EUROPEAN UNION AGENCY
FOR CYBERSECURITY

DEVELOPING NATIONAL VULNERABILITY PROGRAMMES

Challenges and initiatives

FEBRUARY 2023

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors, please use team@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

CONTRIBUTORS

Thiago Barbizan (Wavestone), Solène Drugeot (Wavestone), Cristian Michele Tracci (Wavestone), Lorenzo Pupillo (CEPS), Javier Gomez Prieto (ENISA), Evangelos Kantas (ENISA)

EDITORS

Javier Gomez Prieto (ENISA), Evangelos Kantas (ENISA)

ACKNOWLEDGEMENTS

ENISA would like to thank all the participants of the interviews and focus groups for their essential input for the development of this report. In addition, we would like to thank all the ENISA colleagues and expert groups for their valuable comments and review of the document.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-587-6, DOI: 10.2824/69116, Catalogue nr TP-04-22-106-EN-N

TABLE OF CONTENTS

TABLE OF FIGURES

EXECUTIVE SUMMARY

Based on the experiences and perspectives gathered from industry players and national governments, as well as on the documentation developed by multiple actors involved with national vulnerability initiatives and programmes, **the EU Coordinated Vulnerability Disclosure (CVD) ecosystem remains fragmented**. Although interesting approaches and initiatives are taking place in some EU Member States, yet **further steps can be done towards an integrated EU vision and action.**

This report shows that, despite recent efforts by national governments in developing CVD policies, **some industry players have taken the lead and developed vulnerability policies and programmes at organisation level**. Nevertheless, among the top industry expectations is that the development of a national or European level CVD policy could help organisations and public administrations to set vulnerability management as a priority and further encourage security practices. In addition, the **alignment of such policies with existing international standards, can greatly help in promoting harmonization**.

As far as vulnerability initiatives are concerned, **Bug Bounties Programmes (BBP) is an area that grew remarkably over the past few years.** BBPs have considerably adapted their business models in offering different type of services, hence different coverages of IT systems and levels of involvement in vulnerability management processes. Today, BBPs platform providers are now cooperating with key public institutions to run customised programmes adapted to their needs and IT infrastructures. Further expansion is expected as long as the community can continue relying on BBPs (i.e., confidentiality of internal information and data protection) and ensuring trust between the stakeholders involved.

In terms of human capital**, researchers play a fundamental role in the disclosure of vulnerabilities. Accordingly, it is interesting to understand motivations, incentives and challenges influencing researchers' contribution**. From their perspective, reputation remains as a one of the key incentives to legally report vulnerabilities, as it leads to fame and recognition. However, legal protection is also highly considered, especially because the **absence, uncertainty or non-clarity of legal conditions can push to illegal channels**.

Collaborative challenges arise in the use of tools to improve vulnerability disclosure processes. For example, when looking into vulnerabilities related to open-source software (OSS) and considering how intertwined commercial and OSS are today, a **need to further improve coordination between OSS developers and private vendors was identified**. Aspects such as OSS vulnerability handling, responsibility and accountability are not yet clearly defined and among actors involved across the IT product supply chains, which may hinder coordination efforts.

Challenges related to technical and technological issues also constitute a key area of discussion and analysis. **A forward-looking perspective on the use of automation as an enabler to efficiently manage vulnerability identification, sourcing and classification** is also provided by this report. It is observed that, as vulnerability analysis and treatment still require human expertise, the risk of deskilling experts due to automated processes may be minimised.

Finally, alignment across different legislation as well as cooperation between industry players and governments are needed to avoid silos. **Harmonisation of CVD practices, coordination and international cooperation among players are essential priorities both from a legal and technical perspectives**. In this regard, ENISA will continue offering advice, publishing guidelines, promoting information sharing, raising awareness, and coordinating CVD-related activities at national and EU level.

1. INTRODUCTION

1.1 CONTEXT AND OBJECTIVES

The implementation process of coordinated vulnerability disclosure (CVD) programmes in the EU is taking place in a heterogeneous manner. Yet, whereas a few Member States count on strategic approaches for the deployment of CVD programmes, some others are showing progress at different speeds without following a common EU approach. Likewise, within a co-existence of heterogenous approaches, common challenges have been identified, notably in the economic, legal, technical and policy dimensions.

The objective of this report is two-fold. First, to gather evidence related to latest developments and trends linked to the implementation of CVD programmes in the EU, and second, to deeply analyse current issues faced by public bodies, industry and researchers at the time of deploying CVD programmes in EU Member States. This report also elaborates on the analysis and conclusions provided by the ENISA report: 'Coordinated Vulnerability Disclosure Policies in the EU'[1].

1.2 TARGET AUDIENCE

The primary target audience of this report is composed by public bodies holding responsibility in the design and implementation of CVD policies in EU Member States. These entities are expected to receive and explore showcased outputs, evidence and results, as a result of a multidisciplinary consultation engaging more than 30 stakeholders. The added value of this ENISA report lies on the facilitation of a discussion framework that helps to identify common approaches for the implementation of CVD programmes across the EU.

The secondary target audience for this report is mainly composed by the general cybersecurity community and entities that are involved in the vulnerability treatment lifecycle, and that can benefit from the insights, challenges, and good practises identified herein.

1.3 REPORT STRUCTURE

This report includes the following chapters:

National CVD policy implementation – The industry perspective. This chapter explores and captures the expectations of the industry regarding the implementation of national CVD programmes and policies.

[1] https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu/@@download/fullReport

Addressing legal challenges for security researchers. This chapter addresses legal issues linked to the engagement of researchers in the disclosure of vulnerabilities. Good practices oriented to minimise the effect of these issues are also presented and discussed.

Addressing collaborative challenges: The use of open-source software and bug-bounty programs. In this chapter, collaborative challenges and approaches are analysed, particularly those related to the use of open-source software and technology. In addition, bug bounty programmes and initiatives are analysed and put into focus.

Addressing technical challenges: Automation initiatives supporting prioritisation and treatment of vulnerabilities. This final chapter focuses on technical issues linked to the use of tools and automated processes to speed up and support the vulnerability disclosure processes and interactions.

1.4 METHODOLOGICAL APPROACH

A three-step approach was followed oriented to (i) build an in-depth understanding of the CVD state of play, (ii) obtain specific data on latest CVD, and finally (iii) draw conclusions and recommendations useful for policymakers in charge of the design and implementation of CVD policies and programmes. The three steps are presented below:

1. Desk research. Collection and analysis of findings gathered from available literature. When selecting the sources, particular attention was given to the relevance, quality and reliability of sources, their geographical coverage and their pertinence to research scope outlined. To perform an efficient data analysis, an analytical framework was developed allowing to treat data in a structured manner.

2. Target consultation. A total of 13 interviewees and 2 focus groups involving more than 30 stakeholders were carried out. Interviewees were invited to answer 25 questions covering current challenges and future perspectives allowing to take further steps towards a common EU approach in the implementation of CVD programmes and policies. Two focus groups were conducted to discuss key aspects linked to use of open source as driver of collaborative frameworks and relations between CVD and bug bounty programmes.

3. Analysis of findings. By establishing correlations between desk research analysis and outputs of consultations with stakeholders, the obtained findings were treated in an aggregated manner. This work has allowed the elaboration of the primary information, and the identification of trends and evidence showcased in the distinct chapters along the report.

The research and analysis were mostly based on a qualitative approach, enabling to shed light on real life experiences and testimonials. It also served to identify other areas of analysis that would help to tackle current identified challenges in this report.

2. NATIONAL CVD POLICY IMPLEMENTATION – THE INDUSTRY PERSPECTIVE

2.1 CONTEXT

The implementation of national CVD policies is expected to have a significantly positive impact on security research around vulnerabilities, and their timely discovery, reporting and treatment. However, there is little doubt that these national frameworks will also have an impact on industry, as manufacturing becomes highly digitalised and increasingly dependent on technology, software code, and data.

In this section, the report collects the latest trends and industry stakeholders' inputs regarding the **development and implementation of national policies within EU Member States**. The section of the report is structured as followed:

1. Assessment and considerations on the creation of a national policy.
2. Good practices when developing and implementing of a CVD policy.
3. Challenges faced when developing and implementing a CVD policy.

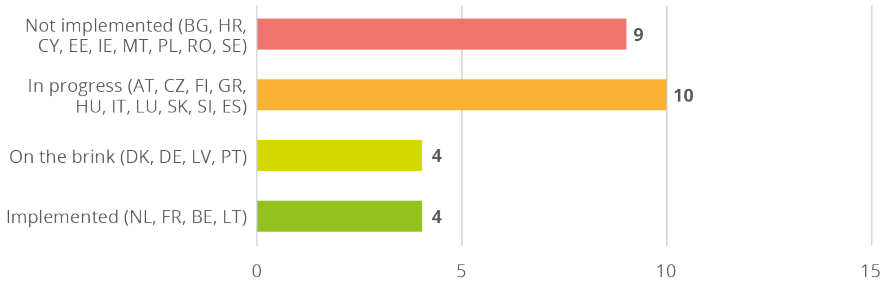
To contextualise this part of the report, the study has referred to the findings from the ENISA study 'Coordinated Vulnerability Disclosure Policies in the EU[2]' especially on the CVD policy state of play in the EU; and enriched these findings with desk research quoted throughout the study.

2.2 ASSESSMENT OF NATIONAL POLICIES

Despite the EU's strong push towards cyber security within a global digital transformation trend, the EU market is fragmented among EU Member States. Belgium, France, Lithuania and the Netherlands are the only four EU Member States with a fully established national CVD policy. Figure 1 presents an exhaustive state of play of the implementation of national CVD policy in the EU.

2 ENISA, 'Coordinated Vulnerability Disclosure Policies in the EU', April 2022. Available at: https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu

Figure 1: Implementation of coordinated vulnerability disclosure policy at national level in Europe, by implementation level

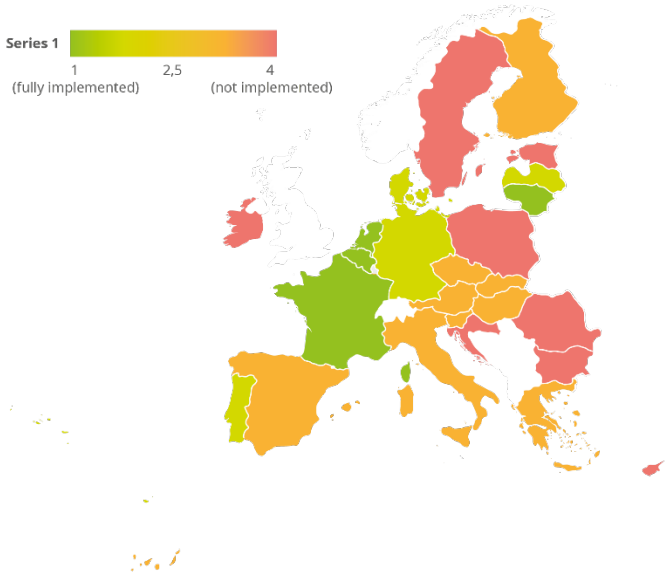


Source: ENISA, Coordinated Vulnerability Disclosure Policies in the EU, April 2022.

