicherheit nur äusserst selten überprüft wird. In der Regel sind nämlich weder die Fachstellen noch die verschiedenen Beauftragten befugt, Kontrollen durchzuführen. Ohne Kontrolle ist es aber nicht möglich, zu beurteilen, ob die Massnahmen wirksam sind oder ob Lücken und Schwachstellen vorhanden sind.

- *Das Sicherheitsbewusstsein ist mangelhaft.*

  In den Departementen und in der Bundeskanzlei werden die Themen der Informationssicherheit sehr unterschiedlich gewichtet. Massgebend für die Sensibilisierung der Mitarbeitenden ist in erster Linie das Engagement der Vorgesetzten und insbesondere der Geschäftsleitungen.

1.3.1.6 Beurteilung des Standes und Folgen

Die heutige Organisation wuchs aus sektoriellen gesetzlichen und materiellen Bedürfnissen. Sie lieferte lange Zeit genügende Resultate. Mit der Entwicklung zu einer Informationsgesellschaft wurden aber die Bedro-

7 Unter *COMSEC* wird die Kommunikationssicherheit verstanden im Sinne der Anwendung von Sicherheitsmassnahmen auf die Telekommunikation, um zu verhindern, dass Unbefugte in den Besitz wertvoller Informationen gelangen, die aus dem Zugriff auf die Telekommunikation und deren Auswertung gewonnen werden könnten, oder um die Authentizität, die Vertraulichkeit und die Integrität der Telekommunikation sicherzustellen.

hungen für Informationen und IKT-Mittel komplexer und dynamischer. Ihnen muss integral begegnet werden, was entsprechende rechtliche und organisatorische Vorkehren sowie erhöhtes Fachwissen und - kompetenz voraussetzt. Es ist offensichtlich, dass die Organisation des Bundes diesen Anforderungen nicht genügt.

Folgende Punkte sind für die Verbesserung dieser Organisation wichtig:

- Die Verantwortung für die Umsetzung der Vorgaben muss bei der Führungsebene bleiben. Diese muss aber auf allen Ebenen kompetenter beraten und unterstützt werden.
- Die künftige Organisation der Informationssicherheit muss sich vermehrt auf die frühzeitige Erkennung und Behandlung der Risiken fokussieren. Dies setzt ein systematisches Risikomanagement im Bereich der Informationssicherheit voraus, das heute grösstenteils noch fehlt. Es verlangt aber auch eine bessere Kontrolle bei der Umsetzung von risikomindernden Massnahmen.
- Die verschiedenen Fachorgane müssen soweit möglich zusammengeführt werden, um Synergien zu nutzen und Skaleneffekte zu erzielen. So können auch die Zuständigkeitsprobleme systemisch gelöst und das interdisziplinäre Fachwissen erhöht werden. Eine vollständige Zusammenführung der Fachorgane ist jedoch nicht möglich. Bei den verbleibenden Fachorganen müssen aber die Zuständigkeiten und Verantwortlichkeiten klarer definiert und die Koordination und der Wissensaustausch verbessert werden.
- Bei den verschiedenen Beauftragten kann durch zunehmende Professionalisierung eine Erhöhung der Kompetenzen erreicht werden. Die Professionalisierung würde verbessert, wenn die Managementaufgaben der Informationssicherheit auf möglichst wenige Funktionsinhaber konzentriert würden.
- Besondere Aufmerksamkeit ist der Funktionstrennung und -zuordnung zu schenken. Die Beauftragten sollten nicht einem Fachbereich unterstellt sein, dessen Risiken sie objektiv und unabhängig beurteilen müssen. Sie sollten auch keine Aufgaben wahrnehmen, die sie in einen Interessenkonflikt verwickeln könnten.

Die vorstehenden Ausführungen zeigen auf, dass eine Zusammenlegung der drei Ausschüsse anzustreben ist. Es liegt jedoch auf der Hand, dass die gewünschte Zusammenlegung der Ausschüsse nicht dazu führen soll, dass die einzelnen Themen (Klassifizierung, Datenschutz oder technische Sicherheit) nicht mehr speziell behandelt werden. Diese Behandlung soll lediglich in einem konsolidierten Gremium stattfinden, das seine Agenda nach dem tatsächlichen Bedarf festlegt.

1.3.2 Neuregelung der Organisation auf Stufe Bund

Die Vorlage trägt den Ergebnissen des bundesrätlichen Prüfauftrags bezüglich der heutigen Organisation der Informationssicherheit Rechnung. Die Lösung des Gesetzesentwurfs liefert die Grundlage für eine Klärung und Vereinfachung der diesbezüglichen Zuständigkeiten und Verantwortlichkeiten. Sie legt auch ein Schwergewicht auf die Kompetenzbildung der Stellen, die für den Vollzug zuständig sind, durch die Unterstützung und Beratung durch Sachverständige und durch einen verstärkten Informationsaustauch zwischen diesen Stellen. Der Entwurf sieht in der Folge eine einzige Beauftragtenrolle (Informationssicherheitsbeauftragte/r), ein einziges Koordinationsorgan sowie eine Fachstelle des Bundes für Informationssicherheit, die alle Querschnittaufgaben der Informationssicherheit wahrnehmen sollen, vor. Mit der beantragten Neuregelung sollen in der Bundesverwaltung die Vollzugsstrukturen der bisherigen Bereiche des Informationsschutzes und der Informatiksicherheit vollständig zusammengelegt werden.

1.3.2.1 Informationssicherheitsbeauftragte

Die neue Rolle des Informationssicherheitsbeauftragten ist für den Vollzug des Gesetzesentwurfs zentral. Diese neue Funktion ist vor allem eine Managementfunktion. Die Informationssicherheitsbeauftragten werden sich nicht primär mit hochtechnischen Informationssicherheitsfragen befassen, sondern im Auftrag ihrer Behörde (oder der Departemente und der BK) die Fachorganisation der Informationssicherheit steuern sowie die Umsetzung der beschlossenen Massnahmen überprüfen. Schwergewichte werden sie auch auf das Risikomanagement sowie auf die Koordination mit anderen Bereichen legen müssen. Eine wirksame, risikogerechte Aufgabenerfüllung durch die Informationssicherheitsbeauftragten setzt - neben einer klaren Unterstützung durch die Geschäftsleitung- eine enge Zusammenarbeit mit den Stellen, die für das allgemeine Risikomanagement, den Datenschutz und die Sicherheit zuständig sind, voraus. Die Informationssicherheitsbeauftragten werden also als Drehscheibe zwischen der Geschäftsleitung und den Stellen, die für die Umsetzung der Massnahmen zuständig sind, agieren.

Bei den Departementen und der Bundeskanzlei wird diese neue Funktion die bisher getrennten Rollen der Informationsschutzbeauftragten und Informatiksicherheitsbeauftragten ersetzen. Der Bundesrat soll auf Verordnungsebene beschliessen, ob eine entsprechende Zusammenlegung der Funktionen auf Stufe Verwaltungseinheit zweckmässig und erforderlich ist.

1.3.2.2 Konferenz der Informationssicherheitsbeauftragten

Es ist ein deklariertes Ziel dieses Gesetzes, ein möglichst einheitliches Sicherheitsniveau für die verschiedenen Bundesbehörden und Organisationen zu erreichen. Aufgrund der verfassungsmässigen Unabhängigkeit der Behörden kann dieses einheitliche Sicherheitsniveau nur erreicht werden, wenn in Bezug auf die Informationssicherheit trotz teilweise unterschiedlicher Bedürfnisse eine möglichst einheitliche Fachdoktrin herrscht. Aufgrund ihrer Stellung haben die Informationssicherheitsbeauftragten (Art. 84) umfassende Kenntnisse der Situation und der Probleme der Informationssicherheit in ihrem Zuständigkeitsbereich, insbesondere der Umsetzbarkeit und Wirksamkeit der Vorschriften und Massnahmen. Es bietet sich daher an, als Koordinationsorgan eine Konferenz dieser Beauftragten zu institutionalisieren.

Die vorgesehene Konferenz der Informationssicherheitsbeauftragten wird sich hauptsächlich mit der behördenübergreifenden Koordination des Vollzugs beschäftigen. Sie wird dabei eine wichtige Rolle für die Bildung einer einheitlichen Doktrin sowie für den nötigen Erfahrungsaustausch spielen. Die Informationssicherheitsbeauftragten der Departemente und der Bundeskanzlei sowie ein Vertreter des EDÖB sollen ebenfalls Einsitz haben. Für strategische Fragen der Informationssicherheit soll die Konferenz auch Fachexperten aus den Kantonen, der Wissenschaft oder der Wirtschaft beiziehen können.

Diese Konferenz wird für die Bundesverwaltung den heutigen Koordinationsausschuss für den Informationsschutz im Bund (ISchV) sowie den Ausschuss Informatiksicherheit (BinfV) ersetzen, wobei die technischen Angelegenheiten weiterhin in unterstellten Fachorganen behandelt werden sollen.

1.3.2.3 Fachstelle des Bundes für Informationssicherheit

Die Informationssicherheit muss nach einem integralen Ansatz organisiert, gesteuert und überprüft werden, Aufgaben nach diesem Gesetz, die heute bereits bestehen, werden von verschiedenen Fachorganen wahrgenommen. In der Folge werden sie nach einer sektoriellen Betrachtungsweise konzipiert und angegangen sowie kaum aufeinander abgestimmt. Eine verbesserte Koordination alleine wird nicht genügen, um dem integralen Ansatz der Informationssicherheit zu verwirklichen. Die Fachstelle ist in der Vorlage vor allem als Kompetenzzentrum für die behördenübergreifenden Aufgaben konzipiert. Es kommen ihr deshalb keine Weisungsbefugnisse zu: Sie handelt grundsätzlich immer auf Antrag oder im Auftrag einer verpflichteten Behörde. Ihr Auftrag ist unterstützend und beratend zu verstehen.

Die konkreten behördenübergreifenden Aufgaben der Fachstelle werden abschliessend im Gesetz festgehalten. Nebst Beratung und Unterstützung soll die Fachstelle auch beauftragt werden können, die Risiken beim Einsatz neuartiger Technologien zu beurteilen oder im Rahmen wichtiger behördenübergreifender Projekte die Belange der Informationssicherheit zu steuern und zu koordinieren. Eine weitere Kernaufgabe der Fachstelle soll (auf Antrag der verpflichteten Behörden) die Prüfung sicherheitsrelevanter Aspekte bestimmter Prozesse, Mittel und Dienstleistungen darstellen. Wird bestätigt, dass diese betreffenden Prozesse, Mittel oder Dienstleistungen die Standardanforderungen des Bundes erfüllen, können sie standardisiert werden und somit auch von anderen Behörden oder Organisationen des Bundes eingesetzt werden (Aufwandreduktion). Ferner soll sie auch beauftragt werden dürfen, Sicherheitskontrollen und -audits durchzuführen. Schliesslich soll die Fachstelle im internationalen Verhältnis als Ansprechstelle für Fachkontakte mit ausländischen und internationalen Stellen im Bereich der Informationssicherheit gelten. Diese Rolle ist für die Umsetzung völkerrechtlicher Verträge erforderlich (s. Art. 90 sowie Ziff. 4.2).

Der Bundesrat soll auf Verordnungsebene die Organisation der Fachstelle regeln. Hierzu soll er bestimmen, welche Aufgaben die Fachstelle selbst oder in Zusammenarbeit mit anderen Bundesstellen erfüllen soll. Aktuell nehmen in der Bundesverwaltung viele Stellen Querschnittaufgaben im Bereich der Informationssicherheit wahr, die zum gesetzlichen Pflichtenheft der künftigen Fachstelle des Bundes gehören. Die Fachstelle soll z.B. für die Bundesverwaltung bestimmte Aufgaben übernehmen, die heute durch das ISB-Sec und die IOS wahrgenommen werden. Die Aufgaben bestehender Verwaltungseinheiten werden demzufolge auf Verordnungsebene neu definiert und bestimmte Schnittstellen überprüft werden müssen.

Der Bundesrat wird in diesem Zusammenhang selbstverständlich noch über die heikle Frage der administrativen Zuordnung der Fachstelle entscheiden müssen. Diese Frage soll im Interesse der Organisationsautonomie des Bundesrates nicht auf formell-gesetzlicher Stufe beantwortet werden. Die Ansiedelung der Fachstelle soll dem Bundesrat erst beantragt werden, wenn klar ist, welche Aufgaben und Kompetenzen ihr zugewiesen werden, und ein detailliertes Konzept zur Umsetzung der gesetzlichen Vorgaben für die Bundesverwaltung und die dadurch verpflichteten Organisationen des öffentlichen und privaten Rechts vorliegt.

1.3.3 Neuregelung für die Bundesverwaltung und weitere verpflichtete Organisationen

Im behördenübergreifenden Rahmen verfügt die Fachstelle des Bundes für Informationssicherheit also *bei Design* über keine *rechtliche* Durchsetzungskraft. Für die Bundesverwaltung sowie für die verpflichteten

Organisationen des öffentlichen und privaten Rechts, die den Vollzugsbestimmungen des Bundesrats unterstehen, kann der Bundesrat hingegen der Fachstelle weitere Kompetenzen erteilen sowie ihre Verhältnisse zur Führungslinie und zu den Informationssicherheitsbeauftragten differenziert gestalten. Obschon die Verantwortung für die Umsetzung der Vorgaben grundsätzlich bei der Führungsebene bleiben muss, hat sich im Rahmen der Gesetzgebungsarbeiten eine klare Mehrheit der Beteiligten für eine verstärkte Durchsetzungskompetenz der Fachstelle, insbesondere im Bereich Kontrollen, ausgesprochen.

In diesem Zusammenhang wurde von einigen Stellen verlangt, dass bereits jetzt Optionen zur Organisation des Vollzugs innerhalb der Bundesverwaltung mit Vor- und Nachteilen zugewiesen und zum Entscheid vorgelegt werden. Dabei sollten ein Modell mit komplett dezentraler Vollzugsorganisation und reiner Koordinationsfunktion der Fachstelle sowie eines mit zentraler Weisungsbefugnis der Fachstelle gegenüber den Informationssicherheitsbeauftragten der Departemente gegenübergestellt werden. Obschon die Erstellung und die Beurteilung solcher Umsetzungsmodelle zwingend notwendig sind, können derartige Fragen erst zu einem späteren Zeitpunkt seriös beantwortet werden. Bevor über die detaillierte Umsetzung in der Bundesverwaltung entschieden werden kann, müssen die übergeordneten Grundsätze dieser Vorlage, ihre materiellen Inhalte sowie die behördenübergreifenden Verhältnisse geklärt werden.

2 Erläuterungen zu den einzelnen Artikeln

2.1 Bundesgesetz über die Informationssicherheit

Titel

In Bezug auf den Titel des Erlasses sind zwei Präzisierungen wichtig:

- Der Erlass stellt kein allgemeines Informationssicherheitsgesetz dar. Er richtet sich primär an die Bundesbehörden sowie an zu bestimmende Organisationen des öffentlichen und privaten Rechts, die Aufgaben des Bundes erfüllen. Dritte können zwar vom Gesetz erfasst werden, wenn sie mit Informationen oder mit Mitteln und Einrichtungen der Informations- und Kommunikationstechnologie (IKT-Mitteln) des Bundes umgehen. Dies geschieht jedoch nur durch die Anwendung der relevanten Bestimmungen durch eine Behörde oder eine Organisation des Bundes.
- Beim Begriff "*Informationssicherheit*" wird grundsätzlich auf die derzeit gängigen Normenwerke abgestellt. Die Informationssicherheit umfasst demnach die Gesamtheit aller Anforderungen und Massnahmen, mit denen die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Nachvollziehbarkeit von Informationen sowie die Verfügbarkeit und die Integrität von IKT-Mitteln geschützt wird. Die Informationssicherheit darf nicht auf die IKT-Sicherheit reduziert werden. Sie umfasst nämlich alle Bearbeitungsvorgänge, also auch Papierdokumente sowie mündliche Äusserungen, und nicht nur die Bearbeitung von Informationen mittels der elektronischen Infrastruktur des Bundes. Vom Begriff wird auch die Umsetzung der Schutzanforderungen der Datenschutzgesetzgebung oder anderer Gesetze, die Anforderungen an den Schutz von Informationen festlegen, erfasst.

Ingress

S. Ziff. 4.1.

2.1.1 Allgemeine Bestimmungen

Art. 1

Diese Bestimmung fasst den Zweck des Erlasses in allgemeiner Form zusammen.

Abs. 1 weist darauf hin, dass sowohl die Informationen als solche als auch die IKT vom Gesetz erfasst werden. Der Begriff "Information" wird im vorliegenden Informationssicherheitsgesetz (ISG) nicht definiert, da im Erlass auf Legaldefinitionen verzichtet wird und der Begriff im ISG sich mit dem umgangssprachlichen Gebrauch deckt. Das Gesetz macht grundsätzlich auch keinen Unterschied zwischen "Informationen" und "Daten": Beide Begriffe werden unter den Begriff "Informationen" subsumiert. Im Gesetz wird der Begriff "Daten" nur dann verwendet, wenn Personendaten nach dem DSG betroffen sind. Mit dem Begriff "*IKT-Mittel*" werden im ISG alle Einrichtungen, Geräte, Systeme und Anwendungen erfasst, die zur elektronischen Bearbeitung (inkl. Speicherung und Kommunikation) von Informationen verwendet werden. Zur ausdrücklichen Erwähnung der IKT im Zweckartikel s. Ziff. 1.2.2.1.

Abs. 2: Sicherheit ist kein Selbstzweck. Der Schutz der Informationen dient bestimmten öffentlichen Interessen bzw. Eigeninteressen des Bundes als Institution. Geschützt werden hier also primär die Interessen des Bundes bzw. der Schweiz und nicht diejenigen Dritter. Diese Interessen werden abschliessend aufgelistet (Bst. a-e). Die Liste orientiert sich im Wesentlichen an der bereits bestehenden Liste von Art. 7 Abs. 1 BGÖ. Diese nennt die Bereiche, in denen der Zugang zu amtlichen Dokumenten eingeschränkt, aufgeschoben oder

verweigert werden kann. Die Liste von Art. 1 Abs. 2 ISG ist allerdings mit derjenigen des BGÖ nicht völlig identisch, da die Ziele und der Geltungsbereich des BGÖ und des vorliegenden Entwurfs nicht die Gleichen sind (zu den Verhältnissen zwischen ISG und BGÖ, s. Art. 3 Abs. 1).

Das vorliegende Gesetz schützt folgende Interessen:

- Bst. a: Der Schutz der Entscheidungs- und Handlungsfähigkeit der Bundesbehörden durch Massnahmen der Informationssicherheit ist ein Kerninteresse dieses Gesetzes. Die Bundesbehörden sind für die Erfüllung ihrer verfassungsmässigen und gesetzlichen Aufgaben immer mehr von der Verfügbarkeit, der Integrität sowie, in bestimmten Fällen, der Vertraulichkeit ihrer Informationen sowie vom zuverlässigen Funktionieren der Informatikinfrastruktur abhängig (s. auch Art. 7 Abs. 1 Bst. a und b BGÖ sowie Ziff. 2.2.2.1.1-2 der BGÖ-Botschaft).
- Bst. b: Mit diesem Interesse werden in erster Linie Informationen aus dem Bereich des Polizei-, Zoll-, Nachrichtendienst- und Militärwesens und der Landesversorgung sowie die Mittel, welche die Bundesbehörden zur Sicherstellung der inneren und äusseren Sicherheit einsetzen geschützt. Derartige Informationen weisen oft einen erhöhten Bedarf an Vertraulichkeit auf, da ihr Missbrauch existenzgefährdende Folgen für den Staat, die Bevölkerung oder bestimmte Personen oder Personengruppen haben kann. Aus demselben Grund müssen die IKT-Mittel der Behörden, welche zur Unterstützung von kritischen Sicherheitsaufgaben eingesetzt werden, auch in Krisenzeiten stets verfügbar und funktionstüchtig bleiben (s. auch Art. 7 Abs. 1 Bst. d BGÖ sowie Ziff. 2.2.2.1.3 der BGÖ-Botschaft).
- Bst. c: Die Aussenbeziehungen zählen gemeinsam mit den Sicherheitsfragen zu den sensitiven Bereichen staatlicher Tätigkeit. Im Vordergrund steht hier die Wahrung der Vertraulichkeit von Informationen. Insbesondere die Informationsbeschaffung über Situationen und Vorgänge im Ausland sowie die Absichten ausländischer und internationaler Behörden sind für die Führung der Aussenpolitik und die Pflege der Aussenbeziehungen von grosser Bedeutung. Für die erfolgreiche Verhandlungsführung ist es entscheidend, dass die entsprechenden Strategien und Absichten nicht zur Kenntnis der Gegenpartei oder der Öffentlichkeit gelangen. Ähnliches gilt für diplomatische Schritte im zwischenstaatlichen Verkehr. Zu erwähnen ist schliesslich, dass die Schweiz auf Grund internationaler vertraglicher Verpflichtungen oder anerkannter Staatenpraxis gehalten sein kann, gewisse ausländische Dokumente nicht öffentlich zugänglich zu machen (s. auch Art. 7 Abs. 1 Bst. d BGÖ sowie Ziff. 2.2.2.1.4 der BGÖ-Botschaft).
- Bst. d: Die unberechtigte Bekanntgabe oder die Verfälschung bestimmter Informationen sowie aus diesem Bereich die Störung von Informationssystemen der Bundesbehörden können zu erheblichem Schaden für die wirtschafts-, finanz- oder währungspolitischen Interessen der Schweiz führen. Beim heutigen unerbittlichen internationalen Wettbewerb gewinnen diese wirtschaftlichen Interessen zusätzlich an Bedeutung (s. auch Art. 7 Abs. 1 Bst. f BGÖ sowie Ziff. 2.2.2.1.6 der BGÖ-Botschaft).
- Bst. e: Hier wird der Bereich *Compliance*, d.h. die Einhaltung der gesetzlichen und vertraglichen Verpflichtungen der Bundesbehörden zum Schutz von Informationen erfasst, die nicht unter die Bst. a-d fallen. Die Bundesbehörden bearbeiten nämlich zur Erfüllung ihrer gesetzlichen Aufgaben sehr viele Informationen, die sie aufgrund verschiedenster gesetzlicher Bestimmungen schützen müssen (z.B. DSG, RVOG, ParlG, NBG, BÖB, FHG, HMG, usw.) oder die sie von Dritten nur unter Bedingung der Gewährleistung eines angemessenen Schutzes. Berufs-, Geschäfts- und Fabrikationsgeheimnisse oder die Wahrung der Vertraulichkeit und Integrität von Personendaten stellen zwar keine unmittelbaren Eigeninteressen des Bundes dar. Wenn bekannt wird, dass die Bundesbehörden ihre Verpflichtungen zum Schutz dieser Informationen nicht einhalten, kann jedoch ihre Vertrauenswürdigkeit erheblich darunter leiden. Bst. e stellt somit ein Auffangbecken für alle Informationen dar, welche die Bundesbehörden bearbeiten und schützen, aber nicht unbedingt klassifizieren müssen. Er schützt überdies das Interesse der Bundesbehörden an der Aufrechterhaltung ihrer hohen Vertrauenswürdigkeit. (s. auch Art. 7 Abs. 1 Bst. e, g und h BGÖ sowie Ziff. 2.2.2.1.5 und 2.2.2.1.7-8 der BGÖ-Botschaft).

Art. 2

Art. 2 erfasst den institutionellen bzw. verwaltungsorganisatorischen Anwendungsbereich.

Abs. 1 legt fest, welche Behörden verpflichtet werden, das Gesetz in ihrem Zuständigkeitsbereich anzuwenden. Als verpflichtete Behörden werden die Bundesversammlung bzw. die eidgenössischen Räte, der Bundesrat, die eidgenössischen Gerichte (Bundesgericht, Bundesstrafgericht, Bundesverwaltungsgericht, Bundespatentgericht), die Schweizerische Bundesanwaltschaft und ihre Aufsichtsbehörde sowie - im Interesse der Währungs- und Wirtschaftspolitik des Bundes - die Schweizerische Nationalbank genannt. Alle diese Institutionen unterstehen in ihrer Tätigkeit als Behörden keiner unmittelbaren Weisungsbefugnis einer anderen Behörde. Sie sollen aber infolge des behördenübergreifenden Informationsflusses für ihren eigenen organisatorischen Zuständigkeitsbereich zur Anwendung dieses Erlasses verpflichtet werden. Sofern das Gesetz

Rechtsetzungsdelegationen enthält, spricht es diese Behörden stets als "*die verpflichteten Behörden*" an. Zu den Gründen, weshalb alle Bundesbehörden vom Gesetz erfasst werden sollen, s. Ziff. 1.2.2.2.

Es versteht sich, dass das Gesetz bei einzelnen Regelungen der verfassungsmässigen Stellung und den Besonderheiten der verschiedenen Behörden bzw. Institutionen Rechnung zu tragen hat. Es enthält daher z.B. Ausnahmen von der Pflicht zur Personensicherheitsprüfung (PSP) bei den vom Volk gewählten Personen sowie Ausnahmen bei bestimmten Vollzugszuständigkeiten, insbesondere im Bereich der eidgenössischen Gerichte. In denjenigen Bestimmungen des Erlasses, die nur Pflichten für bestimmte Behörden oder Organisationen enthalten, werden diese entsprechend spezifiziert (s. z.B. Art. 19, 33 Abs. 4, 35, 36 und 84 Abs. 1). Auf der Ebene des Gesetzes kann aber nicht die gesamte Vollzugsorganisation der verschiedenen Behörden und die Kompetenzen ihrer Organe bzw. Stellen festgelegt werden. Dies hat durch die entsprechende Vollzugsrechtsetzung der einzelnen Behörden zu erfolgen.

Abs. 2 berücksichtigt, dass die in Absatz 1 erwähnten Behörden sich nur beschränkt mit eigentlichen Vollzugsaufgaben zu befassen haben und dass die ihnen unterstellten Organisationen im Bereich ihrer gesetzlichen Aufgaben von den neuen Regelungen im Rahmen ihrer Zuständigkeiten unmittelbar verpflichtet sein sollen. Die Aufteilung zwischen Behörden und unterstellten Organisationen soll insbesondere sicherstellen, dass das unterschiedliche Organisationsrecht der erfassten Behörden von der neuen Regelung nicht angetastet wird. Einerseits sollen die verpflichteten Behörden selbst keine untergeordneten Vollzugsaufgaben übernehmen müssen, andererseits sollen aber die erfassten Organisationen keine vom Organisationsrecht abweichenden Rechtsetzungs- oder Entscheidbefugnisse erhalten. Der Begriff "*verpflichtete Organisationen*" wird im Interesse der gesetzestechnischen Vereinfachung der nachfolgenden Artikel als Kurzbezeichnung eingeführt. Es handelt sich insbesondere um die Parlamentsdienste, die Verwaltungen der einzelnen eidgenössischen Gerichte, die Departemente, die Bundeskanzlei, die Bundesverwaltung einschliesslich der dezentralen Verwaltungseinheiten sowie die Armee.

- Bst. d sieht eine grundsätzliche Unterstellung unter das Gesetz vor für Organisationen des öffentlichen und privaten Rechts, die Verwaltungsaufgaben des Bundes im Sinne von Art. 2 Abs. 4 RVOG erfüllen und dabei der Aufsicht des Bundes unterstehen (s. dazu Art. 8 Abs. 4 und 5 RVOG). Es sind dies insbesondere Organisationen, die durch Gesetz gegenüber Privaten verfügungsbefugt sind. In diesem Zusammenhang Voraussetzung für eine Unterstellung ist, dass diese Organisationen im Rahmen der Erfüllung ihrer Verwaltungsaufgaben sicherheitsempfindliche Tätigkeiten (s. Abs. 3) ausüben. Die Unterstellung gilt nur für diese Verwaltungsaufgaben. Es nicht praktikabel, im Rahmen des vorliegenden Erlasses abschliessend und auf Dauer die einzelnen unterstellten Organisationen zu bestimmen. Der Bundesrat soll deshalb auf Verordnungsebene festlegen, wer unterstellt ist und in welchem Ausmass (s. Art. 87 Abs. 4).
- Bst. e: Bund und Kantone sind für ihre jeweilige Aufgabenerfüllung auf eine sehr enge Zusammenarbeit angewiesen. Sie tauschen sehr viele Informationen untereinander aus. Darunter fallen auch klassifizierte Informationen des Bundes. Die IKT-Infrastrukturen und Systeme des Bundes und der Kantone werden zudem vermehrt untereinander vernetzt. Dadurch wird das Risiko erhöht, dass sich Angriffe sowie Bedrohungen im Zuständigkeitsbereich einer Behörde auf die Zuständigkeitsbereiche anderer Beteiligter ausbreiten. Die Kantone sind für ihre eigene Informationssicherheit selbst zuständig. Wenn sie aber Bundesaufgaben unter unmittelbarer Aufsicht des Bundes erfüllen, dann gelten grundsätzlich die Vorgaben des Bundes auch für sie. Das Gesetz sieht eine Unterstellung der Kantone nach risikobasierten Kriterien vor: Sie sollen nur für die Erfüllung von Aufgaben unterstellt werden, wenn sie dabei im Auftrag des Bundes und unter seiner unmittelbaren Aufsicht sicherheitsempfindliche Tätigkeiten (s. Abs. 3) ausüben.

  Kantonale Behörden und Stellen, die Bundesrecht in eigener Kompetenz umsetzen, werden vom Gesetz nicht erfasst. Vom ISG nicht speziell geregelt ist die Vernetzung von kantonalen Netzwerken und Bundesnetzwerken. In solchen Fällen müssen die Behörden des Bundes und der Kantone der Situation angepasste Sicherheitsmassnahmen vereinbaren, die das vom Gesetz für die Bundesbehörden verlangte Schutzniveau materiell gewährleisten. Zum Vollzug durch die Kantone, s. Art. 89.

Abs. 3 umschreibt den für die Anwendung dieses Gesetzes zentralen Begriff der "*sicherheitsempfindlichen Tätigkeit*". Die Ausübung einer sicherheitsempfindlichen Tätigkeit ist nämlich nicht nur Voraussetzung für die Anwendung des Gesetzes auf Organisationen des öffentlichen und privaten Rechts, die Verwaltungsaufgaben erfüllen, und auf die Kantone, sondern auch für die Durchführung von Personensicherheitsprüfungen oder von Betriebssicherheitsverfahren bei Dritten, die mit Aufträgen des Bundes betraut werden sollen. Die sicherheitsempfindliche Tätigkeit wird im Kontext der Informationssicherheit definiert. Bei ihrem materiellen Inhalt steht - wie im heutigen BWIS - der Umgang mit Informationen im Vordergrund. Bei ihrer Definition wurde auf Parallelität zu den Regelungen über den Schutz klassifizierter Informationen sowie über die Sicherheit beim Einsatz von IKT-Mitteln geachtet.

- Bst. a: Mit der Anführung der Klassifizierungsstufe VERTRAULICH als Ausgangspunkt für die Definition der sicherheitsempfindlichen Tätigkeit wird implizit festgelegt, dass die Sicherheitsempfindlichkeit einer Tätigkeit erst dann angenommen wird, wenn die Interessen nach Art. 1 Abs. 2 mindestens *erheblich* beeinträchtigt werden können. Sicherheitsempfindlich beim Umgang mit klassifizierten Informationen ist zudem nicht der blosse "*Zugang*" zu diesen Informationen, sondern deren tatsächliche und berechtigte "*Bearbeitung*". Mit anderen Worten übt z.B. das Reinigungspersonal in der Regel keine sicherheitsempfindliche Tätigkeit nach dem vorliegenden Gesetz aus, obwohl die Wahrscheinlichkeit gross ist, dass es während seiner Tätigkeit hin und wieder faktischen Zugang zu klassifizierten Informationen erhalten wird, weil die Mitarbeitenden die Sicherheitsvorschriften nicht immer einhalten.

  Erwähnt ist auch der Umgang mit klassifiziertem Material. Es handelt sich dabei um verschiedene Materialien und Gegenstände, deren Existenz oder Beschaffenheit als solche vor der Kenntnisnahme durch Unberechtigte geschützt werden muss oder deren Eigenschaften klassifizierte Informationen vermitteln können: das Material *ist* bzw. enthält also die Information. Betroffen sind hauptsächlich Rüstungsgegenstände, Waffensysteme oder integrierte Kommunikationssysteme. Häufig schreibt ein Drittstaat, der die Lieferung an die Schweiz bewilligt hat, eine Klassifizierung solcher Materialien und Gegenstände vor. Die Schweiz kennt entsprechende Klassifizierungen bis heute nur im Armeebereich; im Zivilbereich (z.B. Polizei und Grenzwachtkorps) fehlte bis anhin eine entsprechende Grundlage, die nun mit dieser Bestimmung implizit geschaffen wird.
- Bst. b: Hier werden Tätigkeiten erfasst, die mit besonderen Zugriffsrechten auf IKT-Mittel der beiden höheren Sicherheitsstufen verbunden sind oder bei deren Ausübung Personen in der Lage sind, z.B. durch Datendiebstahl oder Sabotage die Interessen nach Art. 1 Abs. 2 erheblich zu beeinträchtigen. Die blosse Benützung dieser IKT-Mittel wird also nicht als sicherheitsempfindlich betrachtet (ob die Anwender eine sicherheitsempfindliche Tätigkeit ausüben entscheidet sich aufgrund der Inhalte der bearbeiteten Informationen). Bst. b erfasst vor allem bestimmte Administratoren oder Anwendungsverantwortliche.
- Bst. c: Als sicherheitsempfindlich wird schliesslich der Zugang zu den in Art. 31 geregelten Sicherheitszonen der Informationssicherheit bezeichnet, weil das Schadenspotenzial bei Spionage oder bei Sabotage in diesen Zonen aufgrund der darin befindlichen Informationen und IKT-Mittel sehr hoch ist.

