Deutscher Bundestag **Drucksache 20/14887**

20. Wahlperiode 04.02.2025

Antwort

der Bundesregierung

auf die Kleine Anfrage der Fraktion der CDU/CSU
– Drucksache 20/14226 –

Digitale Souveränität in der Bundesverwaltung – Beschaffung und Einsatz von IT-(Sicherheits-)Produkten durch den Bund als öffentlichen Auftraggeber

Vorbemerkung der Fragesteller

Am 19. Juli 2024 kam es weltweit zu IT-Ausfällen in zahlreichen Branchen. Betroffen waren auch Unternehmen und Betreiber Kritischer Infrastrukturen in Deutschland (www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240719_weltweite_IT-Ausfaelle.html). Ein fehlerhaftes Update einer IT-Sicherheitssoftware einer US-amerikanischen Firma sorgte für Abstürze von Computern mit Windows-Betriebssystemen. Gleichzeitig gab es auch Probleme bei der Verbindung zu Apps und Dienstleistungen des Clouddienstes Microsoft 365 innerhalb von Microsofts Cloudplattform Azure. Durch die Vorfälle kam es beispielsweise zur vorübergehenden Einstellung des Flugbetriebs am Flughafen Berlin-Brandenburg, zu der Schließung von Ambulanzen und der Verschiebung von aufschiebbaren Eingriffen am Universitätsklinikum Schleswig-Holstein und zu einem späteren Handelsstart an der Börse London. Die technischen Probleme hatten auch Folgen für Stadtverwaltungen. In Pforzheim etwa waren der E-Mail-Verkehr und die Telefonanlage gestört und das Bürgerzentrum, die Ausländerbehörde sowie die Kfz-Zulassungsbehörde nur eingeschränkt erreichbar (www.spiegel.de/netzwelt/web/flughafen-ber-muss-nach-it-stoerung-betrieb-einstellen-weltweite-netz-ausfaelle-a-f318d93e-aacd-4f46-870b-6de1fd9a8b6d). In der Presse firmierte das Ereignis als „größter IT-Ausfall der Geschichte“ (www.businessinsider.de/wirtschaft/crowdstrike-diese-firma-steckt-hinter-groesster-it-panne-der-geschichte/).

Die Bundesverwaltung und die Bundesregierung selbst waren von dem IT-Vorfall zwar nicht betroffen (www.spiegel.de/netzwelt/web/flughafen-ber-muss-nach-it-stoerung-betrieb-einstellen-weltweite-netz-ausfaelle-a-f318d93e-aacd-4f46-870b-6de1fd9a8b6d). Allerdings wurde die Brisanz von digitalpolitischen Abhängigkeiten und daher die Relevanz digitaler Souveränität im Allgemeinen deutlich. Das gilt erst recht vor dem Hintergrund, dass die Bundesverwaltung vom einwandfreien Funktionieren und der uneingeschränkten Verfügbarkeit von IT-Systemen abhängig ist (www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/IT-Sicherheitskriterien/it-sicherheitskriterien_node.html; www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Grundsaetzliche-Aussagen/grundsaetzliche-aussagen_node.html).

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 4. Februar 2025 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

In diesem Kontext gibt es eine Reihe von Vorschlägen für Maßnahmen zur Steigerung der digitalen Souveränität. Eine Studie des Leibniz-Zentrums für Europäische Wirtschaftsforschung (ZEW) in Mannheim vom Oktober 2024, die im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) angefertigt wurde, betont wie schon in der Vorgängerstudie aus dem Jahr 2021, dass „[…] die Politik die digitale Souveränität mit einer innovativen Beschaffung, die die Spezifika von Start-ups oder Open-Source-Lösungen berücksichtigt, unterstützen [kann]. Dies kann zur Entstehung von alternativen Angeboten beitragen und Hürden hinsichtlich Interoperabilität und Lock-in-Effekten entgegenwirken." (de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-schwerpunkt-digitale-souveraenitaet.pdf?__blob=publicationFile&v=5, S. 42) Insbesondere dem Bereich der IT-Sicherheitstechnologien sollte die Bundesregierung den Ergebnissen der Studie zufolge die höchste Priorität bei der Vermeidung von digitalen Abhängigkeiten einräumen (de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-schwerpunkt-digitale-souveraenitaet.pdf?__blob=publicationFile&v=5, S. 25 f.).

Die 2. Digitalministerkonferenz weiß offenbar um diese Priorisierungsnotwendigkeit. Mit ihrem Beschluss vom 18. Oktober 2024 stellt sie fest, dass angesichts der zunehmenden Digitalisierung EU-Mitgliedstaaten in der Lage sein müssen, Leistungen im Bereich Cybersicherheit einschließlich Informationssicherheit schnellstmöglich zu beschaffen, um ihre wesentlichen Sicherheitsinteressen zu wahren. Die bisherigen Vorschriften des Vergaberechts erlauben weitreichende Ausnahmen für militärische Zwecke. Sie schlägt vor, Änderungen im Vertrag über die Arbeitsweise der Europäischen Union (AEUV) dahin gehend vorzunehmen, damit auch die Beschaffung von Cyber- und Informationssicherheitsleistungen mit Ausnahmen belegt werden können beziehungsweise jedenfalls gesichert in den Vergabebereich Verteidigung und Sicherheit fallen. Denn nach aktuellem Stand ist es den EU-Mitgliedstaaten verwehrt, in vergleichbarer Art und Weise zu Beschaffungen für militärische Zwecke Beschaffungen zur Härtung der Cyber- und Informationssicherheit tätigen zu können. Den Mitgliedstaaten steht im Bereich Cyber- und Informationssicherheit aktuell keine mit Artikel 346 Absatz 1 Buchstabe b AEUV vergleichbare Rechtsgrundlage zur Verfügung. Zudem wurde die in Artikel 346 Absatz 2 AEUV referenzierte Liste von Waren, Gütern und Dienstleistungen, auf die die Ausnahmen angewendet werden können, seit dem 15. April 1958 nicht mehr überarbeitet. Insbesondere stellt § 117 Absatz 1 Nummer 1 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) der 2. Digitalministerkonferenz zufolge keine vergleichbare Rechtsgrundlage dar. Zwar erlaubt § 117 Absatz 1 Nummer 1 GWB seinem Wortlaut nach Ausnahmen vom Vergaberecht auch dann, wenn ein Auftrag nicht der Erzeugung oder dem Handel mit Kriegsmaterial dient, sondern ausschließlich Verteidigungs- und Sicherheitsaspekte umfasst. Allerdings ist der Prüfungsmaßstab des § 117 Absatz 1 Nummer 1 GWB deutlich strenger (www.berlin-brandenburg.de/wp-content/uploads/TOP_9_SH_Beschluss_Leistungsbeschaffung_Info-_und-Cybersicherheit.pdf).

Weiterhin bereitete das Bundesministerium für Wirtschaft und Klimaschutz unabhängig davon im Rahmen der Wachstumsinitiative ein sogenanntes Vergabetransformationspaket zur Reform des Vergaberechts ober- und unterhalb der EU-Schwellenwerte vor, insbesondere mit dem Ziel, Vergabeverfahren zu beschleunigen. Das Vorhaben beabsichtigt des Weiteren, eine neue Möglichkeit einzuführen, Unternehmen aus bestimmten Drittstaaten in kritischen Bereichen von Auftragsvergaben auszuschließen. Darüber hinaus sollten umweltbezogene und soziale Aspekte als Vergabekriterien definiert werden (background.tagesspiegel.de/digitalisierung-und-ki/briefing/wirtschaftsministerium-will-vergaberecht-per-gesetz-vereinfachen; www.bmwk.de/Redaktion/DE/Pressemitteilungen/2024/09/20240930-habeck-vergabetransformation.html; background.tagesspiegel.de/digitalisierung-und-ki/briefing/vergabetransformationspaket-haelt-es-was-es-verspricht). Der zugehörige Gesetzentwurf wurde am 27. November 2024 im Kabinett von der Bundesregierung verabschiedet (www.bundesregierung.de/breg-de/bundesregierung/bundeskanzleramt/novelle-vergaberecht-2322048).

Vor diesem Hintergrund möchten die Fragesteller aufbauend auf ihrer Kleinen Anfrage vom 23. August 2023, die von der Bundesregierung am 9. Oktober 2023 auf Bundestagsdrucksache 20/8707 beantwortet wurde, aktuelle Sachstände zur Entwicklung, zur Beschaffung und zum Einsatz von IT-Sicherheitsprodukten in der Bundesverwaltung sowie die Bestrebungen der Bundesregierung zur Umsetzung von Vorschläge zur Steigerung der digitalen Souveränität im Bereich der IT-Sicherheitsanwendungen erfragen (Hinweis: Bei den folgenden Fragen mit Bezug zur Bundesverwaltung sind die Nachrichtendienste des Bundes auszunehmen).

Vorbemerkung der Bundesregierung

Cyberkriminelle und staatliche Akteure professionalisieren ihre Arbeitsweise. Sie sind technisch auf dem neusten Stand und agieren aggressiv. Längst haben sie Strukturen für ihre kriminellen Dienstleistungen etabliert. Deutschland setzt der Bedrohung eine tragfähige Cybersicherheitsarchitektur entgegen. Diese Cybersicherheitsarchitektur muss unter allen Umständen funktionsfähig bleiben.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet die Sicherheitslage in den fünf Dimensionen Bedrohung, Angriffsfläche, Gefährdung, Schadwirkung und Resilienz, wobei die Resilienz den vier anderen Dimensionen positiv entgegenwirkt (vgl. https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html).

Cyberbedrohungen gingen im vergangenen Jahr von diversen Gruppierungen aus. APT-Gruppen (= Advanced Persistent Threats) betrieben beispielsweise Cyberspionage und starteten Angriffe auf Behörden der auswärtigen Angelegenheiten, der Verteidigung und der öffentlichen Sicherheit und Ordnung. Auch Unternehmen und Institutionen, die in diesen Bereichen tätig sind, waren betroffen. Darüber hinaus wurde die arbeitsteilige cyberkriminelle Schattenwirtschaft weiterhin professioneller: Sogenannte Access Broker handelten mit erbeuteten Zugangsdaten. Andere Cybercrime-Gruppen nutzten Zero-Day-Schwachstellen (d. h. Schwachstellen, für die es noch kein Update gibt), zum Datendiebstahl.

Auch die Angriffsflächen vergrößerten sich mit der weiter fortschreitenden Digitalisierung und damit einhergehenden Vernetzung von Einrichtungen der Bundesverwaltung untereinander.

Über alle Arten von Cyberbedrohungen nehmen die Gefährdungen stetig weiter zu. Von einem Ransomware-Angriff auf einen kommunalen IT-Dienstleister Ende Oktober 2023 waren beispielsweise 72 kommunale Kunden mit rund 20 000 kommunalen Arbeitsplätzen betroffen. Die Folge waren teils monatelange Ausfallzeiten.

Eine weitere Folge erfolgreicher Cyberangriffe sind exorbitante „Lösegeldzahlungen“ für durch Ransomware-Angriffe verschlüsselte Daten. Für gestohlene exfiltrierte Daten wurde dabei im Schnitt fast dreimal so viel gezahlt wie für erbeutete verschlüsselte Daten.

