BSA RECOMMENDATIONS ON THE EU CYBER-RESILIENCE ACT (CRA)

EXECUTIVE SUMMARY

BSA | The Software Alliance ("BSA")[1] is the leading advocate for the global software industry before governments and in the international marketplace.

Our members[2] are at the forefront of software-enabled innovation that is fueling global economic growth and digital transformation by helping enterprises in every sector of the economy operate more efficiently, securely and in a privacy-protective way. BSA's members are enterprise software companies that offer technology services that other organizations use—such as cloud storage services, customer relationship management software, and workplace collaboration software—to make their own operations more efficient, innovative, and successful.

BSA welcomes the EU Commission's overall objective in its proposal on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (EU Cyber-Resilience Act, hereafter "CRA")[3] to improve the cybersecurity of products with digital elements to "enable businesses and consumers to use products with digital elements securely" by mitigating the risk of incidents or attacks that can affect an entire organization or a whole supply-chain. We particularly welcome the Commission's risk-based approach and based on the principles of the EU New Legislative Framework (NLF) legislation setting out essential requirements as a condition for the placement of certain products on the internal market.

Effective cybersecurity regulation is crucial to enabling digital transformation and protecting health and safety. Cybersecurity regulation will be most effective if it is risk-based, clear, consistent with product safety and other EU Cybersecurity legislations, and harmonized with internationally recognized standards and best practices. In that regard, BSA put together detailed best practices for secure software development, secure software capabilities, and secure software lifecycle considerations. **The BSA Framework for Secure Software[4] is**

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry. Its members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

[2] BSA's members include: Adobe, Akamai, Alteryx, Atlassian, Autodesk, Bentley Systems, BlackBerry, Box, Cisco, Cloudflare, CNC/Mastercam, CrowdStrike, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Intuit, Kyndryl, MathWorks, McAfee, Microsoft, Okta, Oracle, Prokon, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454

[4] https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf

intended to establish an approach to software security that is flexible, adaptable, outcome-focused, risk based, cost-effective, and repeatable. Indeed, the different types and uses of software carry different risks; for example, the software behind a mobile phone game may pose far less threat to cyber or physical security than the software operating an electricity grid's control system. To manage the risks associated with software, companies should build software development processes around careful analysis of the risks associated with their products intended use, the potential resulting impacts, and their organization's risk tolerance. With an understanding of risk tolerance, they can prioritize security activities in their software development and lifecycle management processes, enabling informed decisions about where to prioritize improvements and how to align financial and human resources. Risk is intended to guide software development organizations and vendors to address security considerations in operational processes and product security capabilities according to the level of risk associated with the use of the product. This could serve as an effective way of raising practices throughout industry in a risk-based approach.

In that regard, BSA recommends for the EU co-legislators to focus on the below objectives to ensure a balanced and effective Cyber Resilience Act:

I. Scope : Clarifying the exclusion of Software-as-a-Service (SaaS)

II. The need for harmonization with other EU legal instruments on cybersecurity to ensure clarity and certainty for businesses and consumers

III. Scalable conformity assessment

IV. Clarifying the methodology used to identify and update the list of critical products

V. Clarifying the concept of "substantial modification" for Software updates

VI. Recognizing the Software Bill of Materials (SBoM) as a promising but limited tool

VII. Promoting International Standards based on stakeholders' expertise

VIII. Use of a Known Exploited Vulnerability Catalogue

IX. End of Software Maintenance

X. Applicability of Product Security Requirements & Transparency Measures

XI. Third party component manufacturers

I. Scope : Clarifying the exclusion of Software-as-a-Service (SaaS)

The CRA expressly removes Software-as-a-Service (SaaS) from the scope of the Regulation in Recital 9, aligned with the EU Commission's impact assessment on the CRA. However, the Recital makes an exception to the exclusion of SaaS by stating that "remote data processing" relating to a product (including standalone software) is part of the scope. Remote data processing is defined in Article 3 (2) as "any data processing at a distance for which the software is designed and developed by the manufacturer or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions". Additionally, article 3(1) defines "products with digital elements" as "*any software* or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately".

This seems to be a case of the exception swallowing the rule – at least for the majority of cases where the SaaS service is accessed by a software client (the 'product'). This is because exactly what makes Software- as-a-Service (SaaS) different from on- premise software – i.e. that it is hosted and operated by the SaaS provider ('manufacturer') or under their responsibility – is exactly what classifies it as 'remote data processing' under the scope of the Regulation. Platform-as-a-Service (PaaS) products provide developers with a framework to build software applications. PaaS products differ from on-premise software in the same way that SaaS products differ from on-premise software. PaaS products are hosted and operated by the PaaS provider ('manufacturer') or under their responsibility, which would classify as 'remote data processing' under the CRA.

The language used in the CRA is ambiguous as to whether SaaS and PaaS are actually excluded from the scope, since SaaS and PaaS fundamentally rely on "remote data processing," which is in scope.

Specifically, we understand that, as the text stands, where a product with digital elements within the scope of CRA relies on a cloud-based service, this service will be in scope of the CRA as well if it conforms to two specific scenarios. Firstly, if the cloud-based service supports one of the functions of such product with digital elements and, secondly, if that cloud-based product is developed by the manufacturer of the relevant digital product or under its responsibility.

A number Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) include these characteristics. Therefore, there is a real risk of the current draft text creating a situation where SaaS and PaaS services are brought unintentionally into scope. This is despite the Commission's stated view, in Recital 9 and in its impact assessment, that they are not.