Four other Member States intend to set up a policy. In these cases, a proposal is either being examined at the level of policymakers or is tested in pilot projects. 10 other EU Member States are in the process of implementing a national CVD policy or are preparing to do so. However, failure to reach an agreement at the political or legislative level has slowed down such a process. Finally, nine Member States have not implemented a CVD policy and the process for establishing one has not yet started.

Implementation of CVD policy at national level in Europe Figure 2 below presents a mapping of the state of play in the implementation of CVD policies in the EU Member States. The map divides countries based on a scale between (1) to (4), where (1) indicates that the country has a policy in place, and (4) indicates that the countries have no policy in place. The values in between indicate either that the process of implementing a policy is in progress, or that the country is just on the brink of implementing one.

Figure 2: Implementation of coordinated vulnerability disclosure policy at national level in Europe, EU map



Source: ENISA, Coordinated Vulnerability Disclosure Policies in the EU April 2022, (author's derived perception).

From the mapping of the state of play of CVD implementation, a relative greater maturity can be seen of western European countries compared to other European regions. Conversely, southern European countries and central and eastern European countries are rather lagging in this process.

With this state of play in mind, the EU Member States are encouraged by the European Commission, Parliament and ENISA to set up national cybersecurity strategies and resilience programmes, surely including notions and action plans on vulnerability management[3]. The EU landscape on CVD may evolve due to the **NIS2 directive**[4] and **cyber resilience act**[5] pointing out the importance of vulnerability considerations and encouraging EU Member States to take further action.

Consulted industry experts pointed out that regardless of the existence or not of national policy actions, **industry players (private companies) have already initiated CVD initiatives at company level.** On one hand, most actors involved in vulnerability management see these private initiatives as an efficient move towards the creation of a safe IT ecosystem. In this sense, the European Commission encourages private companies to set adequate vulnerability strategies including mitigation measures in the case that a vulnerability cannot be patched immediately (e.g. due to requiring testing before deploying to production environment). The initiatives should include an appropriate incident response mechanism and guidelines on information security, business continuity and organisational resilience[6].

On the other hand, isolated company initiatives may create heterogeneity among practices making it more difficult for national governments to harmonise practices within a national policy on CVD. Along these lines, consulted stakeholders pointed out the importance for **policy makers to consider already implemented industry initiatives on CVD**, for instance ISO standards (ISO/IEC 30111:2019 and ISO/IEC 29147:2018), and may consider sector or infrastructure-specific standards. The importance of aligning international cooperation, industries and standards (to minimise the impact on already existing strategies and foster international exchanges) is also reinforced by the OECD in their report 'Encouraging vulnerability treatment'[7] which sets guidelines for policymakers on how to define a public policy**.**

In line with considerations presented in ENISA's report 2022 on Coordinated Vulnerability Disclosure[8], **ENISA's role was to facilitate harmonisation** and guide EU Member States in the development and implementation of national policies. This role **particularly applies in support-related activity** and the **elaboration of CVD guidelines at EU level**. The idea would be to provide governmental entities with guidelines on vulnerability management, dedicated processes and related responsibilities. Progress can be made, for example, through a standard

3 Joint Research Centre, 'Cybersecurity, our digital anchor', European Commission, June 2020. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC121051
4 Think Tank, 'The NIS2 directive: A high common level of cybersecurity in the EU', European Parliament, 16 June 2022. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
5 Cyber Resilience Act, ongoing consultation, European Commission. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en
6 Joint Research Centre, 'Cybersecurity, our digital anchor', European Commission, June 2020. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC121051
7 OECD, 'Encouraging policy treatment: Overview for policy makers', *OECD Digital Economy Papers*, February 2021. Available at: https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf?expires=1661940957&id=id&accname=guest&checksum=FBFCA250E5A156B4D347D519897CC15C
8 ENISA, 'Coordinated Vulnerability Disclosure Policies in the EU', April 2021. Available at: https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu

template for implementation at EU level (and later transposed at national level for all public entities) with some specifications for certain countries and potentially for industries and sectors.

2.3 GOOD PRACTICES WHEN DEVELOPING AND IMPLEMENTING A NATIONAL COORDINATED VULNERABILITY DISCLOSURE POLICY

A national or European CVD policy could help organisations and public administrations set vulnerability management as a priority and encourage security practices.

Based on the OECD report 'Encouraging vulnerability treatment', policy makers are spurred to follow a set of guidelines when developing a national policy covering CVD. To start with, policy makers should understand the underlying **motivations and barriers faced by stakeholders involved in CVD**. In this sense, policy makers would ensure that the planned objectives of the national CVD policy cover all stakeholders' needs and support the creation of a safer digital environment.

Consulted experts both from industry and national agencies recommended that national CVD policies should be developed with a particular attention given to content, format, transparency and coherence.

- Content and format of national CVD policies. The content of a policy should be clear and written in both the **national language of the country and English** (for foreign security researchers). Authors of such a policy should address it to **all stakeholders** involved in vulnerability disclosure and should clarify the roles, responsibilities, and governance within national CVD. Importantly, the necessity of adding a section on the roles of companies (e.g., code owners, manufacturers), prosecutors, and judges (often in charge of monitoring lawsuits initiated by organisations on security researchers) was pointed out. Prosecutors should be careful to examine each case thoroughly, and in accordance with the applicable CVD policy, before deciding whether to prosecute or not.

  Similarly, due to the nature of their involvement in lawsuits, judges should be aware of their role and responsibilities and have knowledgeable about the underlying legislation to conduct trials of security researchers that are being sued by a CVD counterparty. On this, EU Member States could follow the example of the United States' 'Judiciary Launches Vulnerability Disclosure Program' (October 2021), which provides clear guidelines for security researchers on the best way to safely report vulnerabilities[9].

  Along these lines, industry players emphasised the importance of defining the notion of 'responsible disclosure' which enables security researchers to safely report vulnerabilities to security teams or other responsible organisations. Another aspect to be considered is the limit between 'ethical and unethical' behaviour (i.e. what is allowed/not allowed) not only to avoid creating grey areas for researchers when reporting vulnerabilities but also to support judges in their assessment.

9 Judiciary Launches Vulnerability Disclosure Program, United States Courts, October 2021. Available at: https://www.uscourts.gov/news/2021/10/13/judiciary-launches-vulnerability-disclosure-program.

Lastly, a section of the policy should mention rewards provided to researchers for finding a vulnerability as this should be the main incentive for researchers to legally report their findings (subject covered in Section 4).

- Transparency of national CVD policies. While organisations tend to invest more resources in developing CVD policies, information presented in them sometimes remains high-level and not precise enough. Industry players pointed out that the policy should present its **objectives, scope, IT tools and disclosure process**. To set the scope, it is necessary to define which IT infrastructure will be exposed to security researchers (external stakeholders) or submitted to the verification of the internal security team only. 'Website vulnerabilities' (publicly exposed) are often discovered by external researchers, while 'infrastructure vulnerabilities' that are rather managed internally for confidentiality purposes. Lastly, industry players emphasised that having a defined vulnerability equity process (VEP) is a recommended practice whenever a national/ governmental entity is involved in the disclosure procedure.

- Coherence of national CVD policies. Any CVD policy developed at EU, national or organisational level (by private companies) should be coherent with already existing initiatives mainly present in the industry; in other words, **it shouldn't overlap with or contradict any other policy** (e.g., general data protection regulation [10]). Additionally, the revised **NIS directive**[11] and the proposed **cyber resilience act** will both cover aspects related to CVD policies. Therefore, policy makers should take a holistic approach and ensure coherence among these initiatives. Additionally, **ENISA and the European Commission** may agree and document an EU governance, the ownership of CVD issues and the roles of these EU institutions.

Although not a part of the CVD ecosystem, other important aspect to consider is '**government vulnerability disclosure' (GVD).** As opposed to a CVD policy which may involve multiple parties and is usually made public, GVD means "internal policymaking structures that governments need to implement in order to adequately assess and weight the potential costs and benefits of immediately disclosing knowledge of previously unidentified cybersecurity vulnerabilities, versus retaining that knowledge based upon carefully considered and time-limited justifications"[12]. Together with the notion of GVD stands the **Vulnerability Equity Process (VEP)** allows vulnerabilities to be reviewed and decisions to be made on whether to share them with affected companies, allowing entities to patch or withhold them for operational purposes[13]. More importantly, the VEP process should clearly define the roles and responsibilities of the parties involved. The main risks associated with GVD while not having a transparent VEP process are the following:

10 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (general data protection regulation). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

11 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. Available at: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

12 Cyber Threat Alliance, 'More_Sunlight_Fewer_Shadow, guideline for estabilishing & Strengthening government vulnerability disclosure policy', February 2021. Available at: https://cyberthreatalliance.org/wp-content/uploads/2021/02/More_Sunlight_Fewer_Shadows.pdf

13 Mozilla, 'The Vulnerabilities Equities Process', May 2017. Available at: https://blog.mozilla.org/press/files/2017/05/VEP-WhatWeKnow.pdf

- **No oversight of government hacking**. An independently verified VEP process ensures that all the benefits and drawbacks of disclosing or not disclosing a vulnerability are being considered before deciding.
- **Leak of government information**. There has been a steep increase in vulnerability information leaks from governments, some of which led to the creation of WannaCry and NotPetya ransomware. Withholding vulnerability information indefinitely takes away from the valuable time vendors have to implement fixes and reduce the impact to industry and society.
- **Parallel discovery**. Simultaneous vulnerability discovery by researchers is a real phenomenon[14] and it is evident in cases like Spectre and Meltdown. When a government discovers a vulnerability, it can be assumed that this vulnerability has been found by other parties as well, potentially leaving consumers, organisations, and even their own agencies at risk.

Global cooperation across different legislation as well as cooperation between industry players and governments need to be strengthened to avoid silos.

