BDI

INNONATION

POSITION | DIGITAL POLICY | CYBERSECURITY

Cybersecurity Act 2

German Industry's recommendations on the Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881.

24 April 2026

Executive Summary

The ever-increasing cybersecurity threat landscape requires both regulators, industry and operators of critical infrastructures to adopt risk-adequate cybersecurity measures. Such concrete measures should be supported by a lean regulatory framework that outlines requirements and provides companies with the necessary support framework. In recent years, with the NIS2 Directive, the Critical Entities Resilience (CER) Directive, the Cyber Resilience Act (CRA), RED-DA 2022/30, the Cyber Solidarity Act, the EU Cyber Blueprint, the 5G Cybersecurity Toolbox (5G Toolbox) and the Digital Operational Resilience Act (DORA) the European co-legislators have adopted a complex set of rules and regulations. With its revision of the Cybersecurity Act, the European Commission has missed an opportunity to streamline the regulatory framework, which would have been urgently needed. The Cybersecurity Act 2 (CSA 2) is not the cybersecurity trailer to the digital omnibus that German industry had hoped for.

German industry's policy recommendations

The European Commission's proposal contains important measures to strengthen the European Cybersecurity Agency (ENISA). A powerful and well-equipped ENISA is integral to increase Europe's cyber resilience. ENISA must be upgraded to a powerful implementation unit and reliable partner that closely monitors the implementation of cybersecurity regulations, advises companies and provides them with up-to-date threat assessments.

In general, German industry perceives the high number of implementing acts which the Commission's proposal entails as critical. Since German industry is a strong advocate of the ordinary legislative procedure which allows for meaningful and transparent stakeholder involvement, requirements should be directly regulated in the CSA 2 based on a mandatory impact assessments and transparent stakeholder involvement rather than through implementing acts.

While it is certainly commendable that the development of cybersecurity certification schemes is to be geared towards the needs of industry, this will not cut the Gordian knot. Instead, the European Commission and European industry should focus on implementing the CRA to strengthen the cyber resilience of products. Under the current governance and processes, the development of cybersecurity certification schemes has proven impractical, slow, bureaucratic and costly. EU wide cybersecurity certification can be a valuable instrument to strengthen trust and market transparency, provided that certification schemes are technically defined, risk based, internationally aligned and developed in close cooperation with industry, but should remain voluntary in their application.

Bundesverband der Deutschen Industrie e.V. / Federation of German Industries
EU Transparency Register: 1771817758-48 | German Lobbyregister: R000534
Steven Heckler and Philipp Schweikle | Innovation, Security and Technology | www.bdi.eu

Therefore, German industry proposes the following changes to the draft Cybersecurity Act 2:

ENISA

German industry supports that ENISA's budget is significantly increased. Considering the ever-increasing cyber-threat landscape and the evolving necessity for a strong European cybersecurity agency, it is paramount that ENISA is sufficiently staffed and has an adequate budget.

German industry perceives ENISA's contribution to developing a shared cybersecurity situational awareness as the single most important task that ENISA has to fulfil to enhance Europe's cyber resilience. To this end, the single-entry point for incident reporting must be swiftly established and it must be ensured that ENISA shares such analyses always immediately with all entities from sectors listed in Annexes I and II to Directive (EU) 2022/2555.

German industry appreciates that ENISA shall consult and cooperate with relevant stakeholders from across industry sectors. We believe that a close involvement of industry representatives in ENISA's technical work is crucial to ensure that ENISA receives real-world expertise and delivers results according to stakeholders' needs. In this regard, the continuation of the ENISA Advisory Group is a very positive step, however, ample industry involvement must be ensured. In addition, German industry supports further strengthening ENISA's coordinating role to avoid duplication of guidance and implementation efforts across overlapping cybersecurity frameworks while avoiding that ENISA replaces or bypasses recognised international standardisation bodies or national authorities.

The proposed fee mechanisms in Articles 46 and 47 creates an additional financial burden on companies and conformity assessment bodies of currently unknown magnitude, making it impossible to accurately forecast compliance costs. Under these provisions, manufacturers and conformity assessment bodies will face fees for participation in and issuance of certificates under European certification schemes, as well as fees for technical testing tools provided by ENISA. Therefore, these fees should be eliminated entirely. Cybersecurity certification serves a critical public policy objective and should be funded through public budgets rather than imposing additional costs on industry.

European Cybersecurity Certification Framework (ECCF)

Considering the experience with the implementation of the EU CSA in terms of the drafting of product-group-specific cybersecurity certification schemes, German industry would have appreciated if the European Commission had significantly streamlined and refocused the scheme-related articles from the CSA 2. In fact, we perceive the Cyber Resilience Act as better suited to enhance the cyber resilience of products throughout the EU since (1) the CRA introduces cybersecurity requirements that are binding for all products with digital elements placed on the European market, and since it (2) entails a more transparent and inclusive process in terms of stakeholder involvement for developing product-related requirements than the EU CSA. However, in general, EU-wide harmonised certification can simplify compliance with regulatory requirements for companies and deepen the European single market. To harness this potential, the process to develop cybersecurity certification schemes must be lean and entail industry involvement to ensure certification schemes that reflect industry's needs and the current state of technology. Should the European co-legislators opt for continuing the implementation of the ECCF, it should only be applied for non-product categories, i.e. services, that are not covered by the CRA, it must remain completely voluntary and should – wherever possible – build on existing standards. For higher assurance schemes, requirements should remain proportionate, risk based and technology neutral, and should avoid discriminatory approaches based on country of origin.

Trusted ICT Supply Chain Framework

In light of increasing geopolitical conflicts and Europe's reliance on global value chains, German industry in general supports enhancing Europe's resilience against external shocks and influence by

third countries. Secure and reliable ICT supply chains are crucial both for the proper functioning of essential and important entities and of society as a whole as well as for production processes. While German industry supports the European Commission's intention to enhance the resilience of ICT supply chains in general, we perceive the concrete proposal outlined in Articles 98 to 117 in need of far-reaching improvement. For several sectors, such as the automotive industry, that are producing goods for the entire single market, an EU-wide applicable framework is significantly better than 27 national approaches. We recommend that the European co-legislators ensure that beyond non-technical concerns (e.g. geopolitical and legal policy), technical, risk-based criteria are also given consideration.