The Cyber Resilience Act is meant to be a tailored piece of legislation aimed to work in parallel with other cybersecurity legislations, such as the NIS Directive currently (and NIS2 once it enters into force). Therefore, since the CRA is meant to be the first EU piece of legislation on IoT security, it should come as an intersection between cybersecurity legislation and product safety. For example, as mentioned in Recital 9, cloud services (including SaaS) are now considered as essential entities under the NIS2 Directive and will therefore need to comply with all its cybersecurity and risk-management requirements listed in Article 18 and 20 of the NIS2 Directive[5], thereby making compliance with the CRA cyber-risk management

[5] Risk management activities are listed in Article 18 and include i) risk analysis and information system security policies; ii) incident handling; iii) business continuity and crisis management; iv) supply chain security; v) security in network and information systems acquisition, including vulnerability handling and disclosure; vi) testing and auditing; and vii) the use of cryptography and encryption. In addition, any significant incident needs to be reported by the manufacturer under the provisions laid out in Article 20.

requirements, as well as those pertaining to reporting requirements (see below, Section II) redundant and lead to compliance issues.

Alongside this, the CRA needs to offer greater clarity in relation to the kinds of software products that are in scope. Our understanding of Article 3(1), and indeed the policy intention of the CRA as a whole, is that these are products with digital elements that are placed on the market and downloaded/hosted by the user. Therefore, software that is offered over a browser and hosted centrally, such as SaaS or PaaS, are in principle excluded. Rather than an implicit assumption, in order to ensure legal clarity, we would welcome that the CRA makes this explicit in the legal text itself.

Finally, an inclusion of SaaS or PaaS, rather than a specific exclusion, from the proposed CRA would only add unnecessary complexity that might deter businesses from using cloud-based software.

II. The need for harmonization with other EU legal instruments on cybersecurity to ensure clarity and certainty for businesses and consumers

Cybersecurity has been one of the key areas where the EU adopted several legal instruments (EU Cybersecurity Act[6], the current NIS Directive[7], as well as its ongoing review, the NIS2 Directive[8], and the delegated act of the Radio Equipment Directive, among others) to protect citizens and businesses against the risks arising from cybersecurity incidents and its potentially devastating impact on infrastructure, businesses or even citizens. BSA welcomes and shares this objective.

Against this backdrop, as a general principle, we believe it is of paramount importance, for legal clarity and the effectiveness of EU cybersecurity policy, to align and harmonize the CRA with the definitions, requirements and schemes proposed in these existing legislations. Indeed, the CRA's itself stresses this very objective, i.e. "the Union regulatory landscape should be *harmonised* by introducing cybersecurity requirements for products with digital elements. In addition, *certainty for operators and users should be ensured across the Union, as well as a better harmonisation of the single market*, creating more viable conditions for operators aiming at entering the Union market" (Recital 4, our emphasis). We offer suggestions below to accomplish this objective.

A) Harmonizing the requirements for incident notification and reporting obligations

Harmonizing laws and policies within and between governments globally is a priority for BSA and its members, and is highlighted in BSA's 2023 Global Cyber Agenda[9], "Enhancing Cyber Policy, Advancing Digital Transformation" because it supports overall product security and supply chain resilience.

1) The definition and types of "incidents"

The CRA mentions, through the text, cybersecurity "incidents" without defining those in article 3. Instead, the reference is any incident "having an impact on the *security of their products* with digital elements" (Recital 35).

To *Product Security* Incident Response Teams (PSIRTs), this is likely to be interpreted as referring to vulnerabilities. PSIRTs typically deal with vulnerabilities discovered or reported in the product and would see 'incident' through this lens. As such, it will likely cover the same ground as the vulnerability reporting requirement (see section II A) 3) below), except that with the mention of *any* incident being subject to notification, there is no threshold. Not only is this duplicative, it is also controversial because it suggests reporting vulnerabilities *before*

[6] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[7] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[8] The NIS2 Directive reached a political agreement in Trialogues on May 12, 2022. On June 22, the Council's COREPER adopted the political agreement while the lead ITRE parliamentary committee adopted it on July 13. It is now up to the Council's ministerial configuration and EU Parliament's plenary to adopt it, paving the way to its entry into force in the Fall 2022.

[9] Enhancing Cyber Policy, Advancing Digital Transformation: BSA'S 2023 Global Cyber Agenda

mitigations are in place – which goes against well-established Coordinated Vulnerability Disclosure practices and international standards such as ISO 29147 and 30111.

The text of the political agreement on NIS2, however, defines "incident" as "any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems" (Article 4) and important and essential entities are required to notify any incident having a significant impact on the provision of their services. **We recommend adopting a similar approach for incidents under the CRA.** In other words, we should be looking at incidents that **compromise the manufacturer's own network and information systems** and subsequently impact the security of products on the market. This amounts to a subset of corporate IT attacks that are **directed against the product development environment**, which we have seen have a devestating impact in supply chain attacks such as SolarWinds.

Second, further to the type of incident, there is also a question of threshold. In the current NIS Directive, only "incidents having a significant impact on the continuity of the essential services they provide" shall be notified (Article 14 paragraph 3). In the political agreement on NIS2, the "significant incident" threshold is also used to trigger the notification obligation (Article 20 "reporting obligations"). However, the CRA merely mentions "any incident having an impact on the security of those products" with digital elements to trigger the reporting obligations for manufacturers" (Recital 19 and Article 11 paragraph 2). The "significant incidents" thresholds set by the two NIS Directive is an appropriate one, as incident reporting obligations should focus on incidents that are truly "significant" so that both notifying entities and competent authorities are not overburdened with the reporting of minor or irrelevant incidents. Indeed, broadening the scope of incidents too high will divert operational resources away from addressing and remediating significant threats and lead to a culture in which the impact of security breaches are trivialized given the high volume of notifications. Potentially even more damaging, if the definition of 'incident' is not clarified and it is interpreted as applying to product vulnerabilities rather than attacks against the manufacturer's own network and IT systems, the lack of threshold opens up the perspective of notifying any and all vulnerabilities, with huge security ramifications. **Therefore, for those reasons, and taking into account the need for consistency, harmonization and legal certainty, the CRA should align on the two NIS Directives and use the "significant incident" threshold[10],** in line with existing international standards such as ISO/IEC 27035.