Further to the elements of content, format, transparency and coherence, as mentioned by a consulted representative of a national cybersecurity agency, CVD matters and the creation of a policy should be set as a **priority by governments**, however, should not create national silos or leave some industry sector aside. While a **European approach may be seen as the preferred method,** one should note that such a policy or guidelines should remain applicable to all sectors. Specific sectors such as energy management and supply and underlying critical public infrastructure may need a particular treatment when dealing with vulnerability management; setting up a regulatory framework and action plan may become mandatory[15]. This may require a reinforced cooperation between 'Intra-EU' governments and industry players in the context of public private partnerships.

Recommendations were also provided by CVD experts on the **implementation of such a national policy**.

A **collaborative approach between policy makers, industry actors**, **academia and researchers** should be emphasised at the implementation stage, to ensure an optimal coverage, an adequate set-up and applicability of the national policy and efficient adoption among stakeholders. Additionally, industry experts have mentioned the possibility to **appoint a national institution** to monitor the adoption and implementation of such a policy, similar to the way it is done in the United States (US) by the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB). In the US implementation, the White House has given the mandate to OMBs to foster the implementation of CVD policy at federal level. OMBs specified that the DHS would be the leading agency drafting the text to be re-used and adapted by each agency. To do so, the DHS used a Binding Operational Directive (CISA)[16], which has the force of law. All federal agencies were obliged to transpose the CVD policy unless they applied for an exception. Together with this directive, the Cybersecurity and Infrastructure

14 Herr, T. and Schneier, B., 'Taking stock: Estimating vulnerability rediscovery', Belfer Center, July 2017, Available at: https://www.belfercenter.org/publication/taking-stock-estimating-vulnerability-rediscovery

15 Peter Firstbrook, Sam Olyaei, Pete Shoard, Katell Thielemann, Mary Ruddy, Felix Gaehtgens, Richard Addiscoott, William Candrick, 'Top Trends in Cybersecurity 2022', *Gartner report*, February 2022.

16 CISA, 'Binding Operational Directive 22-01- Reducing the Significant Risk of Known Exploited Vulnerabilities', *Regulation*, November 2021. Available at: https://www.cisa.gov/binding-operational-directive-22-01

Security Agency (CISA) has made available some guidelines and a vulnerability disclosure policy (VDP) template[17] which has been written to align with Department of Justice's Framework for a Vulnerability Disclosure Program for Online Systems[18].

In addition to **allocating roles among vulnerability management governmental actors**, this type of directive could aim at **fostering trust and transparency among actors** by separating offensive functions (e.g., military, cyber defence) from digital security agencies and ENISA, and establishing transparent processes regarding how the government handles vulnerability information. This aspect was also emphasised by the OECD when mentioning the offensive roles of governments[19]. Some governments' ambiguity on vulnerability management can undermine other stakeholders' trust and the effectiveness of national policies to promote CVD. For this reason, most stakeholders could be suspicious when reporting such vulnerabilities. Therefore, from some non-governmental stakeholders' point of view, governments should demonstrate that they are trusted counterparties. One way to do this would be to transparently inform on the separation of the government's defensive and offensive functions at institutional level when dealing with CVD.

In the implementation of national policies it is equally important to **raise awareness and educate top management of organisations** within the industry. Decision makers should be aware and trained on the issue in order to smooth the adoption of CVD practices that are aligned with the national policy and define a solid governance around vulnerability management. This top-down approach should help **change mindsets through trainings exercises, the promotion of CVD good practices and awareness raising** addressed to all stakeholders. Final users should be trained and informed on how to benefit from it and understand its value-added.

2.4 CHALLENGES FACED WHEN DEVELOPING AND IMPLEMENTING A NATIONAL COORDINATED VULNERABILITY DISCLOSURE POLICY

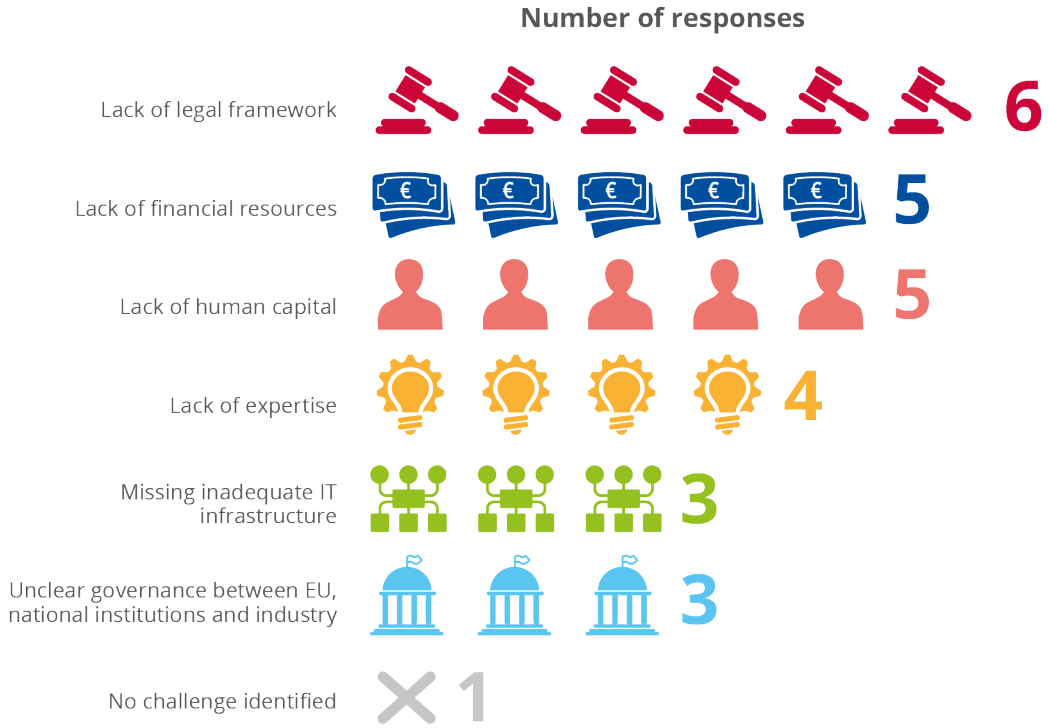
Among the 13 industry actors and experts in CVD consulted in the context of this study, a total of nine stakeholders have replied to questions by providing several answers, each regarding challenges faced when developing and implementing a national CVD policy. Figure 3 presents the list of challenges that were the most frequently encountered by stakeholders when developing and implementing CVD policies.

17 CISA, *Vulnerability Disclosure Policy Template*. Available at: https://www.cisa.gov/vulnerability-disclosure-policy-template

18 Cybersecurity Unit, U.S. Department of Justice, *Framework for a Vulnerability Disclosure Program for Online Systems*, July 2017. Available at: https://www.justice.gov/criminal-ccips/page/file/983996/download

19 OECD, 'Encouraging policy treatment: Overview for policy makers', *OECD Digital Economy Papers*, February 2021, Page 20, Box 3. Available at: https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf?expires=1661940957&id=id&accname=guest&checksum=FBFCA250E5A156B4D347D519897CC15C

Figure 3: Challenges encountered by stakeholders involved in coordinated vulnerability disclosure policy development and implementation



Source: Findings from interviews, Q3) What are the main challenges regarding the vulnerability policies' development and implementation? Interviewees (N=9).

The **lack of legal framework** and therefore no clear guidance in terms of cooperation among actors at national and EU level is the most important challenge. This challenge also generates uncertainties for national policy makers when framing the legal protection provided to security researchers (covered in Section 4 of this report).

With regard to **lack of financial resources**, the budget dedicated to IT systems or products security tends to be significantly lower than the one allocated to development and innovation. Moreover, this budget is usually dedicated to operational tasks, i.e., report treatment and triage of vulnerabilities. However, it is rarely used to write policies or guidelines or to train employees on CVD-related topics, such as 'security-by-design', or develop advanced (and automated) solutions to deal with reported vulnerabilities. Consequently, this results in other pain points related to insufficient human capital and expertise. Indirectly, this also affects the rewards attributed to researchers who usually target monetary compensations for their findings.

The **lack of human capital and expertise** are often interdependent, and both affect the efficient management of operational tasks on dealing with vulnerabilities and the production of a policy. As developing a CVD policy is not seen as a priority, staff and experts are not trained for it and are often allocated to other activities. While Subject Matter Experts for writing the section linked to technical topics on CVD may be available, the complexity appears when writing legal

information which require layers and particular legal expertise. As opposed to national cybersecurity agencies that may have the capacity to involve lawyers to discuss legal questions and produce the legal content of the policy, private organisations may struggle due to their limited network and/or insufficient financial resources. In both public and private entities, staff in charge of triage and vulnerability management are often not enough to efficiently process all the reports received from researchers; this resulting into frustration on the reporters' side and higher risk due to pending untreated vulnerabilities. Due to limited human resource capacities, any CVD policy and process becomes difficult to achieve and scale.

Another challenge pointed out by industry players was the **unclear cooperation and governance among EU institutions**. Together with a vulnerability disclosure policy, governments should define how industry, governments and EU institutions should collaborate, define the dependencies and information management (e.g. access and retention), **hence the importance of having a clear VEP in place** (Section 3.3). This VEP is necessary for industry players to benefit from a stable, secure and framed environment in which roles and responsibilities are clearly defined. Additionally, this transparency should support the effort to create 'capacity building' among EU countries, private actors and international institutions, as pointed out by the Federal Ministry of the Interior, Building and Community of Germany, in 2021 in the report entitled *'Cyber Security Strategy for Germany 2021'*[20].

Lastly, a national CVD policy should be created and implemented by considering the underlying **IT infrastructure used by states and private actors**. Experts pointed out issues linked to **inadequate IT systems and old-fashioned infrastructure** that represent a barrier to the implementation of automated CVD processes. This issue tends to complicate the vulnerability treatment procedure and often leads to manual processing of vulnerability-related tasks, which is time-consuming.

This list of challenges mentioned above is not exhaustive. Among others, there is rather **low attractiveness for security researchers to report vulnerabilities in a controlled manner**. If reporting is perceived as a cumbersome or risky process, the researchers may opt for a form of full disclosure of their findings or forgo the disclosure entirely. In extreme cases, they might favour 'grey or illegal markets'[21]. This could be partially explained by the insufficient **legal protection for security researchers** when legally reporting vulnerabilities, which is a gap that a regulatory framework could fill. This notion is covered in more detail in the next Section.