Any measures to enhance the security of ICT supply chains has to properly reflect operational and supply-chain realities and therefore include a structured consultation mechanism with essential and important entities under the NIS2 Directive. Risk assessments and mitigation measures must remain realistic, technically feasible and must account for sector-specific realities. Before any restrictive measure is imposed, the availability of alternative suppliers, the maturity of the relevant alternative technologies, the product lifecycle and the criticality of the ICT asset in question must all be considered carefully. A phase out or more restrictive measures constitute a fundamental encroachment on rights of ownership. Therefore, it should only be applied in cases of evident and significant risk to the resilience of an entity or infrastructure. In addition, where mitigation measures are introduced, realistic transition timelines aligned with supply-chain realities should be established. If new ICT supply chain security requirements compel EU companies to remove certain components from "high-risk suppliers" costs could reach millions of euros per component type and company. These expenditures serve broader societal security goals rather than direct business interests, placing affected companies and their European customers at a competitive disadvantage in both EU and global markets. Henceforth, a full compensation for such ICT products, components and services must be provided by the Member States or the EU to offset these publicly motivated costs. Finally, before introducing the ICT supply chain framework, the European co-legislators must ensure that there is not only a perceived but a real regulatory deficit. Currently, existing rules, such as the GDPR or sector-specific cybersecurity and / or supply chain requirements, could already function as mitigating measures against interference in some sectors but are not sufficiently applied. Hence, while German industry supports the European Commission's intention to enhance the resilience of ICT supply chains in general, we perceive the concrete proposal outlined in Articles 98 to 117 in need of far-reaching improvement.

In general, we believe that future-oriented requirements should always be considered first when seeking to improve the resilience of industries and infrastructure, since they result in the lowest costs for industry and society alike. To ensure proportionality of the requirements, BDI urges the European co-legislators to differentiate between entities falling within on the one hand NIS 2 Annex I, and on the other hand Annex II and those mentioned in Recital 133 respectively. Given their high level of systemic relevance for Europe's society as a whole and other industry sectors, for entities operating in sectors listed in NIS 2 Annex I, any measure taken should be based on a thorough risk-based assessment and applied solely where other proportionate and effective risk management measures are not sufficient to adequately address the identified ICT-related and cyber security risks, and provided that appropriate compensation is paid, a continuous supply is secured, no decline in performance is ensured and realistic transition periods are agreed. To ensure realistic timeframes, the European Commission must consider the availability of alternative components, the availability of qualified personnel, and the interplay with other political goals, such as the energy transformation or the expansion of mobile networks. In contrast, for companies under Annex II of the NIS 2 Directive, the requirements emanating from the ICT Supply Chain Framework should be strictly limited to forward-looking, risk-based management measures, reflecting their lower level of systemic criticality. Therefore, grandfathering should be applied, both with regard to the companies concerned and to the products they develop and manufacture.

Table of Content

Recitals

Recital 32 – Early alert service

In light of the growing cyber threat landscape, German industry strongly supports any measure that helps essential and important entities to receive up-to-date information and current cyber threats. In this regard, we encourage ENISA to swiftly set up an early alert service to increase awareness of cyber threat indicators and recommendations on mitigation measures. Early alerts issued by ENISA should be limited to publicly known vulnerabilities and should complement existing vulnerability reporting and coordinated disclosure processes under Regulation (EU) 2024/2847. Premature dissemination of vulnerability details subject to ongoing mitigation or coordinated disclosure processes should be avoided. The respective information should be made available to all companies falling within the scope of Directive (EU) 2022/2555 through one platform that contains the information from the early alert service, the trends in cyber threats and incidents identified by ENISA (cf. Recital 33), and the information generated from the Single Entry Point for Incident Reporting established by the Data Omnibus.

Recital 34 – Analyses of cyber threats, incidents, including regular analysis in NIS2 sectors and products categories under Regulation (EU) 2024/2847

German industry appreciates the proposal to enhance the shared situational awareness of the cyber threat and incident landscape by ENISA analysing trends in cyber threats and incidents. The respective information should be made available to all companies falling within the scope of Directive (EU) 2022/2555 through one platform that contains the information from the early alert service (Recital31), the trends in cyber threats and incidents identified by ENISA, and the information generated from the Single Entry Point for Incident Reporting established by the Data Omnibus.

Recitals 77 and 79 – Cyber posture of entities

In light of the existence and global recognition of ISO 27001 or TISAX, German industry questions the necessity to develop another cybersecurity security certification scheme under the European Cybersecurity Certification Framework as it poses the risk to duplicate existing and well-functioning mechanisms. Since Member States can make the utilisation of certain certification schemes by essential and important entities mandatory, German industry sees the risk that companies that already fulfil ISO 27001 or equivalent norms might have to be additionally certified against the new “cyber posture of entities” certification scheme, which would result in unnecessary bureaucratic work without increasing the cyber-resilience of these entities. Therefore, the cyber posture of entities schemes should only be developed as an additional, completely voluntary certification mechanism which companies, which deem international standards as too far-reaching or burdensome, can utilise to demonstrate compliance with the NIS 2 Directive.

Recital 83 – European Cybersecurity Certification Assembly

Despite the existence of the Stakeholder Cybersecurity Certification Group (SCCG), in the past, the development of European cybersecurity certification schemes lacked an effective and meaningful involvement of all relevant industry representatives. Therefore, should the European co-legislators decide to continue the development of European cybersecurity certification schemes, the creation of the European Cybersecurity Certification Assembly is a practical idea to promote better stakeholder involvement. It must be ensured that all companies that wish to join the assembly can do so, have a right to speak out, and are granted access to all current documents regarding the development of European cybersecurity certification schemes.

Title I: General Provisions

Article 2 – Definitions

Regarding Art. 2 number 29: The cyber posture of entities should refer to the level of cybersecurity with respect to the specific cybersecurity and not general security requirements a company has to adopt. Otherwise, also non-cyber security requirements would have to be taken into account which is beyond the scope of this regulation and Directive 2055/2022.