In allen Dimensionen hat sich die IT-Sicherheitslage deutlich verschärft:

Der russische Angriffskrieg auf die Ukraine führt unmittelbar zu vermehrten Attacken auf Verbündete der Ukraine (u. a. Deutschland) durch russlandfreundliche Cybergruppierungen oder auch mutmaßlich staatliche Stellen. Dabei müssen ebenfalls Sekundäreffekte zur Zerstörung von IT-Infrastruktur berücksichtigt werden.

Die stetig wachsende Komplexität der IT-Landschaft mit zunehmender Vernetzung von Behörden untereinander, mit Unternehmen, Bürgern sowie Cloud-Diensten erweitert die Wirkungsbreite von Angriffen auf einzelne Institutionen.

Gleichzeitig erwartet die Bevölkerung zu Recht einen auch mit IT funktionierenden Rechtsstaat und einen Fortschritt der Digitalisierung der öffentlichen Verwaltung.

Mit der Expertise des BSI, der Strafverfolgungsbehörden und den Verantwortlichen für Informationssicherheit in der Bundesverwaltung wird der oben dargestellten Gefährdungslage effektiv entgegengewirkt.

Durch die Veröffentlichung sensibler Informationen wäre die in langjährigen Prozessen erarbeitete Resilienz der Informationstechnik des Bundes erheblich gefährdet.

Der Aufbau von Expertise, IT-Sicherheitsinfrastruktur, Prozessen und Resilienzfaktoren beansprucht umfangreiche Ressourcen und insbesondere Zeit. Der Wiederaufbau nach einem erfolgreichen Cyberangriff könnte aber einen solchen Schaden anrichten, dessen Behebung potentiell ein Vielfaches davon kosten würde.

Mit Blick auf die in immer kürzeren Abständen auftretenden kritischen Sicherheitslücken, den Zeitbedarf für das Patchen dieser Lücken und vor dem Hintergrund einer unbekannten Menge an möglichen Zero-Day-Exploits ist jederzeit mit Angriffen zu rechnen. Sollte mit absehbar verfügbaren Mitteln derzeit kein Angriff durchführbar sein, führt dies angesichts der schnellen technologischen Entwicklung zu keiner Reduzierung der Gefährdungslage, denn einmal veröffentlichte Informationen zur Sicherheitsarchitektur und deren Änderung lassen sich über die Zeit aggregieren und analysieren und mit zukünftigen technischen Möglichkeiten für einen erfolgreichen Cyberangriff auf die IT der Bundesverwaltung ausnutzen. Im Bereich der Informationssicherheit kommt der strategischen Vorausschau daher eine überragende Bedeutung zu.

Bereits wenige Kenntnisse über mögliche Schwachstellen reichen Cyberkriminellen oder staatlichen Akteuren aus, um die gesamte IT-Infrastruktur von Behörden unbrauchbar zu machen (vgl. u. a. oben skizzierte Angriffe auf Kommunalverwaltungen, Angriff auf Berliner Kammergericht, Hackerangriff auf den Deutschen Bundestag).

Darüber hinaus spielen bedeutende technische Entwicklungen bösartigen Akteuren im digitalen Raum in die Karten. Beispielsweise kann heute in einer noch vor kurzer Zeit kaum absehbaren Qualität künstliche Intelligenz genutzt werden, um aus der (auch aggregierten) Darstellung von Sicherheitsprodukten oder Offenlegung von aktuellen Softwareentwicklungen konkrete Angriffsvektoren abzuleiten. In der Folge würde sich die Lage in allen vier Dimensionen Bedrohung, Angriffsfläche, Gefährdung und Schadwirkung dramatisch verschlechtern. Die Sicherstellung der Staats- und Regierungsfunktion wäre massiv gefährdet.

Die Bundesregierung beantwortet die im Rahmen des parlamentarischen Fragerechts angefragten Sachverhalte gegenüber dem Deutschen Bundestag grundsätzlich öffentlich, transparent und vollständig, um dem verfassungsrechtlich verbrieften Aufklärungs- und Informationsanspruch des Deutschen Bundestages zu entsprechen. Soweit erfragte Informationen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind oder den Grundrechten Dritten entgegenstehen, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann, und gegebenenfalls alternative Formen der Informationsvermittlung zu suchen, die das Informationsinteresse des Parlaments unter Wahrung der berechtigen Geheimhaltungsinteressen der Regierung befriedigen (Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 124, 161,193).

Nach sorgfältiger Abwägung ist die Bundesregierung zu der Auffassung gelangt, dass die Beantwortung der Kleinen Anfrage nicht durchgängig offen erfolgen kann.

Die Antwort zur Frage 3 wird als „VS - NUR FÜR DEN DIENSTGEBRAUCH“ gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern und für Heimat (BMI) zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) eingestuft und als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.*

Die IT-Infrastruktur der Bundesregierung ist jeden Tag einer Vielzahl unterschiedlicher Angriffe ausgesetzt. Zur Aufrechterhaltung der Staats- und Regierungsfunktion ist diese Infrastruktur angemessen zu schützen. Eine Beeinträchtigung oder sogar ein Ausfall aufgrund erfolgreicher Cyberangriffe muss auch in der Zukunft bestmöglich verhindert werden.

Informationen zu den in der Frage aufgeführten IT-Sicherheitsprodukten beziehen sich unmittelbar auf die Fähigkeiten der Abwehr von Cybergefährdungen der Bundesbehörden. Ein Bekanntwerden der Information würde das Staatswohl in hohem Maß gefährden, denn damit würde es etwaigen Angreifern ermöglicht, konkrete Hinweise zu den in der Bundesverwaltung eingesetzten Schutzmaßnahmen zu erhalten.

Die Fragen 6 bis 11,13 bis 25 können auch nicht in eingestufter Form beantwortet werden. Es gelten die oben aufgeführten Erwägungen. Es besteht das Risiko aufgrund der Informationen zu den erfragten IT-Sicherheitsprodukten und Softwareentwicklungen unmittelbar auf die Fähigkeiten der Abwehr von Cybergefährdungen der Bundesbehörden schließen zu können.

Die darüber hinaus erfragte Zuordnung eingesetzter IT-Sicherheitsprodukte auf einzelne Ressorts oder Behörden würde es Angreifern deutlich vereinfachen, Sicherheitslücken auszunutzen und einzelne Teile der Bundesregierung gezielt anzugreifen. Die insoweit erbetenen Informationen zielen auf den Einsatz von IT-Sicherheitsprodukten in jeder einzelnen Bundesbehörde ab. Mit der Beantwortung würde offengelegt, wie sich einzelne Ressorts oder Behörden vor Cyberangriffen schützen. Dies würde potentiellen Angreifern wichtige Hinweise für etwaige Angriffe liefern. Eine Aufschlüsselung nach Ressorts oder Behörden könnte außerdem zu Rückschlüssen über die Sicherheitserheblichkeit der dort jeweils verarbeiteten Daten führen und so lohnende Angriffsziele identifizieren. Wird beispielsweise eine Sicherheitslücke bei einem der eingesetzten Produkte bekannt, könnten Angreifer diese schnell ausnutzen, da bekannt ist, welche Behörde dieses Produkt einsetzt. Dies gefährdet die Arbeitsfähigkeit und damit unmittelbar die Erfüllung des gesetzlichen Auftrags der betroffenen Behörden. Aufgrund der Vernetzung der Behörden untereinander hätte eine solche Ausnutzung einer Schwachstelle erhebliche Auswirkungen auf die Informationssicherheit der gesamten Bundesverwaltung und könnte unmittelbar die Gewährleistung der Handlungsfähigkeit der Bundesverwaltung gefährden.

Aus den genannten Gründen muss potentiellen Angreifern verborgen bleiben, welche IT-Sicherheitsprodukte in welchen Behörden zum Schutz der Infrastrukturen der Informations- und Kommunikationstechnik (IKT) und darin verarbeiteten Daten aktuell eingesetzt werden.

Unter Kenntnis der durch die Bundesverwaltung eingesetzten Produkte könnten Angreifer produktspezifische Schwachstellen ausmachen und diese gezielt ausnutzen. Vor allem in der Zusammenschau mit der Antwort der Bundesregierung zur Kleinen Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache

* Das Bundeskanzleramt hat die Antwort als „VS - NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

20/8707 ließe sich durch Aggregation und direkten Vergleich detaillierte Erkenntnisse ableiten, die die Entwicklung des Einsatzes und der Beschaffung von IT-Sicherheitsprodukten in der Bundesverwaltung zeigen.

Die Handlungsfähigkeit der Bundesregierung ist auch dadurch gefährdet, wenn in diesem Kontext die Geheimschutzbetreuung nichtöffentlicher Stellen bekannt wird. Denn das Bekanntwerden der Geheimschutzbetreuung nichtöffentlicher Stellen kann diese zum Ziel von besonderen Gefährdungen, insbesondere durch ausländische Nachrichtendienste, werden lassen. Dies erhöht die Gefahr der Kompromittierung von Verschlusssachen, auch von Verschlusssachen, die nicht im Kontext der Fragestellung stehen. Zudem erleichtert dies Angriffe auf die Lieferkette der IT-Sicherheitsprodukte mit der möglichen Folge, dass die IT-Sicherheitsfunktion des Produktes erlischt. Gerade durch die Nichtoffenbarung der Geheimschutzbetreuung soll verhindert werden, dass Verschlusssachen in den nichtöffentlichen Stellen zusätzlich gefährdet werden. Des Weiteren können diese Informationen Geschäftsgeheimnisse im Sinne des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) darstellen und sind entsprechend zu schützen.

Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Aufgabenerfüllung der Behörden des Bundes nicht ausreichend Rechnung tragen, weil insoweit auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, 78 [139]). Schon die Angabe, mittels welcher technischer Mittel die Behörden des Bundes den Cybergefahren begegnen, könnte zu einer Analyse der Verwundbarkeiten und Änderung des Angriffsverhaltens führen, die eine weitere Abwehr der Cybergefahren unmöglich machen würde. In diesem Fall wäre ein Ersatz durch andere Instrumente nicht möglich.

Würden potentielle Angreifer detaillierte Kenntnis über Verbreitung und Details der jeweiligen IT-Sicherheitsprodukte erhalten, wäre ein Angriff auf die jeweilige Behörde deutlich einfacher zu gestalten und mit sehr hoher Erfolgsaussicht verbunden. Zum Beispiel würde die Kenntnis über die jeweilige Firmware oder Softwarestand die Angreifenden in die Lage versetzen, gezielt Zero-Day-Exploits der eingesetzten IT-Sicherheitsprodukte zu identifizieren oder zu erwerben und diese Schwachstelle auszunutzen. für Zero-Day-Exploits i. d. R. keine Gegenmaßnahmen wie z. B. Sicherheitsupdates des Herstellers möglich sind, wären die Behörden einem Angriff ungeschützt ausgesetzt.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl und entgegenstehende Grundrechte Dritte gegenüber dem parlamentarischen Informationsrecht in diesem Fall überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber der Pflicht der Aufrechterhaltung der Staats- und Regierungsfunktion der Bundesrepublik Deutschland zurückstehen.

