Brussels, March 2021

BSA | THE SOFTWARE ALLIANCE'S FEEDBACK ON THE REVISED DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS (NIS 2.0)

BSA | The Software Alliance (BSA)[1] welcomes the opportunity to comment on the Commission's revised Directive on security of network and information systems (herewith "NIS 2.0 Directive"). BSA is the leading advocate for the global software industry. BSA members 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.[2]

The threat landscape has increased considerably since the adoption of the NIS Directive in 2016, and the objectives of the Directive are more relevant than ever. Today, cyber incidents rank among the most important business risk globally. BSA and its members support the overall objective and horizontal approach of the review to strengthen security and resilience in Europe. The emphasis on risk management is an important step forward in holistically addressing cyber risk, and the distinction between "essential" and "important" entities maintains a risk proportionate approach.

BSA welcomes the following elements in the review, which should be preserved throughout the legislative process:

- The NIS 2.0 Directive must clearly remain the horizontal legislative building block upon which different *lex specialis* address sector-specific issues, in consistency with existing instruments[3]; NIS 2.0 will be debated at the same time as the proposed Regulation on Digital Operational Resilience for the Financial Sector ("DORA"[4]); it will be very important to clarify and streamline overlaps and possible conflicting requirements between DORA and NIS 2.0;
- The proposal introduces some helpful elements to improve harmonization across the EU such as the one-stop-shop concept for many essential entities in the "digital infrastructure" category;

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. 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.

BSA's members include: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, Box, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] BSA, How Enterprise Software Empowers Businesses in a Data-Driven Economy, January 2021

[3] These instruments include but are not limited to the General Data Protection Regulation, the European Electronic Communications Code, the e-Privacy Directive and the DORA Proposal.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595&qid=1614078728136

- While the scope of the Directive is expanded to cover a larger range of 'digital infrastructures,' the Commission rightfully favored a horizontal approach looking to regulate sectors rather than products; thereby considering that the Cloud services' inclusion in Annex III in the current NIS Directive covers software products, notably through the Software-As-A-Service (SaaS) principle;
- The draft review maintains liability exemptions for covered entities who report incidents, in consistency with the current NIS Directive Articles 14(3) and 16(3).

Key BSA Recommendations

BSA would like to offer comments on a non-exhaustive list of areas that could be improved to help better achieve the Directive's objectives and incentivize a holistic, effective and responsible approach to cybersecurity. Our recommendations, further detailed below, primarily seek to:

ENSURE CONSISTENCY AND COORDINATION

- Maintain precedence of NIS 2.0 over sector-specific resilience legislation, and consistency of definitions and supervisory authorities' coordination between NIS 2.0 and other legislation, in particular the DORA proposal;
- Avoid potential overlap of reporting requirements for entities that service essential entities and important entities;
- Clarify information sharing governance and strengthen public-private cooperation;
- Propose dedicated resources for CSIRTs to acquire real-time threat intelligence.

ENSURE A PROPORTIONATE RISK MANAGEMENT APPROACH

- Consider a more precise definition of Cloud Service Providers (CSPs) to further support a risk-based approach;
- Clearly reference internationally accepted standards, in particular for risk management, and avoid any technology mandate in the context of encryption;
- Ensure the threshold for initial incident notification focuses on truly significant incidents and that the timeline is extended to at least 72 hours;
- Adopt a proportionate and incentivizing approach to supervision and enforcement, that reflects that risk management and incident reporting requirements apply the same way to important and essential entities.

ENSURE ALIGNMENT WITH INTERNATIONAL STANDARDS AND BEST PRACTICES

- Preserve the voluntary nature of cybersecurity certification processes (as provided under the EU Cybersecurity Act), in alignment with international practices;
- Draw from industry-driven, international best practices to support an organic development of Coordinated Vulnerability Disclosure in Europe.