Abs. 3 enthält weitere Abweichungen von der bisherigen Regelung in Art. 19 Abs. 1 BWIS. So stellt nach dem vorliegenden Gesetz der regelmässige Zugang zu besonders schützenswerten Personendaten, deren Offenbarung die Persönlichkeitsrechte der Betroffenen schwerwiegend beeinträchtigen könnte, keine sicherheitsempfindliche Tätigkeit mehr dar. Der Umgang mit Geschäfts- und Fabrikationsgeheimnissen soll ebenfalls nicht als sicherheitsempfindlich im Sinne des ISG gelten. Zu beachten bleibt, dass ein Teil der Schutzbedürfnisse im Bereich der Personendaten sowie der Geschäfts- und Fabrikationsgeheimnisse über die Regelungen im Bereich der IKT-Mittel abgedeckt wird. Eine andere wichtige Änderung im Vergleich zur heutigen Regelung liegt darin, dass das Element der Regelmässigkeit bei der Ausübung der aufgeführten Tätigkeiten nicht Bestandteil der Sicherheitsempfindlichkeit dieser Tätigkeiten ist. Die einmalige Bearbeitung von als VERTRAULICH klassifizierten Informationen gilt also für das ISG bereits als sicherheitsempfindlich. Diese Änderung ist in Bezug auf die Sicherheitsüberprüfung von Dritten, die Aufträge des Bundes ausführen sollen, notwendig. Da diese Kategorie von Personen ihre Tätigkeiten nicht ständig im Kontrollbereich der verpflichteten Behörden oder Organisationen ausüben werden, müssen *für sie* differenzierte Voraussetzungen für die Unterstellung unter die PSP gelten.

Zum Verhältnis zu den Personensicherheitsprüfungen, s. Ziff. 1.2.4.

Art. 3

Abs. 1: Mit einem Vorbehalt für die Bestimmungen des BGÖ wird klar festgehalten, dass der Geltungsbereich des Öffentlichkeitsgesetzes durch die Regelung der Informationssicherheit in keiner Art und Weise eingeschränkt wird. Informationen, die nach dem ISG klassifiziert worden sind, fallen nicht unter den Vorbehalt von Art. 4 BGÖ (Spezialbestimmungen, die bestimmte Informationen als geheim bezeichnen). Demnach finden die Bestimmungen des BGÖ über den Zugang zu amtlichen Dokumenten auch auf Informationen Anwendung, die nach dem ISG klassifiziert worden sind.

Die Beurteilung von Dokumenten im Verfahren nach dem BGÖ erfolgt unabhängig von den Regelungen des ISG. Bei Gesuchen um Zugang zu amtlichen Dokumenten überprüft die zuständige Stelle also unabhängig von einem allfälligen Klassifizierungsvermerk, ob der Zugang zu gewähren, zu beschränken, aufzuschieben oder zu verweigern ist. Die Klassifizierung von Informationen kann bei der Beurteilung von Dokumenten nach BGÖ jedoch als Indiz für die Nichtöffentlichkeit des entsprechenden Dokuments gewertet werden. Der Entscheid zur Klassifizierung setzt nämlich eine Beurteilung des Schutzbedarfs der Information hinsichtlich einer Beeinträchtigung der öffentlichen Interessen nach Art. 1 Abs. 2 ISG voraus, die im Grunde genommen

materiell einer Beurteilung über die Einschränkung, Aufschiebung und Verweigerung des Zugangs nach Art. 7 Abs. 1 BGÖ entsprechen müsste. Die Bestimmungen über die Klassifizierung sind inhaltlich so gestaltet, dass sie dem Ausnahmekatalog nach Art. 7 BGÖ inhaltlich nicht widersprechen müssten.

Im Übrigen ist darauf hinzuweisen, dass der Anwendungsbereich des ISG im Grundsatz weiter als jener des BGÖ gefasst werden soll, indem das ISG für sämtliche Bundesbehörden anwendbar sein soll. Es konzentriert sich zudem nicht nur auf den Schutz der Vertraulichkeit, sondern schützt auch die Verfügbarkeit, Integrität und Nachvollziehbarkeit von Informationen.

Abs. 2 regelt das Verhältnis des neuen Erlasses zu den zahlreichen Bundesgesetzen, die Anforderungen an den Schutz der Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit von Informationen oder an die Verfügbarkeit und Integrität von IKT-Mitteln festlegen (s. Art. 4 Abs. 2 Bst. a-d). Die Bestimmungen des ISG sollen für solche Gesetze ergänzende Anwendung finden. Dies bedeutet, dass das ISG einen einheitlichen Rahmen zur Beurteilung des Schutzbedarfs dieser Informationen und zur Umsetzung der spezialgesetzlichen Sicherheitsanforderungen an diese Informationen schafft.

Das Beispiel des DSG vermag diesen Grundsatz zu erläutern. Das DSG enthält die Anforderungen an die rechtmässige Bearbeitung sowie an den Schutz von Personendaten. Es versteht sich, dass Personendaten im Aufgabenbereich der Bundesbehörden weiterhin nach den Regeln des Datenschutzgesetzes bearbeitet werden müssen und dürfen. Da allerdings das DSG selbst wenig detaillierte Vorschriften über organisatorische, personelle, technische und physische Schutzmassnahmen enthält, sollen die entsprechenden Vorschriften des vorliegenden Gesetzes auf die Bearbeitung von Personendaten als ergänzendes Recht angewendet werden. Sofern schliesslich Personendaten auch als wesentlich - etwa für die Wahrung der öffentlichen Sicherheit - zu beurteilen sind, sollen sie nach den entsprechenden Vorschriften des vorliegenden Gesetzes behandelt und gegebenenfalls klassifiziert werden.

Abs. 3: Der Bundesrat hat in der NCS am Grundsatz der dezentralen Regulierung der KI festgehalten. Soweit sektorspezifisch formell-gesetzlicher Handlungsbedarf besteht, muss die entsprechende Fachgesetzgebung angepasst werden (s. Ziff. 1.1.2.2 und 1.2.6). Mit dem ISG verfügt der Bund aber über besondere Instrumente im Bereich der Informationssicherheit, auf welche gewisse Regulatoren und KI-Betreiber zugreifen möchten, insbesondere die PSP. Auf Interesse stossen z.T. auch die Bestimmungen über die Klassifizierung oder über die Sicherheit beim Einsatz von IKT. Bestimmte KI greifen bereits heute auf diese Instrumente des Bundes zu. Dies ist z.B. der Fall im Bereich der Kernkraftwerke, in welchem der Bund bestimmte Massnahmen der Informationssicherheit vorschreibt (s. Art. 5 und 24 KEG). Auch im Bereich der Luftraumüberwachung (Skyguide) werden bestimmte Angestellte vorgängig einer PSP unterzogen. Neu sollen auch gewisse Angestellte der nationalen Netzgesellschaft, die das Übertragungsnetz für Elektrizität auf gesamtschweizerischer Ebene betreibt (Swissgrid), der PSP unterstellt werden. Es wird deshalb festgehalten, dass die Spezialgesetzgebung für eine Unterstellung unter das ISG (oder Teile davon) massgebend ist.

Zur entsprechenden Änderung der Spezialgesetzgebung, s. auch Ziff. 2.9 und 2.10.

2.1.2 Allgemeine Massnahmen der Informationssicherheit

Art. 4

Art. 4 erfasst den materiellen Inhalt der Informationssicherheit sowie die wichtigsten Grundsätze, nach welchen sie umgesetzt werden muss. Er ergänzt somit den Zweckartikel (Art. 1), indem er die detaillierten Schutzziele darlegt.

Abs. 1 hält fest, dass die verpflichteten Behörden und Organisationen den Schutzbedarf der Informationen, für die sie zuständig sind, beurteilen müssen. Der Schutzbedarf der Informationen wird hinsichtlich der potenziellen Beeinträchtigung der Interessen nach Art. 1 Abs. 2 erhoben und in Bezug auf die detaillierten Kriterien von Abs. 2 definiert. Der spezifische sachbedingte Schutzbedarf wird implizit sehr häufig von anderen Gesetzen vorgegeben (s. auch Art. 1 Abs. 2 Bst. e sowie Art. 3 Abs. 2).

Abs. 2: In sachlicher Hinsicht nennen Lehre und Praxis meistens vier jeweils nach den Umständen zu gewichtende Schutzkriterien der Informationssicherheit, nämlich die Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Informationen. Oft werden noch weitere Schutzkriterien erwähnt, die aber grundsätzlich durch die in Abs. 2 aufgeführten Kriterien oder allenfalls durch eine Kombination derselben abgedeckt werden, z. B. die Authentizität (in diesem Gesetz unter "Integrität" erfasst), die Zurechenbarkeit oder die Nichtabstreitbarkeit (in diesem Gesetz von den Kriterien der "Integrität" und der "Nachvollziehbarkeit" abgeleitet).

- Bst. a: Der Grundsatz der Vertraulichkeit wird dahingehend konkretisiert, dass Informationen nur Berechtigten zugänglich sein sollen. Der Kreis der Berechtigten ergibt sich aus dem Kontext der jeweiligen gesetzlichen Aufgabenerfüllung sowie dem Inhalt und der Bedeutung der Information. Entsprechend kann

der Kreis der Berechtigten auf wenige Personen beschränkt oder sehr gross sein. Wenn die Informationen öffentlich zugänglich gemacht werden sollen, ist der Kreis uneingeschränkt.

- Bst. b: Die Verfügbarkeit der Informationen ist nicht absolut zu verstehen, doch ist es für die Entscheid- und Handlungsfähigkeit der Behörden und Organisationen erforderlich, dass sie im Rahmen der gesetzlichen Aufgabenerfüllung die notwendigen Informationen rechtzeitig abrufen können. Die Anforderungen an die Verfügbarkeit von Informationen sind höher, wenn diese für die Erfüllung von wesentlichen Aufgaben stets und unterbruchlos verfügbar sein müssen. Dies gilt insbesondere dann, wenn diese Informationen elektronisch bearbeitet werden.
- Bst. c: Die Wahrung der Integrität (Unversehrtheit und Richtigkeit) der Informationen ist eine wichtige Teilaufgabe des Schutzes von Informationen, die - im Hinblick auf die Vertrauenswürdigkeit der Behörden - auch für Informationen von Bedeutung ist, die zur Veröffentlichung bestimmt sind. Sie ist auch für das korrekte Funktionieren der IKT-Mittel entscheidend.
- Bst. d: Die nachvollziehbare Bearbeitung der Informationen ist insbesondere für alle öffentlichen Verfahren (Strafverfahren, Beschwerdeverfahren, usw.) von grosser Bedeutung, aber auch für die Wahrnehmung von Kontroll- und Aufsichtsfunktionen und das Vorgehen bei Missbräuchen.

Die verpflichteten Behörden und Organisationen müssen also eine Beurteilung des Schutzbedarfs von Informationen vornehmen und bestimmen, in welcher Hinsicht und wie stark die Informationen geschützt werden müssen (Sicherheitsanforderungen). Der Schutz der Vertraulichkeit ist z.B. nur erforderlich, wenn diese Vertraulichkeit aus einem rechtlichen Grund (z.B. DSG, Geschäfts- oder Fabrikationsgeheimnisse Dritter oder Art. 14 ISG) gewährleistet werden muss. Zu beachten ist aber auch, dass bestimmte Informationen höhere Anforderungen an den Schutz ihrer Integrität oder Verfügbarkeit haben können, ohne dass diese besonderen Anforderungen gesetzlich festgelegt sind, etwa dann, wenn die entsprechenden Informationen für die Aufgabenerfüllung einer Behörde unbedingt richtig bzw. verfügbar sein müssen. Dies trifft insbesondere für Informationen und IKT-Mittel zu, die geschäftskritische Prozesse unterstützen. Der Schutzbedarf ergibt sich also auch aus der Wichtigkeit der Erfüllung der gesetzlichen Aufgaben, in welchen oder zu deren Unterstützung die Informationen verwendet werden.

Abs. 3: Der Schutz der Verfügbarkeit und der Integrität der IKT-Mittel stellt für eine integrale Informationssicherheit eine wichtige Ergänzung der erwähnten vier Kriterien dar. Obwohl sich diese Anforderung grundsätzlich bereits aus Abs. 2 Bst. b und c ergibt, wird die Anforderung nach einem angemessenen Schutz vor Missbrauch und Störung noch ausdrücklich erwähnt, weil die IKT-Unterstützung der Geschäftsprozesse immer mehr an Bedeutung gewonnen hat. Ihr gutes Funktionieren stellt heute sogar eine unentbehrliche Voraussetzung für die effiziente Aufgabenerfüllung der Bundesbehörden dar.

Abs. 4: Die Informationssicherheit muss risikobasiert, zweckmässig und wirtschaftlich umgesetzt werden. Eine möglichst objektive Beurteilung der Risiken soll für die Umsetzung von Sicherheitsmassnahmen massgebend sein (s. Art. 6 und 7). Es versteht sich, dass eine absolute Sicherheit ein unerreichbares Ideal darstellt, und dass der Aufwand für die Behebung verbleibender kleinerer Sicherheitslücken unverhältnismässig hoch werden kann. Die zuständigen Behörden und Organisationen müssen daher darauf achten, dass ihre Massnahmen zweckmässig und wirtschaftlich sind. Entsprechend ist durch die Linie bei der Verfolgung der Schutzmassnahmen eine Güterabwägung zwischen Sicherheitskosten und -nutzen vorzunehmen.

In diesem Kontext wird auch der Grundsatz der Benutzerfreundlichkeit aufgeführt. Personen, die Informationen bearbeiten oder mit IKT-Mitteln umgehen, müssen oft bestimmte Verhaltensvorschriften einhalten, damit die Informationssicherheit gewährleistet ist (z.B. muss die Bürotür abgeschlossen oder eine E-Mail verschlüsselt werden). Erschweren aber Sicherheitsmassnahmen die Aufgabenerfüllung der Mitarbeitenden zu sehr, ist erfahrungsgemäss die Wahrscheinlichkeit gross, dass sie entweder nicht eingehalten oder gar absichtlich umgegangen werden.

Art. 5

Sicherheit ist Chefsache. Art. 5 umschreibt den Inhalt der obersten Führungsverantwortung im Bereich der Informationssicherheit. Er richtet sich deshalb nur an die verpflichteten Behörden (Art. 2 Abs. 1), welche diese Verantwortung alleine tragen.

In Abs. 1 werden die verpflichteten Behörden aufgefordert, die Informationssicherheit in ihrem Zuständigkeitsbereich zu organisieren.

- Bst. a: Die Informationssicherheit muss nach dem Stand der Lehre und der Technik organisiert, umgesetzt und überprüft werden. Mehrere unverbindliche Fachnormen formulieren sogenannte *Best Practices* in Bezug auf das Management der Informationssicherheit (z.B. DIN ISO/IEC Norm 27'001 und 27'002). Besonders wichtig an diesen Normen ist, dass sie einerseits in der Praxis erprobt wurden und dass sie ande-

rerseits nach dem erforderlichen integralen Ansatz aufgebaut sind. Sie legen ausserdem Anforderungen für die Umsetzung von Sicherheitsmassnahmen fest, die auf die Bedürfnisse der jeweiligen Behörden, Organisation oder von Teilen derselben zugeschnitten werden können.

Kleinere Behörden (z.B. Bundespatentgericht, Militärkassationsgericht und Aufsichtsbehörde der Bundesanwaltschaft) werden selbstverständlich keine derartige Organisation alleine aufbauen können. Das Gesetz lässt es aber zu, dass z.B. die eidgenössischen Gerichte den Aufbau einer einzigen gemeinsamen Organisation beschliessen, welche gleichzeitig die Unabhängigkeit der verschiedenen Gerichte wahrt.

- Bst. b: Die Verwirklichung von Informationssicherheit betrifft viele Fachbereiche, z.B. die Finanzen (finanzielle Auswirkungen der Organisation und der Massnahmen), die Personaldienste (Aufgaben des Personals), die Bereiche Recht und Compliance (Rechtsgrundlagen der Informationssicherheit), die Informatik (Einflüsse der Informationssicherheit auf den Einsatz der IKT sowie Umsetzung der Anforderungen in IKT-Systemen) und den Bereich Risikomanagement und Controlling (Informationssicherheit als Teil des Risikomanagements). Eine wirksame Informationssicherheit verlangt deshalb, dass die erwähnten Fachbereiche die Anliegen der Informationssicherheit mittragen, dass sie an der entsprechenden Beschlussfassung beteiligt werden und dass die Massnahmen fachbereichsübergreifend koordiniert werden.

Abs. 2: Für die Sicherheit im Allgemeinen ist es wichtig, dass die Aufgaben und Zuständigkeiten klar und eindeutig geregelt werden. Dies gilt besonders für die Informationssicherheit, da viele Fachbereiche Anforderungen an die sichere Bearbeitung von Informationen festlegen oder für die Umsetzung des vorliegenden Gesetzes Teilverantwortungen tragen werden. Unklare Zuständigkeiten können dazu führen, dass wesentliche Risiken nicht identifiziert werden, dass sich niemand für die Umsetzung bestimmter risikomindernder Massnahmen verantwortlich fühlt oder dass niemand die Risiken bewusst trägt.

In Abs. 3 werden die verpflichteten Behörden aufgefordert, bestimmte Grundsätze, welche die Absicht der verpflichteten Behörde hinsichtlich der Informationssicherheit bekannt geben sollen, für ihren Zuständigkeitsbereich festzulegen.

- Bst. a: Die Ziele der verpflichteten Behörde geben das Sicherheitsniveau vor, das erreicht werden soll (SOLL-Zustand der Informationssicherheit). Diese Ziele setzen eine Kosten-Nutzen-Analyse voraus (wie viel Sicherheit will die Behörde haben und wie viel darf sie kosten) und sollen für die Erteilung der erforderlichen Ressourcen massgebend sein. Beispiel: Geschäftsgeheimnisse Dritter, die von den Behörden oder Organisationen des Bundes bearbeitet werden, müssen vor unberechtigter Kenntnisnahme geschützt werden. Will man diese Informationen gegen die aktivsten, ressourcenreichsten Nachrichtendienste der Welt schützen, dann sind die zu treffenden Massnahmen wesentlich kostspieliger als diejenigen, die man treffen wird, wenn die Behörde das relativ hohe Risiko in Kauf nimmt, dass diese fremden Nachrichtendienste sich diese Informationen beschaffen werden. Die vorgesehenen Wirksamkeitsprüfungen (s. Art. 24 Abs. 2) richten sich an diesen Zielen aus.
- Bst. b: Hier soll insbesondere geregelt werden, wie die unterstellten Organisationen mit Risiken umgehen sollen, welche Risiken sie ohne weiteres tragen dürfen und welche Risiken der Behörde rapportiert werden müssen (Risikoakzeptanz). Auch wenn die meisten Risiken der Informationssicherheit auf der operativen Ebene (Departement, Amt oder sogar unterstellte Einheit) behandelt und getragen werden können, können bestimmte Risiken eine strategische Ausprägung haben. Dies ist insbesondere der Fall bei Risiken in Zusammenhang mit als GEHEIM klassifizierten Informationen (Art. 14 Abs. 3) oder mit IKT-Mitteln der Sicherheitsstufe «sehr hoher Schutz» (Art. 21 Abs. 3). Strategische Risiken sollen der betroffenen Behörde kommuniziert werden, bevor ein Ereignis eintritt.
- Bst. c: In jeder Organisation gibt es immer wieder Personen, welche die Informationssicherheit nicht ernst nehmen und vorschriftswidrig oder unsorgfältig mit Informationen oder IKT-Mitteln umgehen. Sehr oft werden solche Verstösse *a priori* entschuldigt und entsprechend nicht untersucht. Diese Verstösse können jedoch erhebliche Auswirkungen zur Folge haben. Sie sollten also nicht einfach als Kavaliersdelikte betrachtet werden. Die verpflichteten Behörden müssen deshalb die Vorschriften konsequent durchsetzen und die Folgen bei Missachtungen festlegen und erläutern.

Abs. 4: Die verpflichteten Behörden müssen für die regelmässige und stufengerechte Information der Führungskräfte und des Personals in Bezug auf die Belange der Informationssicherheit sorgen. Es geht z.B. darum, dass Änderungen in den Organisations- und Zuständigkeitsregelungen mitgeteilt werden, oder dass das Kader sowie die Fachspezialisten über die Ursachen und Folgen von Vorfällen informiert werden. Eine regelmässige Kommunikation muss erfolgen, weil das Kader und das Personal dadurch das Bekenntnis der Geschäftsleitung für die Informationssicherheit wahrnehmen und auf Änderungen reagieren können. Sie erlaubt es ihnen auch, in ihrem eigenen Zuständigkeitsbereich die Lehren aus Vorfällen zu ziehen. Kader und Personal sollten auch entsprechend geschult werden.

Art. 6

Art. 6 verpflichtet die Behörden und Organisationen, ein Risikomanagement im Bereich der Informationssicherheit zu betreiben (zum Risikomanagement, s. Ziff. 1.2.3.2).

Abs. 1 legt fest, dass die verpflichteten Behörden und Organisationen die Risiken identifizieren, bewerten, beurteilen und überprüfen müssen, und zwar sowohl in ihrem eigenen Zuständigkeitsbereich als auch im Rahmen der Zusammenarbeit mit Dritten. Idealerweise sollten alle verpflichteten Behörden und Organisationen einheitliche Methoden verwenden. Der Bundesrat wird hierzu Standardanforderungen und -massnahmen definieren (s. Art. 88). Dies im Wissen darum, dass die Kriterien für die Risikoakzeptanz, die für die Bewertung der Risiken massgebend sind, von den jeweiligen verpflichteten Behörden gestützt auf ihre eigenen Bedürfnisse an Informationssicherheit festgelegt werden (s. auch Art. 5 Abs. 3 Bst. a und b).

Die Beurteilung der Risiken setzt profunde Kenntnisse der gesetzlichen Aufgaben und der entsprechenden kritischen Geschäftsprozesse, die regelmässige Beurteilung der Bedrohungen und Gefahren für die zu schützenden Werte, die Analyse der Schwachstellen sowie die Einschätzung der Eintrittswahrscheinlichkeit und des potentiellen Schadensausmasses bestimmter Risiken voraus. Der Risikomanagementprozess im Bereich der Informationssicherheit muss laufend durchgeführt werden. Dies gilt insbesondere für den Informatikbereich, denn neue Malware wird täglich entwickelt. Anwendungen und Sicherheitssoftware müssen entsprechend dauernd aktualisiert werden.

Nach Abs. 2 müssen die erforderlichen Massnahmen zur Risikovermeidung oder -reduktion getroffen werden. Selbstverständlich können Risiken auch in Kauf genommen bzw. getragen werden (s. Abs. 3). Sie sollten aber nicht ignoriert werden. Risiken können vermieden werden, indem auf eine bestimmte, zu riskante Tätigkeit ganz verzichtet wird (z.B. wird auf ein Informatikvorhaben verzichtet, für welches die Umsetzung von risikogerechten Massnahmen wirtschaftlich nicht vertretbar ist; oder es wird beispielsweise untersagt, als GEHEIM klassifizierte Informationen mit vernetzten IKT-Mitteln zu bearbeiten). Die zu treffenden Massnahmen gehören zu folgenden Kategorien, die sich z.T. überschneiden:

- *Organisatorische Massnahmen:* z.B. Erlass von Rechtsgrundlagen, Festlegung der Sicherheitspolitik und -organisation, Zuteilung klarer Verantwortlichkeiten und Zuständigkeiten, Klassifizierung von Informationen, Trennung von sicherheitsempfindlichen Funktionen, Zutrittsregelungen und -kontrollen für Personen, allgemeine Kontrollen, Zugriffsregelungen auf Systeme, Erstellung von Informationssicherheitskonzepten für IKT-Mittel, Organisation der Behandlung von Vorfällen.
- *Personelle Massnahmen:* z.B. Ausbildung und Sensibilisierung, vertragliche Verpflichtung zur Einhaltung der Informationssicherheit, Durchführung von PSP, regelmässige persönliche Gespräche mit Schlüsselpersonen zur Förderung der bewussten Wahrnehmung von bestimmten Gefahren, Umschreibung und Durchsetzung von Sanktionen.
- *Technische Massnahmen:* z.B. Verschlüsselung von Informationen, Redundanz von wichtigen Diensten, Schutz vor Malware, starke Authentifizierung, Zugriffsschutz zu Netzwerken.
- *Bauliche Massnahmen*: z.B. Umzäunung von sicherheitsempfindlichen Perimetern, Verwendung von Sicherheitsschliesssystemen, Einrichtung von Sicherheitszonen und -räumen, Einsatz von Überwachungsanlagen.

Abs. 3 legt fest, dass Risiken, die nach der Umsetzung der vorgesehenen Sicherheitsmassnahmen bestehen bleiben (sogenannte Restrisiken) oder Risiken, die nicht vermindert werden sollen, klar auszuweisen sind. Die Entscheidungsträger sind für ihre diesbezügliche Güterabwägung in dokumentierter Form auf diese Risiken und die potenziellen Auswirkungen hinzuweisen. Die verbleibenden Risiken müssen nachweisbar akzeptiert und auch entsprechend getragen werden.

Abs. 4 hält fest, dass das Risikomanagement im Bereich der Informationssicherheit zwingend auf allen Stufen in den allgemeinen Risikomanagementprozess des Bundes integriert werden muss. Auch wenn das vorliegend geforderte Risikomanagement fachspezifisch ist und deshalb von Fachspezialisten gesteuert und betrieben werden muss, bleibt die Informationssicherheit ein Anliegen, das die Bewirtschaftung von üblichen Geschäftsrisiken betrifft. Die verpflichteten Behörden müssen deshalb die Zusammenarbeit der Fachorganisation des allgemeinen Risikomanagements mit der Fachorganisation der Informationssicherheit regeln.

Art. 7

Abs. 1 verlangt, dass die Behörden und Organisationen sich bei der Festlegung ihrer Sicherheitsanforderungen und -massnahmen an den Standardanforderungen und -massnahmen des Bundesrats nach Art. 88 orientieren. Für Behörden und Organisationen, die dem Bundesrat nicht unterstellt sind, besteht keine Pflicht, diesen Standards zu folgen. Da ein wichtiges Ziel dieses Gesetzes darin besteht, behördenübergreifend möglichst einheitliche Sicherheitsstandards zu erreichen, wird der Bundesrat verpflichtet, standardisierte Anfor-

derungen und Massnahmen nach dem Stand der Lehre und der Technik festzulegen. Die Wirtschaftlichkeit gebietet, dass nicht jede Behörde oder Organisation das Rad neu erfinden muss, wenn gute, in der Praxis erprobte Lösungen von einer anderen Behörde oder Organisation entwickelt oder gefunden worden sind.

Abs. 2: Die Sicherheitsmassnahmen müssen sich nach dem Stand der Lehre und der Technik richten. Die Informationssicherheit ist ein relativ junger Aufgabenbereich, der sich regelmässig weiterentwickelt. Auch wenn die Organisationsgrundsätze eine bestimmte Stabilität und Reife erreicht haben, weil sie den allgemeinen Organisationsgrundsätzen im Bereich des Risikomanagements entsprechen, werden regelmässig bessere organisatorische Massnahmen entwickelt, die wirksamer oder wirtschaftlicher sind. "*Sich nach dem Stand der Lehre zu richten*" bedeutet also im Kontext dieses Absatzes, dass die verpflichteten Behörden und Organisationen erprobte organisatorische Lösungen und Ansätze (*best practices)* anwenden sollen.

Neue Entwicklungen erfolgen im Bereich der technischen Informationssicherheit sehr rasch, insbesondere bei den IKT-Mitteln, aber auch bei der Sensorik (z.B. Feuer-, Hitze- oder Bewegungsdetektoren) oder bei der Schliesstechnik (z.B. Schliesssysteme für Türen). Es ist sehr wichtig, dass Sicherheitsmassnahmen nicht auf veralteten Technologien basieren, sondern gegen aktuelle Bedrohungen Wirkung zeigen.

Art. 8

Als Dritte gelten nach diesem Gesetz alle Behörden, Organisationen und Personen des öffentlichen oder privaten Rechts, die keine verpflichteten Behörden oder Organisation nach Art. 2 sind und deshalb grundsätzlich unabhängig von diesen Behörden und Organisationen handeln. Die Bundesbehörden sind für ihre Aufgabenerfüllung häufig auf eine Mitwirkung der Privatwirtschaft oder anderer Stellen angewiesen. Die auftragserteilenden Behörden und Organisationen haben dafür zu sorgen, dass bei der Auftragserteilung und -ausführung die gesetzlich vorgesehenen Massnahmen eingehalten werden.

Diese Zusammenarbeit mit Dritten sowie die einzuhaltenden Sicherheitsmassnahmen werden in der Regel vertraglich geregelt. Grundsätzlich sollten Dritte erst dann Zugang zu Informationen oder zu IKT-Mitteln des Bundes erhalten, wenn sie die erforderlichen Massnahmen umgesetzt haben. Das ISG verlangt von den verpflichteten Behörden und Organisationen auch, dass sie die Umsetzung der Massnahmen überprüfen. Schliesst der Auftrag die Ausübung einer sicherheitsempfindlichen Tätigkeit ein, so müssen die verpflichteten Behörden und Organisationen die erforderlichen PSP (s. Art. 32 ff.) einleiten bzw. die Durchführung eines BSV (s. Art. 56 ff.) beantragen.

Art. 9

Zu Vorfällen im Bereich der Informationssicherheit wird es auch in Zukunft kommen. Es ist deshalb nötig, einen einheitlichen und effektiven Ansatz für den Umgang mit solchen Vorfällen anzuwenden. Die verpflichteten Behörden und Organisationen müssen zunächst die erforderlichen Massnahmen treffen, um Informationssicherheitsvorfälle überhaupt frühzeitig identifizieren zu können (z.B. regelmässige Kontrollen, Sensoren, Alarmanlagen, Netzwerküberwachung, regelmässige Auswertung von Log-Files, usw.). Sie müssen ein Verfahren festlegen, nach welchem vorgegangen werden soll, wenn Ereignisse oder Schwachstellen identifiziert werden, sowie klare Zuständigkeiten für die Behandlung der Vorfälle zuweisen. Interne und externe Mitarbeitende müssen zudem wissen, wie sie beim Eintreten eines Ereignisses zu reagieren haben, damit dessen Auswirkungen minimiert werden können.

Damit aus Vorfällen gelernt wird, müssen die verpflichteten Behörden und Organisationen dafür sorgen, dass die Ursachen eines Vorfalls abgeklärt und ausgewertet werden. Die Identifizierung und Behandlung von Vorfällen soll so kontinuierlich verbessert werden.

Art. 10

Die Behörden müssen im Bereich der Informationssicherheit ein "Business Continuity Management" (BCM) betreiben. BCM bedeutet, dass alle notwendigen Vorkehrungen getroffen werden, damit die Behörden ihre Kernaufgaben selbst in ausserordentlichen Situationen termingerecht erfüllen können (s. auch Art. 6 Abs. 3 RVOG). Aufgrund der zunehmenden Abhängigkeit vom Einsatz der IKT zur Auftragserfüllung sind die Risiken und Vorsorgeplanungen im Bereich der Informationssicherheit zwingend in das allgemeine BCM der Behörden aufzunehmen. Das Gesetz verlangt die Erstellung solcher Vorsorgeplanungen nur für die unverzichtbaren Aufgaben der verpflichteten Behörden, und nicht für diejenige der verpflichteten Organisationen. Für die Bundesverwaltung bedeutet dies, dass der Bundesrat dafür sorgen muss, dass die *aus seiner strategischen Sicht* kritischsten Aufgaben der Bundesverwaltung und der Armee identifiziert werden. Obschon sie vom Gesetz nicht dazu verpflichtet werden, sind die Departemente und die Verwaltungseinheiten frei, für ihre kritischen Aufgaben, die nicht vom Bundesrat erfasst werden, Vorsorgeplanungen zu erstellen.

Art. 11

Zum Kontroll- und Auditwesen, s. Ziff. 1.2.3.3.

