Open Regulatory Compliance

Feedback on Cybersecurity Act (CSA) Revision

2.6 | Inputs & contributions

Deliverable:	2.6
Category:	Inputs & contributions
Owner:	Cyber Resilience SIG
Status:	Shipped
License:	CC-BY-SA 4.0
Date:	December 2025

Feedback to call for evidence on Cybersecurity Act Revision

Context

Provide feedback to the EU Commissions open call for evidence as part of its initiative to revise the Cybersecurity Act (CSA). Urge for a stronger technical and strategic role for ENISA in light of the recent funding issues of the US CVE program and the increased importance of vulnerability handling in EU legislation.

Feedback (PDF) provided on June 20, 2025 (reference: F3567995).

Goals

- Urge the EU Commission to increase ENISAs mandate regarding CVE handling
- Avoid disproportionate reliance on U.S. government funding for CVEs

Feedback

> *[!NOTE]*
> *~~Feedback must be provided in a comment box (so no formatting option). Text length is limited to 4,000 characters.~~*
>
> *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, ENISAs role as a CVE Numbering Authority (CNA) is important and industry welcomes ENISAs 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.MITREs 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 USAs CISA and the UKs NCSC.While we recognise the importance of NIS2s 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 Europes 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.Best regards,

Acknowledgments

The following people have contributed to this document either directly or indirectly (e.g. by raising questions):

Dirk-Willem van Gulik,
James Lovegrove,
Jeremy Stanley,
Luis Villa,
Olle E. Johansson,
Roman Zhukov,
Tobie Langel,
and Ulises Gascon.

If you have contributed to this document and arent properly acknowledged or if you want to edit or remove your name, please let us know by opening an issue and we will fix this right away.