ENSURING CONSISTENCY AND COORDINATION

NIS 2.0 Precedence & Coordination with the DORA Proposal (Article 2.6)

The NIS 2.0 and DORA proposals overlap both in terms of scope and substance (for instance, the latter applies to 'critical ICT third-party providers' and refers to terms such as 'ICT risks'). NIS should constitute the regulatory focal point for material resilience requirements, and duplication and inconsistency between DORA and NIS 2.0 should be avoided. First, DORA and NIS 2.0 do not currently offer clear definitions that would provide a clear and consistent framework for their interactions. Sectoral legislation should refer to definitions that either match legal terminology or are defined in other EU legislation such as the NIS Directive and the NIS 2.0 proposal. This would greatly improve legal clarity and consistency both for entities covered and supervisory authorities (See BSA position paper on DORA and overlapping requirements with NIS 2.0 [5]). In addition, DORA empowers the Lead Overseer to provide recommendations to critical ICT third-party providers; as a result, two sets of authorities would conduct overlapping supervision over the same services, with the risk of inconsistent resilience and security requirements for digital/ICT services in the EU.

- Recommendation: The NIS 2.0 should provide the baseline for other legislation to build upon. The legislator should seek to clarify and harmonize terms and definitions applicable to cybersecurity and resilience in the DORA and NIS 2.0 proposals. In addition, the cooperation between the Lead Overseer and the NIS 2.0 national competent authorities, as well as the articulation of the substantive scope of their respective powers, should be formalized.

In this respect, NIS 2.0 Article 2.6 currently proposes that sector-specific resilience legislation shall have precedence over the NIS framework where such acts "require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements *are at least equivalent in effect to the obligations laid down in this Directive."* While this provision aims to create legal certainty but might be problematic in practice.

First of all, the proposed precedence rules make sense when the sector-specific acts regulate the entirety of the security aspects of all services provided by certain entities, but does not if a sector-specific act affects only a part of certain entities. For cross-sector services such as cloud, regulatory consistency can only be properly achieved if the basic level of requirements (foreseen by NIS 2.0) applies identically across all sectors in which those digital entities operate, rather than having NIS 2.0 applying in most sectors but not to certain sectoral elements.

Secondly, the criterion of whether certain sector-specific requirements are at least identical in effect to those in NIS 2.0 may not always be easy to assess and may also evolve over time (for instance, in a situation where a sector-specific act is stricter on incident reporting but less strict on encryption measures.

- Recommendation: The provision in Article 2.6 should state that if sector-specific resilience acts do not foresee a clear precedence rule over NIS 2.0, the legislator must ensure sufficient alignment and/or co-ordination of these acts with the relevant provisions of the NIS 2.0 Directive in order to avoid duplication or overlaps, e.g. in terms of cybersecurity risk management measures or requirements to notify incidents or significant cyber threats. That obligation should not prevent sector-specific frameworks from adding additional requirements that go beyond the basic level of protection foreseen under the NIS 2.0 framework.

[5] BSA feedback on the proposed Digital Operational Resilience for the Financial Sector (DORA) Regulation

Potential Overlap of Reporting Requirements (Article 20)

Many essential entities – those described as digital service providers in the current NIS Directive and defined as essential entities in NIS 2.0, including Cloud Service Providers (CSPs) – provide services to other defined as essential entities (operators such as airlines, financial services companies, etc.) that are already subject to sector-specific regulation. In this configuration and in case of an incident or outage, the NIS 2.0 proposal does not currently offer sufficient clarity on whether the service provider is obliged to report directly to the regulators or whether this obligation lays with the customer (Article 20.2). If the service provider would be required to undertake the reporting, this could breach confidentiality and contractual obligations, for instance in the context of a standard cloud service agreement where incidents are notifiable to the customer.

In addition, the essential entity might be using several essential entities as providers. In this case, it might be the only one that can determine the exact impact, if any, of the incident. Laying the reporting obligation onto the service provider might therefore lead to incomplete or inaccurate reporting.