Abs. 1 verlangt von den verpflichteten Behörden und Organisationen, dass sie die Einhaltung der Vorschriften regelmässig überprüfen. Grundsätzlich obliegt diese Kontrolle den Linienvorgesetzten. Die Informationssicherheitsbeauftragten werden aber gemäss Art. 84 Abs. 2 Bst. c ebenfalls Kontrollen und Audits im Auftrag ihrer Behörde durchführen.

Abs. 2 richtet sich nur an die verpflichteten Behörden. Eine periodische unabhängige Prüfung ist notwendig, denn sie soll sich hauptsächlich auf die Wirksamkeit der Organisation der Informationssicherheit fokussieren. Diese Organisation schliesst natürlich die Aufgaben derjenigen Personen ein, die für die ordentlichen Kontrollen zuständig sind. Der Entscheid sowohl über die Periodizität der Wirksamkeitsprüfung als auch über die Stelle, welche die Prüfung durchführen soll, obliegt der betroffenen Behörde. Die Behörden können z.B. ihre interne Revisionsstelle oder eine externe Firma oder Stelle beauftragen. Sie können auch die Fachstelle des Bundes für Informationssicherheit (s. Art. 86 Abs. 1 Bst. c) beauftragen. Der Bundesrat kann zudem die EFK ersuchen, solche Prüfungen durchzuführen.

Art. 12

Abs. 1 legt fest, dass die Klassifizierung von Informationen zwingend ist, sofern die Kriterien zur Klassifizierung nach Art. 14 erfüllt sind. Heute ist jede verpflichtete Behörde grundsätzlich frei, ihr eigenes Klassifizierungssystem (wenn überhaupt), ihre eigenen Klassifizierungsgründe sowie ihre eigenen Bearbeitungsvorschriften festzulegen. Einige Vorfälle in den letzten Jahren haben gezeigt, dass diese unterschiedliche Behandlung klassifizierter Informationen zu erhöhtem Misstrauen führen kann. Eine einheitliche Regelung der Klassifizierungsstufen und -gründe ist nötig.

Mit Abs. 2 soll auf Gesetzesebene festgehalten werden, dass die Klassifizierung von Informationen angesichts des Öffentlichkeitsprinzips sowie auch des mit der Klassifizierung verbundenen Aufwandes grundsätzlich die Ausnahme darstellen soll.

Abs. 3 hält fest, dass die Klassifizierung nach Möglichkeit zu befristen ist. Die Schutzwürdigkeit von Informationen nimmt oftmals mit der Zeit ab oder erübrigt sich nach einem bestimmten Ereignis (z.B. Veröffentlichung eines Berichts oder Ende einer bestimmten Massnahme). Die Klassifizierung derartiger (beispielsweise nicht mehr aktueller) Informationen rechtfertigt sich dann nicht mehr. Sie würde bloss unnötigen Aufwand verursachen oder zu Problemen nach der Archivierung der Informationen führen. Informationen, die für längere Zeit klassifiziert bleiben müssen, erfordern zudem zunehmend andere technische Schutzvorkehrungen als jene, die nur eine befristete Schutzwürdigkeit haben.

Soweit eine Klassifizierung auf Zeit im Voraus nicht möglich ist, wird durch die in Abs. 4 enthaltene Pflicht, die Notwendigkeit der Klassifizierungen periodisch zu überprüfen, sichergestellt, dass Informationen nicht unnötig klassifiziert bleiben.

Art. 13

Abs. 1: Die verpflichteten Behörden müssen festlegen, wer für die Klassifizierung zuständig ist. In der Bundesverwaltung wird diese Zuständigkeit heute der Verfasserin oder dem Verfasser eines Dokuments zugewiesen, weil sie am Besten den Schutzbedarf der Informationen sowie allfällige Risiken einschätzen können. Die Regelung des Bundesrats soll aber für die anderen Bundesbehörden nicht verbindlich sein. So können diese auch entscheiden, dass die Klassifizierung z.B. durch die Behördenleitung, durch eine zentrale zuständige Stelle oder nur durch die Linie erfolgen darf. Der Begriff "klassifizierende Stelle" ist insbesondere für den Entscheid betreffend den Kreis der berechtigten Empfänger, die Entklassifizierung, die Archivierung und die Vernichtung von klassifizierten Informationen wichtig, aber auch für allfällige vorläufige Schutzmassnahmen, die getroffen werden müssen, wenn klassifizierte Informationen gefährdet werden (s. Art. 18).

In Abs. 2 wird die Verbindlichkeit der Klassifizierung geregelt. Ist eine Information klassifiziert, wird sie auf ihrem weiteren Weg sozusagen von dieser Klassifizierung begleitet. Wer Zugang zu einer solchen Information erhält, muss die Vorgaben einhalten, die mit der Klassifizierung verbunden sind. Eine Änderung oder Aufhebung der Klassifizierung darf im Grundsatz nur von der Stelle vorgenommen werden, welche die Klassifizierung festgelegt hat. Es versteht sich, dass auch hier der Dienstweg, die Dienstaufsicht und die entsprechenden Weisungsbefugnisse der vorgesetzten Stellen bzw. Aufsichtsbehörden zum Tragen kommen. Letztere können Entscheide der klassifizierenden Stelle gegebenenfalls korrigieren.

Art. 14

Zu den Zielen der Klassifizierungsregelung: s. Ziff. 1.2.3.4.

Art. 14 regelt die materiellen Voraussetzungen für die Klassifizierung von Informationen für alle verpflichteten Behörden und Organisationen und legt die Klassifizierungsstufen fest. Der vorgeschlagene Text be-

schränkt sich auf eher allgemeine Kriterien für die Klassifizierung und nimmt direkten Bezug auf die in Art. 1 Abs. 2 Bst. a-d umschriebenen und zu schützenden öffentlichen Interessen. Der Verweis auf diese Interessen ist jedoch eingeschränkt: Der Schutz der öffentlichen Interessen nach Bst. e stellt keinen eigenen Grund zur Klassifizierung dar. Mit dem Schutz dieses Interesses soll nämlich die rechtmässige Bearbeitung von Informationen sichergestellt werden, deren Schutz in anderen Gesetzen vorgesehen oder mit Dritten durch Vertrag vereinbart wird. Personendaten nach dem DSG oder Geschäfts-, Fabrikations- oder Berufsgeheimnisse werden also grundsätzlich nicht klassifiziert, es sei denn, dass einzelne Informationen zum Schutze eines Interesses nach Art. 1 Abs. 2 Bst. a-d klassifiziert werden müssen. Dasselbe gilt für Informationen, die bei den Gerichten oder Staatsanwaltschaften im Rahmen ihrer ordentlichen Verfahren bearbeitet werden. Die Mehrheit dieser Informationen sind Personendaten, die zwar schützenswert sind, die aber aufgrund des vorliegenden Gesetzes nicht klassifiziert werden müssen. Hingegen können bzw. sollen die besonderen Massnahmen, die zum Schutz solcher Informationen getroffen werden, klassifiziert werden. Werden z.B. besonders schützenswerte Personendaten in einem Informationssystem bearbeitet, dann muss das entsprechende Informationssicherheitskonzept klassifiziert werden.

Für die Klassifizierungsstufe selbst ist der *Grad der Beeinträchtigung* massgebend, den eine Kenntnisnahme durch Unberechtigte den Interessen nach Art. 1 Abs. 2 Bst. a-d zufügen kann. Für die Zuweisung zu einer Klassifizierungsstufe ist massgebend, ob die Kenntnisnahme durch Unberechtigte die betroffenen Interessen:

- *beeinträchtigen kann:* Klassifizierungsstufe INTERN;
- *erheblich beeinträchtigen kann:* Klassifizierungsstufe VERTRAULICH;
- *schwerwiegend beeinträchtigen kann:* Klassifizierungsstufe GEHEIM.

Diese Qualifizierungen stellen unbestimmte Rechtsbegriffe dar, die unter Berücksichtigung der Risikopolitik noch zu konkretisieren sind. Obschon das Kriterium der Schwere der potenziellen Beeinträchtigung der Interessen nach Art. 1 Abs. 2 Bst. a-d für die Klassifizierung massgebend ist, genügt es alleine nicht. Es muss auch eine vernünftige kausale Verbindung zwischen der unberechtigten Kenntnisnahme der Information und dieser potenziellen Beeinträchtigung der geschützten Interessen geben. Erforderlich ist somit, dass auch die Eintrittswahrscheinlichkeit des Schadens berücksichtigt wird. Die Klassifizierung einer Information entspricht also dem Ergebnis einer Risikobeurteilung und soll somit den tatsächlichen *Schutzbedarf* dieser Information wiedergeben.

Bei der Beurteilung des Schutzbedarfs von Informationen *politischer Natur* ist besondere Zurückhaltung erforderlich. Zwar wird der Schutz der freien Meinungs- und Willensbildung der verpflichteten Behörden und Organisationen von Art. 1 Abs. 2 Bst. a (Entscheidungsfähigkeit) erfasst. In einer modernen Demokratie gehört es aber zur normalen Regierungstätigkeit, dass politische Ideen, Vorschläge, Konzepte und Entscheide in der Öffentlichkeit besprochen und gegebenenfalls (auch heftig) kritisiert werden. Die Klassifizierung darf also nicht dazu dienen, bestimmte Sachverhalte der öffentlichen Debatte zu entziehen, wenn kein *überwiegendes* öffentliches Interesse dafür besteht.

Der hier aufgeführte Vorschlag mit drei Klassifizierungsstufen entspricht formell der heute geltenden Regelung der ISchV. Wie eingangs erwähnt, werden die Grenzwerte für die Klassifizierung in den jeweiligen Stufen aber erhöht (über das Verhältnis zum Öffentlichkeitsprinzip s. Art. 3 Abs. 1).

Abs. 1: Eine Klassifizierung als INTERN wird verlangt, wenn eine Bekanntgabe der Information eine Beeinträchtigung der öffentlichen Interessen nach Art. 1 Abs. 2 Bst. a-d zur Folge hat. Als Kriterium zwischen "nicht klassifiziert" und "klassifiziert" gilt somit auch für eine bloss "einfache" Beeinträchtigung der betreffenden Interessen, dass qualifizierte Anhaltspunkte vorliegen, welche die Klassifizierung als INTERN zu begründen vermögen. So darf der potenzielle Schaden, der durch eine Kenntnisnahme durch Unberechtigte entstehen kann, nicht einfach vernachlässigbar sein: Die Beeinträchtigung der Interessen nach Art. 1 Abs. 2 Bst. a-d muss vielmehr spürbar sein.

Wenn es um *sicherheitsrelevante Informationen* im Sinne von Art. 1 Abs. 2 Bst. b geht, ist der Schwellenwert für die Klassifizierung als INTERN meistens relativ rasch erreicht. INTERN wird auch am häufigsten für derartige Fälle verwendet. So können einzelne Sicherheitsunterlagen zu IKT-Mitteln oder einfache Einsatzpläne von Sicherheitskräften in der Regel als INTERN klassifiziert werden. Es ist aber z.B. auch denkbar, dass das Bekanntwerden eines Zeitplans für die Umsetzung einer konkreten Massnahme bestimmten Personen einen ungerechtfertigten Vorteil verschaffen könnte. Auch wenn damit die Massnahme als solche nicht verhindert würde, würde ihre gesetzeskonforme Umsetzung und somit die Entscheidungs- und Handlungsfähigkeit der betroffenen Bundesbehörde zumindest beeinträchtigt. Eine zeitlich befristete Klassifizierung des Zeitplans als INTERN wäre in diesem Fall gerechtfertigt.

Pauschale Klassifizierungen als INTERN sind grundsätzlich vorschriftswidrig. Die (hypothetische) Praxis einer Organisationseinheit der Bundesverwaltung, wonach alle Besprechungsnotizen und Sitzungsprotokolle von vornherein als INTERN klassifiziert würden, ohne auf den tatsächlichen Schutzbedarf der Informationen einzugehen, widerspräche sowohl dem Geist des BGÖ als auch der Regelung von Abs. 1. Hingegen wäre beispielsweise die Klassifizierung von Sitzungsprotokollen *mit operativem Inhalt* aus dem Bereich von fedpol gerechtfertigt. Allerdings *können* Informationen aus den Arbeiten parlamentarischer Kommissionen in der Regel als INTERN klassifiziert werden. Damit kann Klarheit darüber geschaffen werden, welche Informationen aus der parlamentarischen Arbeit zum Schutz der freien Meinungs- und Willensbildung des Parlaments nur für einen beschränkten Personenkreis bestimmt sind.

Abs. 2: Für die Klassifizierung als VERTRAULICH wird verlangt, dass die Interessen nach Art. 1 Abs. 2 Bst. a-d bei einer unberechtigten Kenntnisnahme "*erheblich beeinträchtigt*" werden können. Im Vergleich zur heutigen Regelung, wonach bloss ein unqualifizierter "Schaden" verlangt wird (Art. 6 ISchV), stellt die vorgeschlagene Neuregelung eine Erhöhung der Anforderungen zur Klassifizierung dar.

Die detaillierte Konkretisierung des Begriffs "*erhebliche Beeinträchtigung*" muss unter Berücksichtigung der Risikopolitik ebenfalls noch erfolgen. Mit dem gewählten Ausdruck wird jedoch ein deutlicher Schaden verlangt, z.B.:

- Die freie Meinungs- und Willensbildung der verpflichteten Behörden wird vorübergehend unrechtmässig erschwert;
- Eine verpflichtete Organisation wird vorübergehend handlungsunfähig;
- Die Erfüllung bestimmter Aufgaben einer Behörde oder Organisation wird über längere Zeit erheblich erschwert;
- Bestimmte Ressourcen der Armee oder der Sicherheitsorgane des Bundes sind vorübergehend einsatzunfähig;
- Die Position der Schweiz in Rahmen von internationalen Verhandlungen wird erheblich erschwert;
- Die Sicherheit von Personen oder Gruppen von Personen wird gefährdet;
- Dem Bund entsteht ein erheblicher finanzieller Schaden.

Abs. 3: Für die Klassifizierung als GEHEIM (höchste Klassifizierungsstufe) wird verlangt, dass die Interessen nach Art. 1 Abs. 2 Bst. a-d bei einer unberechtigten Kenntnisnahme "*schwerwiegend beeinträchtigt*" werden können. Wie bei den Klassifizierungsstufen INTERN und VERTRAULICH muss auch bei dieser Klassifizierungsstufe der Schlüsselbegriff "*schwerwiegende Beeinträchtigung*" noch konkretisiert werden. Mit der gewählten Formulierung wird jedoch ein besonders grosser Schaden für den Bund verlangt, z.B.:

- Eine verpflichtete Behörde ist vorübergehend entscheidungs- oder handlungsunfähig oder ihre Entscheidungs- oder Handlungsfähigkeit ist über längere Zeit besonders ernsthaft erschwert;
- Die Erfüllung unverzichtbarer Aufgaben einer verpflichteten Organisation wird vorübergehend verhindert oder über längere Zeit ernstlich erschwert;
- Wesentliche Ressourcen der Armee oder der Sicherheitsorgane des Bundes sind einsatzunfähig;
- Leib und Leben von Bevölkerungsgruppen werden gefährdet;
- Das Erbringen unverzichtbarer Dienstleistungen durch kritische Infrastrukturen wird unterbrochen;
- Besonders sicherheitsempfindliche Funktionen eines Kernkraftwerks werden sabotiert;
- Der Bund erleidet einen schwerwiegenden finanziellen Schaden.

Art. 15

Abs. 1 umschreibt die Voraussetzungen für den Zugang zu klassifizierten Informationen, der wiederum Voraussetzung für das Bearbeiten der entsprechenden Informationen ist. Der Grundsatz "*Kenntnis nur wenn nötig*" gilt für jede einzelne klassifizierte Information. Es besteht also kein allgemeines Recht, Zugang zu allen klassifizierten Informationen zu haben. Dies trifft auch für Prüf-, Kontroll- oder Aufsichtsorgane zu, die gegebenenfalls zwar ein allgemeines Informationsrecht haben, aber die für jede einzelne klassifizierte Information den Nachweis dafür erbringen müssen, dass sie zur Erfüllung ihres Auftrags tatsächlich von den betreffenden Informationen Kenntnis haben müssen. Bei einem vertraglich vereinbarten Zugangsrecht müssen die entsprechenden Verträge den Zugang zu klassifizierten Informationen vorsehen und deren Bearbeitung regeln. "Gewähr bieten" für einen sachgerechten Umgang setzt voraus, dass die Personen, die klassifizierte Informationen bearbeiten sollen, entsprechend ausgebildet worden sind. Ferner müssen sie gegebenenfalls den Nachweis für die Fähigkeit erbringen, die erforderlichen technischen und physischen Sicherheits-

massnahmen einhalten zu können. Für als VERTRAULICH oder GEHEIM klassifizierte Informationen kann zudem die Durchführung einer PSP (s. Art. 32 ff.) eine weitere Bearbeitungsvoraussetzung darstellen.

Abs. 2: Die Mehrheit der Länder und internationalen Organisationen, mit welchen die Schweiz ein Abkommen zum Austausch klassifizierter Informationen abgeschlossen hat, verlangt, dass ihre klassifizierten Informationen ausschliesslich von Personen mit ihrem Bürgerrecht oder mit Schweizer Bürgerrecht bearbeitet werden (sogenannte "Drittstaatenausschluss-Klausel"). Derartige Informationen dürfen also Personen anderer Nationalität grundsätzlich nicht zugänglich gemacht werden. Vorbehalten bleibt eine vorgängige Bewilligung der Verfasserin bzw. des Verfassers der klassifizierten Informationen.

Art. 16

Abs. 1: Klassifizierte Informationen müssen so bearbeitet werden, dass sie vor unberechtigter Kenntnisnahme geschützt werden. Dieser Schutz muss während der ganzen Dauer der Schutzwürdigkeit der betreffenden Informationen gewährleistet werden. Informationen, die klassifiziert sind, werden nicht archiviert, solange sie nach den Bestimmungen des ISG noch schutzwürdig sind.

Gemäss Abs. 2 müssen klassifizierte Informationen einen Hinweis auf die klassifizierende Stelle enthalten. Dieser Hinweis ist insbesondere für die Entklassifizierung, die Archivierung und die Vernichtung von klassifizierten Informationen wichtig, aber auch für allfällige vorläufige Schutzmassnahmen, die getroffen werden müssen, wenn klassifizierte Informationen gefährdet sind (s. Art. 18).

Abs. 3: Sofern die Schweiz mit einem bestimmten Land oder einer bestimmten internationalen Organisation ein Abkommen zum Austausch von klassifizierten Informationen abgeschlossen hat, wird die Bearbeitung der Informationen, die unter den Geltungsbereich dieses Abkommens fallen, nach den besonderen Vorschriften dieses Vertrags geregelt. Liegt kein solcher Vertrag vor, richtet sich die Bearbeitung klassifizierter Informationen aus dem Ausland nach den Vorschriften des ISG und seiner Ausführungserlasse.

Art. 17

Art. 17 Abs. 1 enthält einen Vorbehalt des Verfahrensrechts der Bundesversammlung sowie desjenigen der Gerichte und der Staatsanwaltschaften. Für die Bekanntgabe klassifizierter Informationen (z.B. im Rahmen der Verwendung derselben als Entscheidgrundlage oder als Beweismittel) soll das jeweilige Verfahrensrecht zur Anwendung kommen. Die Verfahrensgesetze des Bundes enthalten selbst Regelungen darüber, wie weit solche Informationen den Verfahrensbeteiligten zur Einsicht freigegeben werden bzw. wie weit sie im Rahmen öffentlicher Verfahren bekannt werden dürfen oder wie weit Zeugen die Aussage unter Hinweis auf gesetzliche Geheimhaltungspflichten verweigern können (s. etwa Art. 47, 150, 153 und 154 ParlG, Art. 56 Abs. 2 und 59 Abs. 2 BGG, Art. 16 Abs. 2, 18 Abs. 2, 27 und 28 VwVG, Art. 40 Abs. 3 VGG oder Art. 70, 170, 173 Abs. 2 und 194 Abs. 2 StPO sowie Art. 45, 48 Abs. 2, 77 MStP; s. auch Art. 58 der Verordnung vom 24. Oktober 1979 über die Militärstrafrechtspflege (SR 322.2)).

Gemäss Abs. 2 kann allerdings vor dem Entscheid über eine Bekanntgabe klassifizierter Informationen der klassifizierenden Stelle Gelegenheit gegeben werden, sich zu den Klassifizierungsgründen zu äussern und zu den allfälligen Auswirkungen einer Bekanntgabe angehört zu werden. Das zuständige Organ bzw. Gericht entscheidet dann unter Würdigung der Umstände über das weitere Vorgehen.

Art. 18

Die hier formulierten Pflichten entsprechen inhaltlich den heute geltenden Artikeln 15 und 16 ISchV. Sofern die klassifizierende Stelle aus der Information nicht ersichtlich ist, hat die Meldung an die zuständige Aufsichtsbehörde zu ergehen, welche im Rahmen ihres pflichtgemässen Ermessens das weitere Vorgehen bestimmen muss.

Art. 19

Abs. 1 verlangt vorweg von den verpflichteten Behörden (und nicht von den Organisationen), dass sie ein Verfahren zur laufenden Umsetzung und Verbesserung der Informationssicherheit beim Einsatz von IKT-Mitteln festlegen. Das Verfahren muss die sicherheitsmässigen Aufgaben, Kompetenzen und Verantwortungen derjenigen Stellen festhalten, die den Einsatz von IKT-Mittel planen und beschliessen sowie IKT-Mittel entwickeln, betreiben, verwalten, ändern, warten, überprüfen und schliesslich ausser Betrieb setzen. Das Verfahren schliesst insbesondere die materiellen Regelungen von Art. 20-26 ein.

Alle Bundesbehörden verwenden bereits heute ein solches Verfahren. Diese Verfahren müssen aber systematisiert und wo nötig ergänzt werden. Die wichtigsten Verfahrensetappen müssen vereinheitlicht werden. Oft wird zudem die Durchführung des Verfahrens nicht oder nur teilweise überprüft. Nur sehr selten werden die umgesetzten Massnahmen auf deren Wirksamkeit überprüft.

Gemäss Abs. 2 obliegt die Zuständigkeit für die Durchführung des Sicherheitsverfahrens derjenigen Behörde oder Organisation, die den Einsatz von IKT-Mitteln in Auftrag gibt (Leistungsbezüger). Der Leistungsbezüger ist nämlich für die Geschäftsprozesse sowie für die Umsetzung der Sicherheitsanforderungen verantwortlich. Er muss deshalb seine Geschäfts- und Sicherheitsanforderungen derjenigen Stelle, welche die IKT-Mittel betreibt (Leistungserbringer), klar kommunizieren.

In Abs. 3 wird der Grundsatz festgelegt, dass das Sicherheitsverfahren (oder mindestens die betreffenden Verfahrensschritte) bei einer Veränderung der Risiken wiederholt werden muss. Informationssicherheit ist ein Zustand, der sich kontinuierlich und dynamisch verändert. Die verpflichteten Behörden müssen deshalb die periodische oder risikobasierte Überprüfung des Sicherheitszustands und die Wiederholung des Verfahrens festlegen.

Art. 20

Die Schutzbedarfsanalyse nach Abs. 1 stellt den ersten Schritt im Sicherheitsverfahren dar. Eine Stelle, welche die Entwicklung, die Beschaffung oder die Änderung eines IKT-Mittels durchführt oder in Auftrag gibt, will dieses IKT-Mittel für bestimmte Zwecke und für eine festgelegte Lebensdauer einsetzen. Dieser erste Schritt in Bezug auf die Umsetzung der Informationssicherheit besteht darin, bei der Bestimmung des Einsatzzwecks des IKT-Mittels die Geschäftsprozesse zu bestimmen, die mit dem einzusetzenden IKT-Mittel unterstützt werden sollen, sowie die Informationen zu identifizieren, die damit bearbeitet werden sollen. Zu diesem Zeitpunkt - also in der Planungsphase – muss der Leistungsbezüger den Schutzbedarf der Informationen gemäss Art. 4 Abs. 1 erheben sowie die potenziellen Auswirkungen einer Störung oder eines Missbrauchs des einzusetzenden IKT-Mittels auf die Interessen nach Art. 1 Abs. 2 beurteilen. Bei der Beurteilung des Schutzbedarfs muss auch berücksichtigt werden, dass IKT-Mittel meistens in einer bestimmten technischen und/oder logischen Umgebung (sog. Architektur) vernetzt und betrieben werden. Die frühzeitige Identifizierung von Vernetzungen und Abhängigkeiten hilft auch, die Sicherheitsmassnahmen dort umzusetzen, wo sie am wirksamsten sind.

Heutzutage wird z.T. entweder keine Beurteilung des Schutzbedarfs vorgenommen oder sie wird erst dann eingeleitet, wenn das IKT-Mittel bereits in Betrieb ist. Die nachträgliche Umsetzung von Sicherheitsmassnahmen ist in der Regel aber viel schwieriger zu bewerkstelligen und hat massiv höhere Kosten zur Folge.

Aus der Schutzbedarfsanalyse ergeben sich die Anforderungen an den Schutz der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit der Informationen sowie an die Verfügbarkeit und die Integrität des IKT-Mittels. Die Schutzbedarfsanalyse ist auch massgebend für die Sicherheitseinstufung des IKT-Mittels nach Art. 21.

In Abs. 2 wird der Fall einer Behörde oder Organisation geregelt, die eine neue Technologie (Hard- oder Software) - also nicht nur ein neues IKT-Mittel - einsetzen will. Hier soll die betroffene Behörde oder Organisation die Risiken beurteilen, die mit dem Einsatz dieser neuen Technologie verbunden sind, bevor sie sie einsetzt. Es wird ferner verlangt, dass die Behörde oder Organisation ihre Risikobeurteilung der Fachstelle des Bundes für Informationssicherheit mitteilt. Mit der Orientierung der Fachstelle soll sichergestellt werden, dass neue Technologien möglichst nur einmal beurteilt werden und dass alle verpflichteten Behörden und Organisationen davon entsprechenden Nutzen ziehen können. Das Vorlegen der Risikobeurteilungen soll auch dazu dienen, die Konformität der neuen Technologien zu den bestehenden, auch strategischen, Grundlagen zu prüfen.

Die verpflichteten Behörden haben gemäss Art. 86 Abs. 1 Bst. d die Möglichkeit, die Fachstelle des Bundes zu beauftragen, diese Risikobeurteilung durchzuführen.

Art. 21

Art. 21 systematisiert und vereinheitlicht die Sicherheitseinstufung von IKT-Mitteln für alle verpflichteten Behörden und Organisationen. Die geltenden Vorschriften der Bundesverwaltung sehen nur zwei Stufen vor: einen generellen Schutzbedarf und einen erhöhten Schutzbedarf. Das neue Einstufungsmodell mit drei Stufen orientiert sich am Standard des Deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI).

Die Sicherheitseinstufung ist in erster Linie eine Massnahme zur Identifizierung der Kritikalität eines bestimmten IKT-Mittels in Bezug auf die öffentlichen Interessen nach Art. 1 Abs. 2. Die Zuweisung zu einer Sicherheitsstufe gibt auch vor, welche Sicherheitsanforderungen gelten und wie die Schutzmassnahmen definiert werden müssen (s. Art. 22-24). Der Bundesrat soll für jede Sicherheitsstufe in Bezug auf den Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit standardisierte Sicherheitsanforderungen und -massnahmen festlegen (s. Art. 88). Die Standardisierung der Sicherheitsanforderungen und -massnahmen ist für einen effizienten und sicheren behördenübergreifenden Informationsaustausch zwingend notwendig. Sie hat wichtige Vorteile: Vorab werden den Entwicklungs- und Beschaffungsstellen von

IKT-Mitteln klare zu erfüllende Sicherheitsanforderungen vorgelegt, welche ihnen bei der Implementierung der Sicherheit in die IKT-Mittel helfen werden. Sodann werden die Kosten der Sicherheit transparenter und einfacher berechenbar und planbar (Sicherheitskosten sind Projektkosten).

Abs. 1: Die Sicherheitsstufe «Grundschutz» gilt für alle IKT-Mittel, die keine besonderen hohen Anforderungen an den Schutz der Informationen aufweisen (s. auch Art. 22). Personendaten, INTERN klassifizierte Informationen sowie weitere Informationen, die zwar in Bezug auf ihre Vertraulichkeit geschützt werden müssen, aber nicht einen hohen Schutz benötigen, werden mit so eingestuften Mitteln bearbeitet.

Abs. 2: Für IKT-Mittel der Sicherheitsstufe «hoher Schutz» gelten - neben den Anforderungen des Grundschutzes - besondere Sicherheitsanforderungen und -massnahmen, z.B. das Erfordernis der Erstellung eines Informationssicherheitskonzepts sowie die Durchführung einer PSP bei Personen, die solche Mittel betreiben, verwalten, warten oder überprüfen sollen.

- Bst. a: IKT-Mittel gehören in diese Sicherheitsstufe, wenn die Informationen, die damit bearbeitet werden sollen, hohe Anforderungen an die Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit vorweisen. Die jeweiligen Anforderungen werden hinsichtlich einer potenziellen erheblichen Beeinträchtigung der Interessen nach Art. 1 Abs. 2 beurteilt, die durch die Verletzung eines der vier genannten Schutzkriterien verursacht werden kann. Bei als VERTRAULICH klassifizierten Informationen ist die potenzielle Beeinträchtigung bereits in der Definition der Klassifizierungsstufe enthalten (*erhebliche* Beeinträchtigung). Die IKT-Mittel, mit welchen als VERTRAULICH klassifizierten Informationen bearbeitet werden sollen, gehören somit in die Stufe «hoher Schutz». Dies trifft auch für IKT-Mittel zu, die für die Bearbeitung von besonders schützenswerten Personendaten oder von Geschäfts- oder Fabrikationsgeheimnissen benützt werden sollen, sofern der potenzielle Schaden bei einer Verletzung der Vertraulichkeit dieser Informationen erheblich ist.
- Bst. b: Wenn mit einem IKT-Mittel Geschäftsprozesse unterstützt werden, deren Ausfall zu einer erheblichen Beeinträchtigung der Handlungsfähigkeit einer Behörde führen kann, dann ist das IKT-Mittel ebenfalls dieser Sicherheitsstufe zuzuweisen. Bst. b ist aber eigentlich bereits in Bst. a enthalten, denn IKT dienen ausschliesslich zur Bearbeitung von Informationen und haben keinen Selbstzweck. Die Störung und der Missbrauch der Funktionsfähigkeit des IKT-Mittels selbst werden aber als Einstufungsgrund in das Gesetz aufgenommen, weil diese Regelung für viele Nicht-Spezialisten wesentlich verständlicher ist.

Abs. 3: IKT-Mittel gehören in die Stufe «sehr hoher Schutz», wenn die Informationen, die damit bearbeitet werden sollen, sehr hohe Anforderungen an die Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit aufweisen. Der Aufbau dieser Bestimmung ist identisch mit Abs. 2, wobei der potenzielle Schaden *schwerwiegend* sein muss. Es geht hier zum Beispiel um IKT-Mittel, mit welchen als GEHEIM klassifizierte Informationen bearbeitet werden, oder solche, deren Ausfall den Interessen nach Art. 1 Abs. 2 schwerwiegenden Schaden zufügen kann.

Art. 22

Abs. 1: Die Praxis hat gezeigt, dass mit einer Anzahl bestimmter und vordefinierter Anforderungen und Massnahmen die Risiken für eine Mehrheit der IKT-Mittel auf ein tragbares Mass reduziert werden können. Die Gesamtheit aller solchen Anforderungen und Massnahmen bildet den Grundschutz. Der Vorteil eines definierten und standardisierten Grundschutzes besteht darin, dass die Behörden und Organisationen für IKT-Mittel dieser Stufe keine detaillierten und aufwändigen Risikobeurteilungen durchführen müssen. Die verpflichteten Behörden müssen festlegen, welches minimale Sicherheitsniveau sie für alle ihre IKT-Mittel verlangen wollen. Die Festlegung eines Grundschutzes ist keine technische Angelegenheit, die von Fachexperten beschlossen werden soll. Sie ist eine Führungsaufgabe, welche das Abwägen von Sicherheitszielen und Kosten voraussetzt. Je nach Stärke des Grundschutzes können nämlich die umzusetzenden organisatorischen, personellen, technischen und physischen Massnahmen teurer oder weniger teuer ausfallen.

Abs. 2 legt den Grundsatz fest, dass alle IKT-Mittel, unabhängig von der ihnen zugewiesenen Sicherheitsstufe, die Anforderungen des Grundschutzes erfüllen müssen. Der Grundschutz wird somit auch als Fundament definiert, auf welches IKT-Mittel der Sicherheitsstufen «hoher Schutz» und «sehr hoher Schutz» aufbauen müssen. Die Massnahmen des Grundschutzes müssen somit auch relativ flexibel und modular ausgestaltet werden. Sind bestimmte Massnahmen bei einem besonderen IKT-Mittel nicht umsetzbar, so müssen andere Massnahmen zur Anwendung kommen, die einen gleichwertigen Schutz ermöglichen.