1. Für welche IT-Sicherheitsprodukte wurden mit Referenz zur Antwort der Bundesregierung zu Frage 9 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707 seit 4. Oktober 2023 Zertifizierungen für den Einsatz in der Bundesverwaltung nach welchem Zertifizierungsschema beim Bundesamt für Sicherheit in der Informationstechnik (BSI) beantragt, bei welchen davon wurde eine positive Zertifizierungsaussage getroffen, und bei welchen davon befand sich der Hauptsitz des Herstellers des IT-Sicher-
heitsprodukts außerhalb der EU (bitte nach Produktname, Art der beantragten Zertifizierung, Zertifizierungsaussage, Hersteller, Hauptsitz des Herstellers aufschlüsseln)?

   a) Für IT-Sicherheitsprodukte des Produkttyps Firewall?

b) Für IT-Sicherheitsprodukte des Produkttyps Datendiode?

c) Für IT-Sicherheitsprodukte des Produkttyps VS Guard?

d) Für IT-Sicherheitsprodukte des Produkttyps Schadsoftwareerkennung?

e) Für IT-Sicherheitsprodukte des Produkttyps Hypervisor?

f) Für IT-Sicherheitsprodukte des Produkttyps Separation Kernel?

g) Für IT-Sicherheitsprodukte des Produkttyps Mobile Device Management?

h) Für IT-Sicherheitsprodukte des Produkttyps Netzwerkmanagement?

i) Für IT-Sicherheitsprodukte des Produkttyps Schlüsselspeicher- und Verteilkomponente?

j) Für IT-Sicherheitsprodukte des Produkttyps Key-Management-Software?

k) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Funksysteme?

l) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Satellitensysteme?

m) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für analoge Leitungen?

n) Für IT-Sicherheitsprodukte des Produkttyps Dateiverschlüsselung?

o) Für IT-Sicherheitsprodukte des Produkttyps Festplattenverschlüsselung?

p) Für IT-Sicherheitsprodukte des Produkttyps Sicherer mobiler Datenträger?

q) Für IT-Sicherheitsprodukte des Produkttyps Faxverschlüsselung?

r) Für IT-Sicherheitsprodukte des Produkttyps Telefonverschlüsselung?

s) Für IT-Sicherheitsprodukte des Produkttyps Funkgeräte?

t) Für IT-Sicherheitsprodukte des Produkttyps E-Mail-Verschlüsselung?

u) Für IT-Sicherheitsprodukte des Produkttyps VPN-Client?

v) Für IT-Sicherheitsprodukte des Produkttyps Sichere mobile Lösung?

w) Für IT-Sicherheitsprodukte des Produkttyps Sicherer Messenger?

x) Für IT-Sicherheitsprodukte des Produkttyps VPN-Gateway?

y) Für IT-Sicherheitsprodukte des Produkttyps Datenschleusen (optional auch mit Datenwäschekomponente)?

z) Für IT-Sicherheitsprodukte Verschlüsselung Layer 1?

aa) Für IT-Sicherheitsprodukte Verschlüsselung Layer 2?

bb) Für IT-Sicherheitsprodukte des Produkttyps Intrusion Detection System?

cc) Für IT-Sicherheitsprodukte Threat Detection System?

Die Fragen 1 bis 1cc werden gemeinsam beantwortet.

Zum grundsätzlichen Verfahren wird auf die Antwort zu Frage 9 der Kleinen Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/8707 verwiesen. Sofern die Hersteller einer Veröffentlichung zugestimmt haben, werden laufende Zertifizierungsverfahren auf der Webseite des BSI veröffentlicht. Das gleiche gilt für abgeschlossene Zertifizierungsverfahren. Das BSI hält jedoch

nicht durchgängig nach, ob und wo in der Bundesverwaltung die zertifizierten Produkte zum Einsatz kommen.

2. Für welche IT-Sicherheitsprodukte und IT-Sicherheitsdienste wurden seit März 2022 Zertifizierungen für den Einsatz in der Bundesverwaltung nach welchem Zertifizierungsschema beim BSI beantragt, bei welchen davon wurde eine positive Zertifizierungsaussage getroffen, und bei welchen davon befand sich der Hauptsitz des Herstellers des IT-Sicherheitsprodukts außerhalb der EU (bitte nach Produktname, Art der beantragten Zertifizierung, Zertifizierungsaussage, Hersteller, Hauptsitz des Herstellers aufschlüsseln)?

   a) Für IT-Sicherheitsprodukte und IT-Sicherheitsdienste des Produkttyps DDoS-Schutz?

   b) Für IT-Sicherheitsprodukte und IT-Sicherheitsdienste des Produkttyps Web Application Firewall?

   c) Für IT-Sicherheitsprodukte und IT-Sicherheitsdienste des Produkttyps Domain Name Server?

   d) Für IT-Sicherheitsprodukte und -dienste des Produkttyps Reverse Proxy?

   e) Für IT-Sicherheitsprodukte und IT-Sicherheitsdienste des Produkttyps Content Delivery Network?

Die Fragen 2 bis 2e werden gemeinsam beantwortet.

Die Zertifizierung nach den CC (= Common Criteria) geschieht auf Herstellerantrag ohne Konkretisierung des Einsatzzwecks. Sofern die Hersteller einer Veröffentlichung zugestimmt haben, werden laufende Zertifizierungsverfahren auf der Webseite des BSI veröffentlicht. Das gleiche gilt für abgeschlossene Zertifizierungsverfahren. Das BSI hält jedoch nicht durchgängig nach, ob und wo in der Bundesverwaltung die zertifizierten Produkte zum Einsatz kommen.

3. Für welche IT-Sicherheitsprodukte mit Referenz zur Antwort der Bundesregierung zu Frage 10 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707 wurden seit 4. Oktober 2023 Zulassungen für den Einsatz in der Bundesverwaltung durch welchen behördlichen Anwender beim BSI beantragt, bei welchen davon wurde eine positive Zulassungsaussage getroffen, und bei welchen davon befand sich der Hauptsitz des Herstellers des IT-Sicherheitsprodukts außerhalb der EU (bitte nach Produktname, beantragendem behördlichen Anwender samt des ihm zuzuordnenden Geschäftsbereichs der Bundesregierung, Zulassungsaussage, Hersteller des IT-Sicherheitsprodukts, Hauptsitz des Herstellers des IT-Sicherheits-
produkts aufschlüsseln)?

   a) Für IT-Sicherheitsprodukte des Produkttyps Firewall?

   b) Für IT-Sicherheitsprodukte des Produkttyps Datendiode?

   c) Für IT-Sicherheitsprodukte des Produkttyps VS Guard?

   d) Für IT-Sicherheitsprodukte des Produkttyps Schadsoftwareerkennung?

   e) Für IT-Sicherheitsprodukte des Produkttyps Hypervisor?

   f) Für IT-Sicherheitsprodukte des Produkttyps Separation Kernel?

   g) Für IT-Sicherheitsprodukte des Produkttyps Mobile Device Management?

   h) Für IT-Sicherheitsprodukte des Produkttyps Netzwerkmanagement?

i) Für IT-Sicherheitsprodukte des Produkttyps Schlüsselspeicher- und Verteilkomponente?

j) Für IT-Sicherheitsprodukte des Produkttyps Key-Management-Software?

k) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Funksysteme?

l) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Satellitensysteme?

m) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für analoge Leitungen?

n) Für IT-Sicherheitsprodukte des Produkttyps Dateiverschlüsselung?

o) Für IT-Sicherheitsprodukte des Produkttyps Festplattenverschlüsselung?

p) Für IT-Sicherheitsprodukte des Produkttyps Sicherer mobiler Datenträger?

q) Für IT-Sicherheitsprodukte des Produkttyps Faxverschlüsselung?

r) Für IT-Sicherheitsprodukte des Produkttyps Telefonverschlüsselung?

s) Für IT-Sicherheitsprodukte des Produkttyps Funkgeräte?

t) Für IT-Sicherheitsprodukte des Produkttyps E-Mail-Verschlüsselung?

u) Für IT-Sicherheitsprodukte des Produkttyps VPN-Client?

v) Für IT-Sicherheitsprodukte des Produkttyps Sichere mobile Lösung?

w) Für IT-Sicherheitsprodukte des Produkttyps Sicherer Messenger?

x) Für IT-Sicherheitsprodukte des Produkttyps VPN-Gateway?

y) Für IT-Sicherheitsprodukte des Produkttyps Datenschleusen (optional auch mit Datenwäschekomponente)?

z) Für IT-Sicherheitsprodukte Verschlüsselung Layer 1?

aa) Für IT-Sicherheitsprodukte Verschlüsselung Layer 2?

bb) Für IT-Sicherheitsprodukte des Produkttyps Intrusion Detection System?

cc) Für IT-Sicherheitsprodukte Threat Detection System?

Die Fragen 3 bis 3cc werden gemeinsam beantwortet.

Auf die Vorbemerkung der Bundesregierung wird verwiesen. Die Beantwortung der Frage erfolgt eingestuft als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ gemäß der Allgemeinen Verwaltungsvorschrift des BMI zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA). Die Informationen können der Anlage entnommen werden.*

Da es sich bei den Aufzählungspunkten 3d, 3y, 3bb und 3cc nicht um Produkttypen des VS-Produktkataloges gemäß § 52 VSA handelt, kann die Bundesregierung dazu keine Aussage treffen.

* Das Bundeskanzleramt hat die Antwort als „VS - NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

4. Für welche IT-Sicherheitsprodukte wurden seit März 2022 Zulassungen für den Einsatz in der Bundesverwaltung durch welchen behördlichen Anwender beim BSI beantragt, bei welchen davon wurde eine positive Zulassungsaussage getroffen, und bei welchen davon befand sich der Hauptsitz des Herstellers des IT-Sicherheitsprodukts außerhalb der EU (bitte nach Produktname, beantragendem behördlichen Anwender samt des ihm zuzuordnenden Geschäftsbereichs der Bundesregierung, Zulassungsaussage, Hersteller des IT-Sicherheitsprodukts, Hauptsitz des Herstellers des IT-Sicherheitsprodukts aufschlüsseln)?

   a) Für IT-Sicherheitsprodukte und IT-Sicherheitsdienste des Produkttyps DDoS-Schutz?

   b) Für IT-Sicherheitsprodukte und IT-Sicherheitsdienste des Produkttyps Web Application Firewall?

   c) Für IT-Sicherheitsprodukte und IT-Sicherheitsdienste des Produkttyps Domain Name Server?

   d) Für IT-Sicherheitsprodukte und IT-Sicherheitsdienste des Produkttyps Reverse Proxy?

   e) Für IT-Sicherheitsprodukte und IT-Sicherheitsdienste des Produkttyps Content Delivery Network?

Die Fragen 4 bis 4e werden gemeinsam beantwortet.

Da es sich bei den aufgeführten Produkttypen nicht um Produkttypen des VS-Produktkataloges gemäß § 52 VSA handelt, wurden für Produkte dieser Produkttypen keine Zulassungen von der Bundesregierung ausgesprochen.

5. Handelt es sich bei der genua GmbH um einen bundesbehördlichen Bedarfsträger, und wenn nein, warum ist es unter Bezugnahme auf Anlage 1 der Antwort der Bundesregierung zu Frage 10 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707 möglich, dass unter Bezugnahme auf die Antwort der Bundesregierung zu Frage 4 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707, wonach eine Zulassung für ein Produkt nur durch einen bundesbehördlichen Bedarfsträger beantragt werden kann, die genua GmbH nicht nur der Hersteller, sondern auch gleichzeitig der Antragsteller für die Zulassung des Produkts vom Produkttyp Firewall mit dem Namen genuate NdB WebRTC ist?