Since many European companies are also established in third countries, the definition of high-risk suppliers should be limited to such entities that are controlled by a third country. Additionally, the European co-legislators should apply a more nuanced and thus, risk-based approach by also giving consideration to technical risk-parameters of products.

German industry would welcome the implementation of the following amendments to the current draft law:

(29)‘cyber posture of entities’ means entities’ level of cybersecurity with respect to the specific *cyber* security requirements;

(30)‘high-risk supplier’ means either of the following:

(a) an entity *controlled by* ~~*established in*~~ a third country posing cybersecurity concerns designated in accordance with Article 100, or ~~*controlled by such third country,*~~ by an entity established in such third country, or by a national of such third country;

(b) an entity designated in accordance with Article 103 (7) and entities controlled by that entity;

Title II: ENISA (The European Union Agency for Cybersecurity)

Article 4 – Objectives of ENISA

German industry perceives ENISA as the core institution to strengthen Europe’s cyber resilience. Therefore, we welcome the strong overall mandate that the CSA 2 envisions for ENISA. Since the damage caused by cyber attacks to industry in Germany last year amounted to 202.4 billion Euros, German industry would welcome a very strong interaction between ENISA, the German Federal Security Agency (BSI), and the private sector to ensure that ENISA’s work is geared at reducing the negative repercussions emanating from the evolving threat landscape. Furthermore, ENISA should coordinate market surveillance across the EU to ensure a level playing field for all market participants, irrespective of where they are based in the EU.

In the area of post-quantum cryptography, ENISA should contribute technical expertise and stakeholder coordination to established international standardisation processes. The development or approval of cryptographic standards should remain within globally recognised standard-setting frameworks to ensure interoperability and avoid fragmentation.German industry would welcome the implementation of the following amendments to the current draft law:

2. ENISA shall assist Member States and, where appropriate, Union entities in implementing horizontal and sectoral Union policies and legislation related to cybersecurity, including market surveillance activities. *ENISA shall coordinate market surveillance activities across the Union*

to ensure equal treatment of all market participants regardless of their establishment within the Union.

Article 11 – Shared cybersecurity situational awareness

In light of the ever-increasing cyber threat landscape, German industry perceives ENISA's contribution to developing a shared cybersecurity situational awareness as an important task that ENISA has to fulfil to enhance Europe's cyber resilience. It must be ensured that ENISA shares such analyses always immediately with all entities from sectors listed in Annexes I and II to Directive (EU) 2022/2555. Only by sharing the information from the repositories and analyses mentioned in Article 11 (1) (a), (b), (c), (d) and (e) with essential and important entities can such entities enhance their cyber resilience accordingly.

It must be ensured that companies do not have to report the same incident to several institutions. Rather, all competent authorities at the national and European level must have access to the information reported by essential and important entities through the Single Entry Point for Incident Reporting to ENISA.

German industry would welcome the implementation of the following amendments to the current draft law:

3. ENISA *shall share* ~~*may make*~~ the analyses, advice, guidance, best practices and reports referred to in paragraph 2 *with essential and important entities listed in Annexes I and II of Directive (EU) 2055/2022* ~~*public*~~, in agreement with the contributing entities referred to in paragraph 2.

Article 12 – Early Alerts

Time is of essence when it comes to the mitigation of cyber threats. Therefore, we welcome that ENISA is empowered to share its early alerts with essential and important entities listed in Annexes I and II of Directive (EU) 2055/2022. By receiving this information in a timely, essential and important entities can implement measures to increase the cyber resilience of their entities. This would help ensuring that their entity is not affected by the respective cyber threat. This would have the potential to significantly reduce the economic damage caused by cyber threats. ENISA should set up the early alert service for entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555 no later than one year after the coming into force of the CSA 2.

German industry would welcome the implementation of the following amendments to the current draft law:

3. *By no later than one year after the coming into effect of this Regulation,* ENISA shall offer an early alert service to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555.

Article 13 – Support in incident response and review

German industry in general welcomes the idea that ENISA in cooperation with Europol and CSIRTs or other competent authorities as applicable shall establish a helpdesk and shall share situational awareness on cyber threats and the incident landscape. However, ENISA must ensure that the helpdesk is sufficiently staffed to even help a significant number of essential and important entities in the situation of an accentuated crisis. Otherwise, companies might rely on the respective help and do not receive it when required.

Article 35 – ENISA Advisory Group

ENISA should carry out its work based on expert knowledge from various stakeholder groups. Therefore, German industry welcomes the establishment of the ENISA Advisory Group. We especially appreciate the vast industry representation foreseen in Article 35 paragraph 1. To ensure the rotation between industry representatives we appreciate the working procedures established in paragraph 4. It must be ensured that the guidance provided by the Advisory Group is taken into account by the Management Board and the Executive Directors as well as his/her Deputy.

Article 69 – Cooperation with stakeholders

German industry appreciates that as part of its official mandate, ENISA is asked to cooperate with relevant stakeholders from across industry sectors. We believe that a close involvement of industry representatives in ENISA's technical work is crucial to ensure that ENISA receives real-world expertise and delivers results according to stakeholders' needs.

Title III: European Cybersecurity Certification Framework

German industry recognises the benefits that certification brings for entities integrating components into their systems or buying ICT products from third parties. In this regard, German industry supports the European Commission's aspiration to diffuse cybersecurity certification across product groups. However, we perceive the Cyber Resilience Act as the most appropriate regulatory framework to this end. Considering the experience with the implementation of the ECCF in terms of the drafting of product-group-specific cybersecurity certification schemes, German industry would have appreciated if the European Commission had significantly streamlined and refocused the scheme-related articles from the EU CSA. In fact, we perceive the Cyber Resilience Act as better suited to enhance the cyber resilience of products throughout the EU since (1) the CRA introduces cybersecurity requirements that are binding for all products with digital elements placed on the European market, and since it (2) entails a more transparent and inclusive process in terms of stakeholder involvement for developing product-related requirements than the EU CSA. Despite our general hesitance with regard to the continuation of the ECCF, we recognise that EU-wide harmonised certification can simplify compliance with regulatory requirements for companies and deepen the European single market. To harness this potential, the process to develop cybersecurity certification schemes must be lean and entail industry involvement to ensure certification schemes that reflect industry's needs and the current state of technology. Should the European co-legislators opt for continuing the implementation of the ECCF, it should only be applied for non-product categories, e.g. standalone services, that are not covered by the CRA, it must remain completely voluntary and should – wherever possible – build on existing standards.