Art. 23

Abs. 1: Für IKT-Mittel der Sicherheitsstufen «hoher Schutz» und «sehr hoher Schutz» genügen die Anforderungen und Massnahmen des Grundschutzes nicht. Für solche Mittel wird zuerst die Durchführung einer objektbezogenen Risikoanalyse verlangt. Das Schwergewicht liegt dabei auf dem Schutz derjenigen Krite-

rien, welche erhöhte Schutzanforderungen haben. Wenn ein IKT-Mittel aufgrund erhöhter Anforderungen an die Verfügbarkeit in die Stufe «hoher Schutz» eingestuft wird, es aber gleichzeitig keine erhöhten Anforderungen an den Schutz der Vertraulichkeit aufweist, dann müssen in erster Linie die Risiken für die Verfügbarkeit beurteilt werden. Nach der Risikoanalyse muss ein Informationssicherheitskonzept erstellt werden. Die Verantwortung dafür liegt beim Leistungsbezüger, wobei eine enge Zusammenarbeit mit dem Leistungserbringer erforderlich ist. Die Umsetzung der technischen Massnahmen liegt nämlich grundsätzlich im Zuständigkeitsbereich derjenigen Stelle, die das IKT-Mittel betreiben wird und deswegen über das technische Know-how verfügt.

Abs. 2 legt die Zuständigkeiten für die Prüfung und Genehmigung des Informationssicherheitskonzeptes fest. Um sicherzustellen, dass das Informationssicherheitskonzept durch ausgewiesenes fachkundiges Personal geprüft wird, verlangt das Gesetz, dass diese Prüfung von der oder dem Informationssicherheitsbeauftragten (Art. 84) vorgenommen wird. Es geht dabei darum, zu prüfen, ob das Konzept die formellen, rechtlichen und geschäftlichen Anforderungen erfüllt, so dass es den tatsächlichen Stand der Informationssicherheit beschreibt und die zu tragenden Restrisiken ausführlich ausweist. Idealerweise sollte die oder der Informationssicherheitsbeauftragte die Erstellung des Informationssicherheitskonzepts begleiten, um allfällige Probleme frühzeitig zu erkennen und gezielt zu lösen. Anschliessend muss das Informationssicherheitskonzept durch die Behörde oder Organisation selbst genehmigt werden. Diese Genehmigung geschieht bereits in der Planungs- oder Konzeptphase, also noch bevor das IKT-Vorhaben sich in der Realisierungsphase befindet. Damit soll sichergestellt werden, dass die Geschäftsleitung frühzeitig ihre Verantwortung in Bezug auf die Informationssicherheit wahrnimmt. Sie soll nicht erst dann entscheiden müssen, wenn das IKT-Mittel kurz vor der Inbetriebnahme steht (s. Art. 25), und bereits wesentliche finanzielle Mittel eingesetzt worden sind.

Abs. 3: Das Informationssicherheitskonzept ist nicht ein Dokument, das bloss einmal - bei der Planung des Einsatzes eines IKT-Mittels - erstellt werden muss und dann in unveränderter Form bestehen bleibt. Die geplanten Massnahmen sind oft nicht identisch mit den tatsächlich umgesetzten Massnahmen. Deshalb muss das Informationssicherheitskonzept laufend aktualisiert werden, um den aktuellen Stand der Sicherheit zu beschreiben. Auch bei Veränderungen der Risiken muss es entsprechend angepasst werden.

Art. 24

Abs. 1 verlangt für alle IKT-Mittel, die sicherheitsmässig zur Inbetriebnahme freigegeben werden sollen, einen Beleg dafür, dass das Sicherheitsverfahren rechtmässig durchgeführt wurde und dass die Massnahmen des Grundschutzes oder gegebenenfalls des Informationssicherheitskonzepts umgesetzt worden sind. Wer diese Prüfung durchführen muss, müssen die verpflichteten Behörden festlegen.

Abs. 2: Für IKT-Mittel der Sicherheitsstufe «sehr hoher Schutz» wird zusätzlich verlangt, dass die Wirksamkeit der umgesetzten Massnahmen geprüft wird. Bei dieser Wirksamkeitsprüfung werden tatsächliche Angriffe gegen das IKT-Mittel ausgeführt, um allfällige Sicherheitslücken und ausnutzbare Schwachstellen zu identifizieren und vor der Inbetriebnahme zu korrigieren (z.B. mittels *Penetration Tests*). Die Wirksamkeitsprüfung wird nur für IKT-Mittel der Stufe «sehr hoher Schutz» verlangt, weil sie mit einem nicht unerheblichen finanziellen Aufwand verbunden ist (0.5 bis 2% der gesamten Investitionskosten).

Art. 25

Abs. 1: Die Geschäftsleitung der leistungsbeziehenden Behörde oder Organisation trägt die Verantwortung für die Informationssicherheit. Es wird deshalb verlangt, dass die Behörden- oder Organisationsleitung ihre IKT-Mittel selbst sicherheitsmässig zum Einsatz freigibt.

Abs. 2: Die Sicherheitsfreigabe bedeutet, dass die Behörde oder Organisation die identifizierten Restrisiken kennt und auch bereit ist, diese zu tragen. Ist sie der Meinung, die Restrisiken seien noch zu hoch, kann sie die Freigabe verweigern und die Umsetzung ergänzender risikomindernder Massnahmen verlangen.

Art. 26

Für eine wirksame Bewirtschaftung der Risiken ist es erforderlich, die Übersicht über alle eingesetzten IKT-Mittel zu wahren. Die verpflichteten Behörden und Organisationen müssen deshalb die IKT-Mittel, die sie einsetzen, in einem Inventar oder einem Portfolio erfassen. Alle IKT-Mittel müssen einer zuständigen Person oder Stelle zugerechnet werden können.

Das Inventar soll unter anderem die Sicherheitseinstufung der IKT-Mittel, den Namen der zuständigen Person oder Stelle, die Sicherheitsunterlagen sowie auch alle erforderlichen Systeminformationen enthalten, die für die Wiederherstellung des Betriebs im Falle einer Störung oder eines Ausfalls des IKT-Mittels erforderlich sind.

Art. 27

Behörden, Organisationen oder Dritte, die im Auftrag der verpflichteten Behörden und Organisationen IKT-Mittel betreiben, sind für die Aufrechterhaltung der Informationssicherheit beim Betrieb derselben verantwortlich. Die internen Leistungserbringer fallen alle unter den Anwendungsbereich dieses Gesetzes und müssen deshalb für ihre Tätigkeiten auch die Art. 19-26 anwenden. Externe Leistungserbringer dagegen gelten als Dritte im Sinne von Art. 8 und müssen vertraglich verpflichtet werden, die Massnahmen dieses Gesetzes einzuhalten. Die verpflichteten Behörden und Organisation, die den Betrieb von IKT-Mitteln in Auftrag geben, müssen ihre IKT-Mittel-bezogenen Anforderungen mit dem Leistungserbringer vereinbaren.

Beim Betrieb muss der Leistungserbringer in Bezug auf die Informationssicherheit folgende Fähigkeiten und Aktivitäten sicherstellen:

- Netzwerkmanagement, z.B.: Rollen und Verantwortlichkeiten; Netzwerkdesign; Security-Audits;
- Trafficmanagement, z.B.: Konfiguration von Netzwerkdevices; Regelungen für Managementzugriffe, Verschlüsselung und Authentifizierung; Firewalls; externe Zugriffe; Zugriffe via Wireless Technologien;
- Netzwerkbetrieb, z.B.: detaillierte Leistungsbeschreibungen und Einhaltung der SLA; Monitoring (inkl. Netzwerküberwachung); Release-, Change-, Life-Cycle-Management; Incident- und Security-Management; Capacity- und Ressource-Management; Desaster- und Recovery-Management;
- Audit-Berichterstattung an die Leistungsbezüger.

Art. 28

Personen, die mit Informationen oder IKT-Mitteln des Bundes umgehen sollen, müssen bestimmte Anforderungen erfüllen. Es liegt in der Verantwortung des Arbeit- bzw. des Auftraggebers, dafür zu sorgen, dass die Arbeit- bzw. Auftragnehmer diese Anforderungen erfüllen.

- Bst. a: Bei der Auswahl der anzustellenden oder zu beauftragenden Personen müssen die Auswahlkriterien der Schutzwürdigkeit der Informationen oder der Kritikalität der IKT-Mittel entsprechen. Die Arbeitgeber sind für ihre Personalentscheide verantwortlich. Die Unterstellung einer Person unter die PSP entbindet sie nicht von dieser Verantwortung.
- Bst. b: Die verpflichteten Behörden und Organisationen müssen ihre Angestellten und Auftragnehmer ausreichend ausbilden. Im Bereich der Informationssicherheit genügt eine einmalige Ausbildung nicht. Die Arbeit- und Auftragnehmer müssen regelmässig geschult und sensibilisiert werden. Besondere Aufmerksamkeit ist der Schulung der Vorgesetzten zu schenken.
- Bst. c: Sofern die Angestellten oder die Auftragnehmer mit Informationen umgehen sollen, die erhöhte Anforderungen an den Schutz der Vertraulichkeit aufweisen, müssen sie zur Geheimhaltung verpflichtet werden. Angestellte des Bundes, die dem BPG unterstellt sind, müssen aufgrund von Art. 22 BPG das Amtsgeheimnis wahren. Bei Dritten, die für den Bund Aufträge ausführen sollen, muss die Geheimhaltungspflicht schriftlich im Vertrag festgehalten werden und bei ihrer Nichteinhaltung mit klaren Folgen verbunden sein.

Art. 29

Wer für eine Bundesbehörde arbeitet oder einen Auftrag ausführt, braucht zur Aufgabenerfüllung unter Umständen einen Zugang zu bestimmten Informationen, IKT-Mitteln oder Räumlichkeiten. Abs. 1 stellt einen zentralen Grundsatz der Informationssicherheit auf. Die Arbeit- und Auftragnehmer sollen nur diejenigen Berechtigungen erhalten, die sie zur Erfüllung ihrer Aufgaben tatsächlich benötigen. Das Risiko eines Missbrauchs kann wesentlich reduziert werden, wenn eine Person nicht ohne Grund Informationen eines anderen Bereichs bearbeiten kann.

Abs. 2 verlangt die laufende Verwaltung dieser Berechtigungen. Es kommt vor, dass ehemalige Angestellte oder Auftragnehmer nach Beendigung des Arbeitsverhältnisses, des Vertrags oder einer besonderen Aufgabe nicht aufgefordert werden, ihren Schlüssel oder ihren Badge zurückzugeben, oder dass ihr Benutzerkonto nicht gesperrt wird. Solche "ungültige" Berechtigungen können in der Folge benutzt werden, um gegen die Interessen des Arbeit- oder Auftraggebers zu handeln. Wenn eine Anstellung, ein Vertrag oder eine Aufgabe beendet ist, müssen die entsprechenden Berechtigungen entzogen werden. Besteht Grund zur Annahme, dass eine Gefährdung der Informationssicherheit vorliegt, müssen die Berechtigungen sofort gesperrt oder entzogen werden. Beide Massnahmen sollen dazu beitragen, das Risiko einer Innentat zu reduzieren.

Abs. 3 verlangt einen geeigneten Prozess zur regelmässigen Überprüfung der Berechtigungen.

Art. 30

Bei den physischen Schutzmassnahmen geht es darum, die Risiken durch physische Bedrohungen zu reduzieren. Zu diesen Risiken gehören unter anderem menschliche Handlungen wie z.B. Spionage, Diebstahl, Vandalismus oder Sabotage. Dazu gehören aber auch Elementarschäden durch Hitze, Feuer, Wasser, Staub, Vibrationen, usw. Für die Beurteilung der Massnahmen des physischen Schutzes, den sogenannten Objektschutz, ist fedpol in Zusammenarbeit mit dem BBL zuständig. Für Teile des VBS und die Armee ist die IOS in Zusammenarbeit mit der armasuisse oder dem BBL zuständig.

Abs. 1 legt den Grundsatz fest, dass die verpflichteten Behörden und Organisationen den physischen Schutz ihrer Informationen und IKT-Mittel in ihren Räumlichkeiten gewährleisten müssen. Zu verhindern ist insbesondere der unberechtigte Zugang zu den Informationen oder IKT-Mitteln etwa durch Zugangskontrollen, Videokameras, Schliesssysteme, Sicherheitsräume und -behältnisse, Akten- und Datenträgervernichtungsgeräte, Sichtschutz, usw. Gegen Elementarschäden werden z.B. Brandmeldeanlagen und automatische Löschanlagen eingesetzt.

Abs. 2 regelt den Fall von Informationen oder IKT-Mitteln, die öffentlich zugänglich sind. Es handelt sich dabei einerseits um Informationen und IKT-Mittel, die von ihrem üblichen Standort (Büro) mitgenommen werden und die anschliessend - ausserhalb des üblichen Sicherheitsperimeters - angemessen geschützt werden müssen. Es handelt sich aber auch um Informationen und Einrichtungen, Verkabelungen und Versorgungsleitungen, die nicht unter der ständigen Kontrolle der Behörde oder Organisation stehen. Besondere Aufmerksamkeit muss z.B. Zugangspunkten wie Anlieferungs- und Ladezonen geschenkt werden.

Art. 31

Der Begriff "Sicherheitszone" wird im ISG für Räumlichkeiten und Bereiche verwendet, in welchen häufig klassifizierte Informationen der Stufe VERTRAULICH oder GEHEIM bearbeitet oder IKT-Mittel der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» betrieben werden und die zu diesem Zweck besonders geschützt werden. Die Ausscheidung dieser Räume bzw. Bereiche als Sicherheitszone stellt eine physische Massnahme der Informationssicherheit dar, die bereits heute beim Bund teilweise ergriffen wird, insbesondere zum Schutz von Serverräumen oder von bestimmten Führungsräumen. Eine Sicherheitszone muss vordefiniert werden, identifizierbar sein und entsprechend geschützt werden. Die Ausführungsbestimmungen des Bundesrats werden voraussichtlich zwei Arten von Sicherheitszonen definieren, je nach Kritikalität der Informationen oder IKT-Mittel. Die Massnahmen in den Sicherheitszonen der jeweiligen Stufen werden risikogerecht auszugestalten sein. Der Bundesrat und die für den Objektschutz zuständigen Bundesstellen (fedpol, BBL, IOS und armasuisse), werden in Zusammenarbeit mit der Fachstelle des Bundes für Informationssicherheit Standardmassnahmen für die Sicherheitszonen festlegen (s. Art. 88).

In Abs. 1 werden zunächst die Voraussetzungen für die Bezeichnung einer Sicherheitszone nach dem ISG festlegt: Im zu bezeichnenden Bereich müssen häufig als VERTRAULICH oder GEHEIM klassifizierte Informationen bearbeitet oder IKT-Mittel der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» betrieben werden. Im Gegensatz zur Gesetzgebung anderer Länder oder internationaler Organisationen (s. auch Abs. 5) besteht für die verpflichteten Behörden und Organisationen nach ISG aber keine Pflicht, solche Bereiche als Sicherheitszone zu bezeichnen. Über ihre tatsächliche Einrichtung entscheidet die Risikobeurteilung.

Abs. 2 legt fest, dass nur identifizierte und berechtigte Personen Zugang zu einer Sicherheitszone erhalten dürfen. Der Zugang muss also für die Erfüllung einer bestimmten Aufgabe erforderlich sein. Dies setzt entsprechende Zutrittskontrollen und die Protokollierung der Zutritte voraus.

Abs. 3 regelt die besonderen Befugnisse der Behörde oder Organisation, die eine Sicherheitszone einrichtet:

- Bst. a: Für die Zutrittskontrolle darf die Behörde oder Organisation biometrische Identifikationsmethoden (z.B. Fingerabdruck oder Iris-Scan) verwenden. Diese Identifikationsmethoden sind wesentlich zuverlässiger als die Identifikation mit einem normalen Ausweis. Sie kommen heute in gewissen Bereichen bereits zum Einsatz.
- Bst. b: Die Mitnahme bestimmter Gegenstände in eine Sicherheitszone kann eingeschränkt werden. Die Mitnahme von Bild- oder Tonaufnahmegeräten (inkl. Smartphones oder Notebooks mit entsprechenden Funktionen) ist in der Regel nur mit besonderer Bewilligung erlaubt.
- Bst. c: Bereiche der Sicherheitszone, die für die Informationssicherheit besonders wichtig sind (z.B. die Zutrittszone zu einem besonderen Serverraum, der Administratorarbeitsplatz oder der Archivraum mit als GEHEIM klassifizierten Informationen), können mittels Videoaufnahmegeräten überwacht werden.

- Bst. d: Beim Ein- oder Ausgang kann die Behörde oder Organisation Taschen- oder Personenkontrollen durchführen lassen. Damit soll verhindert werden, dass Personen ohne Bewilligung Geräte in die Sicherheitszone mitnehmen (s. Bst. b) oder Informationen (z.B. mit einem USB-Memorystick) entwenden.
- Bst. e: Zur Durchsetzung der Informationssicherheitsvorschriften sollen auch in einer Sicherheitszone Bürokontrollen möglich sein. Bei den Bürokontrollen wird unter anderem die Einhaltung der sogenannten "Clean Desk Policy" überprüft (es dürfen keine schutzwürdigen Informationen auf dem Schreibtisch oder anderswo herumliegen, der PC muss gesperrt oder ausgeschaltet sein, Datenträger müssen unter Verschluss gehalten werden, die Schubladen müssen geschlossen sein, der Abfallkorb darf keine klassifizierten Informationen enthalten, usw.). Die Kontrolle darf auch in Abwesenheit der betroffenen Personen, z.B. während der Nacht, stattfinden.

Gemäss Abs. 4 soll die Behörde oder Organisation in bestimmten Sicherheitszonen die Möglichkeit haben, eine störende Fernmeldeanlage nach Artikel 34 Absatz 1ter des Fernmeldegesetzes vom 30. April 1997 (FMG; SR SR 784.10) zu betreiben, wenn dies erforderlich ist. Der tatsächliche Bedarf sowie die Bedingungen für den Betrieb einer solchen Störanlage werden nach dem FMG beurteilt.

In Abs. 5 werden Vorschriften für Sicherheitszonen nach völkerrechtlichen Verträgen (Art. 90) sowie die entsprechenden Vorschriften zum Schutz militärischer Anlagen vorbehalten. In beiden Fällen stellt die Einrichtung einer Sicherheits- bzw. Schutzzone keine Option, sondern eine Pflicht dar (s. z.B. ISA CH-EU).

2.1.3 Personensicherheitsprüfungen

Art. 32

Die Personensicherheitsprüfung (PSP) ist eine vorbeugende Massnahme zum Schutz vor Innentätern. Sie soll das Risiko einer Beeinträchtigung der Interessen nach Art. 1 Abs. 2 identifizieren, das mit der Ausübung einer sicherheitsempfindlichen Tätigkeit durch eine bestimmte Person verbunden ist. Es geht also darum, die Wahrscheinlichkeit einzuschätzen, dass eine bestimmte zu prüfende Person vorsätzlich oder fahrlässig die Interessen nach Art. 1 Abs. 2 beeinträchtigen wird. Dafür werden relevante Daten über die Lebensführung dieser Person erhoben. Gestützt auf diese Daten wird durch dafür ausgebildete Fachspezialisten (*Risk Profiler*) eine Beurteilung des Sicherheitsrisikos vorgenommen. Es versteht sich, dass eine solche Beurteilung nie absolut verlässlich sein kann.

Nachdem sie von der Beurteilung des Risikos durch die zuständige Fachstelle PSP Kenntnis genommen hat, entscheidet alleine die verpflichtete Behörde oder Organisation, ob sie ein allfälliges erhöhtes Risiko tragen will, ob sie dieses mit bestimmten Auflagen reduzieren will oder ob sie es durch Nichtanstellung oder Kündigung vermeiden will.

Für das Verständnis der vorgeschlagenen Regelung sind zwei Punkte wesentlich:

- Die Beurteilung des Sicherheitsrisikos durch die zuständige Fachstelle PSP stellt eine Empfehlung dar. Für den Entscheid über eine allfällige Anstellung bzw. Beauftragung ist einzig die anstellende bzw. Auftrag gebende Stelle zuständig. Das Risiko wird dementsprechend nie von der für die Beurteilung des Sicherheitsrisikos zuständigen Fachstelle PSP getragen. Dies trifft sowohl bei einer Risikoerklärung (es besteht ein Sicherheitsrisiko) als auch bei einer Sicherheitserklärung (es besteht kein Sicherheitsrisiko) zu. Vorgesetzte werden auch dann, wenn der geprüften Person eine Sicherheitserklärung ausgestellt wurde, nicht von ihrer Pflicht entbunden, allfällige erhöhte Risiken in Verbindung mit der geprüften Person zu identifizieren und gegebenenfalls zu bewältigen.
- Die PSP muss risikogerecht eingesetzt werden. Das vorliegende Gesetz legt klare Voraussetzungen für die Durchführung der Prüfung fest. Dies bedeutet nicht, dass diejenigen Funktionen, die bis anhin zusätzlich geprüft wurden, weniger wichtig oder keinem erhöhten Risiko ausgesetzt wären. Für diese Funktionen und für alle anderen Funktionen, die nicht geprüft werden, wird die Verantwortung für die Beurteilung des Sicherheitsrisikos aber einzig und allein der Linie übertragen. Mit der vorgeschlagenen Einführung eines neuen Art. 20*a* BPG werden die Arbeitgeber nach Art. 3 BPG hierfür inskünftig über geeignete Mittel (Auszüge aus dem Strafregister sowie aus dem Betreibungs- und Konkursregister) verfügen.

Art. 33

Art. 33 regelt in Verbindung mit Art. 34 Abs. 1 die Unterstellung der Angehörigen der verpflichteten Behörden und Organisationen. Die verpflichteten Behörden (also nicht die Organisationen nach Art. 2 Abs. 2) müssen für ihren Zuständigkeitsbereich eine Liste derjenigen Funktionen erlassen, für deren Aufgabenerfüllung die Ausübung einer sicherheitsempfindlichen Tätigkeit *erforderlich ist* und die somit geprüft werden sollen. Für die materiellen Voraussetzungen für den Eintrag einer Funktion in die Funktionsliste wird aber nicht einfach das heutige System übernommen. Wie in Ziff. 1.2.4 erwähnt, wird zwar vom Kriterium der

Regelmässigkeit, insbesondere bei der Bearbeitung von klassifizierten Informationen, abgesehen. Entscheidend für die Unterstellung der Bundesangestellten unter die Personensicherheitsprüfung ist aber die Frage, ob die Inhaberin oder der Inhaber einer bestimmten Funktion für ihre oder seine Aufgabenerfüllung eine sicherheitsempfindliche Tätigkeit ausüben *muss*. Wenn eine solche Tätigkeit für die funktionsbedingte Aufgabenerfüllung *erforderlich* ist, dann - und nur dann - muss die Funktion in die Liste der zu prüfenden Funktionen aufgenommen werden.

Einige fiktive Beispiele vermögen die Umsetzung des Prinzips zu erläutern:

- Eine Mitarbeiterin des Bundesamts für Umwelt ist im Rahmen ihrer Aufgaben für die Umweltverträglichkeitsprüfung im Zusammenhang mit militärischen Bauten und Anlagen zuständig. Für ihre Aufgabenerfüllung muss sie klassifizierte Informationen bearbeiten und manchmal Zugang zu militärischen Anlagen haben. Ihre Funktion muss in die Funktionsliste aufgenommen werden.
- Ein Mitarbeiter der Eidgenössischen Finanzverwaltung muss ausnahmsweise die Auswirkungen eines als VERTRAULICH klassifizierten Antrags des EJPD an den Bundesrat beurteilen. Für solche Geschäfte sind normalerweise andere Mitarbeitende zuständig, die aber ferien- und krankheitshalber abwesend sind. Diese Aufgabe gehört grundsätzlich nicht zu seiner Funktion, die dementsprechend nicht auf der Liste aufgeführt werden darf.
- Das Reinigungspersonal einer Behörde hat hin und wieder ungewollten Zugang zu klassifizierten Informationen, wenn es im Rahmen seiner ordentlichen Aufgabenerfüllung die Büros der Bundesangestellten reinigt und letztere die Informationsträger nicht vorschriftsgemäss aufbewahren oder entsorgen. Es gehört aber nicht zum Aufgabenbereich des Reinigungspersonals, klassifizierte Informationen zu bearbeiten. Es darf deshalb nicht in die Liste aufgenommen werden, es sei denn, es sei für die Reinigung innerhalb einer Sicherheitszone zuständig.

Das Kriterium der *Regelmässigkeit*, auch wenn es *de facto* fast immer erfüllt sein wird, ist *de iure* irrelevant. Selbst wenn im Pflichtenheft einer Funktion nur 5% des Arbeitspensums für die Erfüllung sicherheitsempfindlicher Aufgaben vorgesehen sind, soll diese Funktion in die Funktionsliste aufgenommen werden. Dies auch dann, wenn die betroffene Funktionsinhaberin vielleicht während einer längeren Periode gar keine solchen Aufgaben erfüllen muss. Die *Eventualität* der funktionsbedingten Ausübung einer sicherheitsempfindlichen Tätigkeit ist hingegen kein Grund dafür, eine Funktion in die Funktionsliste aufzunehmen.

Die Umsetzung dieses restriktiven Ansatzes setzt voraus, dass die verpflichteten Behörden und Organisationen eine klare Übersicht über die internen und übergreifenden Geschäftsprozesse und Aufgabenbereiche haben, die notwendigerweise mit sicherheitsempfindlichen Tätigkeiten verbunden sind. Sich in diesem Bereich einen Überblick zu verschaffen und diesen zu behalten, stellt gleichzeitig eine grundsätzliche Massnahme im Bereich des Risikomanagements der Informationssicherheit dar. Die Gründe für den Eintrag einer Funktion in die Funktionsliste sollen nachweisbar sein: Die Stellenbeschreibungen (oder Pflichtenhefte) der jeweiligen Funktionen sollen eine genaue Umschreibung der Aufgaben beinhalten, für deren Erfüllung die Ausübung einer sicherheitsempfindlichen Tätigkeit erforderlich ist. Zudem sollen die verpflichteten Behörden und Organisationen unabhängig von einer allfälligen Unterstellung unter die Personensicherheitsprüfung die erforderlichen organisatorischen und personellen Massnahmen treffen, um den Kreis der Personen, die sicherheitsempfindliche Tätigkeiten ausüben müssen, auf das notwendige Minimum zu beschränken.

Mit dem Begriff "*erlassen*" wird klar gestellt, dass es sich um eine formelle Rechtsetzungsdelegation an die verpflichteten Behörden handelt. Die Funktionslisten werden somit in Verordnungen oder Reglementen zu finden sein. In Bezug auf die Bundesverwaltung soll also grundsätzlich am heutigen System festgehalten werden, wonach der Bundesrat im Anhang zur PSPV diese Funktionen bezeichnet (s. Ziff. 1.2.4). Aufgrund der Zuständigkeitsregelungen gemäss RVOG wird er aber weiterhin die Departemente und die Bundeskanzlei ermächtigen können, ihre eigenen, detaillierten Listen zu erlassen.

Art. 34

Abs. 1: Art. 34 legt fest, wer geprüft werden muss.

- Bst. a: Bei Angestellten der verpflichteten Behörden und Organisationen werden nur diejenigen Personen unterstellt, deren Funktion in den Funktionslisten nach Art. 33 enthalten sind. Die Funktionsliste ist also verbindlich. Die Ausnahmen werden in Abs. 3 und 4 geregelt.
- Bst. b: Für Dritte wird die Prüfung durchgeführt, wenn sie im Rahmen eines Auftrages an der Ausübung einer sicherheitsempfindlichen Tätigkeit beteiligt werden.
- Bst. c: Die Voraussetzung für die Durchführung der PSP im internationalen Verhältnis werden durch die entsprechenden völkerrechtlichen Verträge geregelt. Grundsätzlich gilt die Regel von Abs. 2.

Abs. 2: Der Grundsatz von Abs. 1 Bst. b gilt auch für Personen, die im Auftrag einer ausländischen oder einer internationalen Behörde eine sicherheitsempfindliche Tätigkeit ausüben sollen.

Abs. 3 regelt den Fall einer Funktion, welche die Kriterien nach Art. 33 erfüllt aber noch nicht in die entsprechende Liste aufgenommen worden ist. In diesem Fall kann die Prüfung durchgeführt werden, sofern die verpflichtete Behörde zustimmt. Die Liste muss danach angepasst werden.

Abs. 4: Bei Mitgliedern von Behörden, die vom Volk oder als Magistratspersonen von der Bundesversammlung gewählt werden, darf keine vorgängige Personensicherheitsprüfung durchgeführt werden, auch wenn diese Personen oft die sicherheitsempfindlichsten Tätigkeiten ausüben.

Art. 35

In Bezug auf die Prüfstufen enthält das BWIS keine präzise Regelung. Das Legalitätsprinzip verlangt aber aufgrund des tiefen Eingriffs in die Grundrechte der zu prüfenden Personen, die mit der Durchführung der PSP verbunden sind, dass die wichtigsten Modalitäten des Eingriffs auf Gesetzessebene festgehalten werden. Da die Prüfstufen für die Schwere des Eingriffs massgebend sind, müssen sie im Gesetz geregelt werden.

Die Vorlage sieht neu (s. Ziff. 1.2.4) folgende zwei Prüfstufen vor:

- Bst. a: Die Grundsicherheitsprüfung gilt für sicherheitsempfindliche Tätigkeiten, bei deren vorschriftswidriger oder unsachgemässer Ausübung die Interessen nach Art. 1 Abs. 2 erheblich beeinträchtigt werden können. Es handelt sich also aufgrund des erwähnten Schadenspotenzials implizit um: (a) die Bearbeitung von als VERTRAULICH klassifizierten Informationen; (b) die Verwaltung, den Betrieb, die Überprüfung oder die Wartung von IKT-Mitteln der Sicherheitsstufe «hoher Schutz»; und (c) den Zugang zu Sicherheitszonen, in welchen Tätigkeiten nach (a) und (b) ausgeübt werden. Für den Zugang zu Schutzzonen 2 einer militärischen Anlage ist ebenfalls eine PSP dieser Stufe erforderlich.
- Bst. b: Die erweiterte PSP gilt entsprechend für (a) die Bearbeitung von als GEHEIM klassifizierten Informationen; (b) die Verwaltung, den Betrieb, die Überprüfung oder die Wartung von IKT-Mitteln der Sicherheitsstufe «sehr hoher Schutz»; und (c) den Zugang zu Sicherheitszonen, in welchen Tätigkeiten nach (a) und (b) ausgeübt werden. Für den Zugang zu Schutzzonen 3 einer militärischen Anlage ist ebenfalls eine PSP dieser Stufe erforderlich.

Es obliegt den verpflichteten Behörden, die Prüfstufen für die entsprechenden Funktionen und Aufträge festzulegen.

Art. 36

Die Fachstellen PSP können in keinem Fall von sich aus eine PSP einleiten und durchführen; sie benötigen immer einen entsprechenden Auftrag. Einerseits kann es nicht Sache der höchsten Behörden sein, sämtliche Prüfverfahren direkt einzuleiten, andererseits sollte aber auch nicht jede Dienststelle von sich aus solche Aufträge erteilen können. Art. 36 sieht daher vor, dass die verpflichteten Behörden je für ihren Zuständigkeitsbereich diejenigen Stellen bezeichnen, welche zur Einleitung der Prüfverfahren und der entsprechenden Auftragserteilung an die Fachstellen PSP ermächtigt sind. Es handelt sich dabei um eine formelle Kompetenz. In diesem Zusammenhang ist darauf hinzuweisen, dass die einleitenden Stellen häufig nicht identisch mit den Stellen sind, welche nach der Prüfung in Anwendung von Art. 44 über die Übertragung der sicherheitsempfindlichen Aufgabe entscheiden (übertragende Stellen).

Der Bundesrat kann auch, soweit er dies für zweckmässig erachtet, bestimmte Dritte zur Einleitung von PSP ermächtigen. Dies betrifft insbesondere Betriebe, die häufig sicherheitsempfindliche Tätigkeiten für den Bund ausüben und im Besitz einer Betriebssicherheitserklärung nach Art. 68 sind. Es kann auch für die Kantone oder Organisationen nach Art. 2 Abs. 2 Bst. e der Fall sein.

Art. 37

Die Durchführung der PSP erfordert grundsätzlich die Einwilligung der betroffenen Person (Abs. 1). Einzig im Bereich der Armee oder des Zivilschutzes dürfen nach Abs. 2 PSP ohne Zustimmung der betroffenen Person durchgeführt werden. Diese Ausnahme ist notwendig, weil andernfalls Angehörige der Armee oder des Zivilschutzes sich ihrer Dienstpflicht entziehen könnten, indem sie die Durchführung der Prüfung durch Verweigerung der Einwilligung verhindern würden.