- Recommendation: NIS 2.0 should clarify incident notification requirements for essential entities that service other essential entities, as a way to avoid duplicative reporting and avoid requirements that would conflict with contractual obligations. This could be achieved by including Article 16 (5) of the current NIS Directive which reads: "*Where an operator of essential services relies on a third-party [digital service provider] for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator*."

Information sharing (Article 26)

Encouraging timely and voluntary sharing of information about threats, vulnerabilities and incidents is an integral part of preparedness and response to cyber risks. However, an excessive emphasis on near misses might be misleading. Effective threat intelligence sharing requires very resource intensive tools that allow the community to research global security threats in a timely manner, and to aggregate relevant and actionable intelligence. NIS 2.0 lays out an ambitious approach to information sharing arrangements among trusted communities. While BSA sees value in formalizing information sharing arrangements between and among public and private sector entities via appropriate governance mechanisms, this objective should not undermine the investments made by the private sector to build and maintain these capabilities and the level of expertise and resources they require, nor should such information sharing include mandatory incident reporting requirements.

- Recommendation: NIS 2.0 should seek to clarify the governance, resources and operational elements associated with the information sharing arrangements foreseen under Article 26. This should be based on principles of equality, transparency and reciprocity. Public and private should become equal partners. Near misses should not be the focus of these information sharing mechanisms.

Computer Security Incident Response Teams (Article 9)

The proposal seeks to ensure that Member States have well-functioning CSIRTs, establishing essential requirements and tasks to guarantee effective capabilities to deal with incidents and risks and to ensure efficient cooperation at EU level. BSA is encouraged by the efforts to improve CSIRTs resources and resilience. However, the requirements and tasks attributed to CSIRTs are notable for the absence of a requirement for CSIRTs to have resources dedicated to acquiring to real-time threat intelligence and to share this intelligence based in interoperable solutions using the CSIRT networks.

- Recommendation: CSIRTs should be resourced to acquire state of the art global threat intelligence offerings. In addition, in the tasks assigned to CSIRTs we recommend making explicit the need to provide threat intelligence information-sharing between public and private entities based on interoperable solutions.

- Recommendation: The CSIRT network should also prioritize the exchange of interoperable threat intelligence feeds. Interoperability enables cybersecurity communities to communicate using a common language which, aids in a better understanding of cyber-attacks and improves the ability to deploy effective solutions. Improving interoperability will also improve CSIRTs ability to process and consume data.

ENSURE A PROPORTIONATE RISK MANAGEMENT APPROACH

Inclusion of Cloud Computing Service Providers under Annex I of the proposal

As demonstrated further by the COVID-19 pandemic, cloud plays an essential role for data hosting and processing in Europe. Its importance has increased over the past year as many organizations (both private and public) adapted to remote work environments and needed to shift to cloud to scale up their activities and deliver user-friendly online apps and tools. However, while cloud is an essential service, not all cloud services are used for essential or critical functions. NIS 2.0 could support a risk-based approach, so that the “level of security [of cloud services] is commensurate with the degree of risk posed to the security of the digital services they provide” as stated in recital 49 of the NIS Directive. This would help ensure NIS 2.0 takes into account the various non-essential and non-critical functions of the cloud.

- Recommendation: We encourage a more precise definition of Cloud Service Providers (CSPs) so that security requirements apply to cloud services when they provide “critical or important functions.” This could be achieved by creating the possibility to assess cloud services’ context and purpose, and the risk profile of the activities they underpin for the customer. The CSP and its customer could be responsible for determining which cloud services are high risk levels and then prioritizing these for the most stringent measures.

Risk management (Article 18)

BSA welcomes the fact that NIS 2.0 introduces a more comprehensive risk management approach. NIS 2.0 should provide a high degree of legal certainty for essential and important entities with regards to cybersecurity risk management measures. In this respect, it is particularly important that the proposal – which envisages the use of European Commission implementing measures to implement these frameworks – be aligned with international standards, schemes and protocols in this area such as ISO 27000 series which underpin global cyber security risk management practices.