20 Federal Ministry of the Interior Building and Community of Germany, 'Cyber Security Strategy for Germany 2021', 2021. Available at: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf?__blob=publicationFile&v=4

21 OECD, 'Encouraging Vulnerability treatment', *OECD Digital Economy Papers*, February 2021. Available at: https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf?expires=1661940957&id=id&accname=guest&checksum=FBFCA250E5A156B4D347D519897CC15C

3. ADDRESSING LEGAL CHALLENGES FOR SECURITY RESEARCHERS

3.1 CONTEXT

An integral part of national CVD policies is the legal protection of security researchers and the provision of incentives for the legal reporting of vulnerabilities. This section focuses on **identifying legal barriers for security researchers**. The fragmentation of the legal and policy ecosystem with regard to vulnerability disclosure results in concrete challenges, if not constraints, for researchers who are interested in reporting vulnerabilities through legal channels and willing to do so. This observation has been widely documented by ENISA in the 2021 report on CVD and partially covered also by the previous section (Section 3). Contributions from consulted industry players come as illustrative examples based on an industry perspective together with the desk research conducted.

To address this objective, the research focused on three main areas:

1. incentives for security researchers to legally report vulnerabilities;
2. disincentives for security researchers to legally report vulnerabilities;
3. initiatives addressing the lack of legal protection for security researchers.

3.2 INCENTIVES FOR SECURITY RESEARCHERS TO LEGALLY REPORT VULNERABILITIES

In the attempt to have a more comprehensive understanding of the reasons why vulnerabilities are reported through legal channels once they are discovered, perspectives and experiences shared by industry actors pointed towards a variety of incentives.

The primary incentive regards **notoriety**, as security researchers hope for reputational gains from their discoveries and related disclosures. Notoriety can also result in concrete outcomes like professional references, letters of appreciation for university studies, or job offers. Identifying vulnerabilities requires expertise and time, for which researchers want to be properly valued and acknowledged.

A similarly important, but almost contrasting incentive, is the **legal protection** of the researcher. With clarity guaranteed, protection by reporting a vulnerability through legal channels motivates many researchers to favour this route over illegal channels[22]. In a sometimes uncertain legal context, ensuring that ethical hacking activities do not expose researchers to further legal risks

22 FIRST, 'Guidelines and practices for multi-party vulnerability coordination and disclosure. Version 1.1', 2020. Available at: https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1

is seen as necessary. Researchers should be aware of their rights, protections and limits regarding 'coordinated disclosure' to avoid navigating the risks of legal suits. Criminal charges are a serious consequence that all researchers should be aware of when operating in this space.

Regarding ethical behaviour, there is also an honest interest in making the overall **IT ecosystem safer**, without looking for additional gains, even though this does not represent the driving factor all the time. Some researchers or professionals show 'good faith' intentions to improving the state of the internet or the IT environment at large.

Reputational interests are a key driver for researchers to legally report vulnerabilities, as the public proof of vulnerability discovery and disclosure brings fame and recognition.

The role played by **financial incentives** represented an interesting aspect of this inquiry. Diverging opinions among consulted experts emerged though. On one hand, many researchers invest time in discovering and reporting vulnerabilities in exchange for monetary rewards; on the other hand, it was also argued that if money was such a determinant factor, the 'illegal market' (i.e., reselling vulnerabilities illegally) would provide greater financial rewards. Addressing the topic of vulnerability disclosure as a whole would not do justice to the history of this sub-field, recalling the long-lasting battle fought by some researchers to be more recognised, better legally protected and better valued for their work, exemplified by the 'No More Free Bugs' campaign[23]. However, despite the information around the illegal market and vulnerabilities rates remaining opaque and incomplete, there has been sufficient research to show that much greater gains can be achieved through illegal channels[24].

Lastly, research and investigation represent an additional stimulus for many researchers to pursue vulnerabilities. Researchers chase the **intellectual challenge** derived from looking for and eventually discovering vulnerabilities and the **learning opportunity** to further advance one's knowledge and expertise. This is ultimately in line with recurring trends within IT and cyber communities, where a deep curiosity for figuring out how systems work and in solving complex problems pushed through a continuous learning and exploration process.

Unanimously, the target consultations highlighted the **subjectivity of these incentives**, struggling to identify one single explanation valid for all types of researchers. In other words, **intrinsic motivations depend on each individual and vary across the spectrum**, urging policy makers and organisations' legal departments to consider and address a handful of incentives and avoid focusing only on one or two primary drivers.

3.3 DISINCENTIVES PREVENTING LEGAL REPORTING OF VULNERABILITIES

While vulnerability reporting may be driven by multiple incentives, at the same time, some factors might disincentivise researchers and professionals from reporting discovered vulnerabilities legally. Six potential disincentives were reported by consulted industry players.

23 Fisher, D. (2009), 'No more free bugs for software vendors', *Threat Post*, March 2009. Available at: https://threatpost.com/no-more-free-bugs-software-vendors-032309/72484/

24 Perlroth, N., This Is How They Tell Me the World Ends – The cyberweapons arms race, 2021.

The primary reason discouraging the legal disclosure of vulnerabilities concerns the **insufficient legal protection and potential exposure to legal suits**. This finding aligns with the existing research showing the legal challenges that researchers still face (see the 2021 ENISA CVD study and as OECD's "Encouraging Vulnerability Treatment" report[25]). However, this might seem in contrast with what was described in the previous section concerning the incentive to report vulnerabilities legally, namely legal protection (see Section 4.2); the divergences between different jurisdictions might explain this contradiction. In countries where researchers do not risk facing legal consequences, the formal protection offered by ethical disclosure might look like a convincing incentive (e.g. the Netherlands), as opposed to countries where there is no protection in place.

Analysing this argument more in depth, two interesting points are worth observing. The issue regards the insufficient legal protection and the lack of **clarity around the legal framework**, which results in uncertainty and confusion due to unclear policies, undefined responsibilities or unknown legal thresholds. In some situations, researchers are discouraged simply by the fact that they cannot get around the complications of the legal systems and the unclear requirements. Alternatively, a legal framework might indeed exist, but **researchers may not be aware** of it and therefore cannot make mindful decisions about their actions. These instances show two clear areas for policy intervention in the future.

The absence of a clear legal framework as well as unclear conditions for reporting vulnerabilities may disincentivise researchers.

When vulnerabilities are indeed disclosed, ensuring that the handling process is managed properly can have an impact, as often highlighted by best practices as guidelines[26]. **Inefficient or missing follow-up and monitoring** deter future reporting, as it seems that the case is not taken seriously and acted upon in a timely manner. There is consensus on the significance of managing processes and stakeholders effectively and efficiently, both among Subject Matter Experts and previously published research[27] [28], which can be as important as developing secured patches.

Likewise, administrative complications were reported as significant elements as well. **Poor communication among stakeholders** involved in vulnerability reporting (i.e., delayed, unclear, or totally absent responses) is a reason for not engaging in legal disclosures, as highlighted also by publications from other prominent institutions covering this topic, such as the OECD[29] and FIRST[30]. The **administrative burden,** due to the heavy reporting process, together with the fact that most researchers are not used to or not comfortable interacting directly with authorities, should be taken into consideration. Even though these aspects can be seen as marginal, attention is required to implement the needed improvements in the vulnerability disclosure process.

25 OECD, Encouraging Vulnerability Treatment: Overview for policy makers, *OECD Digital Economy Papers*, February 2021, Available at: https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf?expires=1662479285&id=id&accname=guest&checksum=7FDB7BA1D2905EAA43C2CD596A293D40

26 . IoT Security Foundation, Vulnerability Disclosure Release 2.0, September 2021, *Best Practice Guidelines*. Available at: https://www.iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf

27 Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure. Version 1.1 Released Spring, 2020. https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1

28 OECD, Encouraging Vulnerability Treatment: Overview for policy makers, *OECD Digital Economy Papers*, February 2021. Available at: https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf?expires=1662479285&id=id&accname=guest&checksum=7FDB7BA1D2905EAA43C2CD596A293D40

29 OECD, Encouraging Vulnerability Treatment: Overview for policy makers, *OECD Digital Economy Paper*, February 2021. Available at: https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf?expires=1662479285&id=id&accname=guest&checksum=7FDB7BA1D2905EAA43C2CD596A293D40

30 Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure. Version 1.1 Released Spring, 2020. https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1

3.4 INITIATIVES ADDRESSING THE LACK OF LEGAL PROTECTIONS

The lack of legal protection has been addressed through two types of initiatives, touching upon both concrete legal measures and awareness-raising measures.

Firstly, national cybersecurity agencies have been working on **campaigns and projects** meant to further develop an **ethical culture of responsible and coordinated disclosure of vulnerabilities**, such as ANSSI[31]. For instance, in November 2020, in the context of its cooperation with the OEDC, ANSSI has confirmed its willingness to strengthen cooperative efforts towards (i) ensuring security of products and services seen as a crucial issue for the digital security of companies, citizens and administrations and (ii) improving responsible vulnerability management, with the objective of strengthening digital security as a means of stabilising cyberspace[32].

Secondly, guidelines and judicial interpretations aim to better define the **approach and the boundaries of legal actions** between ethical hacking and unauthorised, illegal compromises and breaches, undertaken either by cybersecurity institutions or by judicial branches, like in the US[33].

In addition, the following good practices[34] should be taken into considerations when addressing legal barriers:

- ensure open, clear, and timely communication;
- develop clear CVD policies, being used as a contractual agreement between the organisations and researchers;
- clarify expectations from the organisation that owns the CVD policy and programme,
- clarify legal protections for security researchers;
- train public institutions on CVD to not only restrict CVD to the private sector;
- promote education for all stakeholders involved in CVD vulnerability management (and not only) ethical hackers;
- trigger national policy adaptations to allow security researchers to report vulnerability in a safe legal and IT environment – this may come from a common policy developed and implemented at EU level.

31 Agence National de la sécurité des systèmes d'information, ANSSI France, https://www.ssi.gouv.fr/

32 French National Agency for the Security of Information Systems, 'L'ANSSI continue de s'investir dans les travaux de l'appel de Paris à l'OCDE', *ANSSI news*, November 2020. Available at : https://www.ssi.gouv.fr/actualite/lanssi-continue-de-sinvestir-dans-les-travaux-de-lappel-de-paris-a-locde/

33 The United States Department of Justice, 'Department of Justice announces new policy for charging cases under the Computer Fraud and Abuse Act', 19 May 2022. Available at: https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act

34 Additional sources addressing legal protection are publicly available. See for example: Vulnerability Disclosure Release 2.0, September 2021 Best Practice Guidelines. IoT Security Foundation. Available at: https://www.iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf

4. ADDRESSING COLLABORATIVE CHALLENGES: THE USE OF OPEN-SOURCE SOFTWARE AND BUG-BOUNTY PROGRAMS

4.1 OPEN-SOURCE SOFTWARE – OSS

4.1.1 Context

When it comes to vulnerability discovery and disclosure, effective collaboration between stakeholders and affected parties is essential. However, this is often challenging, especially in the case of **OSS** where the lines of responsibility are sometimes blurred.