The CRA mandates the Commission to develop practical guidance regarding the implementation of the CRA. The CSA should focus on providing ENISA with the right resources to provide advice in that regard, in close cooperation with industry. That would address a need from economic operators in particular regarding system extensions and mixed architectures for critical sectors (e.g., transport, energy, process industries). Such guidance could standardise interface-level compensating measures to ensure that market surveillance authorities can consistently recognise them as CRA-compliant.

While there are significant concerns regarding the articles related to the European Cybersecurity Certification Framework in recognition of the European Commission's preference to continue the development of cybersecurity certification schemes we urge the European co-legislators to adopt at least the following changes to the current proposal:

Article 71 – Objectives and scope of the European cybersecurity certification framework

Since the Cyber Resilience Act introduced cybersecurity requirements for all products with digital elements, German industry questions the development of cybersecurity certification schemes.

In light of the existence and global recognition of ISO 27001 or TISAX, German industry questions the necessity to develop another cybersecurity security certification scheme under the European Cybersecurity Certification Framework as it poses the risk to duplicate existing and well-functioning mechanisms. Since Member States can make the utilisation of certain certification schemes by essential and important entities mandatory, German industry sees the risk that companies that already fulfil ISO 27001 or equivalent norms might have to be certified as well against the new "cyber posture of entities" certification scheme, which could result in unnecessary bureaucratic work without increasing the cyber-resilience of these entities. Therefore, the cyber posture of entities schemes should only be developed as an additional, completely voluntary certification mechanism which companies, which deem international standards as too far-reaching or burdensome, can utilise to demonstrate compliance with the NIS 2 Directive.

German industry urges the co-legislators to leave the utilisation of the European cybersecurity certification schemes voluntary and they should "re-use" existing standards. To avoid regulatory fragmentation across the Union, it should not be envisaged that Member States can define the application of cybersecurity certification schemes as mandatory. Otherwise, this would result in excessive implementation costs, considerable delays and a significant loss of flexibility for companies with only very limited benefits for Europe's cyber-resilience.EU Certification Schemes should avoid duplicating obligations already addressed by the Cyber Resilience Act and should focus on areas not covered by CRA, such as certain standalone services or organisational cyber posture, while remaining voluntary and risk based. The cyber-resilience of products should be increased through other legal acts, in particular the Cyber Resilience Act and the Medical Device Regulation.

German industry would welcome the implementation of the following amendments to the current draft law:

1. The European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes and to attest the following:

    (a) that the ~~*ICT products,*~~ ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their lifecycle;

    (c) that the cyber posture of an entity that has been evaluated in accordance with such schemes *or internationally recognised standards with the same effect* complies with specified cybersecurity requirements.

3. European cybersecurity certification shall be voluntary~~*, unless otherwise specified in Union or national law*~~.

4. *Technical specifications developed by ENISA shall complement, and not replace, international or European consensus-based cybersecurity standards where such standards already exist or are reasonably expected to emerge.*

Article 72 – Public information and consultation

To ensure that cybersecurity certification schemes can be easily implemented by industry, a thorough stakeholder involvement is paramount. While we welcome the establishment of the European Cybersecurity Certification Assembly as a forum for the discussion of strategic priorities, a more in-depth stakeholder involvement is urgently required during the development of cybersecurity certification schemes. Having only an annual meeting with hundreds of stakeholders is not sufficient to ensure that certification schemes account for industry's needs. Therefore, ENISA should be required to set up one working group per scheme comprising all interested industry stakeholder to ensure that they can contribute to the drafting of these schemes in a meaningful manner.

To ensure meaningful multistakeholder input, the Regulation should specify the stakeholder categories to be represented in the Assembly, rather than relying solely on an open-ended reference to "relevant stakeholders". This should include, inter alia, ICT product and service providers (including cloud and digital service providers), essential and important entities under NIS2, SMEs and users and demand-side organisations.

German industry would welcome the implementation of the following amendments to the current draft law:

1. At least *twice* ~~*once*~~ a year, the Commission shall organise, with the support of ENISA, a European Cybersecurity Certification Assembly, inviting ECCG members and other relevant experts from Member States, relevant experts from Union entities and relevant *industry* stakeholders to discuss strategic priorities for harmonisation in the area of cybersecurity certification.

6. *For each candidate cybersecurity certification scheme, ENISA shall establish a working group comprising relevant industry stakeholders to receive practical and technical expertise.*

Article 74 – Preparation and adoption of European cybersecurity certification schemes

German industry welcomes the clarifications regarding the preparation of European cybersecurity certification schemes in general. Nonetheless, we would appreciate if the co-legislators would consider the following aspects:

Paragraphs 1, 5, 6 and 7: In light of the experience of the development of European cybersecurity certification schemes since 2019, it is very reasonable to set a clear timeframe within which ENISA shall develop a candidate scheme and stringent deadlines for the consultation of Member States. The wording of paragraph one should be clarified in such a way as to stress that within 12 months ENISA must have finished the drafting of a candidate scheme.

Paragraph 4: When preparing European cybersecurity certification schemes, ENISA must closely involve industry stakeholders to ensure that the proposal is practicable and meaningful. While we welcome the requirement to involve industry, we urge the co-legislators to introduce a form of involvement of industry representatives that allows for continuous consultation rather than only temporary surveys. The clarification in paragraph 4 is necessary since Article 32 (6) does not specify that the working group shall involve representatives from industry.

German industry would welcome the implementation of the following amendments to the current draft law:

1. No later than 12 months after receiving a request from the Commission pursuant to Article 73, unless otherwise specified in the request, ENISA shall *have* prepare a candidate European cybersecurity certification scheme that meets the requirements set out in Articles 80 and 81.