Art. 38

Das geltende Recht (Art. 19 Abs. 3 BWIS) verlangt, dass die PSP durchgeführt wird, bevor das Amt oder die Funktion übertragen oder der Auftrag erteilt wird. Eine Durchsetzung der (an sich zweckmässigen) geltenden Regelung kann jedoch in der Praxis ohne eine wesentliche Aufstockung der personellen Ressourcen der Fachstellen nicht umgesetzt werden. Deshalb wird in Abs. 1 die Regel für Angestellte der verpflichteten

Behörden und Organisationen abgeschwächt: Es wird nur noch verlangt, dass für diese Personengruppe die PSP eingeleitet wird, bevor die Funktion übertragen wird. Den Arbeitgebern steht es selbstverständlich nach wie vor offen, auf die Erklärung der Fachstelle PSP zu warten, bevor sie die betroffene Person anstellen. In der Praxis werden sie wohl in der Regel im Arbeitsvertrag eine Klausel einfügen, wonach die Ausstellung einer Sicherheitserklärung mit Vorbehalt (Art. 43 Abs. 1 Bst. b), einer Risikoerklärung (Art. 43 Abs. 1 Bst. c) oder einer Feststellungserklärung (Art. 43 Abs. 1 Bst. d) einen Grund für eine sofortige Auflösung des Arbeitsverhältnisses darstellen kann. Zur vorläufigen Risikominderung können die Arbeitgeber einen Auszug aus dem Strafregister oder aus dem Betreibungsregister (Art. 20a BPG) verlangen.

Abs. 2 entspricht geltendem Recht (Art. 19 Abs. 3 BWIS) und ist eine Folge der Untersuchung der Geschäftsprüfungskommission des Nationalrates in Bezug auf die seinerzeitige Ernennung von Korpskommandant R. Nef zum Chef der Armee. Die aufgeführte Regelung wurde mit Änderung des BWIS vom 23.12.2011 beschlossen und ist am 1. Juli 2012 in Kraft getreten.

Abs. 3 regelt den Zeitpunkt der PSP für Dritte, die für eine verpflichtete Behörde oder Organisation einen sicherheitsempfindlichen Auftrag ausführen sollen. In diesem Fall soll die heutige Regelung weiterhin gelten: die PSP muss abgeschlossen sein, bevor die Person mit der Ausübung der sicherheitsempfindlichen Tätigkeit betraut werden darf. Der Grund für die unterschiedliche rechtliche Behandlung zwischen den internen Angestellten und den Dritten liegt beim besonderen Verhältnis der Bundesangestellten zum Bund. Von Angehörigen des Bundes kann grundsätzlich von einer erhöhten Loyalität gegenüber den Interessen des Bundes ausgegangen werden. Zudem arbeiten Angestellte des Bundes meistens direkt beim Arbeitgeber, was eine einfachere Kontrolle ermöglicht.

Gemäss Abs. 4 richtet sich der Zeitpunkt der PSP bei Personen, die aufgrund eines internationalen Abkommens geprüft werden müssen, nach den Vorschriften dieses Abkommens. Auch wenn es nicht ausdrücklich im Abkommen geregelt ist, wird in diesen Fällen immer verlangt, dass eine Sicherheitserklärung ausgestellt wird, bevor eine sicherheitsempfindliche Tätigkeit ausgeübt wird.

Art. 39

Diese Bestimmung regelt die Datenerhebung für die beiden Prüfstufen. Die Datenerhebung orientiert sich weitgehend an der heutigen Gesetzgebung und Praxis. Aufgrund der Reduktion von drei auf nur noch zwei Prüfstufen wurde die Datenerhebung innerhalb der Prüfstufen so reorganisiert, dass die Grundprüfung insbesondere durch die Möglichkeit einer Abfrage aus den Registern der Betreibungs- und Konkursbehörden verstärkt wird.

Bei der Datenerhebung handelt sich für beide Prüfstufen um eine "Kann"-Vorschrift. Die Fachstellen müssen also nicht unbedingt auf alle verfügbaren Mittel zugreifen, um das Risiko zu beurteilen. Dies ist insbesondere bei der erweiterten Prüfung wichtig, weil die Reduktion von drei auf zwei Stufen nicht dazu führen soll, dass die Kosten der PSP massiv erhöht werden. Der Bundesrat, der die Ausführungsbestimmungen zu den PSP erlassen wird, wird darin auch festlegen können, wann welche Daten erhoben werden *müssen*.

Abs. 1: Für die Grundprüfung können folgende Quellen konsultiert werden:

- Bst. a-d: Das Strafregister sowie die Datensammlungen des Nachrichtendienstes sowie der Polizei- und Sicherheitsbehörden des Bundes und der Kantone können Hinweise auf die Vertrauenswürdigkeit und die allfällige Vorbelastung einer Person enthalten. Den Fachstellen PSP wird im BPI das Recht auf online-Zugang zum nationalen Polizeiindex eingeräumt (s. Ziff. 2.6). Die Daten der angeschlossenen kantonalen Polizeiorgane erschliessen sich ihr nun auf einfache und effiziente Art und Weise. Selbstverständlich sind allfällige Ergebnisse im Hinblick auf die vorgesehene Tätigkeit der geprüften Person zu gewichten und in den entsprechenden Zusammenhang zu stellen.
- Bst. e: Die Informationen aus den Registern der Betreibungs- und Konkursbehörden werden benötigt, um die finanzielle Situation der zu prüfenden Personen im Hinblick auf ein allfälliges Sicherheitsrisiko wie z.B. Bestechlichkeit beurteilen zu können.
- Bst. f sieht neu vor, dass auch die Unterlagen und Ergebnisse früherer Sicherheitsprüfungen beigezogen werden dürfen.
- Bst. g: Hier soll explizit festgehalten werden, dass die Fachstellen PSP auch auf Daten aus öffentlich zugänglichen Quellen (z.B. aus dem Internet, mit Suchmaschinen wie Google) zurückgreifen können. Entsprechender Bedarf ergibt sich einerseits aus der vorgesehenen Funktion und allfälligen einzelfallbezogenen Hinweisen. Informationen aus Sozialen Netzwerken, die nicht an die Allgemeinheit gerichtet, sondern nur für geschlossene Personenkreise bestimmt sind, dürfen jedoch nicht erhoben werden.

Abs. 2: Bei der erweiterten PSP können zusätzlich zu den Quellen nach Abs. 1 folgende Quellen konsultiert werden:

- Bst. a: Daten aus den eidgenössischen und kantonalen Steuerregistern können zusätzliche Erkenntnisse über die wirtschaftliche Situation der geprüften Personen liefern, etwa bei offensichtlichen Diskrepanzen zwischen Lebenshaltung und Steuerleistung.
- Bst. b: Die Daten aus den Registern der Einwohnerkontrolle werden nicht immer erhoben, weil sie oft nur einen begrenzten Mehrwert haben. Sie können aber situativ für die Beurteilung der persönlichen Situation der Betroffenen wichtige Hinweise liefern.
- Bst. c: In der erweiterten Prüfung wird die finanzielle Situation der zu prüfenden Person detailliert geprüft. Deshalb können Daten bei Finanzinstituten und Banken, mit welchen die zu prüfende Person Geschäftsbeziehungen unterhält, systematisch erhoben werden.
- Bst. d: Die persönliche Befragung dient dazu, Sachverhalte anzusprechen, die aus den Registerabfragen nicht oder nur unklar hervorgehen.

Abs. 3 regelt die Datenerhebung im Ausland. Die Daten, die nach den Absätzen 1 und 2 in der Schweiz erhoben werden dürfen, dürfen bei Bedarf ebenfalls im Ausland erhoben werden.

Abs. 4 verlangt, dass die Fachstellen PSP für die Beurteilung des Sicherheitsrisikos auf genügend massgebende Daten über einen hinreichenden Zeitraum zurückgreifen können müssen. Sind diese Anforderungen nicht erfüllt, kann nicht beurteilt werden, ob ein Sicherheitsrisiko vorliegt. Gegebenenfalls wird die betroffene Person nach Abs. 5 ergänzend befragt. Dies kann z.B. dann der Fall sein, wenn sich die zu prüfende Person vor der Prüfung längere Zeit in einem Land aufgehalten hat, in dem keine oder keine zuverlässige Datenerhebung möglich ist. Der Ausdruck "*hinreichenden Zeitraum*" ist bewusst offen formuliert worden. Die heutige Regelung von Art. 19 Abs. 3 PSPV, wonach die Fachstellen PSP mindestens auf Daten von fünf Jahren bis zur Einleitung der Grundprüfung und zehn Jahren bis zur Einleitung der erweiterten Prüfung zurückgreifen können müssen, wurde teilweise als unverhältnismässig und zu absolut kritisiert. Zwei Lösungsansätze sind deshalb denkbar: Entweder präzisiert der Bundesrat im Rahmen seiner Ausführungsbestimmungen zu den PSP den Ausdruck "*genügend Daten über einen hinreichenden Zeitraum*" oder die Auslegung dieses Ausdrucks bleibt im Ermessen der Fachstellen PSP.

Abs. 5 sieht vor, dass die Fachstellen PSP die zu prüfende Person unabhängig von der Prüfstufe persönlich befragen können, wenn sicherheitsrelevante Umstände im Rahmen der Datenerhebung entdeckt werden. Eine solche Befragung kann auch dann stattfinden, wenn die Fachstelle PSP im Sinne von Abs. 4 nicht genügend Daten über einen hinreichenden Zeitraum erheben konnte. Diese persönliche Befragung ist nicht zu vermischen mit der Befragung nach Abs. 2 Bst. d. Letztere kann ohne Anhaltspunkte für ein Sicherheitsrisiko durchgeführt werden und ist im Befragungsumfang nicht eingeschränkt. Zur Abklärung besonderer sicherheitsrelevanter Umstände oder zum Erhalt ergänzender Daten über einen längeren Zeitraum kann die Fachstelle PSP auch Drittpersonen befragen. Solche Befragungen dürfen nur mit dem Einverständnis der zu prüfenden Person und der betroffenen Drittpersonen durchgeführt werden.

Abs. 6: Es kommt vor, dass die für die Beurteilung des Risikos erforderlichen Daten nicht nur die geprüften Personen betreffen, sondern auch Drittpersonen. Dies kann beispielsweise bei Bankkontenauszügen einer verheirateten Person der Fall sein. Abs. 6 sieht daher vor, dass diese Personendaten ebenfalls bearbeitet werden dürfen, sofern sie untrennbar mit den Daten über die zu prüfende Person verbunden und für die Beurteilung des Risikos unerlässlich sind. Der Aufwand, der mit dem jeweiligen Einholen der Einwilligung der Drittperson zur Datenbearbeitung verbunden ist, wäre für die Fachstellen PSP unverhältnismässig gross. Aus Transparenzgründen sollen also die Fachstellen PSP diese Drittpersonen über die Datenbearbeitung informieren. Ist die Information nicht oder nur mit unverhältnismässigem Aufwand möglich, ist Art. 18a Abs. 4 Bst. b DSG anwendbar.

Art. 40

Die Mitwirkung von Behörden am Verfahren soll weiterhin unentgeltlich stattfinden (Abs. 1). Dritte, z.B. Banken oder Kreditinstitute, die zur Mitwirkung beigezogen werden, sollen entschädigt werden, wenn der dadurch verursachte Aufwand erheblich ist. Erheblich wird ein solcher Aufwand insbesondere dann, wenn er über die Erstellung von Kontoauszügen u. dgl. hinausgeht und besonders intensive Recherchen durch die ersuchten Dritte erfordert. Der Bundesrat wird die Voraussetzungen und die Höhe solcher Entschädigungen in den Ausführungsbestimmungen regeln.

Art. 41

Abs. 1: Ein bereits eingeleitetes Prüfverfahren wird eingestellt, wenn die zu prüfende Person im Verlaufe des Verfahrens ihre Zustimmung zurückzieht oder die Mitwirkung verweigert oder wenn sie aus einem anderen Grund für die anvisierte Funktion oder für den in Frage stehenden Auftrag nicht mehr in Frage kommt (z.B. Insolvenz der Firma, für welche die zu prüfende Person hätte tätig werden sollen).

Abs. 2 sieht vor, dass sowohl die zu prüfende Person als auch die einleitende Stelle über die Einstellung des Verfahrens informiert werden. Die betroffene Person gilt in der Folge als nicht sicherheitsgeprüft und darf die in Frage stehende sicherheitsempfindliche Tätigkeit nicht ausüben bzw. die entsprechende Funktion nicht übernehmen.

Abs. 3 legt fest, dass nach einer Einstellung des Prüfverfahrens die bei der Fachstelle PSP bereits erhobenen Daten und Akten zu vernichten sind. Vernichtet werden die erhobenen Daten, nicht jedoch die Einstellungserklärung und das Vernichtungsprotokoll. Weder die Einstellungserklärung noch das Vernichtungsprotokoll dürfen aber Daten enthalten, die für die betroffene Person nachteilig sein könnten. Die Ausführungsbestimmungen des Bundesrats werden die Aufbewahrungsdauer der Einstellungserklärung und des Vernichtungsprotokolls regeln.

Art. 42

In der Vergangenheit wurde verschiedentlich bemängelt, dass die geltende Regelung im BWIS nicht ausdrücklich erwähnt, was als Sicherheitsrisiko anzusehen ist. Deshalb soll nun eine entsprechende Norm aufgenommen werden, welche die Rechtsprechung des Bundesverwaltungsgerichts und des Bundesgerichts sinngemäss wiedergibt. Es versteht sich, dass es keine reinen quantitativen Beurteilungsmethoden gibt, wenn es darum geht, das Risiko in Bezug auf menschliche Handlungen oder Unterlassungen einzuschätzen. Deshalb wird eine qualitative Methode angewendet, bei welcher das Vorhandensein und das Zusammenwirken von Risikofaktoren bewertet werden.

Abs. 1: Das Risiko ist in der Lehre das Produkt der Eintrittswahrscheinlichkeit eines Ereignisses und der Auswirkungen dieses Ereignisses. Der für die Unterstellung unter die PSP massgebende Ausdruck "*sicherheitsempfindliche Tätigkeit*" enthält in seiner Definition die Auswirkungen, deren Eintreten vermieden werden soll. Es handelt sich dabei um eine "*erhebliche bzw. schwerwiegende Beeinträchtigung der Interessen nach Art. 1 Abs. 2*". Wenn die zu prüfende Person die Aufgaben, die ihr zugewiesen werden sollen, vorschriftskonform und sachgemäss erfüllt, so kann der Schaden ihretwegen nicht eintreten. Das zu vermeidende Ereignis ist also *e contrario* die vorschriftswidrige oder unsachgemässe Ausübung der sicherheitsempfindlichen Tätigkeit durch die betroffene Person. Ein Sicherheitsrisiko muss somit im Sinne des vorliegenden Gesetzes angenommen werden, wenn die Wahrscheinlichkeit hoch ist, dass die geprüfte Person die sicherheitsempfindliche Tätigkeit vorschriftswidrig oder unsachgemäss ausüben wird und dadurch die Interessen nach Art. 1 Abs. 2 mindestens erheblich beeinträchtigen wird.

Abs. 2 macht klar, dass die Fachstellen PSP sich primär auf die Eintrittswahrscheinlichkeit des Ereignisses fokussieren. Bei der Bewertung einer solchen Wahrscheinlichkeit wird es sich zwangsläufig immer um eine Prognose handeln, die mit Unsicherheiten behaftet ist. Grundlage für diese Prognose bildet die Gesamtheit aller Umstände, wie beispielsweise die Persönlichkeit der betroffenen Person, ihr Vorleben und ihre Lebensverhältnisse, soweit diese Rückschlüsse auf ihr künftiges Verhalten zulassen. In Abs. 2 werden deshalb die Risikofaktoren konkretisiert, die zur Annahme einer hohen Wahrscheinlichkeit für eine Beeinträchtigung führen, indem er persönliche Eigenschaften umschreibt, die besonders risikoträchtig sind. Die Aufzählung orientiert sich inhaltlich an der heutigen Praxis der Fachstellen PSP sowie an der Rechtsprechung des Bundesverwaltungsgerichts und des Bundesgerichts.

Die Umschreibungen zielen zwar im Grundsatz auf möglichst objektiv feststellbare Eigenschaften, doch können diese häufig nur aus Indizien oder aus dem Kontext abgeleitet werden und überschneiden sich partiell. Mit Integrität und Vertrauenswürdigkeit werden vorweg der Charakter sowie die Gewohnheiten und Beziehungen einer Person zu ihrem Umfeld anvisiert. Diese Eigenschaften sind bei der Ausübung einer sicherheitsempfindlichen Tätigkeit die Eignungserfordernisse schlechthin. Liegen diese Eigenschaften vor, kann mit hoher Wahrscheinlichkeit darauf vertraut werden, dass die mit einer solchen Tätigkeit betraute Person loyal zu ihrer Aufgabe steht und die Sicherheitsinteressen des Arbeitgebers oder der Institution wahrt. Welche der Indizien und Zusammenhänge die fehlende Vertrauenswürdigkeit einer Person, ihre mutmassliche Erpressbarkeit oder ihr beeinträchtigtes Beurteilungs- und Entscheidungsvermögen belegen, kann auf der Ebene des Gesetzes nicht spezifiziert, sondern muss letztlich in jeder einzelnen Beurteilung ermittelt und dargelegt werden.

Abs. 3 stellt klar, dass ein Sicherheitsrisiko auch ohne ein Verschulden der betroffenen Person vorliegen kann. Bei der PSP handelt es sich um eine vorbeugende Massnahme zum Schutz überwiegender öffentlicher Interessen vor vorsätzlichen und fahrlässigen Innentaten, die auf eine objektive Gefährdung und nicht auf ein schuldhaftes Verhalten abstellt. Dies im Gegensatz etwa zum Strafrecht, bei dem die Schuld immer Voraussetzung für eine Strafe ist. Anders als im Strafrecht (in dubio pro reo) rangiert somit im Zweifel die Sicherheit des Staates bzw. das Landesinteresse vor den Interessen der betroffenen Person. Es wird ebenfalls festgehalten, dass die Annahme eines Sicherheitsrisikos durch Fakten und tatsächliche Umstände um die zu be-

urteilende Person begründet werden muss. Reine Konjekturen, insbesondere wenn sie die politische Gesinnung der zu prüfenden Person betreffen, sind nicht zulässig.

Abs. 4 soll schliesslich die Unabhängigkeit der Fachstellen PSP für die Beurteilung des Sicherheitsrisikos sicherstellen. Die PSP darf nicht für politische Machenschaften missbraucht werden.

Art. 43

Abs. 1 regelt die verschiedenen Erklärungen der Fachstellen PSP, in welchen das Ergebnis der Beurteilung festgehalten wird:

- Bst. a: Wenn die Fachstelle PSP zum Schluss kommt, dass die geprüfte Person im Hinblick auf die sicherheitsempfindliche Tätigkeit unbedenklich ist, stellt sie eine Sicherheitserklärung aus.
- Bst. b: Stellt die Fachstelle PSP fest, dass von einer geprüften Person bei der Ausübung der sicherheitsempfindlichen Tätigkeit gewisse Sicherheitsrisiken ausgehen, dass diese aber mit bestimmten Auflagen reduziert werden können, stellt sie eine Sicherheitserklärung mit Vorbehalt aus und empfiehlt der übertragenden Stelle entsprechende Auflagen.
- Bst. c: Wenn sie zum Schluss kommt, dass die Ausübung der sicherheitsempfindlichen Tätigkeit durch die geprüfte Person ein Risiko darstellt, stellt die Fachstelle PSP eine Risikoerklärung aus.
- Bst. d: Kann aufgrund der ungenügenden Datenerhebung im Sinne von Art. 39 Abs. 4 eine Person nicht nach den "*règles de l'art*" beurteilt werden, so erlässt die Fachstelle PSP eine Feststellungserklärung.

Abs. 3: Obwohl der formelle Anspruch auf rechtliches Gehör bei einem Realakt (s. Art. 51 Abs. 3) an sich nicht ohne weiteres zum Tragen kommt, soll Abs. 3 sicherstellen, dass die betroffene Person ihre Interessen bereits in diesem Verfahrensstadium angemessen wahren kann. Die Bestimmung sieht daher vor, dass der bzw. dem Geprüften vor der Ausstellung der Erklärungen nach Bst. b-d Gelegenheit zur Stellungnahme zu geben ist. Faktisch heisst dies, dass beim Vorliegen eines Erklärungsentwurfs nach Bst. b-d die betroffene Person in geeigneter Form über den Inhalt zu orientieren und ihr eine angemessene Frist zur Stellungnahme einzuräumen ist.

Art. 44

Gemäss Abs. 1 muss die Erklärung der geprüften Person sowie der Stelle, die für die Übertragung der sicherheitsempfindlichen Tätigkeit zuständig ist, schriftlich mitgeteilt werden. Auch wenn die Erklärung keine Verfügung im Sinne von Art. 5 VwVG darstellt (s. Art. 51 Abs. 3), muss die betroffene Person die Möglichkeit haben, die Ergebnisse der Beurteilung zur Kenntnis zu nehmen und allenfalls den Erlass einer Verfügung zu beantragen. Dieser Absatz entspricht grundsätzlich geltendem Recht (Art. 21 Abs. 2-4 BWIS).

Abs. 2 legt fest, dass die Mitteilung der Beurteilung bei Personen, die vom Bundesrat zu wählen sind, an das antragstellende Departement zu gehen hat.

Abs. 3 regelt den Fall, in welchem eine PSP eingeleitet wird, die betroffene Person aber im Zusammenhang mit einer anderen Tätigkeit nach Bst. a-c ebenfalls einer Prüfung untersteht (z.B. nach Art. 20*b* BPG). In diesem Fall soll die Fachstelle PSP die jeweilige übertragende Stelle über das Ergebnis der Hauptprüfung informieren können. Die Regelung der Prüfung der Vertrauenswürdigkeit nach Art. 20*b* BPG sowie nach Art. 14 MG verlangt, dass beide Verfahren vereinigt werden, wenn eine Person aufgrund des vorliegenden Gesetzes ebenfalls einer PSP unterzogen werden soll.

Abs. 4 ermöglicht es den Fachstellen PSP, bei potenziell gewalttätigen Angehörigen der Armee die nach Artikel 113 MG für das Überlassen oder den Entzug der persönlichen Armeewaffe zuständige Stelle über das Ergebnis ihrer Beurteilung zu informieren. Stellt die Fachstelle PSP im Rahmen einer Prüfung fest, dass die betroffene Person, die militärdienstpflichtig ist, ein erhöhtes Gewaltpotenzial aufweist, soll sie die militärischen Instanzen informieren, damit diese über den Entzug der Armeewaffe entscheiden können.

Art. 45

Art. 45 sieht vor, dass bei einem begründeten Sicherheitsvorbehalt und bei Dringlichkeit die Fachstellen PSP im Sinne der Gefahrenprävention die zuständigen Stellen nach Art. 44 bereits über ihre Erkenntnisse informieren dürfen, bevor das Verfahren abgeschlossen ist. Die zuständige Stelle kann daraufhin vorsorgliche Sicherheitsmassnahmen treffen. Dies entspricht dem geltenden Art. 20 PSPV.

Art. 46

Abs. 1 legt fest, dass die für die Übertragung der sicherheitsempfindlichen Tätigkeit bzw. Funktion zuständige Stelle (übertragende Stelle) nicht an die Erklärung der Fachstelle PSP gebunden ist. Dies entspricht dem heutigen Art. 21 Abs. 4 BWIS. Es ist nicht Aufgabe der Fachstellen PSP, die Verantwortung der Linie für Personalentscheide zu treffen oder einzuschränken, sondern lediglich, die entscheidende Behörde über das

Risiko zu informieren, dass mit der Übertragung einer sicherheitsempfindlichen Tätigkeit an eine bestimmte Personen verbunden ist.

Abs. 2: Vor ihrem Entscheid muss aber die übertragende Stelle von der Erklärung der Fachstelle PSP Kenntnis nehmen, denn nur dann kann sie ihren Entscheid unter Berücksichtigung der allfälligen Risiken treffen.

Abs. 3 ermächtigt die übertragende Stelle, insbesondere gestützt auf die Empfehlungen der Fachstelle PSP, für die Ausübung der sicherheitsempfindlichen Tätigkeit Auflagen zu machen. Diese Auflagen stellen risikomindernde Massnahmen dar, welche meistens personalrechtlicher Natur sind. Die übertragende Stelle kann z.B. verlangen, dass die betroffene Person regelmässig ihre finanzielle Lage offenlegt oder sich Drogentests unterzieht usw. Wichtig ist in diesem Zusammenhang die Präzisierung, dass sich diese Auflagen ausschliesslich auf die Ausübung der sicherheitsempfindlichen Tätigkeit richten müssen und nicht auf die Ausübung anderer Aufgaben beziehen dürfen. Beschliesst z.B. die übertragende Stelle, dass die betroffene Person die sicherheitsempfindliche Tätigkeit nicht ausüben darf, aber für andere, sicherheitsmässig nicht relevante Aufgaben eingesetzt wird, dann dürfen keine Auflagen mehr festgelegt werden. Meistens werden die geeignetsten Auflagen von der Fachstelle PSP empfohlen. Die übertragende Stelle ist aber an diese Auflagen nicht gebunden und kann selber Auflagen bestimmen. Weicht die zuständige Stelle jedoch von den empfohlenen Auflagen ab, dann muss sie die Fachstelle PSP schriftlich informieren (s. Art. 47 Bst. b).

Art. 47

Dieser Artikel statuiert eine Mitteilungspflicht der übertragenden Stelle. Wenn sie einen Entscheid trifft, der von der Beurteilung der Fachstelle PSP abweicht, muss sie dies der Fachstelle PSP mitteilen. Die Mitteilung kann durch einen Vermerk im Informationssystem zur PSP nach Art. 52-54 stattfinden. Es geht darum, dass die Fachstelle PSP den Überblick über die Praxis der übertragenden Stellen behält und die notwendigen Lehren zieht.

Art. 48

Wenn für die zu prüfende Person bereits eine noch gültige und gleichwertige Erklärung ausgestellt wurde, soll aus Gründen der Verfahrensökonomie nach Möglichkeit kein neues Prüfverfahren durchgeführt werden. Art. 48 sieht deshalb vor, dass in diesem Fall darauf verzichtet werden kann. In der Praxis stellt diese Regelung in der Regel kein Problem dar, wenn eine Sicherheitserklärung für die gleiche oder eine höhere Prüfstufe ausgestellt wurde. Probleme können sich aber beispielsweise dann ergeben, wenn einer bestimmten Person für eine höhere Prüfstufe eine Sicherheitserklärung mit Vorbehalt oder eine Risikoerklärung ausgestellt wurde. Es ist nämlich durchaus möglich, dass für die Bearbeitung von als GEHEIM klassifizierten Informationen ein Sicherheitsrisiko besteht, dass aber dieses Risiko in Bezug auf die Bearbeitung von als VERTRAULICH klassifizierten Informationen tragbar ist. Der Bundesrat wird diese "Kann"-Vorschrift auf Verordnungsebene konkretisieren müssen.

Art. 49

Ausländische Sicherheitsbehörden gewähren ausschliesslich sicherheitsgeprüften Personen Zugang zu klassifizierten Informationen, klassifiziertem Material oder Schutz- und Sicherheitszonen. Die zuständige schweizerische Behörde darf die in derartigen Fällen erforderliche Personensicherheitsbescheinigung ausschliesslich Personen, die eine Sicherheitserklärung erhalten haben, ausstellen.

Art. 50

Abs. 1 regelt die ordentliche Wiederholung der PSP. Im Gesetz wird darauf verzichtet, feste Wiederholungsintervalle vorzuschreiben. Es setzt lediglich Leitplanken zur Wiederholung der Prüfung. Grund dafür ist, dass die Wiederholung inskünftig vermehrt dem tatsächlichen Sicherheitsbedarf entsprechend erfolgen soll. Der Bundesrat sollte in seinen Ausführungsbestimmungen die Wiederholungen detailliert regeln. Er kann aber diese Kompetenz selbstverständlich auch den verpflichteten Behörden und Organisationen überlassen, indem er nichts vorschreibt.

Abs. 2 verleiht sowohl der einleitenden Stelle als auch der übertragenden Stelle die Möglichkeit, eine Wiederholung der PSP ausserhalb der gesetzlichen Wiederholungszyklen zu veranlassen. Grund für eine solche vorzeitige Wiederholung ist die Entstehung neuer Risiken bei der betroffenen Person, z.B. die Eröffnung eines Strafverfahrens gegen sie, das einen Bezug zur sicherheitsempfindlichen Tätigkeit aufweist. Diese Regelung entspricht dem geltendem Verordnungsrecht (s. Art. 18 Abs. 2 PSPV).

Im Rahmen seiner Kompetenz zum Erlass ergänzenden Rechts zum Verfahren der PSP (s. Art. 55), wird der Bundesrat auch entscheiden müssen, ob er weitere vorzeitige Wiederholungen der Prüfung einführen will. Eine *Nachprüfung* könnte z.B. bei Sicherheitserklärungen mit Vorbehalt nützlich sein, um die Wirksamkeit der angeordneten Auflagen zu prüfen.

Art. 51

Abs. 1 und 2 regeln die Einsicht in die Prüfungsunterlagen sowie die Berichtigung falscher Daten durch die geprüfte Person. Die Regelung entspricht trotz angepasster Formulierung geltendem Recht (s. Art. 21 Abs. 2 BWIS).

Abs. 3: Nach geltendem Recht werden die Erklärungen der Fachstellen PSP in Form einer Verfügung erlassen (s. Art. 20 Abs. 3 BWIS sowie Art. 22 PSPV). Die Qualifizierung der Erklärungen als Verfügung ist rechtlich aber falsch, denn sie haben nur empfehlenden Charakter (s. Art. 21 Abs. 4 BWIS sowie Art. 46 Abs. 1 ISG). Die Rechte der geprüften Personen werden nur dann berührt, wenn die übertragenden Stellen anschliessend die Funktion oder den Auftrag nicht übertragen. Die Erklärungen entsprechen rechtlich eher dem Resultat eines *Assessments*, das die Behörden und Organisationen vor der Anstellung von Schlüsselpersonen häufig durchführen lassen. Auch die Beurteilung der Assessoren wird nicht in Form einer anfechtbaren Verfügung mitgeteilt, weil der Arbeitgeber frei entscheiden kann. Die Erklärungen der Fachstellen PSP stellen Realakte im Sinne von Art. 25a VwVG dar. Für die vorliegende Situation bedeutet dies, dass die betroffene Person innert 30 Tagen nach Erhalt der Erklärung von der Fachstelle PSP eine anfechtbare Verfügung verlangen kann. Der weitere Verlauf des Verfahrens richtet sich nach dem VwVG. Die vorgesehene Regelung wird den Aufwand für die PSP von Stellungspflichtigen im Rahmen der militärischen Rekrutierung verkleinern. Die Fachstellen PSP werden die Ergebnisse der Beurteilung den Stellungspflichtigen einfach mitteilen können und nur bei Bestreitung derselben eine vollständige Verfügung erlassen.

Art. 52

Art. 52 entspricht grundsätzlich geltendem Recht (s. Art. 144-149 MIG).

Abs. 1 hält fest, dass die Fachstellen PSP zur Durchführung und Bewirtschaftung der PSP ein Informationssystem einsetzen müssen.

Abs. 2: Jede Fachstelle PSP ist für die rechtmässige Bearbeitung der Daten, die sie bearbeitet, verantwortlich.

Abs. 3: Bei diesen Daten können auch besonders schützenswerte Personendaten und Persönlichkeitsprofile vorhanden sein (Art. 3 Bst. c und d DSG).

Abs. 4 führt die Daten auf, die im Informationssystem bearbeitet werden.

Abs. 5: Daten, die ausserhalb des Informationssystems bearbeitet werden, müssen darin vermerkt werden. Es handelt sich dabei insbesondere um Papierdokumente und Tonaufnahmen im Rahmen der Befragungen.

Art. 53

Art. 53 entspricht grundsätzlich geltendem Recht (s. Art. 144-149 MIG).

Abs. 1: Abrufverfahren

- Bst. a: Die Fachstellen PSP haben Zugriff auf sämtliche Daten, für die sie zuständig sind.
- Bst. b: Die einleitenden Stellen erhalten nur Zugriff auf diejenigen Daten, die sie anlässlich der Einleitung selbst erfasst haben, sowie auf das Ergebnis der PSP.
- Bst. c legt fest, auf welche Daten die übertragenden Stellen Zugriff haben.
- Bst. d regelt, auf welche Daten die Informationssicherheitsbeauftragten zur Erfüllung ihrer Kontrollaufgaben Zugriff haben.
- Bst. e: Organisationen des Bundes und der Kantone, bei denen Daten erhoben werden, haben nur Zugriff auf Daten zur Identität der zu prüfenden oder geprüften Person. Diese Daten benötigen sie, um überhaupt zu wissen, über welche Person sie Nachforschungen anstellen und Daten liefern sollen.