This section presents information obtained throughout desk research, along with the contributions of industry experts and other actors such as open-source association representatives. This section focuses on the following areas:

1. vulnerabilities' impact, management and treatment within OSS;
2. usage of Software Bill of Materials (SBOMs) within the context of OSS;
3. governance to apply under the perspective of OSS (relating mainly to the attribution of responsibility for vulnerabilities);
4. instances of OSS vulnerabilities within public and private organisations.

4.1.2 Vulnerabilities' impact, management and treatment within OSS

In 2019, the average IT application consists of 70% open-source components which has doubled when compared to 5 years ago[35] (36% of open source code present in IT products in 2015[36]). The product supply chain has become more complex as it includes codes from diverse authors, sources and natures (open source and proprietary). Consequently, developers, public and private organisations and product final users tend to hardly be aware of their risk exposure and whether their IT infrastructure is affected or not by a disclosed vulnerability. The most-frequently mentioned workaround by consulted CVD experts relies on the usage of a software bill of material (SBOM) and/or software composition analysis (SCA)[37] (defined in Section 5.3).

35 Carielli, S., DeMartine, A., Bongarzone, M. and Dostie, P., 'Now tech: Software composition analysis, Q2 2021', Forrester Overview, April 2021.
36 Carielli, S., DeMartine, A., Bongarzone, M. and Lynch, D., 'The state of application security, 2021', Forrester Overview, March 2021.
37 See footnote 35

With this in mind, most industry actors consulted in the context of this study commonly agreed that the **distinction between OSS and proprietary software is questionable**.

In this sense, on one hand, when it comes to vulnerability treatment, OSS code tends to be present in all commercial software (as shown in the case of Log4j[38]). When a vulnerability is discovered in software code, the priority should be to fix it via a **collaborative approach**, regardless of the nature of the software. On the other hand, the distinction between OSS and proprietary software could make sense when it comes to **governance** and mainly **accountability and responsibility** for the vulnerability. For a commercial software, the owner of the impacted code is the product manufacturer which has the responsibility to fix the vulnerability (easily identifiable). For OSS, identifying the code owner and/or the 'adequate person to contact' to manage the vulnerability becomes more complicated as anybody is free to publish, use and edit the code.

There should be a coordinated effort on the management of vulnerabilities between private vendors and OSS developers, given the entanglement of commercial and open-source software.

Diverging opinions related to vulnerability management in OSS co-exist among stakeholders involved in CVD. On one side, some experts claim that vulnerabilities in OSS should be easier to cope with via the above-mentioned **cooperating approach** on finding a fix. Projects such as Alpha Omega initiatives[39] aiming to handle vulnerabilities both in the OSS domain and in the commercial one have proven their efficiency. Additionally, OSS is truly public whereas proprietary software may not always be **fully transparent** on its vulnerabilities. This insufficient transparency could potentially lead to a limited disclosure of vulnerabilities, hence resulting in a less secured use of digital tools. On the other side, other experts tend to favour the usage of proprietary components or products by stating that the open and publicly disclosure of OSS vulnerabilities may lead to **further exploitations** and hence create a more dangerous ecosystem.

Along the lines of the OECD when advising on how to 'overcome co-ordination complexity'[40], most consulted experts agreed to say that with OSS being present in software produced and used worldwide, there should be **an international (or at least EU) coordination effort on the management of vulnerabilities**. This might be the role for ENISA or the European Commission (covered in Section 8) to facilitate information sharing, and support the implementation of joint procedures between Member States. The US Department of Defence recently held a large industry meeting and published a memo[41] touching upon vulnerability management in OSS. This helped in getting a larger of pool of experts from different profiles into the discussion.

In 2020, the European Commission has launched its open-source strategy, aiming at recognising and benefiting from the potential of open-source products and components within EU IT innovations. This was recognised as an important step for the EU institution toward the uptake and promotion of OSS. As part of this strategy, the Commission has emphasised that any open-source code used in the context of this EC strategy to produce IT tools would be

38 Weaver, N., 'What's the deal with the Log4Shell security nightmare?', Lawfare, December 2021. Available at: https://www.lawfareblog.com/whats-deal-log4shell-security-nightmare Log4J vulnerability
39 Alpha Omega project description. Available at: https://openssf.org/community/alpha-omega/
40 OECD, Encouraging Vulnerability Treatment: Overview for policy makers, *OECD Digital Economy Papers*, February 2021. Available at: https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf?expires=1662479285&id=id&accname=guest&checksum=7FDB7BA1D2905EAA43C2CD596A293D40
41 Memorandum for senior pentagon leadership, Commandant of the Coast Guard, Commanders of the Combatant Commands, Defense Agency and Department of Defense Field Activity Directors, 'Software development and open source software', January 2022. Available at: https://dodcio.defense.gov/portals/0/documents/library/softwaredev-opensource.pdf

submitted to systematic vulnerability scanning[42]. In the frame of this strategy, the EC has launched a BBP (described in Section 7.5) for open-source solutions used by public services[43].

4.1.3 Usage of 'software bill of materials' within the context of OSS

Risks due to attacks of software used in public and private organisations are becoming significant enough to consider new mitigating approaches that involve more than risk-based vendor/partner segmentation and scoring. These measures should focus more on requests for evidence of security controls and secure best practices, a shift to a resilience-based thinking, and other efforts[44]. SBOMs have emerged as a key building block in software security and software supply chain risk management. An SBOM is defined by the CISA[45] as a nested inventory, a list of ingredients that make up software components.

Over the past years, multiple regional and governmental institutions and industry organisations have promoted **the usage of SBOMs in security practices and software design and development.** According to the European Telecommunication Standard Institute (ETSI), organisations should consider security management already at the product design and development phases, and encourage the usage of the SBOMs[46]. Along these lines, in the EU at national level, the German Federal Office for Information Security has recommended the adoption of the SBOM of part of their national guidelines[47]. Similarly, the White House has published an 'Executive Order on Improving the Nation's Cybersecurity' (May 2021) which emphasises the importance of transparency and traceability when using open-source code and promotes the use of the SBOM too. Lastly, the report produced by the Open Foundation, titled 'The Open Source Software Security Mobilization Plan[48], provides 10 concrete recommendations including automation efforts, security by design and the utilisation of the SBOM.

Software Bill Of Materials (SBOMs) are seen as an adapted tool to improve software security and software supply chain risk management.

From a reporting perspective the SBOM could be perceived as an advanced version of a 'static registry or database' of IT systems in an organisation. Applying the **SBOM for OSS is seen as complex due to the variety and numerous versions of codes later re-used in different IT products**. Nonetheless, a SBOM could be used at the scale of an organisation that has an in-depth understanding of its IT infrastructure ('know your asset'). With this, the SBOM can be created to show interdependencies between IT products and elements within an entity.

Targeting similar objectives to the SBOM, the '**Software Composition Analysis' (SCA)** was presented in a Forrester article entitled 'Now tech: Software composition analysis, Q2 2022'[49]. This tool is defined as a product "that scans an application (without executing it) to identify vulnerabilities, license risks, conflicts, and noncompliant usage in open-source and third-party

42 European Commission communication, 'Open source software strategy 2020–2023', C(2020) 7149 final, October 2020. Available at: https://ec.europa.eu/info/sites/default/files/en_ec_open_source_strategy_2020-2023.pdf

43 European Commission's Open Source Programme Office starts bug bounties. Available at https://ec.europa.eu/info/news/european-commissions-open-source-programme-office-starts-bug-bounties-2022-jan-19_en

44 Peter Firstbrook, Sam Olyaei, Pete Shoard, Katell Thielemann, Mary Ruddy, Felix Gaehtgens, Richard Addiscoott, William Candrick, 'Top Trends in Cybersecurity 2022', *Gartner report*, February 2022.

45 Software Bill of Materials, CISA. Available at: https://www.cisa.gov/sbom

46 Antipolis, S., 'ETSI releases report on coordinated vulnerability disclosure – Helping organizations fix security vulnerabilities', ETSI, 17 February 2022. Available at: https://www.etsi.org/newsroom/press-releases/2029-2022-02-etsi-releases-report-on-coordinated-vulnerability-disclosure

47 ENISA, 'Coordinated Vulnerability Disclosure Policies in the EU', April 2021. Available at: https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu

48 Open Source Security Foundation and Linux foundation, The Open Source Software Security Mobilization Plan, 2022. Available at: https://openssf.org/oss-security-mobilization-plan/

49 Sandy Carielli with Amy DeMartine, Melissa Bongarzone, Peggy Dostie, Now Tech: Software Composition Analysis, Q2 2021, *Forrester Overview*, April 2021.

components, guiding users on where and how to remediate these flaws". Going beyond the software components, this tool offers interesting capabilities to cope with versions issues along with workarounds on how to better define remediating actions.

4.1.4 Governance under the perspective of OSS

When talking about governance for vulnerabilities found in OSS, the focus is placed on the **responsibility, liability and accountability** of such an event.

- **Responsibility** refers to the obligation to perform the task or comply with the rule.
- **Accountability** implies answerability for the outcome of the task or process.
- **Liability** is the state of being legally responsible for something.

The vulnerability handling process and the responsibility and accountability of discovered OSS vulnerabilities remain points of contention.

With these definitions in mind, industry experts confirmed that **clear and standardised guidelines should be produced in order to define these three notions** and guide governments and private organisations in the development of their policies. Responsibility may be distinct from liability. In this case, developers would not be liable for code they openly shared. This public code would be accepted as a common infrastructure and the response to a vulnerability found on the latter should be a public effort – liability would not be put on the developer (or its company). On the contrary, the **liability may be put on the commercial companies relying on OSS** that produce and design products based on open source codes while knowing that the code is affected by a vulnerability but deciding not to patch it. A **gap remains when it comes to allocating accountability** to an individual or an entity.

4.1.5 Instances of OSS vulnerabilities within public and private organisations

In Italy, a catalogue of OSS[50] used by public administration was created by the Agency for Digital Italy) and the Digital Transformation Department. Each public administration has the obligation to store the purchased and used OSS in this library. However, software is not always regularly maintained by public administrations that are often unaware of technical dependencies on other IT products. In the past, several public administrations have been attacked with the same exploit due to interdependencies of IT systems. Due to an insufficient knowledge of its IT system, the Italian public administration was unable to implement automation or rapidly identify risks on IT infrastructure when a vulnerability was reported. On top of being risky, this has pointed out a limit of the OSS catalogue. Another issue is that an OSS may be recorded once in this catalogue, however future software or code versions are rarely encoded.