4. When preparing the candidate scheme, including, where applicable, supporting technical specifications, ENISA shall consult stakeholders in a timely manner by means of a formal, open, transparent and inclusive consultation process *and by setting up a dedicated working group in which all interested industry stakeholders can participate*. ENISA shall also cooperate with relevant public authorities in the Member States and with relevant Union entities to gather their expert advice in relation to the preparation of the candidate scheme and, where applicable, supporting technical specifications. When transmitting the candidate scheme to the Commission pursuant to paragraph 6, ENISA shall describe the manner in which it has complied with this paragraph.

5. To improve transparency and predictability, ENISA shall publish and regularly update an action plan for developing and maintaining schemes, including key milestones and consultation timelines. ENISA and the Commission shall publish summaries of stakeholder feedback received during feasibility studies, scheme development and maintenance, and explain how such input informed revisions.

6. Technical specifications underpinning European cybersecurity certification schemes shall, by default, be publicly available. Certification schemes should not rely on non-public or restricted technical specifications as mandatory elements.

Article 75 – Maintenance of a European cybersecurity certification scheme

Since technology and thus threat vectors are constantly evolving, German industry appreciates the establishment of a maintenance procedure for European cybersecurity certification schemes. With regards to Article 75 (3) we strongly encourage the European co-legislators to ensure an obligatory involvement of industry in this process since companies are the main users of such schemes.

German industry would welcome the implementation of the following amendments to the current draft law:

3. ENISA *shall* ~~*may*~~ organise the involvement of the private sector for the maintenance of a scheme in the form of an ad hoc working group in accordance with the maintenance strategy referred to in paragraph 1.

Article 78 – Presumption of conformity as a tool to support regulatory compliance

German industry supports the approach of using certification as an optional tool to facilitate regulatory compliance. To leverage certifications across the Digital Single Market, certification outcomes should be consistently recognised across Member States and should not trigger additional national evidence requirements beyond the EU scheme. Consequently, companies should have certainty that, if they choose to certify their overall cyber posture, products, services or processes under a European scheme, this will be sufficient to demonstrate compliance with EU legal requirements, without the possibility for Member States to demand additional evidence. At the same time, it is important that certification schemes retain their voluntary nature and serve as a supportive mechanism for achieving

regulatory objectives. Certification should help simplify compliance while preserving innovation and technological openness.

Article 80 – Security objectives of European cybersecurity certification schemes

The more than 20 objectives listed in Article 80 represent a random collection of requirements that mix product obligations (cf. CRA Annex I), duties for service providers, and expectations for development processes. In contrast to the CRA, whose objectives in Annex I Part I(2) are explicitly risk-based, Art. 80 formulates its objectives in absolute terms, without considering proportionality or risk. In addition, many of the objectives duplicate existing requirements from other regulations such as the CRA and NIS2, which creates unnecessary overlap and potential inconsistencies. To avoid this fragmentation, the individual objectives in Article 80 should be removed. Instead, the regulation should reference the established objectives already defined in the relevant regulations, in particular the CRA and NIS2.

German industry recommends that Article 80 (2) should be deleted. Allowing the European Commission to change the security objectives of certifications could create legal uncertainty, and could be used to add non-technical risks after the legislation is passed.

German industry recommends the following concrete changes to the legislative proposal:

~~*1. The Commission is empowered to adopt delegated acts in accordance with Article 119 to amend paragraph 1 of this Article by adding or modifying security objectives in order to ensure that they reflect the latest technological development and new related threats as well as adoption of new Union legislation setting out the demonstration of compliance and the presumption of conformity through European cybersecurity certification with relevant cybersecurity requirements of that legislation.*~~

Article 81 – Elements of European cybersecurity certification schemes

According to Article 81 (3) (c), Member States may propose extension profiles introducing additional requirements for specific product categories. However, such extensions are only viable if they are uniformly adopted across all Member States and apply to the certification scheme as a whole. Allowing divergent national extensions would undermine the objective of harmonisation, create fragmentation within the internal market, and impose significant additional administrative and compliance burdens on companies. To safeguard legal certainty and ensure the effectiveness of the certification framework, extension profiles must therefore be applied consistently at EU level.

Furthermore, to preserve the harmonisation objectives of the European cybersecurity certification framework, certification schemes and any associated extension profiles should remain strictly technical in nature. They should not be used to introduce ownership-based, jurisdiction-based or other non-technical requirements which would be more appropriately addressed through separate regulatory instruments.

What is missing in Article 81, is an obligation on ENISA to ensure that all schemes under the ECCF include a mechanism that enables ‘continuous conformity’ without constant recertification. Unfortunately, the term only appears in Recital (93). Article 81 (2) (a) contains some approaches, but does not go far enough. Unfortunately, the only certification scheme that exists (EUCC) suffers from the recertification requirement: software with the certificate would usually be outdated and have known security vulnerabilities. So you either use a current, secure version without a certificate, or an outdated, insecure version with a certificate. CSA2 therefore needs to move significantly further away from a product-based approach with a few exceptions.

Article 83 – Conformity self-assessment

To keep the bureaucratic burden associated with the implementation of the European cybersecurity certification schemes for companies proportionate, we welcome the possibility for conformity self-assessment in relation to ICT products, ICT services, ICT processes, managed security services or cyber posture of entities that present a low risk corresponding to assurance level “basic”. This approach is especially suitable for mass market ICT products, ICT services and ICT processes which have a low level of criticality.

Article 86 – National cybersecurity certification schemes and certificates

German industry welcomes the European Commission’s proposal that national cybersecurity certification schemes, and the related procedures for the ICT products, ICT services, ICT processes, managed security services and cyber posture of entities that are covered by the subject matter and scope of a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 74 (9). This helps to foster the European digital Single Market and reduces the bureaucratic burden for companies which otherwise might have to comply both with national and the European certification framework. Moreover, it also enhances the clarity for consumers on the European market which otherwise could be easily confused whether the two certification schemes are equivalent in providing information about the cyber resilience of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities.