2) The timing for the notification

With regards the **timing** for the incident notification, the current NIS Directive requires a notification "without undue delay" (Article 14 paragraph 3) while NIS2 which relates to higher risk incidents impacting critical infrastructure services, only requires the full incident notification after 72 hours.

Moreover, companies also have a duty to report personal data breach "without undue delay and, where feasible, not later than 72 hours after having become aware" of the breach under the GDPR (Article 33 and Recital 85), or assist their entreprise customers where they act as a data processor. While not applying to cybersecurity incident *per se*, it is yet another process and another non-harmonized deadline for companies to comply with.

[10] The NIS2 Directive defines a significant incident as ''any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, **the manufacturer,** which has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned**:** has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage. "

The CRA, however, adopts yet a different time period as it requires a notification "without undue delay and in any event within 24 hours of becoming aware". (Article 11 paragraph 2).

We recommend that the reporting timing threshold set by the current NIS Directive be adopted in the CRA. It is the most appropriate one as the deadline to notify should be both workable and meaningful. Therefore, the CRA should seek to maintain the current practice as established by the existing NIS Directive ("without undue delay"), in order to ensure alignment with other notification requirements in existing privacy and security legislation (e.g. GDPR). Indeed, where the cause of an incident resides with a SaaS cyber security vendor, it is industry practice to first remediate the incident before notifying the affected entity of the nature of the incident. Hence, setting a notification requirement to notify external agencies within a 24-hour is unrealistic as the reporting obligations would have to come first and only after should the notifying entity having effectively mitigated the incident. This would be detrimental to the product's end-user, be it a business or a consumer.

Moreover, the CRA should clarify **when the "24 hours" period starts.** The mention of "after becoming aware" appears in the matter too ambiguous, thereby lacking legal clarity and certainty.

We recommend that the period of 24h starts no sooner than when the the incident has been triaged by the appropriate incident response team of the manufacturer's enterprise. The manufacturer should have a "reasonable belief" that a significant incident has occurred, and be able to assign a level of importance or urgency to incidents, which then determines the order in which they will be investigated and reported. Reasonable belief should be understood to mean the entity's belief that, upon investigation, the reliable information it considered at the time, provided clear and convincing evidence that the entity was the victim of the type of incident covered by the CRA.

This approach is already used for personal data breaches under GDPR. The WP 250 Article 29 Working Party Guidelines on data breach notification state: "[…] the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware"."

The current NIS Directive also mentions the need to report the incident "without undue delay" (Article 14 paragraph 3) thereby implicitly taking into account that threshold.

In terms of **notification of users and the public** at large, the CRA sets no boundaries on their notification. Manufacturers are expected to notify all incidents and to do so without delay. Under NIS 2, on the other hand, recipients of the service are only notified where appropriate and if likely to be adversely affected, whereas the general public is notified only if necessary to deal with or prevent the incident, and only after consulting the entity in question. We suggest similar notification criteria are applied under the CRA.

Also, we encourage the Commission to align the reporting function under the CRA with NIS2, in which the notice goes to the national CSIRT or national competent authority (Article 20 of NIS2). Under the CRA, however, the manufacturer must notify ENISA, which in turn reports to the relevant single point of contact and/ or CSIRT. This appears to add an extra and unnecessary layer in the transmission of the notification which, in itself, delays the reporting itself. In a context where affected entities often race against the clock to contain and mitigate a serious cybersecurity incident, adding contradictory reporting requirements to multiple regulators and under very strict timelines would effectively weaken their security posture.

The software industry also calls for clear and transparent requirements in terms of deadlines and what ENISA needs to report onwards to single point of contact and/or the CSIRTs Network and other public partners. Given the limited resources of ENISA, it must not become a bottleneck when economic operators report into ENISA. We therefore recommend that ENISA reports onwards without undue delay to Member States. The information shared by the economic operators to ENISA grows in value when shared and analyzed together. Since the NIS2 Directive does not lay down such clear structures for equal and transparent partnerships, the CRA can help further improve this balance and eco-system, in particular to avoid a one-way notification framework that only strengthens the information position of ENISA and its partners.

Moreover, we would ask clarifications as to the role of ENISA in the matter since it appears that the mandate to perform its functions under the CRA contradict its legal mandate, which does not give the Agency a formal regulatory oversight or redress powers[11].

3) Notification of actively exploited vulnerabilities

Finally, the CRA lays out an obligation for manufacturers to notify about actively exploited vulnerabilities under 24-hour (Article 11 paragraph 1). This short period implies for the manufacturer to report a vulnerability before that manufacturer had even the chance to issue appropriated patches. This could ultimately undermine the security posture of the affected product with digital elements and jeopardize the security of its users.

BSA recommends using, for the actively exploited vulnerability reporting, the above-mentioned standard set by the NIS Directive for incident reporting i.e. “without undue delay” (Article 14 paragraph 3, see above), with the deadline starting when the actively exploited vulnerability has been confirmed by the manufacturer's response team and working through a coordinated vulnerability disclosure (CVD) programs based on internationally recognized voluntary consensus standards, such as, for example, ISO 29147 and 30111. Such reporting should be limited to high and critical vulnerabilities in-the-wild. Low vulnerabilities with no impact on the product with digital elements should not need to be reported.

B) Harmonized Voluntary Certification Schemes for conformity assessment

Second, for the purpose of legal clarity and harmonization at EU level, we also support the alignment of the EU cybersecurity certification schemes in all related current and upcoming EU cybersecurity legislations (The EU Cybersecurity Act-CSA, the current Directive on security of networks and information systems-NIS as well as its ongoing review- NIS2, etc.) in order to avoid possible conflicts or overlaps.

BSA strongly believes that high standards and due diligence in software development, deployment, and use, throughout its lifecycle, is best adapted to ensure cybersecurity in digital products. Such standards and due diligence are developed through the software community’s best practices that help software developers address important aspects of software security.