An instance of a successful story of OSS in the Italian public administration[51] relies on a public administration which had released its software based on the Italian OSS catalogue prerequisites and on guidelines on the acquisition and reuse of OSS[52] published by the Agency for Digital Italy and Team Digital. The system integrator did face a vulnerability. Because the software was

50 AGID and Digital Transformation Department, 'Catalogue of OSS'. Available at: https://developers.italia.it/en/software.html
51 This instance was shared by an interviewed CVD expert who used to work for the Italian administration (target consultation findings).
52 'Linee Guida su acquisizione e riuso di software per le pubbliche amministrazioni', 2019, https://docs.italia.it/italia/developers-italia/lg-acquisizione-e-riuso-software-per-pa-docs/it/bozza/index.html

open source, a former security researcher of this public administration became aware of the vulnerability and has offered their help to fix it. Needless to say, that this is also a danger as somebody with malicious intentions could have exploited the vulnerability openly shared to the public.

In this effort of clarifying roles and action when reporting a vulnerability, an article entitled 'Coordinated vulnerability disclosure for open source'[53] was published by an IT service management company, so to guide security research within multi-party cooperation when dealing with vulnerability in open-source products.

4.2 CONSIDERATIONS ON OUTSOURCING SECURITY VIA BUG BOUNTY PROGRAMMES

4.2.1 Context

This section focuses on **considerations of bug bounty programmes (BBPs) combined with security-by-design practices**. BBPs are dedicated programmes where security researchers and professionals can submit vulnerabilities they have discovered, in exchange for a compensation. Findings obtained through desk research were compared and combined with outcomes of a focus group, for the sake of identifying areas of agreement and disagreement, trends and shared experiences among experts in this field. Additionally, inputs collected on bug bounties during further interviews were also included whenever they were deemed it relevant. This section focuses on the following research areas:

- structure of BBPs;
- security-by-design;
- BBPs challenges;
- BBPs in public administrations;
- evolution of BBPs;
- ENISA's role in BBPs.

4.2.2 Structure of bug bounty programmes

While various sources have studied BBPs and their variations, some key concepts are worth reiterating[54] [55] [56] [57]. Most BBPs are set up and structured around the following foundational parameters.

53 Gariché, N., 'Coordinated vulnerability disclosure for open source projects', Github, February 2022. Available at: https://github.blog/2022-02-09-coordinated-vulnerability-disclosure-cvd-open-source-projects/

54 Vulnerability Disclosure Release 2.0, September 2021 Best Practice Guidelines. IoT Security Foundation. Available at: https://www.iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf

55 Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure. Version 1.1 Released Spring, 2020. Availabe at: https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1

56 OECD, Encouraging Vulnerability Treatment: Overview for policy makers, *OECD Digital Economy Papers*, February 2021. Available at: https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf?expires=1661940957&id=id&accname=guest&checksum=FBFCA250E5A156B4D347D519897CC15C

57 Algorithmic Justice League, 'BUG BOUNTIES FOR ALGORITHMIC HARMS?', January 2022. Available at: https://drive.google.com/file/d/1f4hVwQNiwp13zy62wUhwIg84lOq0ciG_/view

- **Objectives.** What goals are foreseen by the organising entity[58] (e.g., outsourcing vulnerability research, reinforcing the security posture of the company, providing more transparency)?
- **Scope.** Which part(s) of the IT infrastructure will be exposed within the BBP (qualitative scope definition)?
- **Number of IT assets.** How many assets will the BBPs cover at its outset and what additional assets will potentially be included at a later stage (quantitative scope definition)?
- **Participants.** Who will be involved in the BPP (external stakeholders to the organising entity or internal experts from the company security team, or a combination of the two types of actors)?
- **Timeframe.** How long will the BBP will last for?
- **Rewards.** What are the nature and value of the rewards given to security researchers as a compensation for their findings (usually financial, but not necessarily)?
- **Communication channels**. How will researchers, the organising entity, and any intermediary will communicate?

The setup of a BBP has to follow a well-defined structure, built on an existing solid IT security posture, and a gradual path to ensure a proper management of vulnerability disclosure.

Once a BBP is set-up, it is fundamental for the organising entity to be ready to handle (address and patch) vulnerabilities and manage required operational tasks. Practically, this means that the organisation should anticipate the workload generated by the reception of vulnerability reports by its security team and allocated resources accordingly. Dealing with a vulnerability (including reception of the report, analysis of the issue, treatment of the vulnerability, interactions with reporters and publication of a patch) should be done in a timely manner.

A good way to reduce the initial load of expected reports is, before launching the BBP, to perform a self-assessment of the assets in scope with commonly available tools or services. This way, it is likely that a large percentage of the existing vulnerabilities will be identified and managed even before the BBP programme officially starts.

Concerning the **distinction between internally and externally managed BBPs**, larger companies tend to rely relying on internal security teams, in order to have full control over the reports. While offering many benefits in terms of effectiveness, efficiency and scalability, external BBPs indeed bring other types of challenges, such as a lower level of control over vulnerability information, higher risk of a data breach, the possibility that data is stored outside of the EU, and limitations regarding the publication of vulnerabilities at any point. Besides legal and contractual limitations, it is important to reiterate that the set-up of a BBP must guarantee confidentiality, as it relies on multi-stakeholder trust.

There exist different types of BBP programmes, including three main models[59]:

58 By 'organising entity', we mean an organisation which has decided to run a BBP on its own IT infrastructure.

59 A detailed break-down of types of BBPs was not the primary of objective of this research. For this reason, a simplified distinction has been offered. However, a detailed view can be found here: Algorithmic Justice League, BUG BOUNTIES FOR ALGORITHMIC HARMS?, January 2022. https://drive.google.com/file/d/1f4hVwQNiwp13zy62wUhwIg84lOq0ciG_/view

- **Closed BBPs** are invitation-based programmes involving a restricted number of researchers who are selected and invited to participate exclusively by the organising entity.
- **Hybrid BBPs** are registration-based programmes, involving interested researchers who can freely register and are then vetted by the organising entity before participating.
- **Open BBPs** are public programmes, involving any interested researcher willing to participate.

Notwithstanding the differences that each programme can offer, different types of BBP can be more apt for different organisations. To make a conscious decision, pros and cons and **trade-offs of each model need to be considered by the organising entity**. On one hand, highly secure organisations might initially favour closed BBPs, given the higher level of control that these provide, perhaps considering moving on to different models, or different variations, as the organisation's experience with BBPs matures. On the other hand, open programmes provide greater visibility, offering a brand image based on 'trust and safety' to the organisation. These programmes also allow to draw on a large pool of researchers with their unique skills and ultimately bring value to the security posture of the organising entity, despite the effort and resources needed to manage these larger programmes.

4.2.3 Security-by-design

There is a general consensus on the fact that **BBPs and security-by-design should be seen as complementary concepts** ultimately improving the security of the IT ecosystem. Involving researchers and developers more and more in BBPs should help foster security-by-design, as awareness is raised regarding security issues. Increasing interactions between these actors involved in products' supply chain should result in a virtuous cycle. Additionally, the more vendors and software manufacturers are involved in such programmes, the safer the overall ecosystem becomes.

In parallel, it should be noted that adopting a 'security-by-design' approach brings challenges. For instance, a different approach and mindset for software development and the need to adapt the development practices might generate additional costs (e.g., implementation, training, human resource, consulting services). In the infancy of a security programme, implementing a secure software development lifecycle (SSDL) should remain the priority, followed by a further evaluation of the benefits of BBPs to ensure products security.

The inherent tension between these two perspectives might be reconciled moving forward, embracing the best results of both approaches. Most professionals in the field tend to see **BBPs as sustainable** solutions thanks to their contribution to the market consolidation by creating trust, ensuring safety and raising awareness among actors. Alternatively, bug bounties are sometimes seen as an 'add-on' to an organisation's security programme, rather than a sustainable unique solution to address root causes.

Despite the growing interest in BBPs over the last few years, no security expert has claimed that BBPs can be the be-all and end-all solution to security vulnerabilities for any organisation, but rather an important component of a much larger and articulated architecture, which should include security-by-design.

4.2.4 Bug bounty programmes in public administrations

Public administrations face significant challenges in the establishment of BBPs with financial rewards due to legal limitations and limited budgets. Nonetheless, there are already examples to draw from, both focused directly on public administrations' systems, such as the Hack the Pentagon[60] and Hack U.S.[61], and focused on open-source software, such as the European Commission programme[62] launched in early 2022. These initiatives shows that BBPs are possible even for public organisations, despite existing constraints or hesitations.

A number of platform providers and some major BBPs are currently cooperating with key public institutions to run customised programmes adapted to their needs and infrastructures.

An important point when looking at the varied public administration systems among EU Member States is that ENISA should follow a systematic approach when guiding public administration in their BBP strategy. This method should avoid confusion, as decisions cannot be left to single agencies or individuals, with the risk of ending up with a fragmented system. The reference case in this context comes from the US federal system, where the Cybersecurity and Infrastructure Security Agency (CISA) required all public agencies to establish VDP through the Binding Operational Directive (BOD 20-01), issued by the US., in support of the Office of Management and Budget M-20-32, 'Improving Vulnerability Identification, Management, and Remediation'. This led to establishing best practices across the sector and triggering the VDP adoption even within the private sector.

In line with the observed trends within public administration and stakeholders' feedback, it is reasonable to expect a **continued growth in the adoption of BBPs by public administrations** worldwide. Always following a risk-based approach, the priority tends to initially be on critical infrastructure. Nonetheless, each public administration is left with the choice to implement the BBP strategy according to its specific objectives, needs and IT assets.

4.2.5 Bug bounty programmes challenges

As further BBPs are set up, it is worth noting that main BBPs challenges faced by organisations who already gained significant experience, including:

- difficult identification of IT assets owners and unclear guidelines on how to define who is responsible for fixing vulnerabilities;
- insufficient communication between researchers reporting vulnerabilities, organisations' developers, and organisations' security teams;
- limited resources allocated to security teams, as opposed to development and research,

60 Hackerone, 'Hack the Pentagon' Available at: https://www.hackerone.com/hack-the-pentagon. "'Hack the Pentagon" pilot programme opens for registration', March 2016. Available at: https://www.defense.gov/News/News-Stories/Article/Article/710033/hack-the-pentagon-pilot-programme-opens-for-registration/

61 Hackerone, 'Hack U.S.'. Available at: https://hackerone.com/hack-us-h1c?type=team

62 European Commission, 'European Commission's Open Source Programme Office starts bug bounties', 19 January 2022. Available at: https://ec.europa.eu/info/news/european-commissions-open-source-programme-office-starts-bug-bounties-2022-jan-19_en

- unwillingness of private organisations to publicly disclose vulnerabilities;
- insufficient resources provided by national governments to support BBPs;
- complex definition of the line between 'ethical and acceptable practices' and 'illegal and unacceptable practices' for security researchers.