Ein Antrag auf Zulassung kann nur durch einen (bundes-) behördlichen Bedarfsträger gestellt werden. Für Unternehmen der geheimschutzbetreuten Wirtschaft, die ebenfalls zugelassenen IT-Sicherheitsprodukte zum Schutz von amtlich eingestuften Informationen einsetzen müssen, erfolgt die Antragstellung durch das Bundesministerium für Wirtschaft und Klimaschutz (BMWK). Ein Antrag ist obsolet, wenn der Hersteller eines bereits zugelassenen Produktes eine neue Version seines Produktes im Rahmen der kontinuierlichen Produktverbesserung entwickelt.

Die Firma genua GmbH ist kein bundesbehördlicher Bedarfsträger. Im vorliegenden Fall „genuate NdB WebRTC“ wurde der Antrag auf Zulassung durch das BSI für das durch die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) betriebene Videokonferenzsystem CMS selbst gestellt.

6. Für welche IT-Sicherheitsprodukte mit Referenz zur Antwort der Bundesregierung zu Frage 11 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707 hat die Bundesverwaltung inklusive der IT-Dienstleister des Bundes für welchen behördlichen Anwender der Bundesverwaltung inklusive der IT-Dienstleister des Bundes seit dem 4. Oktober 2023 Verträge zur Beschaffung von IT-Sicherheitsprodukten geschlossen (bitte nach Produktname, Geschäftsbereich der vertragsschließenden Bundesbehörde, bedarfstragendem behördlichen Anwender, Art der Zertifizierung beziehungsweise Zulassungsaussage des beschafften IT-Sicherheitsprodukts, Hersteller des IT-Sicherheitsprodukts, Hauptsitz des Herstellers des IT-Sicherheitsprodukts aufschlüsseln)?

   a) Für IT-Sicherheitsprodukte des Produkttyps Firewall?

   b) Für IT-Sicherheitsprodukte des Produkttyps Datendiode?

   c) Für IT-Sicherheitsprodukte des Produkttyps VS Guard?

   d) Für IT-Sicherheitsprodukte des Produkttyps Schadsoftwareerkennung und Abwehr

   e) Für IT-Sicherheitsprodukte des Produkttyps Hypervisor?

   f) Für IT-Sicherheitsprodukte des Produkttyps Separation Kernel?

   g) Für IT-Sicherheitsprodukte des Produkttyps Mobile Device Management?

   h) Für IT-Sicherheitsprodukte des Produkttyps Netzwerkmanagement?

   i) Für IT-Sicherheitsprodukte des Produkttyps Schlüsselspeicher- und Verteilkomponente?

   j) Für IT-Sicherheitsprodukte des Produkttyps Key-Management-Software?

   k) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Funksysteme?

   l) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Satellitensysteme?

   m) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für analoge Leitungen?

   n) Für IT-Sicherheitsprodukte des Produkttyps Dateiverschlüsselung?

   o) Für IT-Sicherheitsprodukte des Produkttyps Festplattenverschlüsselung?

   p) Für IT-Sicherheitsprodukte des Produkttyps Sicherer mobiler Datenträger?

   q) Für IT-Sicherheitsprodukte des Produkttyps Faxverschlüsselung?

   r) Für IT-Sicherheitsprodukte des Produkttyps Telefonverschlüsselung?

   s) Für IT-Sicherheitsprodukte des Produkttyps Funkgeräte?

   t) Für IT-Sicherheitsprodukte des Produkttyps E-Mail-Verschlüsselung?

   u) Für IT-Sicherheitsprodukte des Produkttyps VPN-Client?

   v) Für IT-Sicherheitsprodukte des Produkttyps Sichere mobile Lösung?

   w) Für IT-Sicherheitsprodukte des Produkttyps Sicherer Messenger?

   x) Für IT-Sicherheitsprodukte des Produkttyps VPN-Gateway?

   y) Für IT-Sicherheitsprodukte des Produkttyps Datenschleusen (optional auch mit Datenwäschekomponente)?

z) Für IT-Sicherheitsprodukte Verschlüsselung Layer 1?

aa) Für IT-Sicherheitsprodukte Verschlüsselung Layer 2?

bb) Für IT-Sicherheitsprodukte des Produkttyps DDoS-Schutz Layer 3?

cc) Für IT-Sicherheitsprodukte des Produkttyps DDoS-Schutz Layer 4?

dd) Für IT-Sicherheitsprodukte des Produkttyps DDoS-Schutz Layer 7?

ee) Für IT-Sicherheitsprodukte des Produkttyps Web Application Firewall?

ff) Für IT-Sicherheitsprodukte des Produkttyps Email Security Gateway?

gg) Für IT-Sicherheitsprodukte des Produkttyps EDR (Endpoint Detection and Response), NDR (Network Detection and Response), XDR (Extended Detection and Response), Device/Port/Schnittstellenkontrolle, UTM (unified Threat Management), Backup/Recovery, DLP (Data Loss Prevention), Archivierung, ersetzendes Scannen, TR-ESOR Langzeitarchivierung, Labeling und APT(Advanced Persistent Threat)-Abwehr, ISMS (Information Security Management System) und SIEM (Security Information and Event Management)?

hh) Für IT-Sicherheitsprodukte Threat Detection System?

7. Für welche IT-Sicherheitsprodukte hat die Bundesverwaltung inklusive der IT-Dienstleister des Bundes für welchen behördlichen Anwender der Bundesverwaltung inklusive der IT-Dienstleister des Bundes seit März 2022 Verträge zur Beschaffung von IT-Sicherheitsprodukten geschlossen (bitte nach Produktname, Geschäftsbereich der vertragsschließenden Bundesbehörde, bedarfstragendem behördlichen Anwender, Art der Zertifizierung beziehungsweise Zulassungsaussage des beschafften IT-Sicherheitsprodukts, Hersteller des IT-Sicherheitsprodukts, Hauptsitz des Herstellers des IT-Sicherheitsprodukts aufschlüsseln)?

   a) Für IT-Sicherheitsprodukte und IT-Sicherheitsdienste des Produkttyps DDoS-Schutz?

   b) Für IT-Sicherheitsprodukte und IT-Sicherheitsdienste des Produkttyps Web Application Firewall?

   c) Für IT-Sicherheitsprodukte und IT-Sicherheitsdienste des Produkttyps Domain Name Server?

   d) Für IT-Sicherheitsprodukte und -dienste des Produkttyps Reverse Proxy?

   e) Für IT-Sicherheitsprodukte und IT-Sicherheitsdienste des Produkttyps Content Delivery Network?

8. Welche Behörde der Bundesverwaltung hat unter Bezugnahme auf die Gesamtheit der in Frage 6 erfragten Informationen Beschaffungen in jeweils wie vielen Fällen durchgeführt, und welche Vergabeverordnung (beispielsweise Vergabeverordnung [VgV], Vergabeverordnung für Aufträge im Bereich Verteidigung und Sicherheit [VSVgV], Unterschwellenvergabeordnung [UVgO]) und welche Vergabeverfahren (z. B. nichtoffenes Verfahren mit Teilnahmewettbewerb, Verhandlungsverfahren mit beziehungsweise ohne Teilnahmewettbewerb, wettbewerblicher Dialog mit Teilnahmewettbewerb) wurde dabei wie oft angewendet (bitte nach beschaffender Behörde, Anzahl der Beschaffungen, Häufigkeit der dabei gewählten Vergabeverordnung und des ggf. darin gewählten Vergabeverfahrens aufschlüsseln)?

9. Welche Behörde der Bundesverwaltung hat unter Bezugnahme auf die Gesamtheit der in Frage 7 erfragten Informationen Beschaffungen in jeweils wie vielen Fällen durchgeführt, und welche Vergabeverordnung (beispielsweise VgV, VSVgV, UVgO) und welche Vergabeverfahren (z. B. nichtoffenes Verfahren mit Teilnahmewettbewerb, Verhandlungsverfahren mit beziehungsweise ohne Teilnahmewettbewerb, wettbewerblicher Dialog mit Teilnahmewettbewerb) wurde dabei wie oft angewendet (bitte nach beschaffender Behörde, Anzahl der Beschaffungen, Häufigkeit der dabei gewählten Vergabeverordnung und des ggf. darin gewählten Vergabeverfahrens aufschlüsseln)?

10. Wann war unter Bezugnahme auf Frage 6 der jeweils letzte Zeitpunkt für die Ausschreibung für das jeweilige IT-Sicherheitsprodukt (bitte nach IT-Sicherheitsprodukt und Zeitpunkt der letzten Ausschreibung aufschlüsseln)?

11. Wann war unter Bezugnahme auf Frage 7 der jeweils letzte Zeitpunkt für die Ausschreibung für das jeweilige IT-Sicherheitsprodukt (bitte nach IT-Sicherheitsprodukt und Zeitpunkt der letzten Ausschreibung aufschlüsseln)?

Die Fragen 6 bis 11 werden gemeinsam beantwortet.

Es wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Fragen nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

12. Warum sind unter Bezugnahme auf die Antwort der Bundesregierung zu Frage 13 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707 und der dazugehörenden Anlage 3 der Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 20/8707 die Informationen nur für die zentral vom Beschaffungsamt geschlossenen Verträge angegeben?

Die in der Bundesverwaltung eingesetzten IT-Sicherheitsprodukte werden nicht zentral erfasst; hierzu besteht auch keine Verpflichtung. Eine Auswertung des erheblichen dezentralen Informationsbestandes im Sinne der Fragestellung ist deshalb nicht möglich, sodass die Beantwortung der Bundesregierung der Frage 13 der Kleinen Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/8707 auf Grundlage vorliegender Erkenntnisse sowie vorhandener Unterlagen und Aufzeichnungen erfolgte.

13. Welche der in Frage 6 erfragten IT-Sicherheitsprodukte kommen seit Vertragsschluss zur Beschaffung in der Bundesverwaltung bei welchem behördlichen Anwender jeweils tatsächlich zum Einsatz, und für welche der in Frage 6 erfragten IT-Sicherheitsprodukte wurden nach Vertragsschluss zur Beschaffung keine Abrufe durch die Bundesverwaltung getätigt (bitte analog zu Frage 6 aufschlüsseln)?

14. Welche der in Frage 7 erfragten IT-Sicherheitsprodukte kommen seit Vertragsschluss zur Beschaffung in der Bundesverwaltung bei welchem behördlichen Anwender jeweils tatsächlich zum Einsatz, und für welche der in Frage 7 erfragten IT-Sicherheitsprodukte wurden nach Vertragsschluss zur Beschaffung keine Abrufe durch die Bundesverwaltung getätigt (bitte analog zu Frage 7 aufschlüsseln)?

15. Wie hoch ist jeweils die Anzahl der Behörden, die die in Frage 6 erfragten IT-Sicherheitsprodukte in ihrer Verwaltung verwenden (bitte analog zu Frage 6 nach Produktnamen, Anzahl der verwendenden Bundesbehörden inklusive IT-Dienstleister des Bundes und dem ihr zuzuordnenden Geschäftsbereich der Bundesregierung aufschlüsseln)?

16. Wie hoch ist jeweils die Anzahl der Behörden, die die in Frage 7 erfragten IT-Sicherheitsprodukte in ihrer Verwaltung verwenden (bitte analog zu Frage 7 nach Produktnamen, Anzahl der verwendenden Bundesbehörden inklusive IT-Dienstleister des Bundes und dem ihr zuzuordnenden Geschäftsbereich der Bundesregierung aufschlüsseln)?