Moreover, to this day, even if some schemes are currently being developed by ENISA (e.g. EUCS), none has been finalized or implemented under the CSA or NIS2 yet. Therefore, any mandatory certification obligations in this legislation would therefore be overly prescriptive and premature in the current context, in particular ahead of the planned evaluation of the CSA “by

[11] For ENISA’s tasks, see Chapter II of Regulation (EU) 2019/881.

28 June 2024" (Article 67, CSA). The use of certification schemes under the CSA or NIS2 should be voluntary and bring a presumption of conformity with the CRA requirements. It should be left to the manufacturer to decide whether or not to use the CSA schemes or to undergo a normal conformity assessment for its products.

The CRA goes into the right direction in its Recital 39 and article 18 paragraphs 3 and 4, stressing that "products with digital elements that are certified (…) pursuant to [the CSA] and which has been identified by the Commission in an implementing act, shall be presumed to be in compliance with the essential requirements of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements" (Recital 39).

However, we have concerns over the potential mandatory certification for certain highly critical products, namely the fact that the CRA gives the EU Commission the power to adopt delegated acts with regards "the potential mandating of certification of certain highly critical products with digital elements based on criticality criteria set out in this Regulation, as well as for specifying the minimum content of the EU declaration of conformity and supplementing the elements to be included in the technical documentation" (Recital 62 and article 6 paragraph 5). First of all, the CRA is silent as to which criteria or methodology the EU Commission will use to identify "highly critical products" as well as which information (e.g. threat/risk assessment), such identification will be based on, nor on which evidence or data it will based its impact assessment, when such impact appears premature to assess and therefore difficult to measure. Moreover, and more importantly, we want to reiterate that to this day, no certification scheme has been finalized or implemented under the CSA or NIS2. To ensure that certification empowers rather than restricts the ability of public sector, industry and consumers alike to deploy and use effective security solutions, any certification scheme should pass the test of market acceptance and uptake. In practice, this means that such schemes are technology-neutral and allow for the use open, transparent, consensus-based processes, and widely adopted international standards where such exist (such as the ISO 27-thousands), and they are not subject to overwhelmingly complex assessment processes (which would result in market bottlenecks and limit the customer choice of "best-in-class" technology). Against this background, BSA is of the opinion that any mandatory certification obligations, for the schemes mentioned in the CRA, would therefore be overly prescriptive and premature in the current context. International recognized standards provide widely vetted, consensus-based information and guidance for defining and implementing effective approaches to cybersecurity and facilitate common approaches to common challenges, thus enabling collaboration and interoperability (see also Section VII below).

In conclusion, as a general principle, we believe that any European cybersecurity certification approach should remain voluntary, aligned with the language of Article 53(4) of the CSA, while enabling self-assessment as the default conformity assessment procedure, to be aligned with international standards and to replace, not add to, national certification schemes[12].

[12] BSA feedback to ENISA on the European Union Cybersecurity Certification Scheme on Cloud Services (EUCS) https://www.bsa.org/policy-filings/eu-bsa-feedback-to-enisa-on-the-european-union-cybersecurity-certification-scheme-on-cloud-services-eucs.

III. Scalable conformity assessment

A) Harmonised standards as the cornerstone of conformity

CRA is about a given product with digital elements having a set of security properties, being subject to a secure development lifecycle and being able to demonstrate those properties and processes for any given version. The main challenge is going to be able to do this at scale.

Security regulation and certification has traditionally focused on high-risk users, data or types of technology. The CRA is about *all* connected products. The CRA lists, in article 24, the conformity assessment procedures, given the type of products with digital elements (general, class I or class II). In order to ensure effective and efficient compliance, it is a necessity that harmonised standards based on international security standards are the cornerstone of conformity.

We also need to recognise that software cybersecurity is more complex than other types of product safety compliance regulation under the NLF. You cannot just resort to randow safety/security checks by taking a random box from the shelf and quickly test its compliance as you might do if, for example, you were checking for a hazardous substance. Modern Operating System Software may have upwards of 80 million lines of code – much of which is created and maintained by others. Even if a third party software library is used with a known vulnerability, it does not mean that vulnerability is exploitable in the context of the software in question. Moreover, as noted in section V below, software is constantly evolving with new releases, meaning the target is always changing.
As a result, in applying the NLF framework to cybersecurity of products we need to take extra care that the expected depth of evidence of following processes, testing and external documentation is proportionate and not overly burdensome.

B) Third party assessment

For the significant minority of products that require third party assessment, the goal will be keep it simple and avoid duplication.

Product assessment for cybersecurity-related purposes is not a new phenomenon. Third-party assessment is required in certifications and authorisations of certain products used in defence, central government, and critical infrastructure environments. But the difference is that it is largely dependent on the choice of the manufacturer whether and when to go after such third-party assessment for their products in order to enter fairly specialised markets.

Conformity assessment under the CRA, on the other hand, is a general requirement for all digital products. The general level includes internal controls, risk assessment and testing as well as outward facing technical documentation and artifacts. Whereas the critical level, where third party assessment by a notified body is a more likely route or mandated, is extraordinarily broad. This needs to be done at scale – and we believe that several principles can help guide the approach, some of which are currently reflected in the Regulation and can be reinforced and others that should be introduced:

- Similarity: reduce assessment effort by accepting one product as representative of a family/category of products for assessment purposes due to them having equitable hardware and/or software
- Reciprocity: eliminate duplication by accepting of other entities' assessments or certification in lieu of one's own (e.g. recognition of assessments from qualified bodies outside EU; reuse of certifications)
- Deltas: only focus on additional requirements not covered by other entities' assessments and do not reassess the whole set
- Attestation: accept assessments from the manufacturer for certain aspects of the wider third-party assessment
- Maintenance: allow certain changes to the product without requiring reassessment.