In addition, Recital 54 states that “use of encryption, and in particular end-to-end encryption should be promoted and where necessary should be mandatory,” while reconciled with law enforcement access needs. Any technology mandate in the context of encryption (strong or weak) would set a dangerous precedent.

- Recommendation: BSA supports strong encryption and stands ready to find appropriate solutions to ensure citizens safeguards and law enforcement in a way that avoid suppressing innovation and put some technology companies at a competitive disadvantage in the global market. We believe that public and private sector should continue foster strong encryption but no technology mandates on encryption should be defined, absent a debate on the fundamental dilemmas this complex issue raises.

Threshold and Timeline of Incident Notification (Article 20)

NIS 2.0 proposes to lower the reporting threshold to incidents that have the 'potential' for loss or disruption caused by an incident, as well as "near misses." This is not a clear threshold and it could lead to entities issuing incident reports of non-significant incidents or even on incidents that in the end do not actually happen. This could trigger a flood of irrelevant incidents' notifications, leading to authorities being overburdened and their – and reporting entities' – resources being misallocated.

- Recommendation: 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. It is therefore of utmost importance to establish a common understanding of what exactly is 'significant,' by exploring existing international framework and/or standards and taxonomies to define thresholds. Reporting near misses should be made voluntary and is best addressed in industry-led groups such as Information Sharing and Analysis Centers (ISACs).[6]

NIS 2.0 also proposes a two-stage incident reporting with an initial notification within 24 hours of the entity becoming aware of the incident (as well as an initial reaction from the competent authority or CSIRT within 24 hours after receiving the initial notification). The deadline to notify should be both workable and meaningful. The time lapse between an entity becoming aware of an incident and the moment it notifies the incident must be used for discovery, analysis, response and gathering the required information. NIS 2.0 should seek to maintain the current practice as established by the existing NIS Directive, and to ensure alignment with other notification requirements in existing privacy and security legislation. For example, the General Data Protection Regulation states that a data breach notification should be done "without undue delay, and where feasible, no later than 72 hours" after becoming aware of the breach.

- Recommendation: The NIS 2.0 notification timeframe in Article 20(4)a should remain aligned with current practice under the NIS Directive, and with other notification requirements timelines, by changing the 24-hour deadline of initial notification into at least 72 hours In addition, the proposed two-stage process for reporting should make use of the one-stop-shop to ensure there is a harmonized reporting channel in place.

Moreover, NIS 2.0 requires that the notifying entity submit a final report to the competent authority "no later than one month after the submission of the [initial notification]" and include "applied and ongoing mitigation measures" in response to an incident. An investigation into a complex cybersecurity incident can often last more than a month, and up to several months depending on the nature of the incident. Mitigation measures may also last more than one month. As a result, it would be impossible for entities to turn in a final report one month only after the initial notification.

- BSA Recommendation: Article 20(4)(c) should require that the final report be submitted to the competent national authorities no later than one month after the entity has finished its forensic analysis and has conducted all other measures necessary to ensure business continuity, including mitigation measures, and handling of the notified incident.

Finally, NIS 2.0 foresees that "where appropriate" and in particular where incidents concern two or more Member States, the competent authority should inform affected Members States and ENISA. The proposal however does not provide more information of what constitutes "appropriate" conditions, nor actions ENISA could/is expected to take on the basis of the information received.

- Recommendation: NIS 2.0 should clarify the conditions in which article 20(6) applies and the way ENISA will process the information it receives on incidents, for what purpose, and ensure that it has added value by providing its cross border analysis of the incident back to the entities and authorities involved (within reasonable timeframes).

[6] See ENISA report on "Information Sharing and Analysis Centres (ISACs) Cooperative models"

Supervision and Enforcement (Article 24; Article 29)

Given the cross-border nature of many digital services, it is helpful that most service providers are brought under the supervision of the competent authority of the main establishment. As a general principle, lawmakers could consider whether other types of services could benefit from main establishment rules to support harmonization of the Digital Single Market and remove unnecessary friction.