17. Wie hoch ist jeweils die Anzahl der Lizenzen für die in Frage 6 erfragten IT-Sicherheitsprodukte, die die Bundesverwaltung inklusive der IT-Dienstleister des Bundes für welchen behördlichen Anwender der Bundesverwaltung inklusive der IT-Dienstleister des Bundes jeweils bezogen hat (bitte analog zu Frage 6 nach Produktnamen, produktverwendenden Bundesbehörden, zuzuordnendem Geschäftsbereich der Bundesregierung und jeweiliger Anzahl der Produktlizenzen aufschlüsseln)?

18. Wie hoch ist jeweils die Anzahl der Lizenzen für die in Frage 7 erfragten IT-Sicherheitsprodukte, die die Bundesverwaltung inklusive der IT-Dienstleister des Bundes für welchen behördlichen Anwender der Bundesverwaltung inklusive der IT-Dienstleister des Bundes jeweils bezogen hat (bitte analog zu Frage 7 nach Produktnamen, produktverwendenden Bundesbehörden, zuzuordnendem Geschäftsbereich der Bundesregierung und jeweiliger Anzahl der Produktlizenzen aufschlüsseln)?

19. Wie hoch ist jeweils die Anzahl der Installationen der in Frage 6 erfragten IT-Sicherheitsprodukte in den jeweils produktverwendenden Bundesbehörden inklusive der IT-Dienstleister des Bundes (bitte analog zu Frage 6 nach Produktnamen, produktverwendenden Bundesbehörden, zuzuordnendem Geschäftsbereich der Bundesregierung und jeweiliger Anzahl der Installationen aufschlüsseln)?

20. Wie hoch ist jeweils die Anzahl der Installationen der in Frage 7 erfragten IT-Sicherheitsprodukte in den jeweils produktverwendenden Bundesbehörden inklusive der IT-Dienstleister des Bundes (bitte analog zu Frage 7 nach Produktnamen, produktverwendenden Bundesbehörden, zuzuordnendem Geschäftsbereich der Bundesregierung und jeweiliger Anzahl der Installationen aufschlüsseln)?

21. Sollten bei der Beantwortung der Fragen 17 und 19 sowie 18 und 20 deutliche Diskrepanzen zwischen der Anzahl der Lizenzen und der Anzahl der Installationen bei bestimmten IT-Sicherheitsprodukten, die von der Bundesverwaltung für einen behördlichen Anwender zur Nutzung beschafft wurden, zutage treten, wie erklärt sich die Bundesregierung ggf. diese Diskrepanzen?

Die Fragen 13 bis 21 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Es wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Fragen nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, so dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

22. Sollte im Rahmen der Beantwortung von Frage 6 hervorgehen, dass für die Bundesverwaltung IT-Sicherheitsprodukte von Herstellern mit einem Firmensitz in einem außereuropäischen Staat beschafft wurden, gab es für diese gelisteten und beschafften IT-Sicherheitsprodukte von Herstellern mit einem Firmensitz in einem außereuropäischen Staat zum Beschaffungszeitpunkt Alternativen von Herstellern mit einem Firmensitz in einem Staat des Europäischen Wirtschaftsraums, in der Schweiz oder in Großbritannien, und wenn ja, warum wurde nicht eine der Alternativen beziehungsweise wurden nicht die Alternativen beschafft (bitte Alternative beziehungsweise Alternativen bei betroffenen IT-Sicherheitsprodukten, Staat, in dem der Firmensitz des Herstellers der Alternative beziehungsweise Alternativen liegt, und Begründungen für Entscheidung gegen die Alternative beziehungsweise Alternativen anführen)?

23. Sollte im Rahmen der Beantwortung von Frage 7 hervorgehen, dass für die Bundesverwaltung IT-Sicherheitsprodukte von Herstellern mit einem Firmensitz in einem außereuropäischen Staat beschafft wurden, gab es für diese gelisteten und beschafften IT-Sicherheitsprodukte von Herstellern mit einem Firmensitz in einem außereuropäischen Staat zum Beschaffungszeitpunkt Alternativen von Herstellern mit einem Firmensitz in einem Staat des Europäischen Wirtschaftsraums, in der Schweiz oder in Großbritannien, und wenn ja, warum wurde nicht eine der Alternativen beziehungsweise wurden nicht die Alternativen beschafft (bitte Alternative beziehungsweise Alternativen bei betroffenen IT-Sicherheitsprodukten, Staat, in dem der Firmensitz des Herstellers der Alternative beziehungsweise Alternativen liegt, und Begründungen für Entscheidung gegen die Alternative beziehungsweise Alternativen anführen)?

Die Fragen 22 und 23 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Auf die Vorbemerkung der Bundesregierung zu den Fragen 6 und 7 wird verwiesen. Soweit die Bundesregierung im angefragten Zeitraum IT-Sicherheitsprodukte von Herstellern mit einem Firmensitz in einem außereuropäischen Staat beschafft hat, waren bestehende Rahmenverträge, fachliche Anforderungen und Ergebnisse öffentlicher Ausschreibungen für die Entscheidung ausschlaggebend.

24. Welche und wie viele der in der Antwort zu Frage 6 genannten Hersteller sind über welchen Zeitraum geheimschutzbetreut nach dem Sicherheitsüberprüfungsgesetz (SÜG)?

25. Welche und wie viele der in der Antwort zu Frage 7 genannten Hersteller sind über welchen Zeitraum geheimschutzbetreut nach dem SÜG?

Die Fragen 24 und 25 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Es wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Fragen nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren und Grundrechte Dritte entgegenstehen, so dass das Staatswohl und die Wahrung von Grundrechten Dritter gegenüber dem parlamentarischen Informationsrecht überwiegen.

26. Für wie viele Mitarbeiterinnen und Mitarbeiter von Herstellern von IT-Sicherheitsprodukten, deren IT-Sicherheitsprodukte in der Bundesverwaltung inklusive der IT-Dienstleister des Bundes, zum Einsatz kommen, wurde ein Sicherheitsüberprüfungsverfahren gemäß Sicherheitsüberprüfungsgesetz durchgeführt (bitte nach Land des Sitzes des Herstellers mit den sicherheitsüberprüften Mitarbeiterinnen und Mitarbeitern aufschlüsseln)?

Für die vom BMWK geheimschutzbetreuten Hersteller von IT-Sicherheitsprodukten wurden 11 132 Sicherheitsüberprüfungsverfahren gemäß Sicherheitsüberprüfungsgesetz (SÜG) durchgeführt. Die Anzahl des sicherheitsüberprüften Personals orientiert sich nicht spezifisch an den Aufträgen zur Herstellung von IT-Sicherheitsprodukten, sondern an dem Gesamt-VS-Auftragsvolumen des jeweiligen Unternehmens. Der Sitz dieser geheimschutzbetreuten Unternehmen befindet sich in Deutschland.

27. Ist die Apple Inc., die in der Anlage 1 der Antwort der Bundesregierung zu Frage 10 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707 als Hersteller der Produkte INDIGO 15.x und INDIGO 16.x vom Produkttyp Sichere mobile Lösung, die auch für den Umgang mit Verschlusssachen (VS) gedacht ist (www.golem.de/news/apple-indigo-ein-ios-fuer-die-deutschen-behoerden-2407-187458.html), genannt ist, gemäß dem das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG; www.gesetze-im-internet.de/bsig_2009/) ändernde IT-Sicherheitsgesetz 2.0, wonach jedes Unternehmen, das Produkte zur Nutzung in Verschlusssachen-Umgebungen herstellt und damit als Unternehmen besonderen Interesses gilt (UBI I; www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Regulierte_Unternehmen/UBI/Flyer.pdf?__blob=publicationFile&v=5), seit dem 1. Mai 2023 gegenüber dem BSI bestimmten Pflichten nachkommen muss, den nun in § 8f BSIG festgeschriebenen Pflichten nachgekommen, und kommt sie diesen Pflichten nach wie vor nach (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Regulierte_Unternehmen/UBI/Flyer.pdf?__blob=publicationFile&v=5; www.gesetze-im-internet.de/bsig_2009/__2.html; www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf)?

a) Hat die Apple Inc. innerhalb der festgesetzten Fristen eine Selbsterklärung zur IT-Sicherheit beim BSI vorgelegt, und wenn ja, zu welchem Zeitpunkt genau?

b) Welche Zertifizierungen im Bereich der IT-Sicherheit wurden in den letzten zwei Jahren gemäß der Selbsterklärung durchgeführt, und welche Prüfgrundlage und welcher Geltungsbereich wurden hierfür festgelegt?

c) Welche sonstigen Sicherheitsaudits oder Prüfungen im Bereich der IT-Sicherheit in den letzten zwei Jahren wurden gemäß der Selbsterklärung durchgeführt, und welche Prüfgrundlage und welcher Geltungsbereich wurden hierfür festgelegt?

d) Wie wird gemäß der Selbsterklärung sichergestellt, dass die besonders schützenswerten informationstechnischen Systeme, Komponenten und Prozesse angemessen geschützt werden, und wird dabei der Stand der Technik eingehalten?

e) Hat das BSI auf Grundlage der Selbsterklärung Hinweise zu angemessenen organisatorischen und technischen Vorkehrungen zur Einhaltung des Stands der Technik gegeben?

f) Hat sich die Apple Inc. gleichzeitig mit der Vorlage der Selbsterklärung zur IT-Sicherheit beim BSI registriert und eine zu den üblichen Geschäftszeiten erreichbare Stelle benannt, wenn ja, wann erfolgte die Registrierung, und welche Geschäftsstelle wurde benannt?

g) Hat die Apple Inc. seit dem 1. Mai 2023 dem BSI Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung geführt haben, oder erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung führen können, gemeldet (bitte aufgeschlüsselt nach Störung, technischen Rahmenbedingungen der Störung, vermuteten oder tatsächlichen Ursachen der Störung, betroffener Informationstechnik, betroffener Einrichtung oder Anlage auflisten)?

Die Fragen 27 bis 27g werden gemeinsam beantwortet.

Nach den im BSI vorliegenden Informationen handelt sich bei der Apple Inc. nicht um ein Unternehmen im besonderen öffentlichen Interesse im Sinne von § 2 Abs. 14 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG); es fällt damit nicht unter die Verpflichtungen des § 8f BSIG.

h) Wurde der Apple Inc. für das Produkt INDIGO das Sicherheitszertifikat vom BSI erteilt, und entsprachen die dazugehörenden informationstechnischen Systeme, Komponenten, Produkte oder Schutzprofile den vom BSI festgelegten Kriterien, und wenn nein, warum nicht?

Die für das Produkt INDIGO ausgesprochenen Zulassungsaussagen (siehe Anlage zu Frage 3) basieren zum einen auf den im VS-Anforderungsprofil „Sichere mobile Lösungen“ niedergeschriebenen Anforderungen des BSI. Zum anderen wurde die Evaluierung auf der Grundlage des Dokuments „Nachweise für eine Evaluierung für eine Zulassung bis VS-NUR FÜR DEN DIENSTGEBRAUCH“ durchgeführt.