While solving some of these challenges will require a longer time span, ENISA is well positioned to provide a substantial contribution either by coordinating the policy debate among all stakeholders involved or by producing public guidelines to support stakeholders' progress on these themes. On one hand, raising public awareness about CVDs and BBPs might result in a larger budget allocation for such programmes and initiatives at the national level; on the other hand, guidelines can better define certain concepts and points that are still unclear.

4.2.6 Evolution of bug bounty programmes

BBPs have evolved over time, presenting today some significant changes. First, there has been a shift in **acceptance** and comfort in having a BBP and in working with the community of researchers, as more organisations establish, rely on and appreciate the advantages on such programmes. Second, BBPs have become more **focused on the quality, rather than the quantity** of the reported vulnerabilities, which seems to be a natural evolution as programmes mature**.** Moreover, BBPs have grown to cover a larger set of IT/digital tools and infrastructure, thanks to the diversity of researchers' expertise working under each programme.

In terms of future evolution, there seems to be overall agreement regarding the expected **exponential and sustained growth of the security research community** in the next few years, this triggering **safer cooperation among actors.** These two trends suggest a strong basis for BBPs moving forward. Additional elements to consider entail the expansion of BBPs' scope in the future to cover, for example, algorithmic harm, as pointed out by forward-looking research in this space[63].

63 Algorithmic Justice League, 'BUG BOUNTIES FOR ALGORITHMIC HARMS?', January 2022. Available at: https://drive.google.com/file/d/1f4hVwQNiwp13zy62wUhwIg84lOq0ciG_/view

5. ADDRESSING TECHNICAL CHALLENGES: AUTOMATION INITIATIVES SUPPORTING PRIORITISATION AND TREATMENT OF VULNERABILITIES

5.1 CONTEXT

An important chapter in vulnerability treatment is the use of automation address technical challenges and increase efficiency and effectiveness. This chapter aims to collect stakeholders' contributions regarding **automation initiatives that can support the prioritisation and treatment of vulnerabilities**. The content of this section relies on desk research and primary data collected within a focus group composed of industry experts on CVD from diverse backgrounds. Information presented in this section is separated into the following two sections:

1. considerations on the usage of automated processes within vulnerability management.
2. CVD tools fostering the usage of automated workflows within vulnerability prioritisation and treatment.

5.2 AUTOMATED PROCESSES WITHIN VULNERABILITY MANAGEMENT

As pointed out in the Gartner report on *Top Trends in Cybersecurity' published in 2022*, ensuring the security of an organisation's products and infrastructure should come from both the organisation *per se* willing to improve its security posture and from security solution providers that regularly innovates and considers emerging technologies when developing their product portfolio. Among others, innovative product development, automation and the usage of artificial intelligence technologies stand out.

As generally agreed by consulted industry players, 'automation' initiatives present a high potential to enhance vulnerability management and are increasingly considered within organisations. Hence, the more automation can be adopted, the better it is. Nonetheless, stakeholders pointed out that substituting human in-depth analysis of vulnerabilities may not be yet possible. Organisations should aim to find the **nature of and balance between processes that could/should be automated** (e.g., repetitive tasks of researchers when seeking vulnerabilities) **and could/should be subject to human expertise**. For instance, the Alpha Omega project for OSS has been focusing on this approach and on identifying the criticality of pieces of software that would need to be overseen by human actions (triaging the vulnerability

and fixing it rather requires human intervention). Otherwise, there are the risks that (i) new vulnerabilities might be introduced, or (ii) vulnerabilities may be only partially fixed and categorised as "fully remediated" while the infrastructure or code remain exposed to risks. Due to the importance of human knowledge, industry experts commonly agreed that the **deskilling of vulnerability experts**[64] **and security researchers should not be the result of the automation** of phases within vulnerability processes.

With this in mind, **automation tends to apply to sourcing and publication rather than vulnerability analysis or treatment**. Automated processes could be restricted to the **reception, filtering, categorisation and acknowledgement of the reports**. These phases present a high potential for automation, as they are time-consuming, with a low value-added and do not require a lot of expertise for being performed. However, an automated triage would only be possible with the usage of a standard numbering methodology to classify vulnerabilities; the CVE numbering method was strongly recommended. This automated referencing was also touched upon by the ETSI, who recommend that each reported vulnerability should be automatically assigned a unique reference number to enable researchers and organisations to track the corresponding ticket[65]. This approach would enable the creation of an organised database of all reported vulnerabilities according to an agreed-upon logic and without human error (example of automation initiative done by the OASIS Common Security Advisory Framework (CSAF) Technical Committee[66], later described in Section 6.3)

Automation is fundamental to scale up the systemic capability in handling vulnerabilities, and may be best suited for the preliminary steps (e.g., sourcing and handling) of the vulnerability disclosure cycle.

5.3 COORDINATED VULNERABILITY DISCLOSURE TOOLS FOSTERING THE USAGE OF AUTOMATED WORKFLOWS WITHIN VULNERABILITY PRIORITISATION AND TREATMENT

Automation could potentially be used when dealing with scoring. The scoring mechanism as it is now can be very subjective (e.g., when a vulnerability is rated with a CVSS[67] score equal or higher than 7, it becomes a patching priority. However, distinguishing a vulnerability rated as a 7 from one rated as a 6.9 is challenging). To cope with this subjectivity, new scoring frameworks are being developed such as (i) Stakeholder-Specific Vulnerability Categorization [68] and (ii) Exploit Prediction Scoring System [69]. If those three scores could be considered jointly and in an automated manner, the end result would be perceived as more reliable.

The SBOM is seen as a great tool to automatically identify interdependencies among products and handle their classification accordingly. Without human intervention, the automated system would draw a list of all affected software based on data encoded in the SBOM. Depending on the nature of affected software and severity of the impact (i.e. namely on high-risk infrastructure), mitigating measures could be put in place to deal with vulnerabilities efficiently.

64 On the issue of delegating threat detection completely to an AI system and its implication for the deskilling of experts, see: CEPS Task Force, Artificial Intelligence and Cybersecurity: Technology, governance and policy challenges, CEPS, 2021, p. 33.
65 ETSI, 'Cyber security – Guide to coordinated vulnerability disclosure', TR 103 838, January 2022. Available at: https://www.etsi.org/deliver/etsi_tr/103800_103899/103838/01.01.01_60/tr_103838v010101p.pdf
66 OASIS Common Security Advisory Framework (CSAF) Technical Committee, 2022. Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf
67 FIRST, 'Common Vulnerability Scoring System SIG'. Available at: https://www.first.org/cvss/
68 Spring, J., Hatleback, E., Householder, A. D., Manion, A. and Shick, D., Prioritizing Vulnerability Response: A stakeholder-specific vulnerability categorization, Carnegie Mellon University, December 2019. Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=636379
69 FIRST, 'Exploit Prediction Scoring System (EPSS)', February 2022, https://www.first.org/epss/

As also mentioned previously, **Software Composition Analysis (SCA)** is yet another way to automate the discovery of vulnerabilities in OSS components, especially in modern DevOps or DevSecOps environments. SCA tools can inspect source code, software packages, binary files, containers and more, and correlate this data with known vulnerability databases for automated discovery. In addition, these tools can automatically create a software bill of materials to further facilitate any future inspections.

The **Common Security Advisory Framework (CSAF)** could be used as a complement to the SBOM to foster automation within vulnerability management**.** The standard is a replacement of the CVRF and was created by the OASIS CSAF Technical Committee[70]. CSAF is currently ready for testing and implementation and will become an official OASIS standard end of 2022[71]. CSAF is a JSON based standard that vastly improved the capabilities of its predecessor CVRF and can be used to share various types of vulnerability information along the supply chain in a vendor-agnostic format.

Lastly, the **Vulnerability Exploitability eXchange (VEX)** documents and attestations[72] can be seen as an enhanced version of 'traditional advisories' and is perceived by experts as a great catalyst to automating vulnerability management. VEX documents are machine readable and are built to support integration into existing and new security management tools, along with broader vulnerability monitoring mechanisms and systems. In addition, VEX can supplement SBOM data and can make its use more effective by allowing an immediate assessment of the exploitability of the vulnerabilities included in a product. The goal of VEX is to support greater automation across the vulnerability ecosystem in terms of disclosure, vulnerability tracking, and remediation.

Overall, on top of supporting an efficient vulnerability prioritisation and treatment, such tools would also **favour organisations' resource management.** In this sense, automation may help to reduce the human workload and/or provide answers that are more specific to a particular environment. A vulnerability may be critical to one user and/or infrastructure because of its configuration and environment, yet might be non-critical to another one.

Lastly, the OECD and the White House have shared a similar recommendation[73] on the usage of **automated and standardised messages** at each stage of the vulnerability treatment among counterparties. These communications may include status updates, requirements to complete a vendor's current stage, next steps, and points of contact for questions, etc. With this, automation could be **an advantage for vendors** as automated communication like 'we know about the vulnerability and are investigating' or 'we are not affected' can reduce the volume of calls and emails received via the support hotline, thereby contributing to better management of resource allocation.

70 OASIS CSAF Technical Committee presentation. Available at: https://www.oasis-open.org/committees/csaf/charter.php

71 https://www.oasis-open.org/2022/08/05/common-security-advisory-framework-v2-0-from-csaf-tc-approved-as-revised-committee-specification/

72 A VEX document is a form of a security advisory that indicates whether a product or products are affected by a known vulnerability or vulnerabilities. Further work will be needed to build out additional use cases to help users understand how to successfully build VEX documents of varying complexity, https://www.cisa.gov/sites/default/files/publications/VEX_Use_Cases_Aprill2022.pdf

73 OECD, Encouraging vulnerability treatment: Overview for policy makers', *OECD Digital Economy Papers*, February 2021, p. 41 – and the White House has published an "Executive Order on Improving the Nation's Cybersecurity", *Briefing room*, May 2021. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

6. CONCLUSIONS

This report has provided a comprehensive overview of the information collected from consulted industry players involved in CVD and national policy makers. For each one of the research areas, the report presents trends, gaps to be offset, recommendations and attention points mentioned by external stakeholders. These findings are supported by secondary data retrieved from a literature composed of ENISA reports, EU and international institutions materials, public administration documentations and private organisation tools and internal policies.