Title IV: Security of ICT Supply Chains

Article 98 – Scope of the framework

In light of increasing geopolitical conflicts and Europe’s reliance on global value chains, German industry in general supports the adoption of measures that enhance Europe’s resilience against external shocks and influence by third countries. Secure and reliable ICT supply chains are crucial both for the proper functioning of essential and important entities and of society as a whole as well as for production processes. Operators of critical infrastructures as well as essential entities and important entities are already taking far-reaching, risk-appropriate measures to protect their systems and processes against cyber-attacks and unauthorised interference by third parties. While German industry supports the European Commission’s intention to enhance the resilience of ICT supply chains in general, we perceive the concrete proposal outlined in Articles 98 to 117 in need of far-reaching improvement. For several sectors, such as the automotive industry and other manufacturing sectors that are producing goods for the entire single market, an EU-wide applicable framework is significantly better than 27 national approaches. We recommend that the European co-legislators ensure that beyond non-technical concerns (e.g. geopolitical and legal policy), also technical, risk-based criteria are given consideration.

As different sectors (e.g., rail infrastructure or energy infrastructure) face different supply-chain exposures and supplier potential, we recommend sector-specific measures. Hence, the framework should be applied in a manner that reflects operational and supply-chain realities and therefore must include a structured consultation mechanism with essential and important entities under the NIS2 Directive and their suppliers. Risk assessments and mitigation measures must remain realistic, technically and legally feasible, and should account for sector-specific realities. Before any mitigating or restrictive measure is imposed, the availability of alternative suppliers, the maturity of the relevant alternative technologies, the product lifecycle and the criticality of the ICT asset in question must all be considered carefully. A phase out or more restrictive measures constitute a fundamental encroachment on rights of ownership. Therefore, it should only be applied in cases of evident and significant risk to the resilience of an entity or infrastructure. In addition, where restrictive or mitigation measures are introduced,

realistic transition timelines aligned with supply-chain realities should be established. New ICT supply chain security requirements may compel EU companies to remove components from “high-risk suppliers” at costs reaching millions of euros per component type and company. These expenditures serve broader societal security goals rather than direct business interests, placing affected companies and their European customers at a competitive disadvantage in both EU and global markets. Henceforth, a full compensation for such ICT products, components and services must be provided by the Member States or the EU to offset these publicly motivated costs. Finally, before introducing the ICT supply chain framework, the European co-legislators must ensure that there is not only a perceived but a real regulatory deficit. Currently, existing rules, such as GDPR, could already function as mitigating measures against non-EU interference in some sectors but are not sufficiently applied.

In their analysis and the subsequent definition of high-risk countries and suppliers, the European Commission must also take into consideration the criticality that an ICT asset poses to the proper functioning of an entity in the scope of this Regulation as well as the extent of damage to other critical infrastructures an ICT asset could create. While certain ICT assets are very critical for the proper functioning of an entity others are utilised for less neuralgic services and therefore, may not need to fulfil the same security requirements.

In general, we believe that future-oriented requirements should always be considered first when seeking to improve the resilience of industries and infrastructure, since they result in the lowest costs for industry and society alike. To ensure proportionality of the requirements, BDI urges the European co-legislators to differentiate between entities falling within on the one hand NIS 2 Annex I, and on the other hand Annex II and those mentioned in Recital 133 respectively. Due to their criticality for Europe’s society as a whole and other industry sectors, for entities in sectors according to NIS 2 Annex I any measure taken should be based on a thorough risk-based assessment and applied solely where other proportionate and effective risk management measures are not sufficient to adequately address the identified ICT-related and cyber security risks, and provided that appropriate compensation is paid, a continuous supply is secured, no decline in performance is ensured and realistic transition periods are agreed. In contrast, for companies under Annex II of the NIS 2 Directive and those mentioned in Recital 133, the requirements emanating from the ICT Supply Chain Framework should be strictly limited to forward-looking as defined hereabove, risk-based management measures, reflecting their lower level of systemic criticality. In this context, grandfathering should be applied, both with regard to the companies concerned and to the products they develop and manufacture.

The EU Member States should strive for a high degree of harmonisation of cybersecurity requirements. Therefore, only in limited well-justified cases should Member States make use of the provision for deviation laid down in Article 98 (3). The current hotch-potch of cybersecurity requirements in the EU caused by the combination of EU regulatory requirements, gold-plating of the former by Member States, and additional national requirements leads to unnecessary bureaucracy, inconsistencies and a lack of regulatory clarity for companies operating in the European Union. Therefore, German industry expressly supports the European Commission’s intention for harmonisation.

To enable companies that produce goods utilising ICT assets falling in the scope of Title IV of the EU CSA 2 to scale their production, the European Commission should always strive to align its approach to a certain high-risk countries and high-risk suppliers with that of the EU’s international partners. For example, when identifying high-risk ICT assets for connected vehicles, the European Commission should consider the Final Rule issued by the US Department of Commerce’s (Department) Bureau of Industry and Security (BIS) on “Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles”. Harmonised regulatory requirements across jurisdictions reduces the costs associated with the adoption of such requirements for companies. Therefore, the European co-legislators should introduce the additional paragraph 4 proposed below.

German industry would welcome the implementation of the following amendments to the current draft law:

4. *The European Commission shall align its measures laid down in paragraph 1 to identify ICT assets in critical ICT supply chains with those defined by its international partners to ensure minimal impact for entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555 and those entities mentioned in Recital 133 of this Regulation.*

Article 99 – Security risk assessments

German industry supports the approach for the security risk assessment laid down in Article 99. However, we urge the European co-legislators to extensively engage with stakeholders from entities falling in the scope of this Regulation to ensure that their expertise on alternative sources for ICT assets as well as the criticality of these ICT assets are taken sufficiently into account when developing risk scenarios and proposing measures to mitigate the identified risks.

When conducting the risk assessment including the extent of damage to other critical infrastructures an ICT asset could create, potential counter-measures that might be taken by entities designated as “high-risk countries” or “high-risk suppliers” must also be considered. Such actors could, for example, retaliate by restricting the availability of products or services essential for the EU market. This could severely impact a wide range of European entities well beyond the scope of NIS2 and inflict significant harm on the broader EU economy and society. To ensure a balanced and comprehensive assessment, the risk analysis should therefore urgently incorporate an evaluation of possible counter-reactions and their systemic consequences.