Das Produkt hat dabei die Anforderungen aus dem VS-Anforderungsprofil erfüllt, die Evaluierung ist mit einem positiven Votum abgeschlossen worden, so dass durch die Zulassungsstelle eine positive Zulassungsaussage getätigt werden konnte

28. Welche Förderprogramme der Bundesregierung zur Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität liefen und laufen seit dem Jahr 2018 (bitte jeweils die finanzielle Ausstattung jeweils für die Jahresscheiben von 2018 bis 2023 nennen)?

Hinsichtlich der Ausstattungswerte für die Jahre 2018 und 2019 wird auf die Antwort der Bundesregierung zu Frage 43 der Kleinen Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/8707 verwiesen. Die erbetenen Angaben für die Jahre 2020 bis 2023 können der nachstehenden Tabelle entnommen werden.

Ressort	Name des Förderprogramms	Ausstattung 2020 (in Euro)	Ausstattung 2021 (in Euro)	Ausstattung 2022 (in Euro)	Ausstattung 2023 (in Euro)
Bundesministerium für Bildung und Forschung (BMBF)	Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt“ (2015 bis 2020) *	54 281 763	67 631 787	50 387 154	33 903 680
BMBF	Zum Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“ (2021 bis 2026)		9 521 400	45 483 673	98 724 562
BMI (BSI)	Förderprogramm für Forschungs- und Entwicklungsvorhaben im Bereich „Cybersicherheit und digitale Souveränität in den Kommunikationstechnologien 5G/6G“ im Rahmen des „45. Elements“ des Konjunkturprogramms der Deutschen Bundesregierung zur Adressierung der Folgen der Corona-Pandemie			14 800 000	20 635 000
BMI (BDBOS)	Förderprogramm „Innovationen im breitbandigen Digitalfunk BOS“		1 300 000	10 200 000	8 000 000

29. Plant die Bundesregierung derzeit, neue Förderprogramme zur Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität aufzulegen, und wenn ja, wie hoch wird die von der Bundesregierung angedachte finanzielle Ausstattung sein?

Die erbetenen Angaben können der nachstehenden Tabelle entnommen werden.

Ressort	Planungen der Bundesregierung
BMBF	Das aktuelle Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“ läuft noch bis Ende 2026. Im Rahmen des Programms werden regelmäßig neue Fördermaßnahmen gestartet.
BMI (BDBOS)	Über das laufende Förderprogramm „Innovationen im breitbandigen Digitalfunk BOS“ hinaus erwägt die Bundesregierung eine weiterführende Fördertätigkeit. Auf diese Weise könnte das Zusammenwirken von Wissenschaft und Forschung sowie der deutschen Wirtschaft im Bereich der einsatzkritischen Mobilkommunikation gefördert wer-den.

30. In Höhe welcher Summe sind finanzielle Mittel im Bundeshaushalt zur Erforschung und Entwicklung von Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität hinterlegt (bitte nach Einzelplan, Kapitel und Titel für die Jahre 2023 und 2024 sowie für den Entwurf der Bundesregierung zum Bundeshaushalt 2025 aufschlüsseln)?

Die erbetenen Angaben können der nachstehenden Tabelle entnommen werden.

Einzelplan	Kapitel	Titel	2023 (in Euro)	2024 (in Euro)	2025 (geplant, in Euro)
06	0023	532 04	4 652 285	4 961 589	2 000 000
06	0023	686 02	8 929 709	18 775 844	
06	0602	544 02	24 650 000	21 000 000	19 000 000
06	0602	685 20	8 000 000	9 000 000	
14	1404	551 04	24 650 000	55 000 000	40 000 000
30	3004	683 20	137 800 000	129 440 000	126 440 000

31. Welche Förderprogramme der Bundesregierung zur nationalen industriellen Marktentwicklung für Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität liefen und laufen seit dem Jahr 2018 (bitte jeweils die finanzielle Ausstattung jeweils für die Jahresscheiben von 2018 bis 2024 nennen)?

Die erbetenen Angaben können der nachstehenden Tabelle entnommen werden.

Ressort	Förderprogramm	Ausstattung 2018 (in Euro)	Ausstattung 2019 (in Euro)	Ausstattung 2020 (in Euro)	Ausstattung 2021 (in Euro)	Ausstattung 2022 (in Euro)	Ausstattung 2023 (in Euro)	Ausstattung 2024 (in Euro)
BMBF	Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt“ (2015 bis 2020)	45 784 984	47 529 929	54 281 763	67 631 787	50 387 154	33 903 680	21 558 677
BMBF	Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“ (2021 bis 2026)				9 521 400	45 483 673	98 724 562	103 441 771
BMI (BSI)	Forschungs- und Entwicklungsvorhaben im Bereich „Cybersicherheit und digitale Souveränität in den Kommunikationstechnologien 5G/6G“					14 800 000	20 635 000	23 450 000

32. Plant die Bundesregierung derzeit, neue Förderprogramme zur nationalen industriellen Marktentwicklung von Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität aufzulegen, und wenn ja, wie hoch wird die von der Bundesregierung angedachte finanzielle Ausstattung sein?

Im Rahmen des aktuellen Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“, werden regelmäßig neue Fördermaßnahmen gestartet, die aktuell noch nicht namentlich benannt werden können.

Des Weiteren wird auf die Beantwortung der Frage 29 verwiesen.

33. Warum wird die Vereinbarung des Bundesministeriums des Innern und für Heimat (BMI) sowie des Bundesministeriums der Verteidigung (BMVg) über eine jeweils zur Hälfte getragene Finanzierung der Agentur für Innovationen in der Cybersicherheit (www.basecamp.digital/cyberagentur-vor-gruendung-neue-details-und-viel-kritik/) unter Bezugnahme auf die Antwort der Bundesregierung auf die Schriftliche Frage 14 auf Bundestagsdrucksache 20/12372 und unter Bezugnahme auf die Antwort der Bundesregierung auf die Fragen 79 bis 81 der Kleinen Anfrage auf Bundestagsdrucksache 20/12829 für den Soll-Ansatz im Bundeshaushalt 2024, wonach das BMI im Jahr 2024 21 Mio. Euro und das BMVg 55 Mio. Euro finanziert, und für den Soll-Ansatz im Entwurf der Bundesregierung für den Bundeshaushalt 2025, wonach das BMI 19 Mio. Euro und das BMVg 40 Mio. Euro finanziert, nicht umgesetzt?

Die Anmeldung für Haushaltsaufstellung erfolgt in Abstimmung zwischen dem BMI und dem Bundesministerium der Verteidigung (BMVg). Aufgrund von Kürzungen im Haushalt des BMI konnte eine paritätische Aufteilung der Finanzierung nicht erfolgen.

a) Welche Finanzierungsgesamtsumme für die Agentur für Innovationen in der Cybersicherheit war ursprünglich unabhängig von der exakten Aufteilung auf das BMI und das BMVg von der Bundesregierung jeweils für das Jahr 2024 und für das Jahr 2025 vorgesehen?

Die erbetenen Angaben können der nachstehenden Tabelle entnommen werden.

2024	**2025**
50 Mio. Euro	80 Mio. Euro

b) Welche Finanzierungsgesamtsumme für die Agentur für Innovationen in der Cybersicherheit ist unabhängig von der exakten Aufteilung auf das BMI und das BMVg von der Bundesregierung jeweils für die Jahre bis 2028 vorgesehen (bitte nach Jahresscheiben aufschlüsseln)?

Die erbetenen Angaben können der nachstehenden Tabelle entnommen werden.

2026	**2027**	**2028**
80 Mio. Euro	80 Mio. Euro	80 Mio. Euro

c) Wie stellen sich die vorgesehenen Ausgaben für die Agentur für Innovationen in der Cybersicherheit jeweils beim BMI und beim BMVg jeweils für die Jahre der mittelfristigen Finanzplanung von 2026 bis 2028 dar (bitte nach Ressort und Jahresscheiben aufschlüsseln)?

Die erbetenen Angaben können der nachstehenden Tabelle entnommen werden.

Ressort	2026	2027	2028
BMI	40 Mio. Euro	40 Mio. Euro	40 Mio. Euro
BMVg	40 Mio. Euro	40 Mio. Euro	40 Mio. Euro

34. Wie sind die Aussagen der Bundesregierung in ihrer Antwort zu Frage 35 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707, wonach „[…] das im deutschen Vergaberecht geltende Gleichbehandlungsgebot bzw. das damit korrespondierende Diskriminierungsverbot (siehe etwa § 97 Absatz 2 des Gesetzes gegen Wettbewerbsbeschränkungen [GWB]) […] jede unmittelbare und mittelbare Benachteiligung von Bietern aus dem Ausland [verbieten]“ und „[…] die Unterscheidung zwischen Unternehmen aus dem EU-Ausland und aus Drittstaaten […] das deutsche Vergaberecht nicht [trifft]“, sowie in ihrer Antwort zu Frage 36 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707, wonach es „[…] in Deutschland keine gesetzlichen Grundlagen für einen kategorischen Ausschluss von Herstellern aufgrund der Verortung ihres Hauptsitzes in einem bestimmten Land [gibt]“, mit dem Vorhaben des sogenannten Vergabetransformationspakets, mit dem die Bundesregierung unter Bezugnahme auf ihre Antwort zu Frage 17 der Kleinen Anfrage auf Bundestagsdrucksache 20/13937 den „[…] bisher strenge[n] Grundsatz der Gleichbehandlung von Drittstaatsanbietern in Vergabeverfahren […]“ einschränken möchte, widerspruchsfrei in Einklang zu bringen, und warum hält die Bundesregierung eine derartige Einschränkung nun für möglich?

Zwischenzeitlich erging neue europäische Rechtsprechung, auf die die Bundesregierung in ihrer Antwort zu Frage 17 der Kleinen Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/13937 Bezug genommen hat. Die Bundesregierung ist bestrebt, diese umzusetzen. Dem Entwurf der Bundesregierung zum Vergaberechtstransformationsgesetz auf der Bundestagsdrucksache 20/14344 ist entsprechend zu entnehmen, dass der Europäische Gerichtshof (EuGH) in der Rechtssache C-652/22 (Kolin Inşaat Turizm Sanayi ve Ticaret) am 22. Oktober 2024 entschieden hat, dass es in die ausschließliche Zuständigkeit der Europäischen Union (EU) (gemeinsame Handelspolitik) fällt, den Zugang von Wirtschaftsteilnehmern aus Drittstaaten zu Vergabeverfahren in den Mitgliedstaaten zu regeln. Die Mitgliedstaaten seien daher nicht befugt, insoweit gesetzgeberisch tätig zu werden oder verbindliche Rechtsakte mit allgemeiner Geltung zu erlassen. Der bislang in § 97 Absatz 2 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) niedergelegte strenge Gleichbehandlungsgrundsatz stellt, soweit er die unterschiedslose Behandlung aller Drittstaatsbieter vorschreibt, eine mitgliedstaatliche und allgemeine Regelung über den Zugang von Drittstaatsbietern zu Vergabeverfahren im Sinne des vorgenannten Urteils dar. Erforderlich ist daher eine Beschränkung dieses Grundsatzes dahingehend, dass diese Bieter nur gleich zu behandeln sind, soweit das Unionsrecht dies fordert. Weitere Einzelheiten können der Gesetzesbegründung auf der Bundestagsdrucksache 20/14344 ab Seite 50 entnommen werden.