BSA also recommends that consideration also be given to weighing the usefulness of information provided in the technical documentation or to the user against the administrative burden, the extent to which it can be known by the manufacturer (e.g. intended use or risks stemming from foreseeable use) and whether it can itself present a risk (e.g. complete information on design and development, outbound documentation on threat modelling).

Finally, a one-stop shop provision should be foreseen for the conformity assessment process. As the CRA states in Article 20 paragraph 2, declarations of conformity "shall be made available in the language or languages required by the Member State in which the product with digital elements is placed on the market or made available". This effectively means that hardware and software manufacturers are required to translate all technical documentation in all 23 official languages. We believe that such an approach is overly prescriptive and risk impeding the ability of manufacturers and vendors, particularly SMEs, to make their products available in all the national markets of their choice within the EU territory.

IV. Clarifying the methodology used to identify and update the list of critical products

Annex III of the CRA lists two classes of "critical products with digital elements": class I and class II, "reflecting the level of cybersecurity risk linked to these categories of products. A potential cyber incident involving products in class II might lead to greater negative impacts than an incident involving products in class I".

The categories of product considered to be critical is very wide and, in many instances, not at all limited by use case. Given the implications for type and depth of conformity assessment, the product categories should be carefully reviewed to ensure their inclusion is proportionate.

The CRA is silent as to what criteria or methodology the EU Commission used to identify the products listed in class I and II, nor which type of information is necessary to make the assessment. Indeed, Recital 25 broadly stresses that "products with digital elements should be considered critical if the negative impact of the exploitation of potential cybersecurity vulnerabilities in the product can be severe due to, amongst others, the cybersecurity-related functionality, or the intended use".

Moreover, we believe the list lacks legal clarity and therefore business certainty as to how the categories of products from class I and II listed in Annex III are defined. Indeed, Recital 27 provides that the Commission should adopt delegated acts [by 12 months since the entry into force of this Regulation] to specify the definitions of the product categories covered under class I and class II as set out in Annex III".

This is particularly important since the CRA allows the Commission, via delegated acts, to update this list of critical products in Annex III (Recital 62). With regards the update of the list, the CRA stresses that the Commission "shall take into account the level of cybersecurity risk related to the category of products with digital elements. In determining the level of cybersecurity risk, one or several of the [a) to e)] criteria shall be taken into account" (Article 6 paragraph 2). While some criteria are listed, the methodology referred to in the article ("one or several of the […] criteria") appears overly broad and lacks clarity as to which criteria are prominent, how many criteria need to be taken into account and how that determination is made. Moreover, it is unclear which criteria are used to determine whether a critical product falls under class I or class II.

We are also concerned by the breadth of the criterion in Article 6 (2c) which states the following *'the intended use of performing critical or sensitive functions, such as processing of personal data'* . Indeed, virtually all connected products today process personal data. Therefore, we believe that the criteria as whether a product with digital elements processes data adds little value to determine whether a product with digital elements should be deemed critical or not, and might lead to unintended consequences of wrongfully designating products as critical products. We therefore recommend amending this criterion laid out in Article 6 (2c) as we believe that the volume of processing personal data is more relevant than processing any personal data at all and should be reflected in the proposal: *'the intended use and scale of performing critical or sensitive functions, such as the volume of processing of personal data;'* This is particularly important as the proposal currently lacks clarity on the importance of, and the methodology upon which, these criteria will be used to determine whether a product should be considered critical, and if so, whether it should fall under class I or II.

Therefore, BSA recommends a clear common approach to categorizing the digital products falling into scope into low, medium and high-risk levels which also accounts of the complex multi-cloud environments in which these products operate (for the latter, see previous section). We would therefore welcome the development in the CRA of a clear mechanism at the EU level for such categorization to ensure alignment and harmonization across the EU single market and avoid fragmented approaches where one product is categorized as low risk in one Member State and as high risk in another Member State. We also support close cooperation between the EU institutions and the national competent authorities to ensure harmonized implementation and enforcement of the CRA.

V. Clarifying the concept of "substantial modification" for Software updates

The CRA includes provisions on "substantial modification" (Recitals 22 and 23), defined in Article 3 (31) as "a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I or results in a modification to the intended use for which the product with digital elements has been assessed". Therefore, for products with digital elements that face such "substantial modification", the CRA provides that "it is appropriate that the compliance of the product with digital elements is verified and that, where applicable, it undergoes a new conformity assessment" (Recital 23).

Nonetheless, we believe that the concept of "substantial modification" is defined too broadly and therefore lacks legal clarity and certainty, in particular when it comes to software. We would instead refer to the EU Commission's 'Blue Guide' on the implementation of EU product rules 2022[13], which refers to "substantial modification" when it comes to software, specifically, as "Software updates or repairs could be assimilated to maintenance operations provided that they do not modify a product already placed on the market in such a way that compliance with the applicable requirements may be affected. As is the case for physical repairs or modifications, a product should be considered as substantially modified by a software change where: i) the software update modifies the original intended functions, type or performance of the product and this was not foreseen in the initial risk assessment; ii) the nature of the hazard has changed or the level of risk has increased because of the software update; and iii) the product is made available (or put into service where this is covered by the specific Union harmonisation legislation)".

Indeed, the CRA mentions specifically software, and in particular software updates, stressing that "software updates or repairs could be assimilated to maintenance operations provided that they do not modify a product already placed on the market in such a way that compliance with the applicable requirements may be affected, or that the intended use for which the product has been assessed may be changed. As is the case for physical repairs or modifications, a product with digital elements should be considered as substantially modified by a software change where the software update modifies the original intended functions, type or performance of the product and these changes were not foreseen in the initial risk assessment, or the nature of the hazard has changed or the level of risk has increased because of the software update" (Recital 22).