Further clarification is needed regarding the respective roles and scope of security risk assessments conducted by the European Commission and by the NIS Cooperation Group. While the latter is clearly limited to critical ICT services, systems, products and supply chains, such a limitation is not evident for Commission-led assessments under Article 99. Clarifying why two distinct mechanisms are necessary, and whether Commission assessments are intended to extend beyond critical ICT assets, would significantly enhance legal certainty, predictability and consistent implementation.

German industry would welcome the implementation of the following amendments to the current draft law:

3.

(a) conduct a security risk assessment, taking into account the consultation of the Member States. The security risk assessment shall include the proposed identification of the key ICT assets as well as the main threat actors, risks and vulnerabilities affecting those assets. The security risk assessment shall develop risk scenarios and propose measures to mitigate the identified risks. *When conducting a security risk assessment according to sentence one of this subparagraph, the European Commission shall consult entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555 and those entities mentioned in Recital 133 of this Regulation.*

4. *When conducting the Union-level coordinated security risk assessments according to paragraph one of this Article, the NIS Cooperation Group shall consult entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555 and those entities mentioned in Recital 133 of this Regulation.*

5. *When conducting the Union-level coordinated security risk assessments, the risk analysis should urgently incorporate an evaluation of possible counter-reactions that might be taken by entities designated as "high-risk countries" or "high-risk suppliers" including their systemic consequences on the broader EU economy and society.*

6. *The Commission shall complete the security risk assessment according to Article 99 (3) (b) within six months.*

Article 100 – Designation of third countries posing cybersecurity concerns

It is sensible to define a third country as high-risk by considering laws and practices in this third country which legally or effectively require entities under this country's jurisdiction to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited, absence of effective judicial remedies, and information concerning cybersecurity groups operating from its territory. However, since the attribution of the geographical origin of cyber-attacks is often inconclusive and measures by public bodies against such practices is not easy, Article 100 (1) (d) should be considered in a proportionate way. It is also not clear why third-country assessments should be tied to sector-specific risk assessments, as most criteria are not sector-specific; assessing countries proactively could simplify the mechanism and increase predictability.

Ownership or control by third-country governments can constitute an important element of cybersecurity risk assessment, particularly where it entails legal obligations, state influence or constraints that may affect data access, vulnerability handling, or operational independence. In addition, security risk assessments conducted under Articles 99 and 100 may directly lead to the designation of individual suppliers as "high-risk", even in the absence of any association with a third country of concern. Such designations may occur without detailed guiding criteria, while triggering significant legal and operational consequences under Article 103. In particular, Article 103 (2)(a)–(f) empowers the Commission to impose far-reaching mitigation obligations on entities in critical sectors, including restrictions such as prohibiting the use of remote data processing. This creates a pathway by which suppliers may be designated as high-risk and subjected to substantial usage restrictions based on non-technical factors. To ensure proportionality, transparency and legal certainty, affected suppliers should therefore be given the opportunity to understand the Commission's concerns and to contribute to the identification of appropriate mitigation measures before any implementing act is adopted pursuant to Article 103 (1).

Moreover, Article 100 should clearly specify that the notion of "exploitation" refers exclusively to malicious exploitation, in line with the definition used in Article 3 CRA. Otherwise, proof-of-concepts commonly developed by security researchers to verify vulnerabilities could be misinterpreted as active exploitation. Without such clarification, third countries could circumvent the CSA 2 criteria by requiring vulnerability disclosures to include proof-of-concepts, which the current draft might incorrectly interpret as evidence of exploitation.

German industry supports the exclusion of high-risk suppliers from the activities listed in Article 100 (4).

Article 102 – Identification of key ICT assets

Since only entities falling within the scope of this Regulation know the exact areas of utilisation of an ICT asset and can therefore evaluate the risk posed by such an ICT asset, the European Commission should extensively consult all affected entities when drafting implementing acts identifying key ICT assets according to sentence one of this paragraph. A suitable mechanism to consult stakeholders must be established.

German industry would welcome the implementation of the following amendments to the current draft law:

1. Where the risk assessment conducted in accordance with Article 99(1) or (3) indicates significant cybersecurity risks in relation to an ICT supply chain, the Commission is empowered to adopt implementing acts identifying key ICT assets used for the manufacturing of products or the provision of services by entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2) of this Regulation. *When drafting implementing acts identifying key ICT assets according to sentence one of this paragraph, the European Commission shall consult entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555 and those entities mentioned in Recital 133 of this Regulation.*

Article 103 – Mitigation measures in the ICT supply chain

When publishing a list of high-risk suppliers and thereby prohibiting the use, installation or integration of any form ICT components or components that include ICT components from high-risk suppliers as identified in accordance with Article 104 in key ICT assets identified in accordance with Article 102 according to Article 103 (1), the European Commission must set realistic time periods for phasing out the relevant ICT assets. In many cases, less than a handful of suppliers develop and produce a specific component. Consequently, replacing a widely utilised component can pose challenges whether due to the time required to source alternative components, or to find an alternative ICT components that possesses an adequate quality and the sufficient accuracy of fit. Moreover, the co-legislators must also take into account the time required for the re-certification of a product or service from which an ICT component must be replaced.

The European co-legislators must note that replacing ICT components in complex OT products is very challenging. Therefore, we urge the European co-legislators to conduct a reality check on the replacement obligations for components from high-risk manufacturers – e.g. replacing a microchip from a large manufacturing plant that is already in use is not only very costly but would also require re-certification and will in many cases be completely impossible without disassembling and reassembling the entire plant. Hence, if certain prohibitions must be enacted the European Commission should, based on a proper assessment of substitution feasibility (technical, economic, and temporal), define phase-out periods reflecting the lifecycles of all relevant sectors, with the aim to mitigate the impact on ongoing projects. Moreover, it must be clarified that such components must not be replaced in end-user products. For example, should semiconductors utilised in connected vehicles and produced in a specific country defined as high-risk by a specific supplier that is classified as high-risk be already installed in a final product such product shall not be recalled. In most cases, replacing an ICT component in a final product will not be feasible and would require scrapping the entire product. Both from an economic and as well as an environmental perspective this would not be acceptable.