Abs. 2: Schnittstellen

- Bst. a regelt, auf welche Daten die Fachstelle für Betriebssicherheit Zugriff hat.
- Bst. b: Damit der Armeestab (wie bis anhin) Anträge für Besuche ins Ausland mit Zugang zu klassifizierten Informationen effizient bearbeiten kann, sollen Daten nach Art. 52 Abs. 4 Bst. a und d über eine Schnittstelle ins Informationssystem Besuchsanträge transferiert werden.
- Bst. c Ziff. 1-3 regelt, auf welche Daten der Führungsstab der Armee zur Kontrolle des Zutritts zu Sicherheitszonen, zur Erfüllung seiner gesetzlichen Aufgaben in Bezug auf das Personalinformationssystem der Armee und zur Durchführung der Rekrutierung der Stellungspflichtigen sowie des für die Friedensförderung vorgesehenen Personals Zugriff hat.

Abs. 3: Weitere Organisationen des Bundes (insbesondere IKT-Leistungserbringer) brauchen die Ergebnisse der PSP, um den Zugang zu Sicherheitszonen zu kontrollieren.

Abs. 4: Die Fachstellen PSP geben den verpflichteten Behörden und Organisationen Listen und Statistiken nur bekannt, wenn sie diese zur Erfüllung ihrer Kontrollaufgaben nach diesem Gesetz benötigen. Derartige Listen werden also nur bei entsprechendem Bedarf geliefert. Die Bekanntgabe solcher Listen erfolgt ausserhalb des Informationssystems nach Art. 52.

Art. 54

Art. 54 entspricht grundsätzlich geltendem Recht (s. Art. 144-149 MIG sowie PSPV).

Abs. 1 schafft die rechtliche Grundlage für die Tonaufnahme der Befragungen.

Abs. 2: Die Aufbewahrungsdauer soll zehn Jahre nicht überschreiten. Falls eine Person bereits mehreren Prüfungen unterzogen wurde, so sind diejenigen Daten, welche Prüfungen betreffen, die länger als zehn Jahre zurückliegen, zu löschen.

Abs. 3 regelt die Vernichtung von Daten einer bereits geprüften Person, welche die Stelle nicht antritt (s. auch Art. 41).

Abs. 5: Daten, die ausserhalb des Informationssystems bearbeitet werden (s. Art. 52 Abs. 5), müssen gemäss Abs. 2 und 3 aufbewahrt und vernichtet werden. Bei der Vernichtung dieser Daten sind gleichzeitig die Vermerke im System zu löschen.

Abs. 6: Sind Akten nach den Archivierungsvorschriften zu archivieren, dürfen sie nicht vernichtet werden.

Art. 55

In Art. 55 werden diejenigen Bereiche aufgeführt, in denen der Bundesrat ergänzendes bzw. gesetzesvertretendes Recht erlassen soll. Es handelt sich dabei also nicht bloss um Ausführungsbestimmungen, für die der Bundesrat auf Grund von Art. 182 BV ohne weiteres zuständig ist.

- Bst. a-b: Hinsichtlich der Organisation ist zu bemerken, dass es heute zwei Fachstellen PSP gibt. Die eine ist bei der Bundeskanzlei angesiedelt und prüft zu Handen des Bundesrats das Top-Kader sowie die Angestellten der anderen Fachstelle PSP. Sie führt deshalb zurzeit ausschliesslich erweiterte PSP mit Befragung durch. Die andere Fachstelle PSP ist im VBS im Armeestab, bei der Informations- und Objektsicherheit angesiedelt und führt die überwiegende Mehrheit der Prüfungen durch. Bst. b belässt die Möglichkeit mehrerer Fachstellen, überlässt es aber dem Bundesrat, ob er an dieser Organisation festhalten will.
- Bst. c-d: der Bundesrat muss in Anwendung von Art. 16 Abs. 2 DSG ergänzendes Recht zum Datenschutz im Rahmen der PSP erlassen. Betroffen sind insbesondere die Organisation der Zuständigkeiten und Verantwortungen für den Datenschutz (inkl. Datensicherheit) im Zusammenhang mit dem Informationssystem nach Art. 52 sowie die periodische unabhängige Kontrolle der Rechtmässigkeit der Datenbearbeitung.

2.1.4 Betriebssicherheitsverfahren

Art. 56

Zum Zweck des BSV, s. Ziff. 1.2.5.

Art. 57

Abs. 1: Als "*Betrieb*" im Sinne des Gesetzes wird nicht unbedingt das ganze Unternehmen erfasst. Betroffen sind vielmehr nur diejenigen Teile und Personen des Unternehmens, die tatsächlich mit dem sicherheitsempfindlichen Auftrag betraut werden.

- Bst. a führt den Hauptanwendungsfall auf: Die Absicht einer verpflichteten Behörde oder Organisation, einen sicherheitsempfindlichen Auftrag nach Art. 56 einem Unternehmen zu erteilen, das sich darum bewirbt. Das BSV stellt grundsätzlich eine nationale Angelegenheit dar. Deshalb müssen sich Betriebe mit Sitz im Ausland, die sich um einen sicherheitsempfindlichen Auftrag aus der Schweiz bewerben wollen, durch denjenigen Staat prüfen lassen, in dem sich ihr Sitz befindet. Die Zuständigkeiten und Prüfmodalitäten sind Bestandteil der entsprechenden völkerrechtlichen Vereinbarungen nach Art. 90. In derartigen Fällen wird bei den ausländischen Sicherheitsbehörden mittels eines sog. "*Facility Security Clearance Information Sheet*" der Nachweis für eine Betriebssicherheitserklärung (BSE) des Auftragnehmers bzw. - falls der betreffende Betrieb noch nicht geprüft wurde - das Einleiten des Prüfverfahrens verlangt.
- Abs. 1 Bst. b erfasst umgekehrt den Fall von Betrieben mit Sitz in der Schweiz, die sich für einen Auftrag aus dem Ausland bewerben wollen und den dortigen Behörden eine Sicherheitserklärung der Behörden

ihres Sitzstaates vorweisen müssen. Dieses Verfahren und die damit verbundene Zertifizierung stellen eine amtliche Tätigkeit dar, die nicht an die Privatwirtschaft übertragen werden kann, weil die ausländischen Behörden ausnahmslos ein amtliches "Sicherheitssiegel" des Sitzstaates des Betriebs verlangen.

Abs. 2 hält fest, dass ein BSV in jedem Fall nur mit Zustimmung des betroffenen Betriebs durchgeführt werden kann. In der Praxis stellt die erforderliche Zustimmung des Betriebs zur Durchführung des BSV allerdings nie ein Problem dar, weil die Betriebe ein finanzielles Interesse an der Auftragserteilung haben.

Abs. 3: Im Anwendungsfall von Abs. 1 Bst. b hat der Bund kein unmittelbares Selbstinteresse an der Durchführung des Verfahrens. Der Bundesrat wird die Frage der Kosten auf Verordnungsebene regeln.

Art. 58

Abs. 1: Das BSV wird nur durchgeführt, wenn bestimmte Kriterien und Voraussetzungen (z.B. Zustimmung) erfüllt werden. Erfüllt der Betrieb diese Kriterien im Laufe des BSV nicht mehr, wird das Verfahren eingestellt. Dies kann nach Bst. d z.B. auch dann der Fall sein, wenn der Betrieb im Falle seines Konkurses oder der Zerstörung der Betriebsstätte durch einen Brand den Auftrag überhaupt nicht mehr erfüllen kann.

Abs. 2 schreibt vor, dass nach der Einstellung des Verfahrens sämtliche mit diesem zusammenhängenden Daten und Akten zu vernichten sind.

Art. 59

Abs. 1 hält vorab fest, dass die BSV durch eine „*Fachstelle für Betriebssicherheit*“ (Fachstelle BS) durchgeführt werden. Innerhalb des Bundes soll sich also (wie bis anhin) eine einzige Stelle mit diesen Verfahren befassen. Die Fachstelle BS wird nur auf *Antrag* (und nicht Auftrag) einer verpflichteten Behörde oder Organisation tätig. Letztere sind aber verpflichtet, einen entsprechenden Antrag zu stellen, falls sie einen sicherheitsempfindlichen Auftrag an einen Betrieb vergeben wollen.

Abs. 2: Die verpflichteten Behörden müssen in ihrem Zuständigkeitsbereich bestimmen, wer den Antrag zur Einleitung stellt. Je nach ihren organisatorischen Bedürfnissen kann dies eine zentrale Stelle sein oder jede Stelle, die über die Kompetenz verfügt, sicherheitsempfindliche Aufträge an Unternehmen der Privatwirtschaft zu vergeben.

Abs. 3 regelt die Zuständigkeit bei einem sicherheitsempfindlichen Auftrag einer ausländischen oder internationalen Behörde. Das Verfahren wird in der Regel mittels einer Anfrage seitens der ausländischen Sicherheitsbehörde (engl. *Facility Security Clearance Information Sheet, FSCIS*) an die Sicherheitsbehörden und einer Bestätigung des interessierten Betriebs eingeleitet. Die Anfrage wird mittels eines standardisierten Ablaufs beantwortet. Die Einzelheiten dieser Verfahren sind durch Verordnung zu regeln.

Art. 60

Abs. 1: Nach Eingang des Antrags zur Durchführung des BSV prüft die Fachstelle BS zunächst, ob die Voraussetzungen zur Einleitung des Verfahrens (z.B. Vorliegen eines sicherheitsempfindlichen Auftrags) vorliegen und leitet gegebenenfalls das BSV ein.

Abs. 2: Können die Risiken für die Informationssicherheit im konkreten Fall durch andere Massnahmen hinreichend minimiert werden, kann die Fachstelle BS aus Gründen der Verwaltungsökonomie auf die Durchführung des BSV verzichten. Wenn der Auftrag z.B. unter Aufsicht der auftragserteilenden Stelle in deren Räumlichkeiten ausgeführt wird und dem Auftragnehmer (Betrieb) keine Unterlagen ausgehändigt werden, reichen beispielsweise unter Umständen entsprechende PSP aus. Verzichtet die Fachstelle BS auf die Durchführung des BSV, so empfiehlt sie auch die Sicherheitsmassnahmen, die sie für zweckmässig betrachtet. In diesem Fall verfügt die Fachstelle BS über keine Durchsetzungskompetenzen mehr.

Art. 61

Nach der Einleitung des Verfahrens nimmt die Fachstelle BS Kontakt mit der auftragserteilenden Stelle (Auftraggeberin) auf und bespricht die Details des Auftrags. Sie legt in Absprache mit der Auftraggeberin die Anforderungen an die Informationssicherheit für die Auftragserfüllung fest. Soweit bereits im Rahmen des Vergabeverfahrens die Ausübung einer sicherheitsempfindlichen Tätigkeit notwendig ist, werden auch bereits für diese Phase die Anforderungen festgehalten. Dies ist insbesondere regelmässig dann der Fall, wenn für die Erstellung einer Offerte während des Vergabeverfahrens die Kenntnisnahme von klassifizierten Informationen erforderlich ist.

Art. 62

Der Begriff "*Eignung*" ist im Sinne der Systematik des öffentlichen Beschaffungsrechts zu verstehen. Zwar stellt die Gewährleistung der Informationssicherheit kein ausdrückliches Eignungskriterium nach Art. 9 BöB dar, der Entwurf fügt es aber für die Ausführung sicherheitsempfindlicher Aufträge ein.

Abs. 1: Die Auftraggeberin hat der Fachstelle BS alle für den Zuschlag in Frage kommenden Betriebe zu melden.

Abs. 2: Die Fachstelle BS beurteilt hierauf, ob diese Betriebe zur Ausführung des sicherheitsempfindlichen Auftrags geeignet sind, oder ob durch die Erteilung des Auftrages an einen bestimmten Betrieb oder an bestimmte Betriebe ein Sicherheitsrisiko nach Art. 64 geschaffen würde. Besteht ein Sicherheitsrisiko in Bezug auf eine Anbieterin, ist diese alsdann in Bezug auf die Informationssicherheit ungeeignet.

Abs. 3: Die Fachstelle BS muss für die Beurteilung der Eignung weisungsungebunden sein. Es geht hier darum, dass diese Beurteilung frei von wirtschaftspolitischen Interessen getroffen wird (s. auch Art. 42 Abs. 4 für die PSP).

Art. 63

Art. 63 schafft die formell-gesetzliche Grundlage für die Datenerhebung zur Beurteilung der sicherheitsmässigen Eignung der Betriebe nach Art. 62 Abs. 2.

Abs. 1 listet auf, welche Daten die Fachstelle BS zur Beurteilung der Eignung erheben kann. Die Modalitäten solcher Anfragen und der entsprechenden Auskunftserteilung sind auf Verordnungsebene zu regeln.

- Nach Bst. a werden die erforderlichen Daten im Wesentlichen beim Betrieb selbst mit dessen Einverständnis erhoben (s. auch Art. 57).
- Bst. b schafft eine formell-gesetzliche Grundlage für Rückfragen der Fachstelle BS beim Nachrichtendienst des Bundes.
- Bst. c ermöglicht es der Fachstelle BS, bei Bedarf Daten über die Firma aus dem Handelsregister oder im Internet zu erheben. Solche Recherchen können wichtige Hinweise zur Vertrauenswürdigkeit der Firma liefern (s. Art. 39 Abs. 1 Bst. g für die PSP).

Abs. 2: Von dieser Möglichkeit wird sie z.B. dann Gebrauch machen, wenn sich ausländische Firmen bei den Bundesbehörden um einen sicherheitsempfindlichen Auftrag bewerben.

Art. 64

Diese Bestimmung stellt das Pendant zu Art. 42 (Beurteilung des Sicherheitsrisikos bei der PSP) dar. Die Risikobeurteilungsmechanismen sind grundsätzlich identisch.

Nach Abs. 1 besteht dann ein Sicherheitsrisiko, wenn konkrete Anhaltspunkte dafür vorliegen, dass der Betrieb mit hoher Wahrscheinlichkeit den sicherheitsempfindlichen Auftrag vorschriftswidrig oder unsachgemäss ausführen würde.

Abs. 2 listet anschliessend die drei wichtigsten Gründe für eine hohe Wahrscheinlichkeit einer vorschriftswidrigen oder unsachgemässen Ausführung des Auftrags auf.

- Bst. a: Dies kann z.B. dann der Fall sein, wenn erhobene Daten zeigen, dass der Betrieb Straftaten begangen hat, die für die Informationssicherheit relevant sind.
- Bst. b: Mit dieser Bestimmung soll der Transfer sicherheitsempfindlicher Informationen an Betriebe verhindert werden, die durch ihre Eigentumsverhältnisse, ihre Organisationsstrukturen oder ihre Geschäftsbeziehungen beispielsweise von ausländischen Nachrichtendiensten oder Organisationen mit kriminellem Hintergrund gesteuert werden.
- Bst. c: Wenn der Betrieb aus einer einzelnen Person besteht (Einzelfirma) oder wenn für die Auftragserfüllung bestimmte Personen unentbehrlich sind (z.B. weil diese Personen Fachexperten sind, die nicht ersetzt werden können, oder weil sie den Betrieb führen und der Auftrag ohne ihren Einsatz nicht erfüllt werden kann), kann die Ausstellung einer Risikoerklärung im Rahmen der PSP für diese Betriebsangehörigen zur Folge haben, dass der Betrieb als Ganzes als Sicherheitsrisiko beurteilt werden muss.

Abs. 3 hält fest, dass das erwähnte Risiko durch die tatsächlichen Umstände des betroffenen Betriebs begründet sein muss. Unerheblich ist dabei, ob den Betrieb selbst oder seine Angehörigen irgendein Verschulden trifft, z.B., wenn die Firma, welcher der Betrieb gehört, von Personen mit nachrichtendienstlichem oder kriminellem Hintergrund gesteuert wird.

Art. 65

Abs. 1: Die Fachstelle BS eröffnet dem betreffenden Betrieb ihre Beurteilung in Bezug auf die Eignung. Ist der Betrieb mit der Risikobeurteilung nicht einverstanden, kann er gegen diese Verfügung Beschwerde beim Bundesverwaltungsgericht erheben (Art. 76 Abs. 3). Die Auftraggeberin kann das Submissionsverfahren bzw. ihre Vertragsverhandlungen mit allen Betrieben, bei denen kein Sicherheitsrisiko erkennbar ist, weiterführen. Sie ist nicht zur Beschwerde berechtigt und wird deshalb über die Beurteilung nur informiert.

Abs. 2: Erkennt die Fachstelle BS in Bezug auf einen oder mehrere Betriebe Sicherheitsrisiken, darf die Auftraggeberin diesem bzw. diesen hingegen weder den Zuschlag erteilen noch den Vertrag mit einem solchen Betrieb abschliessen. Sie schliesst den bzw. die betreffenden Betriebe als sicherheitsmässig ungeeignet aus dem Vergabeverfahren aus. Die Auftraggeberin ist also an die Beurteilung der Fachstelle BS gebunden. Der Grund dafür besteht darin, dass ein Unternehmen oder Betrieb, dem eine Betriebssicherheitserklärung ausgestellt wird, ein staatliches "Sicherheitssiegel" erhält. Die Wahrung der Integrität dieses Siegels kann nur dann sichergestellt werden, wenn der Entscheid über die Eignung von Fachspezialisten getroffen wird.

Art. 66

Abs. 1: Sobald die Auftraggeberin den Zuschlag erteilt hat, informiert sie die Fachstelle BS. Diese leitet die weiteren Schritte des Verfahrens ein.

Abs. 2: Damit die erforderliche Informationssicherheit im Betrieb, der die sicherheitsempfindliche Tätigkeit ausführen soll, sichergestellt ist, müssen entsprechende organisatorische, personelle, technische und physische Massnahmen getroffen werden. In einem Sicherheitskonzept wird deshalb festgehalten, wie die von der Fachstelle BS nach der Einleitung des Verfahrens mit der Auftraggeberin bereits definierten Anforderungen an die Informationssicherheit umgesetzt werden müssen (s. Art. 61).

Abs. 3: In der Regel haben die Betriebe in verschiedensten Bereichen bereits Sicherheitsmassnahmen getroffen, die durch die Fachstelle BS nur noch überprüft und wo nötig ergänzt werden müssen. Alle erforderlichen Massnahmen, die bereits getroffenen sowie die zusätzlich nötigen, werden im Konzept nach Abs. 2 festgehalten. Die notwendigen Daten erhebt die Fachstelle BS direkt beim Betrieb.

Art. 67

Abs. 1: Bei Mitarbeitenden, die eine sicherheitsempfindliche Tätigkeit ausüben sollen, wird eine PSP durchgeführt. Diese Personen werden gestützt auf Art. 34 Abs. 1 Bst. b und gegebenenfalls Bst. c oder Art. 34 Abs. 2 überprüft. Die Prüfstufe richtet sich nach Art. 35.

Abs. 2: die Fachstelle BS entscheidet im Anschluss an die PSP verbindlich, ob die geprüfte Person mit der sicherheitsempfindlichen Tätigkeit betraut werden darf.

Art. 68

Abs. 1: Sobald der Betrieb die erforderlichen Sicherheitsmassnahmen getroffen und damit das Sicherheitskonzept nachweislich umgesetzt hat, stellt ihm die Fachstelle BS eine Betriebssicherheitserklärung (BSE) aus. Die BSE ist eine Verfügung nach Art. 5 VwVG.

Abs. 2: Wird das Sicherheitskonzept durch den Betrieb nicht umgesetzt, was in der bisherigen Praxis nur äusserst selten vorkam, werden die Anforderungen an die Informationssicherheit nicht erfüllt. Deshalb verweigert die Fachstelle BS in derartigen Fällen die BSE und verfügt die Einstellung des Verfahrens. Die Fachstelle BS muss dem Betrieb eine Nachfrist gewähren, um seinen Pflichten nachzukommen, bevor die Verweigerung der BSE verfügt werden darf.

Abs. 3: Die Erteilung bzw. Nichterteilung der BSE stellt - anders als die Sicherheitserklärung im Bereich der PSP - eine Verfügung dar, weil sie für die Beteiligten unmittelbare Rechtswirkungen entfaltet (s. Art. 69 ff.). Ist der Betrieb mit der Verfügung der Fachstelle BS nicht einverstanden, steht ihm die Beschwerde an das Bundesverwaltungsgericht offen (Art. 76 Abs. 1). Die Verfügung wird auch der Auftraggeberin mitgeteilt, weil sie den Betrieb, dem die BSE verweigert wird, nicht mit dem sicherheitsempfindlichen Auftrag betrauen darf (Art. 69). Zu diesem Zeitpunkt hat die Auftraggeberin möglichweise bereits viel Geld in das Projekt investiert. Sie ist in diesem Fall (im Gegensatz zu Art. 65 Abs. 1) also auch zur Beschwerde berechtigt.

Abs. 4: Mit der Befristung der Geltungsdauer der BSE auf fünf Jahre soll sichergestellt werden, dass regelmässig eine Neubeurteilung der sicherheitsmässigen Eignung nach Art. 62 ff. vorgenommen wird. Mit dieser kann wesentlichen Änderungen beim Betrieb, die einen Einfluss auf die Informationssicherheit haben, Rechnung getragen werden.

Art. 69

Die Auftraggeberin ist an den Entscheid der Fachstelle BS gebunden. Sie darf einen Betrieb, dem die BSE verweigert wird, nicht mit einem sicherheitsempfindlichen Auftrag betrauen (s. Art. 68 Abs. 3). Umgekehrt sind Betriebe mit einer gültigen BSE berechtigt, sicherheitsempfindliche Aufträge auszuführen, wenn sie den entsprechenden Zuschlag erhalten und der Vertrag zustande kommt.

Die BSE muss vorliegen, bevor die Auftraggeberin den Betrieb den Auftrag ausführen lässt. Diese Regelung entspricht dem Grundsatz von Art. 38 Abs. 3 im Bereich der PSP.

Art. 70

Abs. 1: Betriebe mit einer BSE sind zur Mitwirkung und Zusammenarbeit verpflichtet. Ihre wichtigste Pflicht besteht darin, die Massnahmen des Sicherheitskonzepts laufend umzusetzen.

Nach Abs. 2 müssen diese Betriebe zudem der Fachstelle BS alle Änderungen melden, die für die Wahrung der Informationssicherheit bei der Erfüllung des sicherheitsempfindlichen Auftrages wesentlich sind. Z.B. sind neue Mitarbeiter zu melden, die mit der Ausübung von sicherheitsempfindlichen Tätigkeiten betraut werden sollen, damit bei ihnen eine PSP durchgeführt wird. Weiter muss der Betrieb die Fachstelle BS und die Auftraggeberin unverzüglich informieren, wenn sich ein sicherheitsrelevanter Vorfall ereignet hat.

Art. 71

Abs. 1 ermächtigt die Fachstelle BS, die Einhaltung der auftragsrelevanten, im Sicherheitskonzept vorgesehenen Sicherheitsmassnahmen im Betrieb zu kontrollieren. Sie kann diejenigen Bereiche des Betriebs, in denen der sicherheitsempfindliche Auftrag ausgeführt wird, überprüfen. Sie kann auch Einsicht in die auftragsrelevanten Unterlagen des Betriebs nehmen. Die Überprüfung kann naturgemäss auch unangemeldet erfolgen. Sie darf nur in Begleitung bzw. in Anwesenheit einer zum Betrieb gehörenden Person, in der Regel mit dem Sicherheitsbeauftragten, durchgeführt werden.

Abs. 2: Die Fachstelle BS kann beim Vorliegen konkreter Anhaltspunkte für eine Gefährdung der Informationssicherheit die erforderlichen Schutzmassnahmen treffen. Die Fachstelle BS kann z.B. die sofortige Einschliessung oder Rückgabe bestimmter Unterlagen oder Materialien verfügen. Falls die Informationssicherheit anderweitig nicht gewährleistet werden kann, ist sie gar befugt, bestimmte Unterlagen oder Materialien sicherzustellen. Dies gilt auch für Fälle, in denen nach dem Konkurs eines Betriebs noch vorhandene Unterlagen oder IKT-Mittel rasch aus der Konkursmasse ausgeschieden werden müssen.

Art. 72

Abs. 1: Bei der Vergabe neuer sicherheitsempfindlicher Aufträge gelten Betriebe mit einer BSE als geeignet im Sinne von Art. 62. Ihre Eignung wird nicht neu beurteilt. Es kommt ein vereinfachtes Verfahren zur Anwendung, das der Bundesrat auf Verordnungsebene regeln wird.

Nach Abs. 2 ist in derartigen Fällen jedoch zu prüfen, ob das bestehende Sicherheitskonzept angepasst werden muss. Dies wäre beispielsweise dann der Fall, wenn der betreffende Betrieb bis anhin "nur" VERTRAULICH klassifizierte Informationen bearbeiten musste, nun aber neu auch GEHEIM klassifizierte Informationen bearbeiten muss.

Art. 73

Betriebe mit Sitz in der Schweiz, die sich für einen sicherheitsempfindlichen Auftrag aus dem Ausland bewerben wollen, müssen den dortigen Behörden eine Sicherheitserklärung der Schweizer Behörden vorweisen (s. Art. 57 Abs. 1 Bst. b und Art. 68 Abs. 1). Die Fachstelle BS stellt Betrieben mit einer BSE deshalb auf ihren Antrag hin eine entsprechende Bescheinigung aus.

Art. 74

Abs. 1: Die BSE wird widerrufen, wenn der Betrieb seine Pflichten nach Art. 70 nicht erfüllt oder im Rahmen einer Wiederholung des Verfahrens eine neue Beurteilung nach Art. 62 ein Sicherheitsrisiko ergibt.

Der Widerruf hat nach Abs. 2 in Form einer Verfügung zu erfolgen, gegen die nach Art. 76 Abs. 3 die Beschwerde an das Bundesverwaltungsgericht offensteht. Das Beschwerderecht steht auch der Auftraggeberin zu, da ein Widerruf auch für sie nachteilig sein kann. Sie kann beispielsweise ein erhebliches finanzielles Interesse daran haben, dass die BSE nicht widerrufen wird.

Art. 75

Das BSV wird wiederholt, wenn beim Ablauf der Gültigkeitsdauer der BSE noch ein sicherheitsempfindlicher Auftrag hängig ist und durch den Betrieb bearbeitet wird. Während des Wiederholungsverfahrens wird die Auftragserfüllung nicht gestoppt. Ist der Auftrag fast erfüllt und wurden keine neuen Aufträge erteilt, wird die Fachstelle BS aus Gründen der Verfahrensökonomie das Verfahren nicht wiederholen. Besteht konkreter Grund zur Annahme, dass in Folge wesentlicher Änderungen beim Betrieb neue Sicherheitsrisiken entstanden sind, ist das Verfahren ebenfalls zu wiederholen.

Art. 76

Abs. 1 gewährt den Organen des Betriebs verschiedene Rechte (Einsicht, Berichtigung, Entfernung, Bestreitung) analog Art. 51 Abs. 1 bei den PSP.

Nach Abs. 2 kann gegen Verfügungen der Fachstelle BS beim Bundesverwaltungsgericht Beschwerde geführt werden. Mit dieser Norm wird ausdrücklich festgehalten, dass vorliegend die Ausnahmebestimmung von Art. 32 Abs. 1 Bst. a des Verwaltungsgerichtsgesetzes (grundsätzliche Unzulässigkeit der Beschwerde gegen Verfügungen auf dem Gebiet der inneren und äusseren Sicherheit des Landes) nicht zur Anwendung kommt. Beruht jedoch eine Verfügung der Fachstelle BS auf nachrichtendienstlichen Informationen, die nicht an den Betrieb oder an die Öffentlichkeit gelangen sollen, dann finden die entsprechenden Verfahrensbestimmungen Anwendung (Art. 27 und 28 VwVG).

Art. 77

Abs. 1: Die Fachstelle BS setzt ein Informationssystem zur Durchführung und Bewirtschaftung des BSV ein. Dieses System existiert seit Jahren und wurde kürzlich völlig neu konzipiert. Die heutige Rechtsgrundlage für das System (Art. 150 ff. MIG) soll aus systematischen Gründen in das vorliegende Gesetz verschoben werden.

Abs. 2: Weil das System besonders schützenswerte Personendaten und Persönlichkeitsprofile enthalten kann, bedarf es einer Grundlage in einem formellen Gesetz (Art. 17 Abs. 2 DSG), welche Art. 77-80 schaffen.

Abs. 3 führt abschliessend alle im Informationssystem gespeicherten Daten auf.

Abs. 4 regelt die Verantwortung für die rechtmässige Bearbeitung der Daten im System und die Sicherheit des Systems selbst.

Art. 78

Art. 78 liefert die notwendige Grundlage, um gewisse Daten aus dem Informationssystem bestimmten Stellen zugänglich zu machen.

- Bst. a: Die Auftraggeberinnen erhalten Zugang zu den Daten, die sie betreffen sowie zur Liste mit allen Betrieben, die über eine BSE verfügen. Dies ermöglicht es ihnen, sich rasch einen Überblick darüber zu verschaffen, ob ein Betrieb bereits über eine BSE verfügt.
- Bst. b: Der Bundesrat kann in seinem Ausführungsrecht bestimmte Betriebe ermächtigen, selbst PSP für ihren Bereich einzuleiten. In diesem Fall müssen diese Betriebe Zugang zu bestimmten Daten des Informationssystems erhalten. Bereits mit dem heutigen System können zudem die Sicherheitsbeauftragen gewisser Betriebe den Prüfungsentscheid und die Sicherheitsstufe (Prüfstufe) der Mitarbeitenden ihres Betriebs abrufen.

Art. 79

Die Regelung der Datenaufbewahrung und -vernichtung entspricht *mutatis mutandis* der für die PSP vorgeschlagenen Regelung (s. Art. 54).

Art. 80

Der Bundesrat muss die erforderlichen ergänzenden Bestimmungen zum BSV erlassen.

2.1.5 Informationssicherheit bei kritischen Infrastrukturen (KI)

Zur Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken, s. Ziff. 1.1.2.2 sowie 1.2.6.

Art. 81-83 regeln die Aufgaben des Bundes zur Unterstützung der KI-Betreiber im Bereich der Informationssicherheit. Für die Teilnahme an der öffentlich-privaten Partnerschaft im Rahmen von MELANI und den Bezug der Dienstleistungen des Bundes ist keine spezialgesetzliche Unterstellung unter das Gesetz im Sinne von Art. 3 Abs. 3 erforderlich. Die Zusammenarbeit erfolgt auf freiwilliger Basis.

Art. 81

Gemäss Abs. 1 betrifft die Unterstützung durch den Bund insbesondere die frühe Erkennung und Bewertung der Bedrohungen und Gefahren für schutzwürdige Informationen und Informationssysteme, die entsprechende Beurteilung der Risiken, die Erkennung von Vorfällen, die Wiederherstellung der Informationssicherheit in der Folge von Vorfällen sowie die Nachbearbeitung von Vorfällen. Es handelt sich für die KI-Betreiber um wichtige Dienstleistungen des Bundes.

Gemäss Abs. 2 führt der Bund einerseits einen nationalen Frühwarnungsdienst, welcher die Bedrohungslage im Bereich der Informationssicherheit laufend analysiert und Informationen über identifizierte Bedrohungen und Gefahren zuhanden der KI-Betreiber aufbereitet, um deren Informationssicherungs- und Risikomanagementprozess zu unterstützen. Andererseits betreibt er eine Anlaufstelle für präventive und reaktive Massnahmen im Bereich der technischen Informationssicherheit (*Governmental Computer Emergency Response Team*, GovCERT), welche technische Analysen – zum Beispiel von Schadsoftware – vornehmen und Empfehlungen für konkrete technische Massnahmen zur Abwehr von Gefahren oder zur Erkennung von Vorfäl-

len abgeben kann. Die mit Aufgaben nach Abs. 2 beauftragten Stellen dürfen zur Erkenntnisgewinnung auch verwundbare Systeme (Honeypots) in Netzwerken simulieren.

Gemäss Abs. 3 sorgt der Bundesrat dafür, dass ein sicherer Informationsaustausch zwischen Bund und KI-Betreibern sowie zwischen den Betreibern selbst stattfinden kann. Bedrohungen und Gefahren betreffen häufig nicht nur ein einzelnes Ziel, sondern mehrere in einem bestimmten Sektor tätige Organisationen oder gar sektorübergreifend alle KI-Betreiber. Die Inanspruchnahme der Dienstleistungen nach Art. 81 und die Teilnahme an der öffentlich-privaten Partnerschaft beruht dennoch vollständig auf Freiwilligkeit. Der Grundsatz des Handelns in Eigenverantwortung der KI wird also implizit wiederholt. Durch einen permanenten Informationsaustausch sollen Transparenz und Vertrauen geschaffen werden. Dadurch gewinnen nicht nur die KI-Betreiber an Know-How, sondern auch die Bundesbehörden in ihrer Eigenschaft als Inhaberinnen und Betreiberinnen von KI. Sie können wichtige Informationen zur Beurteilung ihrer eigenen Risiken und zur Abwehr von Gefahren erhalten.