Some software applications are updated dozens, if not hundreds, of times per day. Given the regularity with which new features and security updates are introduced, this Recital appears to provide that a significant proportion of software releases will require the product to undergo a new conformity assessment. This appears overly prescriptive for any software developer and risks delaying, or even depriving, much needed updates for the customer, many of which improve software security. Indeed because software updates often include software patches, overly burdensome conformity assessments for software updates may actually diminish a software product's security, not improve it. Moreover, many software developers include autonomous updates, precisely to be able to provide their customer with swift and effective updates to the product. By defining the concept of "substantial modification" too broadly,

[13] Commission notice The 'Blue Guide' on the implementation of EU product rules 2022 (Text with EEA relevance) 2022/C 247/01 - EUR-Lex - 52022XC0629(04) - EN - EUR-Lex (europa.eu)

especially when it comes to software updates, the CRA will *de facto* require software developer to undergo multiple conformity assessments during a product's lifetime, thereby overburdening the developer and delaying much needed updates for the customer.

VI. Recognizing the Software Bill of Materials (SBoM) as a promising but limited tool

With regards the vulnerability handling requirements (Annex I Section 2 (1)), the CRA lays out the need to "identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials [SBoM] in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product". Article 10 paragraph 15 further specifies that "the Commission may, by means of implementing acts, specify the format and elements of the software bill of materials".

BSA supports the development and use of SBoMs and considers them to be strong, if limited, tool to improve the cybersecurity of digital products. Overall, the industry is progressing quickly in the creation of SBoMs. We note that a vendor creating and delivering an SBoM will not automatically improve cybersecurity, but with the automation and tooling currently being developed, he can take the information contained in SBoMs into concrete cybersecurity improvements.

However, BSA is concerned that the power to specify the format and elements of an SBoM is left entirely to the EU Commission, via implementing acts. We believe stakeholders, and specifically software developers, are best placed to provide expertise and practical experience as to the format and elements of an SBoM. Indeed, if the EU requirements are not harmonized with industry best practices and internationally recognized standards, it would undermine the value of SBOMs to the EU and its citizens as well as the digital ecosystem more broadly.

SBoMs, combined with the tooling, standards, and automation currently being developed, will improve cybersecurity but unfortunately, are not, a silver bullet. Therefore we would encourage EU institutions to carefully consider these following elements with regards the use of SBoMS in the context of the CRA:

- **SBoMs have not yet achieved the required maturity level and there are no commonly-used standards at this stage** – for example, there is no single globally prescribed method for determining components names – so two different SBoMs authors might use two different identifiers for the same component – this is because software components suppliers define those according to their own needs. Moreover, while versions of certain **SBoM formats** can indeed be used **to document vulnerabilities** in addition to components contained in the product, this is certainly **not its intended use**. Vulnerabilities are discovered frequently after product release, and vulnerability properties could change. The obligation to republish entire SBoMs whenever vulnerabilities are discovered or modified, therefore appears inefficient. An additional benefit of separating vulnerability advisory info from SBOMs is that organizations that choose only to create and use SBoMs within their SDLs can still fulfill reporting obligations mandated by the CRA. In light of this, **we urge regulators to closely work with industry on the standard-based formats that work best, rather than selecting and then requiring specific SBoM standards**. This is of particular importance to ensure that SBoMs practices will be actionable and also aligned as much as possible on international standards and best practices;
- **The EU should also consider challenges specific to the cloud environment**: for example, updates and patches in Software-as-a-Service (SaaS) are usually done on a continuous basis (and automated). This leads to a faster resolution of vulnerabilities. Therefore, requiring SBoMs in the cloud context would make those very quickly outdated. As a consequence, they should only be required for on-premises software. While, at this stage, the CRA specifies that SaaS are not in scope of the Regulation (Recital 9, see

above), we have concerns that such exclusion is not sufficiently clear, notably given the inclusion of remote data processing services (see above);

- **The EU should consider limiting the depth of an SBoM to expedite their delivery and use:** BSA supports the development and use of SBoMs but would recommend limiting the scope of information to be included in SBoMs in the beginning, to focus on building their foundations. In contrast, by limiting the depth of SBOMs, enterprises can begin to reap the benefits of SBoMs, and would not close off the possibility of building out additional requirements as industry develop the people, processes, and technologies, needed to implement a deeper SBoM.
- **The EU should also consider requiring SBoMs only for products with digital elements used in specific contexts.** Currently the proposal requires SBOMs for all products with digital elements, whatever their context of use. As a first step, it may be worth requiring SBoMs in specific cases, for example when products are supplied to Essential or Important Entities under the terms of NIS2.
- In addition to the security concerns, **public disclosure of SBoM could pose a risk to intellectual property as well as product security**. While the SBOM alone does not provide highly sensitive trade secrets like source code, it could still include other proprietary information such as the particular blend of software providers, vendors, and partners used to produce a given offering, which would constitute valuable intellectual property and proprietary information. The text should clarify who the SBOMs should be communicated to, and which action will be taken by authorities as a result. Disclosing SBOMs to customers should be done by default, but for broader stakeholders (such as potential customers), this should be done under non-disclosure agreements. Additionally, using SBOM for vulnerability disclosures or fully including them in the technical documentation could create a roadmap for malicious actors to exploit vulnerabilities.

VII. Promoting International Standards based on stakeholders' expertise

Another key issue with regards cybersecurity requirements for digital products is the need to develop such cybersecurity requirements in line with international standards. We strongly believe that such harmonized cybersecurity requirements based international standards should apply to all digital products. These standards are developed in open, transparent, consensus-based processes, and are widely adopted in the international marketplace. Internationally recognized standards leverage global security expertise from governments, industry, and academia. For example, ISO 27001 "specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organization" and ISO 27017 provides "guidelines for information security controls applicable to the provision and use of cloud services" as well as ISO 15408 on Common Criteria for Information Technology Security Evaluation. The CRA already recognizes such standards in its module H of conformity assessment (i.e. ISO 27034 - application security, IEC 62443 and ISO 9001 -Quality Management System). Additionally, relevant frameworks and publications from the US National Institute for Standards and Technology (NIST) have been leveraged throughout the world, including NIST's 800-53 control set, Risk Management Framework, and Cybersecurity Framework.