When suppliers are designated as “high-risk suppliers”, EU companies may be compelled to remove their components from existing systems. The associated costs and efforts are substantial, running into millions of euros per company. Such compliance measures represent a contribution to a broader societal objective: securing the resilience of the European economy and society as a whole. In effect, impacted companies are bearing costs that are not commercially motivated but serve collective security goals. This places them at a competitive disadvantage both within the EU and, more significantly, in global markets outside the EU. Therefore, these expenditures should be financially compensated. Such compensation would acknowledge that companies are footing the bill in the public interest and would help preserve their competitive position while advancing shared security objectives.

In addition, the adoption of mitigation measures as laid out in Article 103 (2), cannot follow a one size fits all approach as not all measures will be technically feasible or suitable for every system configuration or operational environment. Entities operate with different architectures and risk profiles, and a mitigation measure that is appropriate in one context may not be workable or may even create in another. For this reason, we recommend amending Article 103 (2) to ensure that, while Member States and the Commission may require entities to adopt appropriate mitigation measures under Article 103 (3), the choice of how which exact measures are implemented remains with the entity. This flexibility is necessary to allow operators to integrate measures in a technically sound, proportionate, and operationally compatible manner. At the same time, the effectiveness and adequacy of the chosen implementation should remain subject to oversight by the competent authorities.

Article 104 – Identification of high-risk suppliers

Ownership and control considerations are particularly relevant where they translate into concrete cybersecurity risks. This may be the case where suppliers are subject to third-country legal frameworks that can require cooperation with state authorities without sufficient transparency, judicial oversight or effective legal remedies, or where companies are directly or indirectly state-owned or subject to material state influence. Such governance-related factors can raise legitimate concerns regarding data access, supply-chain integrity, vulnerability handling and long-term operational independence. Where relevant, they should therefore be assessed as part of a broader, evidence-based risk analysis, alongside technical security capabilities and feasible mitigation measures. At the same time, any reliance on ownership or control-related criteria must be applied proportionately, based on demonstrable risk, and should avoid abstract or purely formal classifications that are not linked to concrete cybersecurity outcomes.

When mapping the suppliers providing ICT components and components that include ICT components relevant for the prohibition laid down in the implementing acts adopted in accordance with Article 103 (1), Article 103 (7) or the prohibition referred to in Article 111 (1), the European Commission should extensively consult representatives from entities falling in the scope of this Regulation to utilise industry expertise for alternative sources. Thereby, the European Commission should consider the availability of suppliers of a comparable ICT component which can replace the current supplier and the formers' ability to deliver the respective ICT components at globally competitive costs.

The concept of "control" requires a clearer definition. Greater specificity is needed regarding the type, degree, and demonstrable nature of control required to trigger designation. The concept should be strictly limited to situations involving demonstrable and legally enforceable control such as majority state ownership, binding legal authority to direct corporate decisions, or formal decision-making rights.

While German industry understands the necessity for the European Commission to update the list of high-risk suppliers in light of new geopolitical developments according to Article 104 (7), we urge the European Commission to maintain a high degree of predictability that takes into account typical business processes and always ensures sufficient transposition periods.

German industry would welcome the implementation of the following amendments to the current draft law:

2. For that purpose, the Commission shall map *– based on a thorough consultation of entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555 and those entities mentioned in Recital 133 of this Regulation –* the suppliers providing ICT components and components that include ICT components relevant for the prohibition referred to in paragraph 1. When mapping suppliers according to sentence 1, the European Commission shall consult with a supplier before being designated as "high risk".

Article 105 – Exemption for entities established in or controlled by entities from a third country posing cybersecurity concerns

German industry welcomes the possibility that entities established in or controlled by entities from a third country posing cybersecurity concerns designated in accordance with Article 100 can ask for an exemption from the prohibition. To ensure that the Europe's resilience against external threats is effectively ensured we appreciate that the respective entity shall demonstrate with clear evidence that effective mitigating measures are in place.

German industry stresses that suppliers should be consulted prior to them being designated as "high-risk" to allow them to respond to concerns and propose satisfactory, risk-based mitigation measures before restrictions are imposed. German industry is concerned that suppliers may be designated as "high-risk" and become subject to far-reaching restrictions based on non-technical factors even in the absence of any association with a third country of concern, including restrictions that may affect remote data processing; therefore, clear guiding criteria and due process safeguards are necessary. In this context, assessments of supplier risk should not rely on person-based proxies such as the nationality of individual employees or executives, as such criteria are neither suitable nor proportionate indicators of cybersecurity risk. German industry further emphasizes that global ICT supply chains are a cornerstone of innovation and resilience, and that measures under the CSA should preserve the benefits of diversified and trusted international supply chains rather than introduce de facto localization or ownership requirements.

Article 115 – Penalties

The proposal introduces – at least in part – very high fines of up to seven per cent of an entities total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs. We urge the European co-legislators to reduce these fines to a more proportionate level because the obligations imposed by this law serve mainly societal security goals rather than direct economic interests.

German industry would welcome the implementation of the following amendments to the current draft law:

6. Infringements of Article 103(2), point (a), shall, in accordance with paragraph 3 of this Article, be subject to penalties of a maximum of *0.5* ~~1~~ % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs.

7. Infringements of Article 103(2), points (b) to (g), shall, in accordance with paragraph 3 of this Article, be subject to penalties of a maximum of *1* ~~2~~ % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs.

8. Infringements of Article 103(1), and of Article 111 shall, in accordance with paragraph 3, of this Article be subject to penalties of a maximum of *3* ~~7~~ % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs.

Imprint

Bundesverband der Deutschen Industrie e.V. (BDI) / Federation of German Industries
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

EU Transparency Register: 1771817758-48

German Lobbyregister: R000534

Editors
Steven Heckler
Senior Expert Cybersecurity and Digital Business Identities
Directorate Innovation, Security and Technology
T: +49 30 2028-1523
s.heckler@bdi.eu

Philipp Schweikle
Expert Digital Infrastructure and International Digital Policy
Directorate Innovation, Security and Technology
T: +49 30 2028-1632
p.schweikle@bdi.eu

Document number: D 2224