Art. 82

Informationen bezüglich Gefahren und Indikatoren für Vorfälle im Bereich der Informationssicherheit beinhalten regelmässig Angaben zu Adressierungselementen im Fernmeldebereich (z.B. IP-Adressen, E-Mail-Adressen, Domainnamen). Diesen Adressierungselementen ist inhärent, dass sie sich (zumindest theoretisch) auf bestimmte oder bestimmbare Personen, respektive auf Geräte oder Fernmeldeanschlüsse beziehen, welche wiederum einer bestimmten oder bestimmbaren Person zugeordnet werden können. Entsprechend sind Adressierungselemente potenziell als Personendaten zu betrachten und es bedarf gemäss Art. 4 Abs. 3 und 17 Abs. 1 DSG einer gesetzlichen Grundlage für ihre Bearbeitung.

Abs. 1 sieht entsprechend vor, dass die für die Aufgaben nach Art. 81 zuständigen Stellen Personendaten bearbeiten dürfen. Die Identifikation der betroffenen Person ist allerdings insbesondere bei im Ausland registrierten Adressierungselementen regelmässig nicht oder nur mit erheblichem Aufwand möglich. Sie ist aber für die Gefahrenabwehr auch gar nicht nötig. Da also typischerweise keine Identifikation stattfindet, kann die Datenbearbeitung den betroffenen Personen weder ersichtlich gemacht, noch können sie über die Bearbeitung informiert werden. Der vorliegende Artikel ist entsprechend als *Lex Specialis* zu Art. 4 Abs. 4 DSG zu sehen. Liegt hingegen der Verdacht vor, dass ein (Schweizer) Adressierungselement respektive ein dieses Adressierungselement verwendendes Gerät durch Unberechtigte missbraucht wird, und dass dadurch eine Gefahr entsteht, kann gegebenenfalls der rechtmässige Nutzer oder die rechtmässige Nutzerin des Adressierungselements identifiziert und über den Missbrauch informiert werden. Die Identifikation muss jedoch nicht zwangsläufig durch die zuständigen Behörden erfolgen: Beispielsweise kann im Fall von dynamischen IP-Adressen die vermittelnde Fernmeldedienstanbieterin informiert werden, damit diese die entsprechenden Angaben den betroffenen Kunden weiterleiten kann. Den Kunden wird dadurch ermöglicht, Massnahmen zur Unterbindung weiteren Missbrauchs zu ergreifen und bei Vorliegen einer Straftat diese anzuzeigen.

In Abs. 2 wird die Kompetenz zur Datenbearbeitung für Personendaten eingeräumt, welche im Zusammenhang mit administrativen und strafrechtlichen Verfolgungen und Sanktionen stehen. Solche Personendaten gelten gemäss Art. 3 Bst. c Ziff. 4 DSG als besonders schützenswerte Personendaten und staatliche Stellen bedürfen gemäss Art. 17 Abs. 2 DSG einer formell-gesetzlichen Grundlage, damit sie diese bearbeiten dürfen. Der Austausch von Informationen über kriminelle Infrastrukturen und Missbrauch von Adressierungselementen kann für die Abwehr von Gefahren oder die Erkennung von Vorfällen notwendig sein. Auch wenn der Umstand nicht kommuniziert wird, dass ein Verfahren betreffend eines Adressierungselements eingeleitet oder eine Sanktion verhängt wurde, kann ein Informationsempfänger aus der Angabe, dass ein Adressierungselement für kriminelle Zwecke verwendet wurde, schliessen, dass ein entsprechendes Verfahren läuft. Die in diesem Absatz festgehaltene Kompetenz soll verhindern, dass dieser Austausch nicht mehr stattfinden kann, sobald eine Strafuntersuchung oder eine administrative Sanktion bezüglich eines Adressierungselementes eingeleitet wird.

Abs. 3 räumt Betreibern von IKT-Mitteln sowie Anbieterinnen von IKT-Diensten die Möglichkeit ein, Informationen, welche im Zusammenhang mit Gefahren und Vorfällen im Bereich der Informationssicherheit stehen, freiwillig an die zuständigen Stellen nach Art. 81 zu melden. Aufgrund dieser Bestimmung dürfen sie zur Abwehr von Gefahren und entsprechend zur Verhinderung von Schäden Angaben über von ihnen erbrachte Dienstleistungen, Vermittlungen und andere Vorgänge machen. Sie ermöglicht ihnen dadurch auch die rechtmässige Bearbeitung entsprechender Personendaten. Da durch eine solche Bekanntgabe von Daten die Wahrung von Verteidigungsrechten in einem allfälligen Verfahren beeinträchtigt werden kann, sind entsprechend beschaffte Daten nicht für gerichtliche Zwecke verwertbar. Auf gerichtliche Verfahren finden die jeweiligen Regeln für die Beweiserhebung weiterhin Anwendung.

Art. 83

Der Bundesrat soll auf Verordnungsstufe die Aufgabenteilung und die Zusammenarbeit der Stellen regeln, welche die Aufgaben nach Art. 81 wahrnehmen. Diese sollen gegenüber den KI-Betreibern einheitlich auftreten. Es steht dem Bundesrat demgegenüber frei, wie er diese Stellen intern organisieren will, um die Aufgaben des Bundes möglichst effizient wahrnehmen zu können. Im künftigen Bundesgesetz über den Nachrichtendienst des Bundes sind Kompetenzen des Nachrichtendienstes des Bundes im Bereich Schutz der KI vorgesehen. Die entsprechende Aufgabenteilung und Zusammenarbeit soll im Detail vom Bundesrat festgelegt werden können. Aufgrund der Besonderheiten, welche mit der Bearbeitung von nachrichtendienstlichen Informationen einhergehen, soll der Bundesrat deren Austausch zwischen Bundesstellen sowie deren Bekanntgabe an KI-Betreiber spezifisch regeln. Die zuständigen Stellen sind nicht zwangsläufig im selben Departement anzusiedeln. Um Transparenz zu schaffen und Rechtssicherheit zu gewährleisten, regelt der Bundesrat die Datenbearbeitung sowie den Austausch von Daten zwischen diesen Stellen, wie auch die dabei zu berücksichtigende Datensicherheit.

2.1.6 Organisation und Vollzug

Art. 84

Zur Rolle der Informationssicherheitsbeauftragten: s. Ziff. 1.3.2.1.

Abs. 1: Das Gesetz greift aufgrund des überwiegenden Bedarfs nach einer integralen Steuerung der Umsetzung des vorliegenden Gesetzes in die Organisationsautonomie der Behörden ein: Es verlangt, dass die verpflichteten Behörden sowie die Departemente und die Bundeskanzlei für ihren Zuständigkeitsbereich eine/n Informationssicherheitsbeauftragte/n (international: *Chief Information Security Officer, CISO*) sowie eine angemessene Stellvertretung bezeichnen. Da einerseits eine wirksame integrale Steuerung der Informationssicherheit sowohl politisches, rechtliches, organisatorisches als auch technisches Wissen voraussetzt und andererseits durch die Informationssicherheitsbeauftragten sehr viele Aufgaben wahrgenommen werden müssen, verlangt die praktische Umsetzung, dass mindestens zwei Personen pro Behörde diese Aufgaben wahrnehmen. Es wird jedoch nicht verlangt, dass beide Personen in vollem Umfang dafür eingesetzt werden.

Der Bundesrat selbst muss ebenfalls seine Informationssicherheitsbeauftragten bezeichnen. Hingegen soll die Aufsichtsbehörde der Bundesanwaltschaft aufgrund ihres begrenzten Personalbestandes nicht dazu verpflichtet werden. Die eidgenössischen Gerichte werden nicht einzeln aufgeführt, weil es unverhältnismässig wäre, von den personalmässig ebenfalls relativ kleinen Gerichten (z.B. Bundespatentgericht und Militärkassationsgericht) solche Stellen zu verlangen. Das Gesetz lässt es also zu, dass die eidgenössischen Gerichte z.B. eine einzige Stelle und Stellvertretung für alle Gerichte bezeichnen oder einen anderen Ansatz wählen, der die Behördenautonomie wahrt. Die Bundesämter und die dezentrale Bundesverwaltung werden durch das Gesetz ebenfalls nicht verpflichtet, eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten zu bezeichnen. Der Bundesrat muss im Rahmen der Erfüllung seiner Organisationspflicht auf Verordnungsebene entscheiden, wie die Informationssicherheit bis auf diese Stufe organisiert und gesteuert werden soll.

Abs. 2 umschreibt in allgemeiner Form den Aufgabenbereich und die Zuständigkeit der Informationssicherheitsbeauftragten:

- Bst. a betont, dass die Entscheidkompetenzen und die Verantwortung für die Entscheidungen im Bereich der Informationssicherheit nach wie vor bei der Linie, also bei den zuständigen Behörden und den ihnen nachgeordneten Stellen liegen sollen. Die Informationssicherheitsbeauftragten sollen die Linie aber fachlich beraten und unterstützen.
- Bst. b legt fest, dass die Informationssicherheitsbeauftragten im Auftrag ihrer Behörde oder Organisation die Informationssicherheit sowie das entsprechende Risikomanagement fachtechnisch steuern müssen.
- Bst. c sieht vor, dass die Informationssicherheitsbeauftragten eine allgemeine Pflicht zur Überprüfung der Einhaltung der Vorschriften dieses Gesetzes haben, dass sie ihrer Behörde Bericht erstatten und bei festgestelltem Handlungsbedarf Antrag stellen müssen.
- Bst. d hält fest, dass die Informationssicherheitsbeauftragten festgestellte sicherheitsrelevante Vorfälle sowohl der Fachstelle des Bundes für Informationssicherheit (Art. 86), der Konferenz der Informationssicherheitsbeauftragten (Art. 85) als auch den Stellen, welche die Aufgaben bezüglich Informationssicherheit bei KI wahrnehmen, melden können. Es wird also im behördenübergreifenden Rahmen auf eine Mel*depflicht* verzichtet. Die Mitteilung solcher Vorfälle ist zwar sehr empfehlenswert, aber die Behördenautonomie soll nicht tangiert werden.

Abs. 3: Die Informationssicherheitsbeauftragten müssen in ihrer Stellung und ihrer Aufgabenwahrnehmung unabhängig sein und dürfen keinen materiellen Interessenkonflikten ausgesetzt werden. Eine fehlende Funktionstrennung führt in der Praxis immer wieder zu Problemen beim Vollzug der Sicherheitsvorgaben. So ist z.B. heute noch die Mehrheit der IKT-Sicherheitsbeauftragten den IKT-Leitungen unterstellt. Dabei verfolgen die IKT-Verantwortlichen oft andere Prioritäten als die Sicherheit und aufgrund der Dringlichkeit und/oder der Kosten wird in Projekten regelmässig auf die Umsetzung der erforderlichen Sicherheitsmassnahmen verzichtet. Die Informationssicherheitsbeauftragten sollten auch nicht mit dem unmittelbaren Betrieb von IKT-Mitteln beauftragt oder als Leiter von Projekten, die nicht primär die Informationssicherheit betreffen, eingesetzt werden, denn genau bei solchen Aufgabenkumulationen kollidieren die anderen Anforderungen des Betriebs regelmässig mit einer möglichst objektiven Beurteilung der Sicherheitsrisiken.

Die genaue Ansiedlung der Funktion ist den Behörden bzw. den Departementen und der BK überlassen. Die Lehre, gestützt auf praktische Erfahrungen, zeigt jedoch, dass die Informationssicherheitsbeauftragten am Effektivsten sind, wenn sie relativ nah an der Behördenleitung angesiedelt werden, weil sie so am besten die Geschäftsprozesse überblicken und die Geschäftsanforderungen beurteilen können. Es wäre zudem wünschenswert, die Informationssicherheitsbeauftragten so anzusiedeln, dass sie eine enge Koordination mit den bestehenden Risikomanagern, Datenschutzberatern, Sicherheitsbeauftragten (Objektsicherheit) und, gegebenenfalls, Öffentlichkeitsberatern sicherstellen können.

Art. 85

Zur Konferenz, s. Ziff. 1.3.2.2.

Abs. 1 legt fest, wer in dieser Konferenz ständiges Mitglied ist. Insbesondere müssen die Departemente und die Bundeskanzlei vertreten sein.

Abs. 2 umschreibt die Aufgaben der Konferenz, die alle einer wirkungsvollen Koordination des Vollzugs dienen. Die neu zu schaffende Fachstelle des Bundes für Informationssicherheit (s. Art. 86) soll die Konferenz bei allen wichtigen Belangen der Informationssicherheit konsultieren und einbeziehen. Besonders wichtig ist die Beratung der Fachstelle durch die Konferenz in Fragen der Informationssicherheitsstrategie. Die Konferenz soll auch dazu dienen, Trends oder Risiken zu erkennen und entsprechende Massnahmen vorausschauend zu konzipieren. Nur so können wirksame Lösungen gefunden sowie die erforderliche Akzeptanz geschaffen werden. Wichtig erscheint auch, dass die Koordination mit dem EDÖB ausdrücklich als Auftrag festgehalten ist (Bst. d). Die Konferenz kann für ihre Abklärungen und ihre Meinungsbildung auch Vertreter der Kantone sowie unabhängige Experten beiziehen.

Abs. 3 bestimmt, dass die Konferenz ihre eigene Organisation und Geschäftsprozesse bestimmen soll. Auch über ihre Leitung soll sie selbst entscheiden.

Art. 86

Zur Fachstelle des Bundes für Informationssicherheit, s. Ziff. 1.3.2.3.

Abs. 1 enthält einen Katalog der behördenübergreifenden Aufgaben und Kompetenzen der künftigen Fachstelle:

- Bst. a verpflichtet die Fachstelle zur Beratung der verpflichteten Behörden und deren Informationssicherheitsbeauftragten. Diese können auch die fachliche Unterstützung der Fachstelle anfordern, insbesondere bei der Aufarbeitung von Vorfällen im Bereich der Informationssicherheit.
- Nach Bst. b soll die Fachstelle bei unmittelbaren Gefährdungen der Informationssicherheit vorbeugende Schutzmassnahmen empfehlen können.
- Bst. c: Die verpflichteten Behörden bzw. die von diesen ermächtigten Stellen können die Fachstelle beauftragen, bei ihnen bestimmte Kontrollen und Audits im Bereich der Informationssicherheit durchzuführen. Die Fachstelle darf von sich aus keine solchen Überprüfungen durchführen. Insbesondere für technische Sicherheitsaudits ist hohes Fachwissen erforderlich, das nicht alle verpflichteten Behörden für sich beschaffen sollten: Die Bereitstellung eines Expertenpools ist wirtschaftlicher.
- Bst. d: Die verpflichteten Behörden und Organisationen, die neuartige Technologie einsetzen wollen, sind gemäss Art. 20 verpflichtet, eine Risikobeurteilung durchzuführen. Für Technologien, die besonders wichtig oder die einen breiten Anwendungsbereich haben können, sollen sie der Fachstelle beantragen dürfen, diese Risikoanalyse durchzuführen.
- Bst. e ermächtigt die Fachstelle, auf Antrag der verpflichteten Behörden und Organisationen die Eignung bestimmter Prozesse, Mittel, Einrichtungen, Gegenstände und Dienstleistungen auf sicherheitsrelevante Aspekte zu prüfen. Es geht hier um die sicherheitsmässige Standardisierung von Prozessen, Mitteln, Einrichtungen, Gegenständen und Dienstleistungen. Im Bereich der technischen Informationssicherheit ha-

ben z.B. die IKT-Leistungserbringer ein Interesse daran, zu wissen, ob die technischen Lösungen, die sie entwickeln, die Anforderungen des Bundes erfüllen. Ist das der Fall, dann können sie sie für andere Projekte oder IKT-Mittel wesentlich einfacher einsetzen. Dasselbe gilt auch z.B. für Tresore oder für Dienstleistungen. Die Verantwortung, auch wenn die Anforderungen erfüllt sind, bleibt jedoch immer bei der Behörde oder Organisation, die solche Mittel einsetzt. Diese Kompetenz ist auch für das internationale Verhältnis erforderlich: Die Fachstelle soll die heute fehlende, international übliche Rolle der *National Accreditation Authority* wahrnehmen (s. Ziff. 4.2).

- Bst. f: Wenn wichtige behördenübergreifende Projekte mit wesentlichem Bezug zur Informationssicherheit in Angriff genommen werden, soll die Fachstelle auf Antrag der verpflichteten Behörden die Steuerung und Koordination der Informationssicherheitsbelange innerhalb derselben übernehmen.
- Bst. g: Da das entsprechende Fachwissen für den Bund in der vorgesehenen Fachstelle zusammengefasst werden soll, soll sie auch die Ansprechstelle des Bundes für die inländischen, ausländischen und internationalen Stellen im Bereich der Informationssicherheit sein. Sie wird auch die erforderlichen Rollen im internationalen zwischenbehördlichen Rahmen wahrnehmen (s. Ziff. 4.2.). Andere Behörden oder Organisationen werden aber weiterhin Fachkontakte in diesem Bereich pflegen dürfen.
- Bst. h: Die Fachstelle soll dem Bundesrat jährlich Bericht erstatten.

Gemäss Abs. 3 muss der Bundesrat in seinem Ausführungsrecht die Organisation der Fachstelle regeln. Hierzu wird er festlegen müssen, welche Aufgaben die Fachstelle selbst ausübt oder in Zusammenarbeit mit anderen Bundesstellen erfüllen soll. Der Bundesrat wird in diesem Zusammenhang selbstverständlich auch die Frage ihrer Ansiedelung entscheiden müssen.

Art. 87

Abs. 1: Die Autonomie der verpflichteten Behörden soll nicht in Frage gestellt werden. Sie sollen den Ausführungsbestimmungen des Bundesrats nicht unterstellt werden. Im Gegenzug müssen sie die für den Vollzug dieses Gesetzes erforderlichen Ausführungsbestimmungen für ihren Bereich selbst erlassen. Es wird hier auch festgehalten, dass der Bundesrat den Erlass von Ausführungsbestimmungen in Bezug auf den Umgang mit Bundesratsgeschäften an die Bundeskanzlei delegieren darf (s. auch Art. 15 Abs. 2 RVOG).

Abs. 2: Mit dieser Regelung und Art. 70 ParlG hat die Bundesversammlung alle nötigen Bestimmungen, damit sie und die Parlamentsdienste das ISG und seine Ausführungsbestimmungen direkt anwenden können.

In Abs. 3 wird ein sogenanntes "*Opting-out*" festgelegt: Die Ausführungsbestimmungen des Bundesrats nach Abs. 1 gelten für alle verpflichteten Behörden sinngemäss, sofern sie keine eigenen Ausführungsbestimmungen erlassen. Es versteht sich, dass der Bundesrat die anderen Behörden anhört, bevor er seine Ausführungsbestimmungen erlässt. Dass der Bundesrat für den Erlass der erforderlichen Ausführungsbestimmungen zur Personensicherheitsprüfung und zum Betriebssicherheitsverfahren allein zuständig ist, ergibt sich daraus, dass diese Stellen Teil der Bundesverwaltung sind, deren Organisation Sache des Bundesrates ist.

Abs. 4: Bevor Organisationen des öffentlichen oder privaten Rechts nach Art. 2 Abs. 2 Bst. e dem Gesetz unterstellt werden können, muss beurteilt werden, ob sie sicherheitsempfindliche Tätigkeiten des Bundes ausüben. Der Bundesrat soll für diese Organisationen diese Beurteilung vornehmen und anschliessend den detaillierten Geltungsbereich auf Verordnungsstufe festlegen. Dies kann in den Ausführungsbestimmungen zur Spezialgesetzgebung erfolgen oder in den Ausführungserlassen zu diesem Gesetz. Der Bundesrat kann bei Bedarf nur Teile des Gesetzes von diesen Organisationen anwenden lassen (z.B. Bestimmungen über die Klassifizierung, über den Einsatz der IKT oder über die Personensicherheitsprüfungen).

Art. 88

Abs. 1: Um das erforderliche einheitliche Sicherheitsniveau zu erreichen, soll der Bundesrat Standardanforderungen und -massnahmen nach dem Stand der Lehre und der Technik festlegen. Es handelt sich dabei nicht um grundsätzliche organisatorische Anforderungen und Massnahmen, sondern vorab um Anforderungen untergeordneter Natur, z.B.:

- Standard für die Erhebung des Schutzbedarfs von Informationen in Bezug auf die vier Kriterien von Art. 4 Abs. 2;
- Standardmethode für die Risikobewertung nach Art. 6 Abs. 1;
- Standards für organisatorische, personelle, technische und bauliche Massnahmen nach Art. 6 Abs. 2;
- Standardanforderungen für bestimmte Prozesse und Mittel zum Schutz klassifizierter Informationen nach den Art. 12-18;

- Standardanforderungen und -massnahmen für den Grundschutz, für die Erstellung von Informationssicherheitskonzepten sowie für die Sicherheit von IKT-Mitteln der Sicherheitsstufen «hoher Schutz» und «sehr hoher Schutz» nach den Art. 19-27; usw.

Abs. 2: Der Bundesrat soll die Erarbeitung und Verabschiedung der Standards wenn nötig an untergeordnete Stellen delegieren. Dies betrifft in erster Linie die Fachstelle des Bundes für Informationssicherheit, aber auch z.B. fedpol im Bereich des Objektschutzes. Die IKT-Leistungserbringer des Bundes sollten ebenfalls technische Sicherheitsstandards erarbeiten können und diese gegebenenfalls zwecks Standardisierung durch die Fachstelle auf ihre Eignung für den Bund prüfen lassen (s. Art. 86 Abs. 1 Bst. e). Eine solche Delegation durch den Bundesrat soll aber nicht umfassend erfolgen. Bestimmte technische Massnahmen können wesentliche finanzielle Folgen nach sich ziehen, die nicht unbedingt von untergeordneten Stellen beschlossen werden sollten. Der Bundesrat soll also auch bei einer allfälligen Delegation sicherstellen, dass er die weitreichenden und kostspieligsten Massnahmen selbst beschliesst.

Abs. 3: Die Standards sind für die anderen verpflichteten Behörden nicht verbindlich.

Art. 89

Abs. 1: In Fällen, in denen die Kantone bzw. ihre entsprechenden Behörden und Dienststellen vom Gesetz erfasst werden (s. Art. 2 Abs. 2 Bst. f), müssen sie die erforderlichen Sicherheitsmassnahmen nach diesem Gesetz treffen. Die Bundesstellen erhalten damit aber keine unmittelbaren Weisungsbefugnisse, sondern die Kantone sind für den Vollzug in ihrem Zuständigkeitsbereich grundsätzlich selbst verantwortlich.

Abs. 2: Der Bundesrat soll die Überprüfung der Umsetzung der Massnahmen sowie die Durchführung von Personensicherheitsprüfungen für kantonale Angestellte in seinem Ausführungsrecht regeln. Insbesondere wird er regeln müssen, wie die Umsetzung der Vorschriften durch die Kantone durch die Bundesbehörden gegebenenfalls kontrolliert wird. Es versteht sich, dass er dabei der staatsrechtlichen Stellung der Kantone und insbesondere ihrer Organisationsautonomie Rechnung tragen wird.

In Abs. 3 werden die Kantone verpflichtet, für solche Fälle je eine Dienststelle als Ansprechpartner für die zuständigen verpflichteten Behörden und Organisationen zu bezeichnen. Damit soll sichergestellt werden, dass der Informationsaustausch systematisch stattfindet und die Umsetzung der Massnahmen nach diesem Gesetz koordiniert erfolgt.

Art. 90

Die völkerrechtlichen Verträge im Bereich der Informationssicherheit enthalten vorweg technische Regelungen über die wechselseitige Anerkennung nationaler Vorschriften und Abläufe (bspw. das Personensicherheitsprüfungs- oder Betriebssicherheitsverfahren), Konkordanzlisten über die Anwendung von Klassifizierungen sowie Regelungen über die Durchführung gegenseitiger Kontrollen. Es kann zudem erforderlich sein, dass zum Schutz von Informationen, die dem Bund von anderen Staaten oder internationalen Organisationen zur Verfügung gestellt werden, Vereinbarungen zu treffen sind, die in einzelnen Punkten (z.B. Voraussetzungen für die Klassifizierung, für den Zugang zu oder die Bearbeitung von klassifizierten Informationen oder für die Erteilung der Sicherheitserklärungen) von den gesetzlichen Vorschriften abweichen. Der Lieferant der Informationen kann in solchen Fällen verlangen, mit den empfangenden Bundesbehörden gegebenenfalls einen strengeren oder weniger strengen Schutz seiner Informationen zu vereinbaren. Entsprechend sind in den Vollzugs- und Organisationsbestimmungen, welche die jeweiligen Vertragsschlusskompetenzen zuweisen, die notwendigen Vorbehalte zu verankern. Aus Gründen der Verwaltungsökonomie soll der Bundesrat ermächtigt werden, solche Informationssicherheitsabkommen direkt abzuschliessen.

Eine zunehmende internationale Vernetzung und Zusammenarbeit ist zur Minimierung von Risiken der Informationssicherheit erforderlich. Die Umsetzung der NCS verlangt deshalb, dass der Austausch von Erfahrungen, Forschungs- und Entwicklungsarbeiten, vorfallbezogenen Informationen sowie Ausbildungs- und Übungstätigkeiten verstärkt wird (s. auch Ziff. 1.1.2.2). Der Bundesrat soll deshalb auch ermächtigt werden, völkerrechtliche Verträge zum Austausch von Informationen über Gefährdungen, Schwachstellen und Vorfälle, insbesondere bei KI, abzuschliessen. Es handelt sich hier vor allem um untergeordnete organisatorische und technische Angelegenheiten (z.B. Zusammenarbeit mit anderen GovCERTs; s. Art. 81).

Art. 91

Jedes Gesetz muss periodisch auf seine tatsächliche Umsetzung sowie seine Zweckmässigkeit, Wirksamkeit und Wirtschaftlichkeit, evaluiert werden. Nach Abs. 1 soll der Bundesrat dafür zuständig sein. Die Bundesversammlung muss die Kommission bestimmen, welche die Berichte des Bundesrats behandeln soll (Abs. 2).

Art. 92

Aufgrund der neuen Regelung müssen andere Bundesgesetze angepasst werden.

Art. 93

Die Personen- und Betriebssicherheitserklärungen nach bisherigem Recht sollen aus Gründen der Verfahrensökonomie bis zu ihrem Ablauf gültig bleiben. Der Bundesrat soll die Übergangsfristen zur Anpassung der Vorschriften über die Bearbeitung von klassifizierten Informationen sowie über die Gewährleistung der Informationssicherheit beim Einsatz von IKT festlegen.

2.2 Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit

Art. 2 Abs. 4 Bst. c sowie Art. 19 - 21

Die PSP soll neu schwergewichtig im ISG geregelt werden. Die entsprechenden Bestimmungen des BWIS müssen daher aufgehoben werden.

2.3 Archivierungsgesetz

Art. 6 Abs. 2

Die Archivierung von Unterlagen des Bundes wird durch das BGA einheitlich geregelt. Als Unterlagen gelten insbesondere „alle aufgezeichneten Informationen, unabhängig vom Informationsträger, die bei der Erstellung öffentlicher Aufgaben des Bundes empfangen oder erstellt worden sind“ (Art. 3 Abs. 1 BGA). Die Dienststellen des Bundes haben dem Bundesarchiv alle Unterlagen zur Archivierung anzubieten, „die sie nicht mehr ständig benötigen“ (Art. 6 BGA). Informationen, die klassifiziert sind, fallen heute auch unter die Archivierungsgesetzgebung. Ihr Schutz wird in diesem Zusammenhang durch Schutzfristen nach Art. 9 ff BGA sichergestellt.

Der neue Absatz 2 von Artikel 6 BGA regelt das Verhältnis zwischen dem BGA und dem ISG. Die Bestimmung dient der klaren Abgrenzung der Anwendungsbereiche der beiden involvierten Gesetze. Das BGA regelt die Archivierung, weshalb dieses Verhältnis nicht im ISG, sondern im BGA selbst geregelt wird. Klassifizierte Informationen werden nach Art. 6 Abs. 2 BGA nicht zur Archivierung angeboten, solange sie nach den Bestimmungen des ISG noch schutzwürdig sind. Sobald sie aber in Anwendung der Bestimmungen der Gesetzgebung über die Informationssicherheit entklassifiziert werden können, müssen sie zur Archivierung angeboten werden. Die Klassifizierung und Entklassifizierung richtet sich dabei nach den Bestimmungen des ISG. Klassifizierte Informationen haben mehrheitlich eine zeitlich begrenzte Schutzwürdigkeit und sollen nach den üblichen Regeln des BGA archiviert werden können. Dabei versteht sich, dass die Klassifizierung nicht verwendet werden darf, um sich der Archivierungspflicht zu entziehen.

2.4 Bundespersonalgesetz

Art. 20a

Die Erhöhung des Schwellenwerts für die Durchführung von PSP nach dem ISG soll dazu dienen, diese Massnahme nur noch für Tätigkeiten einzusetzen, die tatsächlich eine erhöhte Sicherheitsempfindlichkeit vorweisen. Es besteht jedoch *trotz des Gesetzes* die Gefahr, dass der Schwellenwert für die PSP in der Praxis herabgesetzt wird bzw. die Anforderungen an die Notwendigkeit einer PSP reduziert werden, wenn die verpflichteten Behörden und Organisationen keine anderen Instrumente zur Verfügung haben, um die Vertrauenswürdigkeit von Bewerberinnen und Bewerbern sowie von Angestellten zu prüfen. Der neue Art. 20*a* BPG soll den Arbeitgeberinnen und Arbeitgebern entsprechende Mittel anbieten: Sie sollen die Möglichkeit haben, von Stellenbewerberinnen und Stellenbewerbern sowie den Angestellten zu verlangen, dass sie einen Auszug aus dem Strafregister und aus dem Betreibungsregister vorlegen. Dies sollte jedoch nicht standardmässig erfolgen, sondern nur sofern dies für die Wahrung der Interessen der Arbeitgeber erforderlich ist. Der Bundesrat soll dazu Ausführungsbestimmungen erlassen.

Art. 20b

Das ISG beschränkt seine Regelung der PSP auf sicherheitsempfindliche Tätigkeiten beim Umgang mit klassifizierten Informationen und IKT-Mitteln sowie beim Zugang zu bestimmten Sicherheitszonen. Diese Tätigkeiten dürften den grössten Teil der erforderlichen PSP betreffen. Es verbleiben aber weitere Tätigkeiten im Aufgabenbereich der Bundesbehörden, bei denen wesentliche Interessen des Bundes erheblich beeinträchtigt werden können, ohne dass die Tätigkeiten unmittelbar den Umgang mit Informationen oder IKT-Mitteln betreffen. Für das Personal des Bundes (mit Ausnahme der Armee und der Nationalbank) gehören solche Regelungen in das BPG. Mit der Einfügung einer neuen Bestimmung über die Prüfung der Vertrauenswürdigkeit in Art. 20*b* BPG soll ein identifizierter Prüfbedarf abgedeckt werden.

- Nach Bst. a kann der Bundesrat Bewerberinnen und Bewerber sowie Angestellte prüfen lassen, die regelmässig die Schweiz im Ausland vertreten sollen und dabei das Ansehen des Bundes erheblich beeinträchtigen könnten. Es handelt sich hierbei primär um das diplomatische und konsularische Personal des

EDA. Eskann aber auch das Personal anderer Departemente betroffen sein, das ähnliche Funktionen wahrnimmt (z.B. beim SECO).

- Nach. Bst. b kann er auch Bewerberinnen und Bewerber sowie Angestellte prüfen lassen, die Entscheidungskompetenzen oder Aufsichtsaufgaben in wesentlichen Finanz- oder Steuerangelegenheiten erfüllen sollen und dabei die finanziellen Interessen des Bundes erheblich beeinträchtigen könnten (z.B. Angestellte, die Entscheidungskompetenzen bei der Vergabe wesentlicher öffentlicher Aufträge haben, oder Personen, die besonders empfindliche Aufgaben in Zusammenhang mit dem Finanzhaushalt erfüllen).

Abs. 2: Der Bundesrat soll in seinem Ausführungsrecht zum BPG die Personengruppen festlegen, die einer Prüfung der Vertrauenswürdigkeit unterzogen werden sollen. Diese Prüfung soll nur bei ausgewiesenem Bedarf angeordnet werden. Die vorliegende Bestimmung darf nicht dazu dienen, die Einschränkung der Prüfgründe nach dem ISG umzugehen.

Abs. 3: Es ist nicht sinnvoll, für die Prüfung der Vertrauenswürdigkeit ein besonderes Verfahren einzuführen, da die abzuklärenden Fragen vom Grundsatz her die gleichen sind, wie bei der Informationssicherheit. Für die Durchführung der Prüfung soll daher auf die Regelung im ISG zurückgegriffen werden. Mit der Übernahme des Verfahrens werden insbesondere auch der Grundsatz des Einverständnisses der betroffenen Person für die Durchführung der Prüfung, die Grundsätze der Datenerhebung, und die Regelungen über die Folgen der Beurteilung zur Anwendung kommen.