Regional, national, or local standards fragment this landscape and increase the costs to customers (including government customers) and decrease both the ability to provide innovative solutions and the number of players competing for business thereby ultimately not only limiting consumer choice but harming the entire digital ecosystem.

In contrast to regional, national, and local standards, laws and policies based on internationally recognized standards enable international interoperability, allow governments and businesses to better communicate at the technical level, have a track record of being developed and updated more efficiently than laws, increase competitiveness, incentivize innovation, and account for how technology is evolving. Ultimately, internationally recognized standards result in digital products that are more effective, efficient, safe and innovative, while also being less expensive. This would ultimately foster a more competitive market and provide a more secure cybersecurity environment for digital products as well as more resilient supply chains. By participating in, and adopting, international standards, the EU could raise and address the cybersecurity concerns with regards digital products without passing costs to consumers, hampering innovation, or limiting competition.

The CRA goes in the right direction with regards conformity assessment as it creates a presumption of conformity for products with digital elements which are in conformity with harmonised standards, which translate the essential requirements of this Regulation into detailed technical specifications (Recital 38). However, the CRA introduces the possibility to adopt common specifications by providing that "where no harmonised standards are adopted or where the harmonised standards do not sufficiently address the essential requirements of this Regulation, the Commission should be able to adopt common specifications by means of implementing acts. Reasons for developing such common specifications, instead of relying on harmonised standards, might include a refusal of the standardisation request by any of the European standardisation organisations, undue delays in the establishment of appropriate harmonised standards, or a lack of compliance of developed standards with the requirements of this Regulation or with a request of the Commission" (Article 19, Recitals 41 and 63). This gives the EU Commission a discretionary power to develop, on its own, common specifications.

This raises concerns not only to harmonization *per se,* but as to the discretionary power of the Commission, in cooperation with stakeholders, based on their practical expertise and experience, to adopt common specifications where stakeholders' consultation is strongly limited. Any such common specifications should be developed with industry participation. Further, this approach seems to run against the EU-US Trade and Technology Council's efforts to "recognise the importance of international standardisation activities."

We would therefore recommend that, "where no harmonised standards are adopted or where the harmonised standards do not sufficiently address the essential requirements of this Regulation", the Commission permits instead reference to one or more widely accepted, open standards (where these standards map to requirements in Annex I). Indeed, Other examples of global organizations creating open standards – relevant to cybersecurity, transparency, and resiliency – are the Internet Engineering Task Force (IETF) (e.g., Supply Chain Integrity, Transparency, and Trust (SCITT)) and OASIS Open (e.g., Common Security Advisory Framework (CSAF)).

Moreover, the 24-months period for the application of the provisions after the entry into force of the CRA (Article 57) also raises a concern. Given the thorough process involved in developing harmonized standards, the envisaged timeframe to develop new ones is too short, meaning that the Commission may *de facto* default towards common specifications. With the standards still under development, they would be deemed to "not exist" under Article 19 and the EU Commission would then be empowered to adopt common specifications. However, even if such standards are not adopted, it is likely that following stakeholders lead and using existing standards and best practices available is a more effective path to the improved security that the European Commission aims to achieve. We would then recommend the co-legislators to extend the transition period to 48 months in order ensure that this more effective path can be followed. This is also true for the notification of notified bodies, which is unlikely to happen in only 24 months.

We strongly recommend the CRA to rely exclusively on international standards, rather than its own technical specifications, as the primary means for demonstrating conformance with corresponding essential requirements. Within this context, we note with concern that Recital 33 states that "these essential requirements should be without prejudice to the EU coordinated risk assessments of critical supply chains (…) which take into account (…), where relevant, non-technical risk factors, such as undue influence by a third country on suppliers". We believe that this is unnecessarily broad and could restrict market access from non-European manufacturers without necessarily improving the effectiveness of the proposal and the intended objective.

VIII. Use of a Known Exploited Vulnerability Catalogue

Annex I Section 1 point 2 of the CRA lists, as "essential cybersecurity requirements to the properties of products with digital elements", that such products "shall be delivered without any known exploitable vulnerabilities".

Article 11 paragraph 1, on the other hand, uses the term "actively exploited vulnerability" in its reporting requirement. The latter is defined (Article 3 (39)), the former is not. In both cases, however, it may be useful to rationalize the terms and to create an external standard against which manufacturers can determine whether to deliver the product with digital elements or notify ENISA.

First of all, there is never a certainty that a product will be 100% secure: cybersecurity is a continuous process, not an end state, and the security of a product changes as its deployment environment changes, as different technology develops, and as attacks evolve.

Second , each vulnerability will not have the same level of impact. Taking into account current industry norms, we would be allowing economic operators to implement a risk-based approach based on numerous factors and situational circumstances like the vulnerability risk level and the criticality of the data and systems impacted. Such an approach would allow entities to focus on remediating the most critical vulnerabilities first and prevent them from avoiding the scanning of the products (this way, keeping those potential vulnerabilities "unknown"), and thereby leading to less secure products being delivered on the market, as well as also being aligned with existing global industry standards and frameworks.

The US Cybersecurity and Infrastructure Security Agency (CISA) maintains a Known Exploited Vulnerability Catalog which may be a useful illustration of this point. This differs from the vulnerability database proposed under NIS 2 (or the CVE Program). The criteria for inclusion here is not just whether a vulnerability exists, nor whether it is technically exploitable, but whether it is being actively exploited in the wild. To give a sense of the difference, in excess of 200,000 CVE categorized vulnerabilities are included in NIST's National Vulnerability Database, while a little more than 850 of those make the Known Exploited Vulnerability Catalog. The value is that it is an authoritative source that allows entities to prioritise remediation of high-risk vulnerabilities. The list could either be co-opted for use under the CRA or a similar catalogue be housed under ENISA.