The criteria used to define the 'main establishment' – based on the Member State where the decisions related to the cybersecurity risk management measures are taken or where the entity has the highest number of employees – may not reflect the reality of entities' operations in Europe and might lead to a more complex supervisory landscape for entities covered.

- Recommendation: For essential and important entities operating in multiple Members States it might be helpful to clarify that, within the same group of undertakings, only entities performing a critical activity as per Annex I and Annex II are subject to the NIS 2.0 rules.

In addition, effective and harmonized implementation of NIS 2.0 will require cooperation between CSIRTs / competent authorities, data protection authorities (pursuant to the GDPR[7]), national financial authorities (pursuant to the DORA proposal, see points above) and other relevant supervisory authorities (for example for trust services pursuant the eIDAS Regulation[8]). For instance, the DORA proposal foresees that European financial supervisory authorities alone will designate certain ICT third party service providers as "critical for financial entities" and will therefore be subject to their heightened oversight obligations (DORA, Article 28). At the same time, the NIS 2.0 proposal qualifies cloud services as providers of essential services and are placed under the supervision of the national competent authority of their main establishment in the EU.

- Recommendation: In order to avoid further fragmentation and double reporting for digital service providers such as CSPs, the proposal should clarify how cooperation between the supervisory authorities will work in practice.

The proposal lists expanded powers for competent authorities. This raises some concerns that this approach is not proportionate and does not create the right incentives. For instance, Article 29 should give a bigger role to documentation and existing mechanisms (such as third-party audits) for entities to demonstrate compliance.

In addition, the proposal lacks clarity on the triggers and appropriate conditions for using specific powers listed in Article 29. For instance, Article 29(f) states that competent authorities "have the power to order [essential] entities to implement the recommendations provided as a result of a security audit within a reasonable deadline." The use of the term 'order' seems to directly contradict the voluntary nature of 'recommendations.' It also does not provide a possibility for an independent body or tribunal to review or appeal formal notices or orders of the competent authority, a requirement which would help balance the proportionality of actions taken, and provide redress.

Moreover, the proposal should also take into account the realities and potential risks associated with some of these supervisory powers. For instance, on-site audits of CSPs may involve accessing data and systems used by many different customers / data controllers, which could be in direct conflict with confidentiality agreements. NIS 2.0 should recognize that in certain cases auditing requirements could be achieved by virtual audits, or by offering to make compliance certifications / third party audit reports available to the customer.

In addition, NIS 2.0 introduces individual liability at chief executive officer or legal representative level in Article 29(5) and an obligation for the management body of important and essential entities to "gain

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1614078685865

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

sufficient knowledge and skills to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity" (Article 17). While these provisions could help to significantly increase cybersecurity awareness at management level, they also appear disproportionate and their objectives unclear. They should not contradict the voluntary nature of some aspects of NIS 2.0 for instance on information sharing.

- Recommendation: Article 29 should adopt a proportionate and incentivizing approach, in particular by including safeguards, recognizing existing mechanisms and clarifying the conditions in which such powers may be used by supervisory authorities (including in view of coordination with other competent authorities). It should also give a bigger role to documentation and existing mechanisms (such as third-party audits) for entities to demonstrate compliance.

ENSURE ALIGNMENT WITH INTERNATIONAL STANDARDS AND BEST PRACTICES

Certification (Article 21)

The 2019 Cybersecurity Act (CSA) foresees the development of voluntary Certification schemes. NIS 2.0 proposes that the European Commission be able to adopt delegated acts that specify which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes. BSA strongly believes that a European certification approach should remain voluntary, be aligned with international standards and replace, not add to, national certification schemes.[9] In the current text, Member States may accept certifications to demonstrate compliance, creating a *de facto* mandatory requirement in some countries and fragmentation in the EU market. In addition, the reference to product certifications creates confusion as the security assessment should be done on the entities and their processes, not on their products. Finally, to this day, no certification scheme has been finalized or implemented under the CSA. Certification obligations foreseen in NIS 2.0 would therefore be overly prescriptive and premature in the current context.

