Open Regulatory Compliance Working Group (ORC WG) Feedback for the Open Call for Evidence for the Revision of the Cybersecurity Act (CSA)

In light of the CSA review and wider need for harmonisation of vulnerability disclosure requirements across several EU regulations (e.g. CRA, NIS2, DORA, AI act) as well as further sharing of supply-chain best-practices, the Open Regulatory Compliance (ORC) Working Group of the Eclipse Foundation wishes to share and reiterate the importance of the Common Vulnerabilities and Exposures (CVE) system and a stronger technical and strategic role for ENISA given its growing international objective:

We recognise the importance of increasing EU resources to ENISA as part of CSA review. Notably, ENISA's role as a CVE Numbering Authority (CNA) is important and industry welcomes ENISA's goal to become a Root CNA.

We also believe that ENISA should step up as a CNA of Last Resort (for Europe, regardless of report or vendors jurisdiction). Secondly, we believe that ENISA should contribute systematically and long term to the CVE system as a whole; in general, and in particular around governance, establishing industry best practices and driving improvements. This also includes a pro-active, operational role, in ensuring that coordinated disclosure processes are followed and that the data is of sufficient quality to be useful in a European setting in general and for compliance with, for example, NIS2 and the CRA in particular. This may, at times, include helping the industry by annotating records, defining vocabulary or by re-publishing advisories after normalisation.

MITRE's role as Secretariat for CVE program plays a key role to provide a resource to boost supply chain resilience. While its recent publicity and uncertainty in funding are regrettable, we are pleased that this matter has been temporarily resolved.

The momentary alarm did however serve as a timely reminder to both governments and industry as to the global importance of a free, distributed and trusted vulnerability intelligence system for supply chain resilience and need for wider global support.

Indeed, this has also been recognised by several European governments who subsequently confirmed their wish to support (technically and financially) and thus we would hope that this support can be mirrored at an EU level, perhaps via ENISA, into a system which is mirrored infrastructure in Europe and co-developed.

We also see the growing role of national Computer Security Incident Response Team (CSIRTs), such as the National Cyber Security Centre (NCSC) in Ireland, largely supporting bug bounty programs, Capture the Flag (CTF) and other activities with local academia, government and businesses, investing in vulnerability discovery and management, and thus it is important to double down on the CVE program in a uniformed, cross-European and international way.

It would also be advisable for the European Commission to include this need for reinforced collaboration in its next inter-institutional dialogue with the USA's CISA and the UK's NCSC.

While we recognise the importance of NIS2's European Vulnerability Database (EUVD), we believe there is still room for better alignment and coordination. The EUVD beta includes identifiers that are not aligned or easily mapped to CVEs. This fragmentation creates confusion for producers and consumers of software bills of materials (SBOMs) and vulnerability data, reduces Europe's ability to defend against criminal and state-sponsored threats, and increases compliance burdens and operational complexity for software teams, open source maintainers, and users. The European Commission should revise the CSA to ensure better alignment between CVE and EUVD systems.

We strongly encourage involving all stakeholders, including the security and open source communities, in an open process as the work EUVD and the EU CNA root progresses.

We remain at your disposal for further information and collaboration.

About the ORC Working Group

The Open Regulatory Compliance Working Group (ORC WG) brings together prominent open source foundations, leading global enterprises, and industry stakeholders to address the growing impact of software regulations on open source. With over 50 members and growing, ORC develops best practices, specifications, and practical resources to help organizations navigate evolving regulatory requirements. Its initial focus is on the European Cyber Resilience Act (CRA), while supporting the long-term security, sustainability, and adoption of open source innovation worldwide. For more information, visit orcwg.org.