Abs. 4: Wenn die nach dieser Bestimmung zu prüfende Person gleichzeitig einer PSP nach dem ISG unterzogen werden soll, so sollen im Interesse der Verfahrensökonomie die beiden Verfahren vereinigt werden.

2.5 Strafgesetzbuch

Art. 365 Abs. 2 Bst. d

Bei der Anpassung dieses Artikels handelt es sich um eine rein formelle Angelegenheit. Da die PSP neu nicht mehr im BWIS sondern im ISG geregelt werden sollen, müssen die Bestimmungen über die zugriffsberechtigten Stellen sowie den Zweck der Datenerhebung aus dem Strafregister entsprechend angepasst werden. Neu wird als Zweck für die Datenerhebung auch die Beurteilung des Sicherheitsrisikos im Rahmen von Prüfungen der Vertrauenswürdigkeit nach der Spezialgesetzgebung aufgeführt. Die Erwähnung der Prüfung des Gewaltpotenzials ist hingegen bereits in Bst. n und p geregelt.

Art. 367 Abs. 2 Bst. i und Abs. 2bis Bst. b

S. Erläuterungen zu Art. 365 Abs. 2 Bst. d.

2.6 Bundesgesetz über die polizeilichen Informationssysteme des Bundes

Art. 15 Abs. 4 Bst. f sowie Art. 17 Abs. 4 Bst. l

Bei der Anpassung dieser beiden Artikel handelt es sich um eine rein formelle Angelegenheit. Da die PSP neu nicht mehr im BWIS sondern im ISG geregelt werden sollen, müssen die Bestimmungen über die zugriffsberechtigten Stellen sowie den Zweck der Datenerhebung aus dem Automatisierten Polizeifahndungssystem und dem Nationalen Polizeiindex entsprechend angepasst werden. Neu werden als Zweck für die Datenerhebung zusätzlich die Beurteilung des Sicherheitsrisikos im Rahmen von Prüfungen der Vertrauenswürdigkeit nach der Spezialgesetzgebung sowie die Beurteilung des Gewaltpotenzials im Rahmen von Prüfungen des Gewaltpotenzials aufgeführt.

2.7 Militärgesetz

Art. 14

Der Entwurf des ISG beschränkt seine vorgeschlagene Regelung der PSP auf gewisse sicherheitsempfindliche Tätigkeiten (s. oben zu Art. 20b BPG). Auch bei der Armee gibt es aber weitere Tätigkeiten, bei denen das Ansehen des Bundes und seiner Institutionen oder wesentliche finanzielle Interessen des Bundes erheblich beeinträchtigt werden können.

Abs. 1 sieht deshalb entsprechend dem vorgeschlagenen Art. 20b BPG vor, dass der Bundesrat im Rahmen seiner Ausführungsbestimmungen zum MG zwei Aufgabenbereiche einer Prüfung der Vertrauenswürdigkeit unterstellen kann:

- Nach Bst. a kann er Angehörige der Armee prüfen lassen, die regelmässig die Schweiz im Ausland vertreten sollen und dabei das Ansehen des Bundes erheblich beeinträchtigen könnten. Es handelt sich hier vor allem um Angehörige der Armee, die im Rahmen von Auslandeinsätzen die Schweiz vertreten oder die Aufgaben im Bereich der militärischen Diplomatie erfüllen.

- Nach. Bst. b kann er zudem Angehörige der Armee prüfen lassen, die Entscheidungskompetenzen oder Aufsichtsaufgaben in wesentlichen Finanzangelegenheiten erfüllen sollen und dabei die finanziellen Interessen des Bundes erheblich beeinträchtigen könnten.

Abs. 2: Der Bundesrat soll in seinem Ausführungsrecht zum MG die Personengruppen festlegen, die einer solchen Prüfung unterzogen werden sollen. Die Unterstellung ist nur bei ausgewiesenem Bedarf anzuordnen, damit eine Umgehung der Einschränkung der Prüfgründe nach dem ISG vermieden wird.

Abs. 3: Wie bei der im BPG vorgeschlagenen Regelung ist es nicht sinnvoll, für diese Prüfung ein besonderes Verfahren einzuführen, da die abzuklärenden Fragen vom Grundsatz her die gleichen sind, wie bei der Informationssicherheit. Für die Durchführung der Prüfung soll daher auf die Regelung im ISG zurückgegriffen werden. Mit der Übernahme des Verfahrens werden insbesondere auch die Grundsätze der Datenerhebung und die Regelungen über die Folgen der Beurteilung zur Anwendung kommen.

Abs. 4: Wenn die nach dieser Bestimmung zu prüfende Person gleichzeitig einer PSP nach dem ISG unterzogen werden soll, sollen im Interesse der Verfahrensökonomie die beiden Verfahren vereinigt werden.

Art. 113 Abs. 5

Mit der Beschränkung der PSP nach dem ISG auf sicherheitsempfindliche Tätigkeiten beim Umgang mit Informationen und IKT-Mitteln wird es erforderlich, die Prüfung des Gewaltpotenzials für Angehörige der Armee, die eine Waffe tragen sollen, auf eine spezialgesetzliche Grundlage zu stellen. Für das Verfahren soll die Regelung des ISG sinngemäss Anwendung finden. Sind zwei Verfahren eingeleitet, sollen sie aus Gründen der Verfahrensökonomie vereinigt werden.

Art. 150 Abs. 4 Aufhebung

Die in dieser Vorschrift bisher enthaltene Kompetenz zum Abschluss von Staatsverträgen zur Wahrung der militärischen Geheimhaltung ist neu in Art. 90 ISG enthalten. Es wird denn auch häufig nicht mehr zwischen ziviler und militärischer Geheimhaltung unterschieden, sondern ein Abkommen für beide Sektoren bzw. über die Geheimhaltung im Allgemeinen abgeschlossen. Zur Sicherstellung der Einheitlichkeit des Rechts ist daher Art. 150 Abs. 4 des Militärgesetzes aufzuheben.

2.8 Bundesgesetz über die militärischen Informationssysteme

5. Kapitel 1. und 2. Abschnitt (Artikel 144–155)

Die Informationssysteme zur PSP und zum BSV werden heute im MIG geregelt. Neu werden beide Informationssysteme direkt im ISG geregelt (Art. 52-54 für die PSP und Art. 77-79 für das BSV). Die beiden entsprechenden Abschnitte im MIG müssen deshalb aufgehoben werden.

2.9 Kernenergiegesetz

Art. 5 Abs. 3

Der geltende Art. 5 Abs. 3 KEG sieht bereits heute vor, dass die Sicherungsmassnahmen soweit erforderlich klassifiziert werden müssen. Die Änderung soll sicherstellen, dass die Klassifizierung dieser Massnahmen sowie die Bearbeitung der entsprechenden klassifizierten Informationen sich nach dem ISG richten.

Art. 24

Die geltende Regelung von Art. 24 KEG sieht bereits Zuverlässigkeitskontrollen für Personen vor, die in Funktionen eingesetzt werden, welche für die nukleare Sicherheit und die Sicherung der Kernanlage wesentlich sind. Bei diesen Personen wird gestützt auf die PSPVK eine PSP durchgeführt. Mit der Neufassung wird der Wortlaut von Art. 24 KEG an die neue Terminologie für Prüfungen der Vertrauenswürdigkeit angepasst, da die Prüfung in sinngemässer Anwendung der Bestimmungen über die PSP des ISG durchgeführt wird.

2.10 Stromversorgungsgesetz

Art. 26a

Die nationale Netzgesellschaft, die das Übertragungsnetz für Elektrizität auf gesamtschweizerischer Ebene betreibt (Swissgrid), verlangt seit Jahren, dass bei gewissen Personalgruppen PSP durchgeführt werden. Angesichts der Kritikalität des Übertragungsnetzes und des entsprechenden Bedarfs an Sabotageschutz soll ins StromVG eine neue Bestimmung über die Durchführung von Prüfungen der Vertrauenswürdigkeit bei besonderen Personengruppen eingefügt werden.

Abs. 1 legt den Grundsatz der Prüfung der Vertrauenswürdigkeit von Angestellten der nationalen Netzgesellschaft fest, die Aufgaben erfüllen sollen, die für die Sicherheit des Übertragungsnetzes auf gesamtschweizerischer Ebene und dessen zuverlässigen und leistungsfähigen Betrieb wesentlich sind.

Nach Abs. 2 soll der Bundesrat den Personenkreis bestimmen, der geprüft werden muss. Dabei soll er sich auf Funktionen beschränken, die bei Sabotagehandlungen oder -unterlassungen einen erheblichen Schaden anrichten können.

Abs. 3: Das Prüfverfahren richtet sich nach den Bestimmungen des ISG über die PSP.

Abs. 4 hält sich an die ähnliche Regelung nach Art. 24 KEG. Die Geschäftsleitung von Swissgrid sowie die Regulatoren (BFE und ElCom) als übertragende Stellen sollen Zugang zu den Daten der Prüfung erhalten.

2.11 Nationalbankgesetz

Art. 16, Sachüberschrift und Abs. 5

Aufgrund ihrer geld- und währungspolitischen Aufgaben (s. auch Art. 1 Abs. 2 Bst. d) soll die Nationalbank als verpflichtete Behörde nach Art. 2 Abs. 1 ISG gelten. Mit der Anpassung von Art. 16 NBG wird ausdrücklich darauf verwiesen, dass das ISG für die Nationalbank gelten soll. Die Sachüberschrift des Artikels wird entsprechend angepasst.

3 Auswirkungen

3.1 Auswirkungen auf den Bund

Informationen werden geschützt, weil eine Verletzung ihrer Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit (s. Art. 4) die Rechte von Dritten verletzen (z.B. Personendaten oder Geschäfts- und Fabrikationsgeheimnisse), wesentliche öffentliche Interessen beeinträchtigen (z.B. die Handlungsfähigkeit der Bundesbehörden, die nationale Sicherheit, die internationalen Beziehungen oder die Landesversorgung) oder der betroffenen Organisation einen Schaden zufügen (z.B. Produktivitätsverlust oder Betriebsstörungen) kann. Informationssicherheit hat zum Ziel, möglichst effektiv und günstig die Eintrittswahrscheinlichkeit und gegebenenfalls das Ausmass eines solchen - auch finanziellen - Schadens zu reduzieren. Ihre Kosten müssen also mit der entsprechenden Reduktion der Risiken abgewogen werden.

Das Gesetz wird nach heutiger Einschätzung eine wesentliche und nachhaltige Verbesserung der Informationssicherheit im Bund bewirken. Es regelt in erster Linie das Management der Informationssicherheit und wird dessen Effizienz erhöhen: Ein effizientes Management verbessert nämlich die Sicherheit oft effektiver, wirtschaftlicher und nachhaltiger als Investitionen in technische Massnahmen. Die Praxis hat zudem gezeigt, dass eine Optimierung des Managements der Informationssicherheit - insbesondere wenn letzteres auf ein effektives Risikomanagement gestützt ist - mittelfristig sogar zu Kosteneinsparungen beitragen kann. Der Entwurf sieht zudem mehrere organisatorische Massnahmen vor, die im Vergleich zu heute nicht nur einen besseren Schutz der Informationen bewirken werden, sondern auch zu relativen Kosteneinsparungen führen sollen, sofern sie konsequent umgesetzt werden. So soll z.B. die Erhöhung der Schwellenwerte für die Klassifizierung die Anzahl klassifizierter Informationen und somit den entsprechenden Aufwand reduzieren (s. Ziff. 1.2.3.4). Bei den Personensicherheitsprüfungen (PSP) werden gleichzeitig der Schwellenwert für die Durchführung einer PSP erhöht und die Anzahl Tätigkeiten, für deren Ausübung eine PSP erforderlich (und zulässig) ist, reduziert. Es sollen also inskünftig weniger PSP durchgeführt werden (s. Ziff. 1.2.4). Ferner werden z.B. die vorgeschlagene Standardisierung von Sicherheitsanforderungen und -massnahmen (s. Art. 88), der verbesserte Informationsaustausch zwischen den Bundesbehörden und die Unterstützung der Bundesbehörden durch die Fachstelle des Bundes für Informationssicherheit (s. Art. 84-86) dazu beitragen, dass das Rad nicht bei jedem Projekt neu erfunden werden muss. Die Neuregelung wird schliesslich die internationale Zusammenarbeit im Sicherheitsbereich erleichtern (s. Ziff. 4.2).

Die notwendige Verbesserung der Informationssicherheit beim Bund wird Kosten nach sich ziehen. Diese können jedoch erst nach der Durchführung der Vernehmlassung sachgemäss abgeschätzt werden. Hierzu sind nämlich Organisations- und Ressourcierungsvarianten in Bezug auf die Informationssicherheitsbeauftragten und die Fachstelle des Bundes für Informationssicherheit sowie präzisere Angaben über die Anzahl der bestehenden IKT-Mittel, die inskünftig in die Sicherheitsstufe «sehr hoher Schutz» gehören werden, erforderlich. Der Bundesrat wird die finanziellen und personellen Auswirkungen des Entwurfs in seiner Botschaft transparent auslegen.

Die Kosten, die vom Gesetz direkt verursacht werden, müssen klar von den Kosten derjenigen Massnahmen unterschieden werden, welche die jeweiligen Bundesbehörden im Rahmen des Vollzugs frei beschliessen können. Das Gesetz regelt nämlich nur das Management der Informationssicherheit und legt weder ein zu erreichendes Sicherheitsniveau noch - mit wenigen Ausnahmen (s. unten) - detaillierte Massnahmen fest. Es ist deshalb nicht direkt umsetzbar: Die Bundesbehörden müssen für ihren Zuständigkeitsbereich eigene Ausführungsbestimmungen erlassen und verfügen dabei - ausser im organisatorischen Bereich - über fast unein-

geschränkten Handlungsspielraum (s. Art. 87 Abs. 1). In diesem Rahmen müssen sie das Sicherheitsniveau festlegen, das sie erreichen wollen (s. Art. 5 Abs. 3 Bst. a), und daraus abgeleitet auf Verordnungs-, Weisungs- oder sogar Projektebene die erforderlichen organisatorischen, personellen, technischen und baulichen Anforderungen und Massnahmen beschliessen, um dieses Niveau zu erreichen. Je höher das zu erreichende Sicherheitsniveau festgelegt wird, desto höher werden die Kosten der Sicherheitsmassnahmen ausfallen. Auf diese Kosten hat das Gesetz selbst keinen Einfluss. Sie können deshalb bei der Beurteilung der finanziellen und personellen Auswirkungen des Gesetzes auch nicht beziffert werden.

Alle Bundesbehörden sind bereits heute verpflichtet, Massnahmen zur Gewährleistung der Informationssicherheit zu treffen. Massgebend für die Beurteilung der Kosten sind dementsprechend diejenigen Bestimmungen des Gesetzes, die neue Aufgaben festlegen oder bestehende Aufgaben und Prozesse ändern. Nachfolgend werden die fünf wichtigsten Kostentreiber des Entwurfs aufgeführt:

1. *Organisation, Steuerung, Umsetzung und Überprüfung der Informationssicherheit (Art. 5 Abs. 1 Bst. a)*: Die vom Gesetz verlangte Neuorganisation wird einen nicht zu unterschätzenden organisatorischen Aufwand nach sich ziehen und finanzielle Ressourcen erfordern. Insbesondere in der Aufbau- und der Einführungsphase wird Fachwissen, das den Bundesbehörden heute teilweise fehlt, beschafft werden müssen. Für das Management und den Betrieb einer solchen internen Organisation werden die Informationssicherheitsbeauftragten zuständig sein. Das Gesetz sieht für jede Behörde sowie für die Departemente und die BK mindestens zwei Informationssicherheitsbeauftragte vor. Die Wahrnehmung dieser Aufgaben soll mehrheitlich mit den bestehenden personellen Ressourcen erfolgen. Der tatsächliche personelle Bedarf wird aber unterschiedlich ausfallen und von der Grösse der Behörde oder Organisation (Personalbestand), von ihrem Aufgabenbereich sowie von der Anzahl und der Kritikalität der von ihr eingesetzten IKT-Mittel abhängen.
2. *Verstärktes Kontroll- und Auditwesen (Art. 11 Abs. 2 sowie z.B. Art. 24 Abs. 2)*: Für die Durchführung von Kontrollen, einer geschäftsüblichen Führungsaufgabe, ist grundsätzlich die Linie zuständig. Die Informationssicherheitsbeauftragten werden im Auftrag ihrer Behörde oder Organisation auch selbst Kontrollen und Audits durchführen. Das Gesetz sieht jedoch zwei neue Arten von Kontrollen vor, die finanzielle bzw. personelle Auswirkungen nach sich ziehen werden: eine unabhängige periodische Prüfung der Wirksamkeit der getroffenen Massnahmen (Art. 11 Abs. 2) sowie eine technische Prüfung der Wirksamkeit für die kritischsten IKT-Mittel (Art. 24 Abs. 2). Die daraus entstehenden Kosten werden von der Periodizität solcher Prüfungen abhängen. Als Grössenordnung können folgende Angaben geliefert werden:
   - *Externe Audits (Art. 11 Abs. 2)*: Gemäss Angaben der EFK sind erfahrungsgemäss für eine kleine Querschnittsprüfung ca. 100 Personentage und für eine grosse Querschnittsprüfung ca. 300 Personentage notwendig.
   - *Technische Wirksamkeitsprüfungen (Art. 24 Abs. 2)*: Im Bund werden schätzungsweise 50 bis 70 IKT-Systeme eingesetzt, die inskünftig der neuen Sicherheitsstufe «sehr hoher Schutz» zugeordnet werden und somit einer derartigen Prüfung unterzogen werden müssen. Erfahrungsgemäss entsprechen die Auditkosten (Personalkosten) dabei in der Regel zwischen 0.5% und 2% der gesamten Investitionskosten für das zu auditierende IKT-System.
3. *Personensicherheitsprüfungen (PSP; Art. 32-55)*: Ein Ziel dieses Gesetzes besteht darin, die PSP zu harmonisieren und zu straffen. Mit den vorgeschlagenen Anpassungen sollen inskünftig weniger PSP durchgeführt werden und die entsprechenden Kosten deshalb mittelfristig gesenkt werden.
4. *Betriebssicherheitsverfahren (BSV; Art. 56-80)*: Heute setzt das VBS zur Durchführung des Betriebssicherheitsverfahrens für militärisch klassifizierte Aufträge zwei Vollzeitstellen ein. Die vom Bundesrat vorgeschlagene Erweiterung des BSV auf den zivilen Bereich und auf die anderen Bundesbehörden wird zu einer Zunahme der betreuten Betriebe und damit zu einem zusätzlichen personellen Aufwand führen. Betriebe, die sich um Aufträge ausländischer Behörden bewerben und dafür eine Betriebssicherheitserklärung brauchen, werden die Kosten des durchzuführenden BSV zu tragen haben (Art. 57 Abs. 3)
5. *Fachstelle des Bundes für Informationssicherheit (Art. 86)*: Die Schaffung dieser neuen Fachstelle wird Reorganisationskosten nach sich ziehen. Diese hängen von der administrativen Zuordnung der Fachstelle sowie vom Ausmass der Zusammenlegung bestehender Fachorgane ab. Obwohl die Fachstelle ihre Aufgaben mehrheitlich mit bestehenden personellen Ressourcen der Bundesverwaltung erfüllen soll, wird ein personeller Mehrbedarf vorhanden sein. Die Fachstelle wird nämlich nicht nur für die Bundesverwaltung, sondern auch für die anderen Bundesbehörden tätig sein. Sie wird überdies neue Aufgaben erfüllen müssen, namentlich:
   - Durchführung von Kontrollen und Audits (Art. 86 Abs. 1 Bst. c): S. oben "*verstärktes Kontroll- und Auditwesen*".

- Prüfung der sicherheitsmässigen Eignung bestimmter Prozesse, Mittel und Dienstleistungen (Art. 86 Abs. 1 Bst. e): Diese neue Aufgabe ist für die angestrebte Standardisierung sowie für die internationale Zusammenarbeit notwendig.
- Steuerung und Koordination der Informationssicherheit bei wichtigen behördenübergreifenden Projekten (Art. 86 Abs. 1 Bst. f). Mit dieser neuen Aufgabe soll einerseits sichergestellt werden, dass bei derartigen Projekten die Zuständigkeiten klar geregelt werden, andererseits aber auch, dass anerkannte Experten das Projekt sicherheitsmässig begleiten.
- Erarbeitung oder Festlegung von standardisierten Sicherheitsanforderungen und Massnahmen nach dem Stand der Lehre und der Technik (Art. 88 Abs. 1 und 2). Diese Massnahme ist für einen möglichst einheitlichen Vollzug notwendig. Sie kann aber auch zu Kosteneinsparungen führen (s. oben).

Der Bundesrat wird die Organisation der Fachstelle auf Verordnungsebene regeln (Art. 86 Abs. 3). Dabei wird er auch entscheiden, welche bestehenden Organe zusammengelegt werden sowie wie und mit welchen Mitteln die Fachstelle ihre Aufgaben erfüllen wird.

3.2 Auswirkungen auf die Kantone und Gemeinden

Die Kantone sind nur betroffen, soweit sie im unmittelbaren Auftrag und unter Aufsicht des Bundes sicherheitsempfindliche Tätigkeiten ausüben (s. Art. 2 Abs. 2 Bst. f sowie Art. 89). Sie müssen in diesem Fall die nach diesem Gesetz erforderlichen Sicherheitsmassnahmen treffen und sind zudem verpflichtet, eine Dienststelle als Ansprechpartner für die zuständigen Bundesbehörden zu bezeichnen. Der Bundesrat soll die Durchführung der Personensicherheitsprüfungen bei Bediensteten der Kantone sowie die Überprüfung der Umsetzung der Massnahmen durch die Kantone auf Verordnungsstufe regeln. Er wird dabei die Autonomie der Kantone berücksichtigen. Die Auswirkungen auf die Kantone werden also gering ausfallen.

3.3 Auswirkungen auf die Volkswirtschaft

Dritte werden nur indirekt vom Gesetz erfasst, das heisst, wenn sie im Rahmen eines Vertrags mit Informationen oder IKT-Mitteln des Bundes umgehen sollen. Betriebe, die sich für zivile Aufträge des Bundes bewerben, die eine sicherheitsempfindliche Tätigkeit einschliessen, werden aufgrund der Einführung des einheitlichen Betriebssicherheitsverfahrens einem solchen Verfahren unterstellt. Mit dieser Unterstellung ist zwar ein geringer zusätzlicher administrativer Aufwand verbunden. Umgekehrt wird dadurch jedoch die Wettbewerbsfähigkeit von Schweizer Unternehmen verbessert, weil das Gesetz die Grundlage für die Abgabe behördlicher Sicherheitserklärungen zu Gunsten Privater schafft, die sich für ausländische oder internationale klassifizierte Aufträge bewerben und dafür eine nationale Sicherheitserklärung benötigen (s. Art. 56-80).

Die Volkswirtschaft wird zudem vom verbesserten Schutz von Geschäfts- und Fabrikationsgeheimnissen, die den Bundesbehörden anvertraut werden, profitieren.

3.4 Auswirkungen auf die Gesellschaft

Die Gesellschaft ist in zweifacher Hinsicht betroffen. Einerseits wird ihr Vertrauen in die sichere Bearbeitung von Informationen durch die Bundesbehörden erhöht. Sie erhält die Gewissheit, dass der Bund die sie betreffenden Informationen (insbesondere Personendaten sowie Geschäfts- und Fabrikationsgeheimnisse) als wichtig betrachtet und sie entsprechend schützt. Andererseits werden die Grundsätze der Klassifizierung von Informationen offen gelegt. Dies ist insbesondere in Bezug auf das Öffentlichkeitsprinzip wichtig, dessen Wirkung durch das vorliegende Gesetz keinesfalls beeinträchtigt werden darf.

3.5 Verhältnis zu nationalen Strategien des Bundesrates

3.5.1 Strategie für eine Informationsgesellschaft in der Schweiz

Der vorliegende Vorentwurf wurde im Vorhaben-Katalog Informationsgesellschaft 2011–2015 (Stand Juni 2013) unter dem Handlungsfeld "Sicherheit und Vertrauen" aufgenommen. Das Gesetz wird klare Grundlagen für die Umsetzung der Sicherheitsanforderungen in den Projekten, die vom Bund durchgeführt werden, schaffen. Zur Strategie: S. Ziff. 1.2.1.1.

3.5.2 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

Zur NCS: S. Ziff. 1.1.2.2; zum Verhältnis zwischen der NCS und dem Entwurf: s. Ziff. 1.2.6; zur Unterstützung der KI-Betreiber im Bereich der Informationssicherheit: s. Art. 81-83.

3.5.3 Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI-Strategie)

Die SKI-Strategie vom 27. Juni 2012 (BBl 2012 7715) hat zum Ziel, die Resilienz der Schweiz im Zusammenhang mit KI zu verstärken. Die Strategie bezeichnet dazu verschiedene Massnahmen in zwei Bereichen. Der Selbstschutz wird verbessert, indem die zuständigen Stellen integrale Schutzkonzepte erarbeiten und

umsetzen. Darin werden infrastrukturspezifische Risiken identifiziert und reduziert. Im Infrastrukturübergreifenden Bereich werden die Zusammenarbeit der Akteure (Behörden, Betreiber) aus den verschiedenen KI-Sektoren verbessert und die Verletzlichkeit von Gesellschaft, Wirtschaft und Staat durch schwerwiegende Ausfälle verringert. Zu diesem Zweck werden Planungen zur Schadensbewältigung bei schwerwiegenden Ausfällen und zur subsidiären Unterstützung der KI-Betreiber bei solchen Ereignissen erarbeitet. Der Bundesrat will die KI-Betreiber in ihren eigenen Schutzbestrebungen unterstützen. Dabei soll auch die grösstmögliche Resilienz im Hinblick auf die Informationssicherheit erreicht werden.

Verschiedene Massnahmen der SKI-Strategie zielen direkt auf Anliegen der verbesserten Informationssicherheit. So sieht z.B. ihre Massnahme 7 die Schaffung von formell-gesetzlichen Grundlagen zur Sicherheitsüberprüfung von ausgewähltem Personal der KI-Betreiber vor. Die Durchführung von Sicherheitsprüfungen soll grundsätzlich im Sinne der NCS in der Spezialgesetzgebung vorgesehen werden (s. Ziff. 1.1.2.2 sowie Art. 3 Abs. 3). Mit dem Entwurf wird auch die Schaffung einer Grundlage zur Durchführung von Vertrauenswürdigkeitsprüfungen bei bestimmten Angestellten der Swissgrid im StromVG beantragt (s. Art. 26a StromVG). Das ISG unterstützt somit auch die Umsetzung der SKI-Strategie.

4 Rechtliche Aspekte

4.1 Verfassungsmässigkeit

Nach Art. 42 BV benötigt der Bundesgesetzgeber für seine Regelungen eine (ausdrückliche oder implizite) Verfassungsgrundlage. Für die angestrebte Gesetzgebung im Bereich der Informationssicherheit bestehen hinreichende Verfassungsgrundlagen. Formal handelt es sich bei den zu erlassenden Regelungen vorweg um Organisationsbestimmungen für die Bundesbehörden. Das Organisationsrecht des Bundes wird zwar als Gesetzgebungskompetenz beim Katalog der Kompetenzausscheidung zwischen Bund und Kantonen in der BV nicht ausdrücklich erwähnt, doch führt Art. 164 Abs. 1 Bst. g BV bei den Zuständigkeiten der Bundesversammlung "die Organisation und das Verfahren der Bundesbehörden" unter den Gegenständen auf, die in der Form des Bundesgesetzes zu erlassen sind (s. etwa den Ingress zum ParlG). Im Weiteren wird in der geltenden Organisationsgesetzgebung auch etwa auf Art. 173 Abs. 2 BV verwiesen, welcher der Bundesversammlung alle Geschäfte zuweist, die in die Zuständigkeit des Bundes fallen und keiner anderen Behörde zugewiesen sind (s. etwa den Ingress (mit Fussnote 1) zum RVOG, zum BGÖ sowie zum ZNDG).

Inhaltlich sollen die Regelungen primär der Wahrung der Sicherheit des Landes im Innern und gegen aussen dienen sowie die Entscheidungs- und Handlungsfähigkeit der Behörden schützen. Insofern stützen sich die Regelungen auch auf Art. 54 Abs. 1 und 2 BV (Beziehungen zum Ausland und Wahrung der äusseren Sicherheit) sowie auf Art. 57 Abs. 1 BV, der den Bund und die Kantone beauftragt, "... im Rahmen ihrer Zuständigkeiten für die Sicherheit des Landes ..." zu sorgen (s. etwas den Ingress zum BWIS).

Nicht unter die erwähnten Ziele fallen die Bestimmungen zum Betriebssicherheitsverfahren, soweit sie für Betriebe vorgesehen sind, die eine Betriebssicherheitserklärung benötigen, um sich für klassifizierte Aufträge ausländischer oder internationaler Behörden bewerben zu können. Diese Regelung wird durch Art. 101 BV abgedeckt, der die Grundlage für die Förderung der Aussenwirtschaft bildet. Die Bestimmungen zum Schutz der KI können sich sowohl auf die Grundlagen im Bereich der inneren und äusseren Sicherheit als auch auf die Kompetenzen des Bundes im Bereich der Landesversorgung (Art. 102 BV) abstützen. Für die Armee kann auf Art. 60 BV verwiesen werden, der die Organisation der Armee zur Bundessache erklärt.

4.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Die Schweiz unterhält mit verschiedenen Staaten und internationalen Organisationen Informationsschutzvereinbarungen (ISA) bzw. Sicherheitsabkommen (*Security Agreements* bzw. *Security Arrangements*; s. SR 0.514). Mit diesen Staatsverträgen hat sich die Schweiz zur Einhaltung gewisser Standards zum Schutz klassifizierter Informationen verpflichtet. Neben der EU hat die Schweiz auch ISA mit der NATO (1997) im Rahmen des Engagements "Partnerschaft für den Frieden" sowie mit der ESA (2004) abgeschlossen. Diese Verträge enthalten einerseits materielle Bestimmungen wie beispielsweise einheitliche Schutzmechanismen für das Bearbeiten von klassifizierten Informationen oder die gegenseitige Anerkennung von Sicherheitsbescheinigungen. Andererseits enthalten sie auch organisatorische und strukturelle Standards. So wird jeweils die für die Umsetzung der Sicherheitsmassnahmen zuständige Stelle genannt (*National Security Authority* oder *Designated Security Authority*). Insbesondere im COMSEC-Bereich werden solche nationale Anlaufstellen verlangt, welche einheitliche Standards im IKT-Bereich festlegen (*National Accreditation Authority* bzw. *Security Accreditation Authority*). Die Fachstelle des Bundes für Informationssicherheit (Art. 86) wird diese Aufgaben und die Verantwortlichkeiten im internationalen Verhältnis übernehmen.

4.3 Erlassform

Der Bundesrat ist bereits in seinem Beschluss vom 12. Mai 2011 zur Erarbeitung von formell-gesetzlichen Grundlagen für den Informationsschutz davon ausgegangen, dass die wesentlichen Regelungen über die Informationssicherheit in der Form des Bundesgesetzes festzulegen sind. Einerseits handelt es sich um wesentliche Organisations- und Verfahrensregelungen für die Bundesbehörden (Art. 164 Abs. 1 Bst. g BV), die infolge der Notwendigkeit der einheitlichen Geltung auch behördenübergreifende Wirkungen entfalten müssen. Andererseits handelt es sich um Bestimmungen, die insbesondere im Bereich der Sicherheitsprüfungen erhebliche Eingriffe in grundrechtlich geschützte Positionen zur Folge haben.

4.4 Delegation von Rechtsetzungsbefugnissen

Die vom Gesetz verpflichteten Behörden werden insbesondere bei der Regelung der Aufgaben, Zuständigkeiten und organisatorischen Massnahmen in ihren Zuständigkeitsbereichen Ausführungsrecht erlassen müssen. Es handelt sich dabei im Grossen und Ganzen nicht um gesetzesvertretendes Verordnungsrecht im Sinne der anerkannten Delegationsgrundsätze, sondern um eigentliches (selbständiges) Ausführungsrecht, dessen materielle Grundzüge im Gesetz angelegt sind und das Privaten keine unmittelbaren Rechte einräumt oder Pflichten auferlegt. Die Verfassung selbst spricht den verpflichteten Behörden grundsätzlich die Kompetenz zum Erlass derartigen Ausführungsrechts zu. Deshalb wird es im Gesetzesentwurf nicht detailliert aufgeführt. Ausdrückliche Delegationsnormen enthält das Gesetz hingegen dort, wo es:

- den Erlass von Ausführungsbestimmungen oder gesetzesvertretendem Verordnungsrecht durch die betroffenen Behörden zur Pflicht macht (z.B. Art. 5 Abs. 1, Art. 19 Abs. 1, Art. 22 Abs. 1, usw.);
- den Bundesrat zum selbständigen Abschluss völkerrechtlicher Verträge ermächtigt (Art. 90).