- Recommendation: In alignment with international practice, NIS 2.0 should reaffirm the voluntary nature of certification schemes and introduce public consultations on any delegated acts that the European Commission would develop under Article 21 of the NIS 2.0 proposal.

Coordinated Vulnerability Disclosure & Creation of a European Vulnerability Registry (Article 6)

Coordinated Vulnerability Disclosure (CVD) is well-developed within the industry.[10] Looking to foster CVD practices in the NIS 2.0 Directive is a laudable concept but would only yield benefits if it is aligned with international standards and best practices, in particular efforts in this space from the Common Vulnerabilities and Exposures (CVE)[11] program which is a widely utilized international mechanism to address vulnerabilities and efficiently track down timely information.[12] In that sense, NIS 2.0 properly specifies that "to avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation agreements with similar registries in third country jurisdictions" (recital 31).

[9] 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

[10] BSA's Guiding Principles For Coordinated Vulnerability Disclosure

[11] As of this writing, there are 156 organizations from 26 countries participating in exchanging vulnerability information in a structured fashion. Currently organizations in Austria, Belgium, Denmark, Finland, France, Germany, Ireland, Latvia, Netherlands, Norway, Romania, Spain, and Switzerland are participating successfully in the CVE Program.

[12] https://cve.mitre.org/

- Recommendation: NIS 2.0 should further draw from international standards for CVD and handling such as ISO/IEC 29147 and ISO/IEC 30111, as well as and industry best practices, such as the CERT Guide to Coordinated Vulnerability Disclosure published by the Software Engineering Institute at Carnegie Mellon University,[13] to ensure alignment with current CVD practices and encourage structured cooperation between public, private and R&D communities. CVD should also be a two-way street, so that public entities should also be obliged to report vulnerabilities and backdoors in IT products they become aware of.

In addition, vulnerability disclosure should be a limited addition of coordinated information sharing by government with industry, not additional obligations that would likely reduce resources available to entities for their own vulnerability management programs or add undue complexity to organizations' existing CVD practices.

- Recommendation: CVD policy should be implemented at the level of individual (important / essential) entities. There are established means for providing structured identifiers for vulnerabilities which are in use globally today in cybersecurity products and services. It is recommended that NIS 2.0 also direct ENISA to integrate with the existing capabilities of Common Vulnerabilities and Exposures (CVE) Program. In addition, the involvement of CSIRTs as trusted intermediaries for vulnerability disclosure might not always be needed, especially when CSIRTs cannot help finding a mitigation to the vulnerability. Vulnerability researchers should have the possibility to report to companies directly as well.

Additionally, BSA strongly cautions against creating a centralized 'European vulnerability registry, ' which may fall short of expectations if the resources, structures, coordination are not appropriate in a very complex environment. Such a registry would likely become a high-value target for attackers, especially if it registers unpatched vulnerability without the appropriate governance and mechanisms in place; it could also lead to potentially having multiple reference numbers for the same vulnerability filed with another globally-used program.

- Recommendation: BSA recommends to not create a centralized 'European vulnerability registry' unless its added-value in view of the current environment can be clearly spelled out. Should the EU decide to create such a registry despite these concerns, it should be voluntary and contain all vulnerabilities already reported – regardless of whether patches are available or not. In addition, ENISA should seek to cooperate with entities before any public disclosure of vulnerability(ies) identified, to ensure that these entities have the opportunity to provide their customers with updates or patches to mitigate the risks of the vulnerability before it is disclosed publicly.

For more information, please contact:
Isabelle Roccia
isabeller@bsa.org

[13] "CERT Guide to Coordinated Vulnerability Disclosure," Software Engineering Institute, Carnegie Mellon University