The information was reported with the aim of capturing industry expectations regarding CVD policies, exploring challenges around CVD policy development, and identifying shared perspectives and trends, along with areas of disagreements. Subsequently, in-depth analysis was conducted to provide a better contextual understanding of all components and actors playing a role in the establishment and development of CVD policies and programmes. In this sense, reported findings and information sources go beyond the EU ecosystem and include international references (e.g. US policy initiatives).

Although the research and analysis has tried to focus on a variety of practical and concrete aspects related to CVD policies, the following main high-level conclusions can be drawn from the study:

- **National CVD policies can be an important example for the industry.** The development of national CVD policies is an important encouragement for industry organizations to set vulnerability management and security practices as a priority. In addition, the alignment with existing international standards around CVD, can greatly contribute to a harmonized approach among all stakeholders.

- **The CVD ecosystem remains fragmented**. This outcome had already been identified and described in detail within the ENISA CVD study (2021). The target consultation carried out in 2022 highlighted industry professionals' perceptions regarding heterogeneity of the CVD ecosystem, and a lack of legal certainty in EU Member States legislative frameworks. There is still an important and mostly unanswered need to strengthen harmonisation, alignment, coordination, and cooperation between industry players and governments.

- **Education and awareness should be prioritised**. Despite the decades-old existence of vulnerabilities and vulnerability management in cybersecurity, a 'security-by-default' product development approach favoured by education and training is still too rarely observed among developers and product manufacturers. Examples still emerge of professionals not getting a full understanding of the issues at stake or the potential solutions available. Therefore, there should be a substantial increase of vulnerability-

related education and awareness embedded in all levels of any code development or product manufacturing training courses.

- **Legal, economic and technological challenges** have been identified and brought under the spotlight and there is a growing effort to address them. Some of the changes needed to address the externalities of the vulnerability market require massive work. Nonetheless, each player can contribute at their own pace, however it needs to be noted that a legal mandate to address vulnerabilities very likely to come (e.g. with the CRA). Concrete solutions focusing on well-defined issues with a potential to be scaled up and expanded into larger initiatives over time will play an equally important role in moving forward the status quo on vulnerability management.

- **Promote 'security and privacy by design' ideologies.** In many cases it far better to be proactive and address security as early as possible in the lifecycle of new products. Significant resources and investment efforts are needed to further promote a security-by-design approach and mindset such as 'SecDevOps[74]' practices and simply prioritising security in IT systems at all levels. Integrating security and privacy thinking from the inception phases of any code development or product manufacturing will likely have the most significant benefit for the EU in the long run.

74 SecDevOps is a management approach that links security and operations teams in an IT context.

7. REFERENCES

1. Agence National de la sécurité des systèmes d'information, ANSSI France, https://www.ssi.gouv.fr/

2. AGID and Digital Transformation Department, ‚Catalogue of OSS'. Available at: https://developers.italia.it/en/software.html

3. Agide + Team Digitale,'Linee Guida su acquisizione e riuso di software per le pubbliche amministrazioni', 2019, https://docs.italia.it/italia/developers-italia/lg-acquisizione-e-riuso-software-per-pa-docs/it/bozza/index.html

4. Algorithmic Justice League, 'BUG BOUNTIES FOR ALGORITHMIC HARMS?', January 2022. Available at: https://drive.google.com/file/d/1f4hVwQNiwp13zy62wUhwIg84lOq0ciG_/view

5. Alpha Omega project description. Available at: https://openssf.org/community/alpha-omega/

6. ANSSI, 'L'ANSSI continue de s'investir dans les travaux de l'appel de Paris à l'OCDE', ANSSI news, November 2020. Available at : https://www.ssi.gouv.fr/actualite/lanssi-continue-de-sinvestir-dans-les-travaux-de-lappel-de-paris-a-locde/

7. CISA, 'Binding Operational Directive 22-01- Reducing the Significant Risk of Known Exploited Vulnerabilities', Regulation, November 2021. Available at: https://www.cisa.gov/binding-operational-directive-22-01

8. CISA, Vulnerability Disclosure Policy Template. Available at: https://www.cisa.gov/vulnerability-disclosure-policy-template

9. Cyber Resilience Act, ongoing consultation, European Commission. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en

10. Cyber Threat Alliance, 'More_Sunlight_Fewer_Shadow, guideline for estabilishing & Strengthening government vulnerability disclosure policy', February 2021. Available at: https://cyberthreatalliance.org/wp-content/uploads/2021/02/More_Sunlight_Fewer_Shadows.pdf

11. Cybersecurity Unit, U.S. Department of Justice, Framework for a Vulnerability Disclosure Program for Online Systems, July 2017. Available at: https://www.justice.gov/criminal-ccips/page/file/983996/download

12. 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. Available at: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

13. ENISA, 'Coordinated Vulnerability Disclosure Policies in the EU', April 2021. Available at: https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu

14. ENISA, Information Sharing and Analysis Centers (ISACs), ENISA publication, 2020a. Available at: https://www.enisa.europa.eu/topics/nationalcyber-security-strategies/information-sharing

15. ETSI TR 103 838, Guide to Coordinated Vulnerability Disclosure, January 2022. Available at: https://www.etsi.org/deliver/etsi_tr/103800_103899/103838/01.01.01_60/tr_103838v010101p.pdf

16. European Commission, 'Open Source Strategy', EC publication, October 2020. Available at: https://ec.europa.eu/info/sites/default/files/en_ec_open_source_strategy_2020-2023.pdf

17. European Commission's Open Source Programme Office starts bug bounties. Available at https://ec.europa.eu/info/news/european-commissions-open-source-programme-office-starts-bug-bounties-2022-jan-19_en

18. Federal Ministry of the Interior Building and Community of Germany, 'Cyber Security Strategy for Germany 2021', 2021. Available at: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf?__blob=publicationFile&v=4

19. FIRST, Common Vulnerability Scoring System SIG. Available at: https://www.first.org/cvss/

20. FIRST, Exploit Prediction Scoring System (EPSS), February 2022, https://www.first.org/epss/

21. FIRST, Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure. Version 1.1 Released Spring, 2020. Available at: https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1

22. Fisher, D. (2009), 'No more free bugs for software vendors', Threat Post, March 2009. Available at: https://threatpost.com/no-more-free-bugs-software-vendors-032309/72484/

23. Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure. Version 1.1 Released Spring, 2020. https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1

24. Hack U.S.. Hackerone. Available at: https://hackerone.com/hack-us-h1c?type=team

25. Hackerone, 'Hack the Pentagon' Available at: https://www.hackerone.com/hack-the-pentagon. 'Hack the Pentagon' Pilot Programme Opens for Registration, March 2016. Available at: https://www.defense.gov/News/News-Stories/Article/Article/710033/hack-the-pentagon-pilot-programme-opens-for-registration/

26. IoT Security Foundation, Vulnerability Disclosure Release 2.0, September 2021, Best Practice Guidelines. Available at: https://www.iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf

27. Joint Research Centre, 'Cybersecurity, our digital anchor', European Commission, June 2020. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC121051

28. Jonathan Spring, Eric Hatleback, Allen D.Householder, Art Manion, Deano Shick, ,Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization', White Paper, December 2019. Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=636379

29. Judiciary Launches Vulnerability Disclosure Program, United States Courts, October 2021. Available at: https://www.uscourts.gov/news/2021/10/13/judiciary-launches-vulnerability-disclosure-program.

30. Lorenzo Pupillo, Afonso Ferreira, Gianluca Varisco, 'Software Vulnerability Disclosure in Europe', CEPS publication, June 2018. Available at: https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/

31. Memorandum for senior pentagon leadership […], Software Development and Open Source Software, January 2022. Available at: https://dodcio.defense.gov/portals/0/documents/library/softwaredev-opensource.pdf

32. Mozilla, 'The Vulnerabilities Equities Process', May 2017. Available at: https://blog.mozilla.org/press/files/2017/05/VEP-WhatWeKnow.pdf

33. Nancy Gariché, 'Coordinated Vulnerability Disclosure for open source', Article, February 2022. Available at: https://github.blog/2022-02-09-coordinated-vulnerability-disclosure-cvd-open-source-projects/

34. Nicole Perlroth, 'This Is How They Tell Me the World Ends', 2021.

35. OASIS Common Security Advisory Framework (CSAF) TC, 2022. Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf

36. OASIS CSAF Technical Committee presentation. Available at: https://www.oasis-open.org/committees/csaf/charter.php

37. OECD, 'Encouraging policy treatment: Overview for policy makers', OECD Digital Economy Papers, February 2021. Available at: https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf

38. Open Source Security Foundation and the Linux foundation, 'The Open Source Software Security Mobilization Plan', Whitepaper, 2022. Available at: https://openssf.org/oss-security-mobilization-plan/

39. Peter Firstbrook, Sam Olyaei, Pete Shoard, Katell Thielemann, Mary Ruddy, Felix Gaehtgens, Richard Addiscoott, William Candrick, 'Top Trends in Cybersecurity 2022', Gartner report, February 2022.

40. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

41. Sandy Carielli with Amy DeMartine, Melissa Bongarzone, Peggy Dostie, Now Tech: Software Composition Analysis, Q2 2021, Forrester Overview, April 2021.

42. Software Bill of Materials, CISA. Available at: https://www.cisa.gov/sbom

43. Sophia Antipolis, 'ETSI RELEASES REPORT ON COORDINATED VULNERABILITY DISCLOSURE - HELPING ORGANIZATIONS FIX SECURITY VULNERABILITIES', ETSI Report, 17 February 2022. Available at: https://www.etsi.org/newsroom/press-releases/2029-2022-02-etsi-releases-report-on-coordinated-vulnerability-disclosure

44. Sven Herpig, Ari Schwartz, 'The Future of Vulnerabilities Equities Processes Around the World', Lawfare, January 2019. Available at: https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world

45. The United States Department of Justice, Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act. May 19, 2022. Available at: https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act

46. Think Tank, 'The NIS2 Directive: A high common level of cybersecurity in the EU', Briefin, European Parliament, June 2022. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

47. Weaver, N., "What's the Deal with the Log4Shell Security Nightmare?", Lawfare, December 2021. Available at: https://www.lawfareblog.com/whats-deal-log4shell-security-nightmare Log4J vulnerability

TP-04-22-106-NN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-587-6
doi: 10.2824/69116