35. Plant die Bundesregierung mit ihrem Vorhaben des sogenannten Vergabe-
transformationspakets nicht nur die Einschränkung des bisher strengen Grundsatzes der Gleichbehandlung von Drittstaatsanbietern in Auftragsvergabeverfahren des öffentlichen Auftraggebers, wie in ihrer Antwort zu Frage 17 der Kleinen Anfrage auf Bundestagsdrucksache 20/13937 angegeben, sondern plant sie beziehungsweise beabsichtigt sie, darüber hinausgehend mit dem Vergabetransformationspaket oder mit anderen Vorhaben die Möglichkeit zu schaffen, für bestimmte Auftragsvergabeverfahren im Bereich der Beschaffung von Cyber- und Informationssicherheitsleistungen und Cyber- und Informationssicherheitsprodukten nur einen nationalen Anbieterkreis zuzulassen?

Der Entwurf des Vergaberechtstransformationsgesetzes der Bundesregierung auf Bundestagsdrucksache 20/14344 sieht eine Änderung des bisherigen § 97 Absatz 2 GWB dahingehend vor, dass die Teilnehmer an einem Vergabeverfahren nur gleich zu behandeln sind, soweit nicht eine Ungleichbehandlung unionsrechtlich oder aufgrund eines Bundesgesetzes geboten oder gestattet ist. Darüberhinausgehende nationale Regelungen sind aufgrund der Entscheidung des EuGHs in Sachen Kolin nicht zulässig (siehe Antwort auf Frage 34). Sie sind daher von der Bundesregierung auch nicht geplant. Soweit die EU keine entsprechenden Regelungen erlassen hat, ist es nach der Entscheidung des EuGH Sache der einzelnen Auftraggeber, im Einzelfall zu prüfen, ob Wirtschaftsteilnehmer aus Drittstaaten, die keinen durch internationale Übereinkunft mit der Europäischen Union garantierten Zugang zum EU-Beschaffungsmarkt haben, zu einem öffentlichen Vergabeverfahren zugelassen werden sollten.

36. Hat sich die Bundesregierung seit Beginn der Legislaturperiode dahin gehend auf europäischer Ebene eingesetzt, dass Änderungen im Vertrag über die Arbeitsweise der Europäischen Union derart vorgenommen werden, dass in Artikel 346 AEUV die Cyber- und Informationssicherheit aufgenommen werden, damit auch Beschaffungen von Cyber- und Informationssicherheitsleistungen mit Ausnahmen belegt werden können beziehungsweise jedenfalls gesichert in den Vergabebereich Verteidigung und Sicherheit fallen, oder plant die Bundesregierung, dies noch bis Ende der Legislaturperiode zu tun, und wenn nein, warum nicht?

Die Bundesregierung verfolgt derzeit keine Pläne in diese Richtung. Die vorgeschlagene Anpassung des Artikel 346 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) würde eine Änderung des europäischen Primärrechts (d. h. der EU-Verträge) voraussetzen. Hierfür bestehen sehr hohe rechtliche Hürden. Die Regelungen zur Änderung des Primärrechts finden sich in Art. 48 des

Vertrag über die Europäische Union (EUV). Auch praktisch hätte der Vorschlag auf Vertragsänderungen kaum Aussicht auf Erfolg. Eine Reihe von Mitgliedstaaten hat sich bisher ausdrücklich gegen Vertragsänderungen ausgesprochen.

37. Hat sich die Bundesregierung seit Beginn der Legislaturperiode dahin gehend auf europäischer Ebene eingesetzt, dass eine Änderung der Richtlinie 2009/81/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über die Koordinierung der Verfahren zur Vergabe bestimmter Bau-, Liefer- und Dienstleistungsaufträge in den Bereichen Verteidigung und Sicherheit derart vorgenommen wird, damit Leistungen der Cybersicherheit und Informationssicherheit explizit vom Anwendungsbereich der Richtlinie 2009/81/EG erfasst werden und die Cyber- und Informationssicherheit dort genannt wird, oder plant die Bundes-

regierung, dies noch bis Ende der Legislaturperiode zu tun, und wenn nein, warum nicht?

Die Bundesregierung prüft eine entsprechende Anpassung der Vorgaben in den EU-Vergaberichtlinien und setzt sich auf EU-Ebene im Rahmen der Konsultationen zur Reform des EU-Vergaberechts für eine Änderung auch der Richtlinie 2009/81/EG ein. Sie hat in der Begründung ihres Entwurfs zum Vergaberechtstransformationsgesetz zudem klargestellt, dass auch die Cyber- und die Informationssicherheit sowie Aspekte der digitalen Souveränität bereits unter der geltenden nationalen und europäischen Rechtslage besondere oder wesentliche Sicherheitsinteressen unter anderem im Sinne von §§ 107 und 117 GWB sein können (siehe in der Begründung zum Gesetzentwurf auf der Bundestagsdrucksache 20/14344 auf Seite 96).

38. Hat sich die Bundesregierung seit Beginn der Legislaturperiode dahin gehend auf europäischer Ebene eingesetzt, dass die in Artikel 346 Absatz 2 AEUV referenzierte und seit dem 15. April 1958 nicht mehr überarbeitete Liste von Waren, Gütern und Dienstleistungen, auf die Artikel 346 Absatz 1 Buchstabe b AEUV Anwendung findet, angesichts des technologischen Fortschritts überarbeitet wird, oder plant die Bundesregierung, dies noch bis Ende der Legislaturperiode zu tun, und wenn nein, warum nicht?

Die Bundesregierung teilt die Ansicht ihrer Vorgängerinnen, dass die am 15. April 1958 angenommene Liste von Waffen, Munition und Kriegsmaterial insbesondere die technologische Entwicklung nicht wiederspiegelt und Militärausrüstung national auch unter Berücksichtigung der sich weiterentwickelnden Technologie ausgelegt werden sollte (vgl. auch die Entschließung des Bundestages zum Bundeswehrbeschaffungsbeschleunigungsgesetz auf Empfehlung des Bundestagswirtschaftsausschusses vom 6. Juli 2022 auf Bundestagsdrucksache 20/2644). Bisher hat die gemäß Artikel 346 Absatz 2 AEUV ausschließlich vorschlagsberechtige Europäische Kommission dem Rat keinen Vorschlag zur Änderung der Liste vorgelegt.

39. Sind in dem durch die Bundesregierung verabschiedeten Gesetzentwurf zur Vergabetransformation neben umweltbezogenen und sozialen Kriterien auch die Einführung von digitalen Aspekten als Kriterien jenseits der von der Bundesregierung in ihrer Antwort zu Frage 17 der Kleinen Anfrage auf Bundestagsdrucksache 20/13937 bereits genannten Einschränkung des „[…] bisher strenge[n] Grundsatz[es] der Gleichbehandlung von Drittstaatsanbietern in Vergabeverfahren […]“ für eine Vergabeentscheidung vorgesehen, wenn ja, welche, und wenn nein, hat die Bundesregierung dies in anderen Vorhaben beabsichtigt oder vorgesehen?

Der Entwurf der Bundesregierung eines Vergaberechtstransformationsgesetzes auf Bundestagsdrucksache 20/14344 legt neben Vereinfachung und Beschleunigung auch einen besonderen Fokus auf Digitalisierung, etwa durch vereinfachte Kooperationen des Bundes und der Länder bei IT-Projekten sowie durch weitgehend digitalisierte Nachprüfungsverfahren. Zudem wird die Beschaffung innovativer Lösungen, die insbesondere auch digitale Aspekte umfassen können, durch den Gesetzentwurf gestärkt. Für offene Standards und Open-Source-Software hat die Bundesregierung Maßnahmen im Änderungsgesetz zum Onlinezugangsgesetz (OZG) getroffen (siehe hierzu ergänzend die Beantwortung von Frage 40).

40. Beabsichtigt oder plant die Bundesregierung, Open Source als Vergabekriterium in Vergabeverfahren zur Beschaffung bei bestimmten Auftragsgegenständen im Zusammenhang mit IT-Produkten für die Bundesverwaltung einzuführen, wenn ja, im Zusammenhang mit welchen Auftragsgegenständen, und wenn nein, warum nicht?

41. Beabsichtigt oder plant die Bundesregierung, Open Source als Vergabekriterium in Vergabeverfahren zur Beschaffung bei bestimmten Auftragsgegenständen im Zusammenhang mit Cyber- und Informationssicherheitsprodukten für die Bundesverwaltung einzuführen, wenn ja, im Zusammenhang mit welchen Auftragsgegenständen, und wenn nein, warum nicht?

Die Fragen 40 und 41 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet. Mit dem Gesetz zur Änderung des OZG, das am 24. Juli 2024 in Kraft getreten ist, und dem dort enthaltenen neuen § 16a E-Government-Gesetz hat die Bundesregierung in dieser Legislaturperiode bereits festgelegt, dass die Bundesverwaltung offene Standards nutzen und Open-Source-Software vorrangig vor Software, deren Quellcode nicht öffentlich zugänglich ist oder deren Lizenz die Verwendung, Weitergabe und Veränderung einschränkt, beschafft werden soll. Die Entscheidung über die konkrete Ausgestaltung obliegt dem jeweiligen Auftraggeber.

42. Plant die Bundesregierung, einerseits im Zuge der vom BMI in seiner Cybersicherheitsagenda angekündigten Ausstattung der Bundesbehörden mit weiterentwickelten IT-Produkten und andererseits der von der Bundesregierung in ihrer Digitalstrategie angekündigten ganzheitlichen Stärkung des Cybersicherheitsökosystem künftig bei IT-Beschaffungsvorhaben des Bundes einen bestimmten Anteil der Sachmittel für IT-Vorhaben des Bundes für Cybersicherheit aufzuwenden?

Das BMI setzt sich dafür ein, dass ein angemessener Mitteleinsatz für die Cybersicherheit als prozentualer Anteil der Ausgaben des IT-Betriebs festgelegt werden sollte. Dies wird im Rahmen des künftigen Gesetzgebungsverfahrens zur Umsetzung der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union erneut zu prüfen sein.

43. Plant die Bundesregierung unter Bezugnahme auf ihre Antwort zu Frage 41 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707, wonach eine Produktzertifizierung nach den Zertifizierungsschemata der Common Criteria, der Technischen Richtlinie, der Beschleunigten Sicherheitszertifizierung (BSZ) und des Network Equipment Security Assurance Scheme (NESAS) keine zukunftsbezogenen Aussagen zur Sicherheit von Updates und Patches eines zu zertifizierenden IT-Sicherheitsprodukts machen, und unter dem Eindruck ihrer Aussagen beispielsweise in ihrer Antwort zu den Fragen 8 bis 12 der Kleinen Anfrage auf Bundestagsdrucksache 20/10149, wonach „[…] mit zunehmender informationstechnischer Komplexität von kritischen (Software-)Komponenten […] ein wesentlicher Teil der Beherrschbarkeit der Technologie im Rahmen der Produktpflege (Softwareupdates, Firmware-Updates, Schließen von Sicherheitslücken) beim Hersteller selbst oder innerhalb der weiteren Lieferkette [verbleibt]“ und wonach „[…] aufgrund der hohen Komplexität kritischer Komponenten und der zu erwartenden stetigen Software/Firmware-Updates […] etwa hohe technische Sicherheitsanforderungen keine ausreichende Sicherheit dahingehend [bieten], dass Hersteller keine missbräuchlichen Zugriffmöglichkeiten auf Hard- und Software implementieren oder sonstige Handlungen vornehmen, die Sabota-

ge oder Spionage ermöglichen“, Änderungen dahin gehend vorzunehmen, dass Produktzertifizierungen des BSI auch zukünftig zu Updates und Patches Aussagen machen können, wenn nein, warum nicht, und welche anderen Maßnahmen ergreift die Bundesregierung, um zukunftsbezogene Aussagen zur Sicherheit von Updates und Patches eines zu zertifizierenden IT-Sicherheitsprodukts machen zu können?