Using such a catalogue as the reference for delivering products with digital elements without known *exploited* vulnerabilities would give clear guidance to manufacturers and market surveillance authorities on applicable vulnerabilities while focusing on the riskiest vulnerabilities rather than ones that a vendor may address with a compensating control, may be mitigated by environmental circumstances, or otherwise be of low risk.

Using the catalogue for notification to ENISA ensures that ENISA and other authorities can maintain an accurate picture where higher-risk *known* exploited vulnerabilities show up in products with digital elements placed on the European market. It incentivizes manufacturers to actively monitor the catalogue and use it to prioritize remediation of third-party vulnerabilities in their products. And it ensures the principle of remediation of the

vulnerability before public disclosure enshrined in international standards for vulnerability management and disclosure (ISO 29147 and 30111).

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

IX. End of Software Maintenance

The CRA requires manufacturers to ensure vulnerabilities are handled effectively for the expected product lifetime or 5 years, whichever is shorter (Article 10 paragraph 6). While this appears fairly straightforward for hardware, the nature of software release cycles makes it somewhat more complex to determine product lifetime and appropriate maintenance periods for software.

Manufacturers must strike a balance between supporting legacy versions of software (e.g. 1.x) and encouraging customers to upgrade and maintain the current version of the software (e.g. 2.x) – with clear security advantages associated with doing so. One interpretation of Article 10 paragraph 6 would be that as soon as the next release is made available, the expected product lifetime of the previous release has reached its conclusion. But for on-premises software, it is perfectly plausible that customers continue to run the previous version of the software, which will continue to function. So it is unclear what is meant by expected product lifetime in this regard.

Certainly, software manufacturers will not be developing, repairing, maintaining and testing a particular software version for 5 years after it is placed on the market. Nor would it be wise to encourage them to do so as it is better for the security posture for users to migrate to newer software releases. Continued support of the legacy version provides a disincentive for users to do so.

In that regard, BSA recommends a clarification that expected product lifetime in software terms means up until a new release is made available, or to add a grace period of 6 months after the new release until end of software maintenance for the previous version.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

X. Applicability of Product Security Requirements & Transparency measures

A) Applicability of Product Security Requirements

BSA welcomes that the security requirements relating to the properties of the product listed in Annex I of the CRA are in most cases subject to the risk assessment in Article 10 paragraph 2 and adopted where applicable. Given that manufacturers' products with digital elements must be assessed against such requirements and that manufacturers can be investigated and held liable - with consequences including withdrawal from the market or fines up to 2.5% of worldwide annual turnover - additional guidance on situations where a particular requirement might not be applicable would be welcome.

Where a product is intended to be used in enterprise settings, for example, the expected level of expertise of the IT employee or employees managing the product is likely to be different to a consumer environment. As such, the expectations regarding secure by default configurations and ability to reset the product to its original state may be different.

Another situation is when two requirements may require a trade-off against one another. For some components, we may see a trade-off between making them updateable and minimising attack surfaces. For example, a power supply may have a central processing unit (CPU) and therefore firmware, which needs protection. Making it read-only is one way of protecting it (i.e. limiting the attack surface), but then the user cannot update it.

B) Transparency measures

Second, we have concerns about the potential security risk of including the following elements in the technical documentation.

- Risk assessments [Annex V.(3)]
- Software Bill of Materials [Annex V.(7)]

This would lead operators to disclose sensitive information and further expose those products to malicious attacks. We would suggest limiting these requirements to including a statement or a summary, specifying that we can implement a procedure to providing complete information to the relevant authorities upon request.

XII. Third party component manufacturers

Articles 11 (7) and 11 (4) recognize that products with digital elements can include (3rd party) components, including open-source components. In cases where the (3rd party) component itself is considered a product with digital elements (made available on the Union market), the obligations of the CRA may apply to a 3rd party component manufacturer or its economic operator. For example, Annex I 2.(4) and Annex I 2.(8) state that "mmanufacturers of the products with digital elements shall", respectively:

- "(4) once a security update has been made available, publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities";
- "(8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken".

From the perspective of a company that works with 3rd party components, we have concerns with these vulnerability handling requirements:

- "user": the term user is not defined. We assume the term refers to an end-user and not the manufacturer or economic operator, which used the 3rd party component in its product. We are concerned that, given the current wording of the requirement, 3rd party component manufacturers may be required to publicly disclose vulnerability information before an end-user has been able to mitigate the vulnerability. Premature, public disclosure by a 3rd party component manufacturer may put the end-user at risk by disclosing information regarding a vulnerability that could be used by malicious actors prior to a patch being made available and the vulnerability being addressed.
- It should further be noted that 3rd party component manufacturers likely do not know the end-users of a product with digital elements that includes the 3rd party component; end-user/customer contact information is likely not shared by the economic operator of the product. The 3rd party component manufacturer may not be able to notify all end-users of available updates (see also Annex I, 1.(3)(k)).
- The third-party component manufacturer is likely unaware how its component is configured by the product's manufacturer. Worse, the product manufacturer may have mitigated the vulnerability (e.g., by not having included the vulnerable code, by determining that the vulnerable code cannot be "executed", etc.) and any action recommended by the 3rd party component manufacturer may be unnecessary or even counter-productive. Therefore, the 3rd party component manufacturer cannot provide end-users with "relevant information" or the "potential action to be taken" as required by Annex I 2.(8) of the draft Act.

Therefore, we recommend that the CRA explicitly considers the role and limitations of 3rd party component manufacturers in the supply chain and that the term "user" is defined.

* * * * *

For further information, please contact:
Thomas Boué, Director General, Policy – EMEA
thomasb@bsa.org or +32.2.274.1315