Eine Produktzertifizierung nach CC, Technischen Richtlinien, BSZ (= Beschleunigte Sicherheitszertifizierung) und NESAS (= Network Equipment Security Assurance Scheme) macht keine zukunftsbezogenen Aussagen zur Sicherheit von Updates oder Patches. Eine Produktzertifizierung bestätigt die Konformität eines ordnungsgemäß bezeichneten Produkts in einer bestimmten Ausprägung (Produktversion) zu den vom BSI festgelegten Kriterien zum Zeitpunkt der Konformitätsbewertung (z. B. eine Norm oder eine Technische Richtlinie in einer bestimmten Version). Werden das Produkt oder die Kriterien verändert, so ist eine neue Konformitätsaussage zu treffen, die das Zertifikat erweitern oder erneuern (Aufrechterhaltung einer Zertifizierung).

Alle benannten Zertifizierungsprogramme stellen Mechanismen zur Aufrechterhaltung von Zertifizierungen bereit, die es ermöglichen, ein geändertes Produkt (z. B. durch eine Software-Aktualisierung oder eine Änderung von Hardware-Elementen) ebenfalls als zertifiziert zu deklarieren. Diese Mechanismen enthalten eine wiederholte Prüfung unter Berücksichtigung der jeweiligen Änderungen, in der Regel mit einem geringeren Testaufwand als für die initiale Zertifizierung. Die Zertifizierungsprogramme werden vom BSI permanent weiterentwickelt und dem technologischen Fortschritt angepasst, sodass Produktzertifizierungen des BSI auch zukünftig zu Updates und Patches belastbare Aussagen machen können.

Ein vereinfachter Prozess, um bestehende Zertifikate um Updates oder Patches zu erweitern, ist für das Programm CC in Pilotierung. Ein Zertifikat für ein (durch Updates oder Patches) geändertes Produkt wird im Programm BSZ generell und im Programm NESAS CCS-GI (= Cybersecurity Certification Scheme) grundsätzlich auf dem Wege einer Rezertifizierung erteilt. Im Programm NESAS CCS-GI haben Antragsteller die Möglichkeit, für ihr zertifiziertes Produkt „geringfügige Aktualisierungen“, definiert als „Anpassungen von Sicherheitsfunktionen oder der Beschaffenheit des Produktes, die der Aufrechterhaltung oder Wiederherstellung der zertifizierten Sicherheitsleistung (als Summe der Sicherheitsaussagen der Produktevaluation) dienen oder die für die Sicherheitsleistung irrelevant sind“, an das BSI zu melden, zusammen mit einem Bericht zur Auswirkungsanalyse und dem Votum der sachverständigen Stelle, die das Produkt im Rahmen der Zertifizierung geprüft hat. Widerspricht die Zertifizierungsstelle nicht innerhalb von 30 Kalendertagen, so gilt das geringfügig aktualisierte Produkt ebenso wie das ursprüngliche Produkt über das bestehende Zertifikat zertifiziert. Innerhalb der benannten Widerspruchsfrist gilt das geringfügig aktualisierte Produkt insofern als vorläufig zertifiziert.

Mit dem im Dezember 2024 in Kraft getretenen sog. Cyber Resilience Act (CRA) werden erstmalig verbindliche horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen für den europäischen Binnenmarkt eingeführt. Die Anforderungen sehen u. a. eine verpflichtende Schwachstellenbehandlung sowie die Bereitstellung von Sicherheitsaktualisierungen vor. Ferner sieht der CRA vor, dass hierzu entsprechende europäische Standards erarbeitet werden, die zum Nachweis der Konformität mit dem CRA genutzt werden können.

44. Welche Möglichkeiten haben die in die Beschaffung von IT-Sicherheitsprodukten betreffenden Vergabeverfahren unterlegenen Bieter jeweils im Rahmen der Verordnung über die Vergabe öffentlicher Aufträge und im Rahmen der Vergabeverordnung für die Bereiche Sicherheit und Verteidigung, gegen eine Vergabeentscheidung Beschwerde beziehungsweise Klage einzureichen, welche Fristen gelten dabei jeweils, und bis zu wie viele Instanzen können hinsichtlich einer Beschwerde beziehungsweise Klage dabei durchlaufen werden?

Unterlegene Bieter haben in Verfahren auf Basis der Vergabeverordnung (VgV) oder Vergabeordnung für die Bereiche Verteidigung und Sicherheit (VSVgV) die Möglichkeit, einen Nachprüfungsantrag bei der jeweils zuständigen Vergabekammer zu stellen, wenn der Auftraggeber einer Rüge des Bieters nicht abhilft. Voraussetzungen und Verfahren sowie die Möglichkeit, in der nächsten Instanz sofortige Beschwerde beim Vergabesenat des jeweils zuständigen Oberlandesgerichtes einzureichen, richten sich nach §§ 160 ff. GWB. Rügen sind beim Auftraggeber innerhalb einer Frist von zehn Kalendertagen nach Erkennen eines Verstoßes grundsätzlich geltend zu machen. Die Frist für einen Nachprüfungsantrag in den dem Beschleunigungsgrundsatz unterliegenden Nachprüfungsverfahren beträgt grundsätzlich 15 Kalendertage ab Mitteilung des Auftraggebers, einer Rüge nicht abhelfen zu wollen (siehe im Einzelnen § 160 Absatz 3 GWB). Die sofortige Beschwerde ist binnen einer Notfrist von zwei Wochen ab Zustellung der Entscheidung der Vergabekammer zu stellen (§ 172 Absatz 1 GWB). Das Oberlandesgericht ist die zweite und letzte Instanz im vergaberechtlichen Nachprüfungsverfahren. Der Bundesgerichtshof kann außerordentlich vom Oberlandesgericht nur im Rahmen einer sogenannten Divergenzvorlage angerufen werden, soweit es von einer Entscheidung eines anderen Oberlandesgerichts oder des Bundesgerichtshofs abweichen will (§ 179 Absatz 2 GWB).

a) Wie viele Verfahren im Zusammenhang mit Beschwerden beziehungsweise Klagen gegen eine Vergabeentscheidung hinsichtlich eines Vergabeverfahrens zur Beschaffung von IT-Sicherheitsprodukten gab beziehungsweise gibt es jeweils in den Jahren 2022, 2023 und 2024?

b) Wie viele Instanzen wurden dabei im Schnitt durchlaufen?

c) Wie lange dauerten die Verfahren dabei im Schnitt?

d) Wie viele der Verfahren sind abgeschlossen, und wie viele Verfahren dauern noch an (bitte für die Jahre 2022, 2023 und 2024 angeben)?

Die Fragen 44a bis 44d werden gemeinsam beantwortet.

Der Bundesregierung liegen die in Frage 44a bis 44d angefragten Zahlen zu Nachprüfungsverfahren gegen Vergabeentscheidungen hinsichtlich von Vergabeverfahren zur Beschaffung von IT-Sicherheitsprodukten nicht umfassend vor. Die Unterrichtungspflichten der Nachprüfungsinstanzen nach § 184 GWB enthalten keinen Bezug zum jeweiligen Auftragsgegenstand. In der zur Beantwortung der Kleinen Anfrage zur Verfügung stehenden Zeit konnten für den Bund folgende Zahlen zu Nachprüfungsverfahren nach §§ 160 ff. GWB bei Stellen des Bundes eruiert werden.

Bei den Vergabekammern des Bundes liegen folgende Zahlen für die Beschaffung von IT-Sicherheitsprodukten (im Sinne der Auflistungen der Kleinen Anfrage, etwa in Frage 1) vor:

a) 2022 ein Verfahren; 2023: kein Verfahren; 2024: ein Verfahren.

b) Nur eine Instanz (Vergabekammer).

c) Fünf Wochen.

d) Alle Verfahren sind abgeschlossen.

Da im Geschäftsbereich BMVg für einzelne Produktsparten keine Einzelstatistiken zu Rügen und Nachprüfungsverfahren geführt werden, war in der zur Verfügung stehenden Zeit keine umfassende Auswertung etwaiger Rügen möglich. Daher beschränken sich die angegebenen Zahlen auf die Nachprüfungsverfahren (I. und II. Instanz). Hierbei wurde der Begriff/ das Verständnis des BSI („Produkte für die Sicherheit in der Informationstechnik werden als IT-Sicherheitsprodukte bezeichnet“) herangezogen. Nicht völlig ausgeschlossen werden kann, dass Beschaffungen, die im Schwerpunkt einen anderen Beschaffungsgegenstand betrafen, Teile von IT-Sicherheitsprodukten enthalten haben, die angesichts der Kürze der Zeit ebenfalls nicht erfasst bzw. identifiziert werden konnten. Daher ergeben sich für den Geschäftsbereich BMVg folgende Zahlen:

a) 2022: drei Verfahren; 2023: kein Verfahren; 2024: kein Verfahren.

b) Im Durchschnitt werden 1,33 Instanzen (zweimal eine Instanz und einmal zwei Instanzen) durchlaufen.

c) Die Verfahren dauerten im Durchschnitt für die erste Instanz fünf bis sieben Wochen, für zwei Instanzen ein Jahr.

d) Die drei oben genannten Verfahren sind abgeschlossen.

45. Wie viele Software-Entwicklungsaufträge bezüglich IT-Sicherheitsprodukten hat die Bundesregierung seit Beginn der 20. Legislaturperiode erteilt (bitte nach Jahren aufschlüsseln)?

    a) Wie viele davon sind bereits fertig entwickelt?

    b) Wie viele befinden sich noch in der Entwicklung?

    c) Wie lange dauert die Entwicklung im Schnitt?

    d) Welche Vertragstypen (beispielsweise Werkverträge, Dienstverträge etc.) lagen dabei in jeweils wie vielen Fällen den Aufträgen zugrunde?

    e) Gibt es ein Standard-Vertragsmuster zur Beschaffung von IT-(Sicherheits-)Produkten, und wenn ja, welcher Vertragstyp liegt dem Standard-Vertragsmuster zugrunde?

    f) In wie vielen Fällen der Gesamtzahl an vergebenen Software-Entwicklungsaufträgen bezüglich IT-Sicherheitsprodukten wurde das Standard-Vertragsmuster verwendet?

Die Fragen 45 bis 45f werden gemeinsam beantwortet.

Die Bundesregierung hat seit Beginn der 20. Legislaturperiode zehn Software-Entwicklungsaufträge bezüglich IT-Sicherheitsprodukten erteilt (5 x 2021, 2x 2022, 1x 2023; 2 x 2024). Davon sind sieben Aufträge fertig entwickelt, sodass sich drei noch in Entwicklung befinden. Bei den sieben fertig gestellten Aufträgen dauerte die Entwicklung durchschnittlich 660 Tage. Für sieben Entwicklungsaufträge wurde ein Standard-Vertragsmuster für Werkverträge genutzt, für drei Aufträge Dienstleistungsverträge ohne Standardvertragsmuster.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333