

LF CRA Stewards Plan

The Cliff Notes Edition

CRob - Chief Technology Officer/Chief Security Architect - OpenSSF/Linux Foundation
Nov 3, 2025

CRA Stewardship Obligations

For People Who Don't Do EU Legislation Goodly



OpenSSF
Cybergoose



OpenSSF

OPEN SOURCE SECURITY FOUNDATION

TL/DR - CRA WAT

So... you “get to” do some CRA, eh?

[Regulation \(EU\) 2024/2847 \(Cyber Resilience Act, CRA\)](#)

The Cyber Resilience Act is a piece of European legislation that will go into full effect December of 2027 that puts new cybersecurity requirements on any “product with digital elements” “put onto” or “made available” on the common market.

Predominantly focused on commercial vendors (“Manufacturers”), it will require proof of due diligence and software development/design activities as well as vulnerability reporting/coordination.

While not directly impacted by or beholden to the upcoming law, open source developers **WILL** be affected by their downstream consumers attempting to meet **THEIR** legal obligations.

A new legal category “Open Source Software Steward” (“Steward” going forward) has been created that broadly defines a handful of obligations for entities such as the Linux Foundation and our numerous sub-projects/foundations.

Stewards have three legal obligations under the CRA.



[LF CRA Steward “One-Pager”](#)

[LF CRA Steward Playbook](#)

- Oct 2026 Vulnerability Reporting for Manufacturers in force
- Dec 2027 All CRA requirements fully enforced for all stakeholders

Why Steward Something?

Not every project needs a Steward (docs-only, specs, archived projects, etc.). Consider taking the Steward role for graduated projects that are used downstream in commercial products sold within the EU*.

Certain capabilities are offered at the LF top-level that may be sufficient for your community's needs. Your community may already have some of these capabilities (such as a security policy, vuln. management team).

Consult with LF Legal for specifics for your projects and particular circumstances.

*Internationally other jurisdictions are considering similar requirements, so "no presence in the EU" does not necessarily exclude us from doing anything.

Requirement 1

Citation	Requirement
Article 24.1	<p>Open-source software stewards shall put in place and document ... a cybersecurity policy to ... <manage the>... effective handling of vulnerabilities ... as laid down in Article 15 ... that policy shall, in particular, include aspects related to documenting, addressing and remediating vulnerabilities and promote the sharing of information concerning discovered vulnerabilities within the open-source community.</p>

Req 1 TL/DR - Projects must have a publicly accessible security and vulnerability handling policy.

Solution 1

If your foundation and projects do not already have a security policy or vulnerability disclosure policy consider:

- Deferring to/using the [LF top-level security/reporting policy](#)
- Fork and update one of these templates
 - [security.md](#) (Vulnerability Disclosure OSS Maintainer CVD Guide)
 - https://github.com/ossf/oss-vulnerability-guide/tree/main/templates/security_policies
- Consider developing a security team-like capability for your projects to assist in these efforts.

Requirement 2

Citation	Requirement
Article 24.2	Open-source software stewards shall cooperate with the market surveillance authorities, at their request, with a view to mitigating the cybersecurity risks posed by a product with digital elements qualifying as free and open-source software.

Req 2 TL/DR - If your Projects are contacted by EU-authorities, assist them as able.

Solution 2

- Know which of your subprojects could be included in downstream commercial products and understand how you will react to requests for documentation or assistance in Coordinated Vulnerability Disclosure (CVD).
- Establish communication paths to security contacts for projects (vulnerability intake, triage, and reporting processes; playbooks; trusted external partners, etc.) .

Requirement 3

Citation	Requirement
Article 24	...The obligations laid down in Article 14(3) and (8) shall apply to open-source software stewards to the extent that severe incidents having an impact on the security of products with digital elements affect network and information systems provided by the open-source software stewards for the development of such products.

Req 3 TL/DR - Projects must report known exploited vulnerabilities related to any cyber security breaches that impact infrastructure supporting those projects to ENISA + National CSIRTs.

Solution 3

- Establish processes to monitor and alert on core infrastructure supporting projects (e.g. CI/CD and other shared services).
- Determine an EU National CSIRT to also report these breaches to along with ENISA via the Single Reporting Platform.
- Develop the capability to quickly assess and provide information around vulnerabilities reported with your projects.

Must's and Could's

The LF **MUST** do some things for our projects and communities. **REVIEW** the [LF CRA Stewards ED/GM One Pager](#) and [LF CRA Playbook](#) for more information.

ENCOURAGE project members to take LFEL1001 [Understanding the EU CRA](#) so they understand more about what is required.

The LF ***COULD*** do more to improve the renown and attractiveness of our communities for contributors, but at additional cost:

- Generate Source and Build SBOMs for Graduated projects.
- Become the CNA-LR (CVE Numbering Authority of Last Resort) for “the open source” (or just “LF*” projects).
- Review and consider encouraging projects to follow the [OpenSSF Open Source Project Security Baseline](#) and generate documentation/artifacts for downstream to consume to ease THEIR CRA obligations.
- Establish a team and a fund to support maintainers implementing these requested security practices.
- Establish an OSS-PSIRT capability for the LF to take the lead on these types of requirements for our whole ecosystem.
- Create guidelines and templates to ease compliance flows for Manufacturers, Stewards, and OSS Developers.

Full text of Applicable Articles

CRA Stewards Obligations

Emphasis added

Area	Citation	Requirement	TL/DR
Cyber Policy	Article 24	<p>1. Open-source software stewards shall put in place and document in a verifiable manner a cybersecurity policy to foster the development of a secure product with digital elements as well as an effective handling of vulnerabilities by the developers of that product. That policy shall also foster the voluntary reporting of vulnerabilities as laid down in Article 15 by the developers of that product and take into account the specific nature of the open-source software steward and the legal and organisational arrangements to which it is subject. That policy shall, in particular, include aspects related to documenting, addressing and remediating vulnerabilities and promote the sharing of information concerning discovered vulnerabilities within the open-source community.</p>	<i>security.md +vuln reporting process/link</i>
	Article 24	<p>2. Open-source software stewards shall cooperate with the market surveillance authorities, at their request, with a view to mitigating the cybersecurity risks posed by a product with digital elements qualifying as free and open-source software.</p>	<i>cooperate with M.S.A. to mitigate risks</i>
		<p>Further to a reasoned request from a market surveillance authority, open-source software stewards shall provide that authority, in a language which can be easily understood by that authority, with the documentation referred to in paragraph 1, in paper or electronic form.</p>	<i>policy posted electronically, translated</i>
Vuln Reporting	Article 24	<p>3. The obligations laid down in Article 14(1) shall apply to open-source software stewards to the extent that they are involved in the development of the products with digital elements. The obligations laid down in Article 14(3) and (8) shall apply to open-source software stewards to the extent that severe incidents having an impact on the security of products with digital elements affect network and information systems provided by the open-source software stewards for the development of such products.</p>	<i>Report vulns and known exploits to the Union</i>

CRA Stewards Obligations, continued

OpenSSF CRA Steward [Checklist](#)

Area	Citation	Requirement	TL/DR
Vuln Reporting	Article 14.1	For the purposes of the notification referred to in paragraph 1, the manufacturer shall submit: A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA . The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established pursuant to Article 16.	<i>establish an EU National CSIRT contact, report known actively exploited vulns to EU National CSIRT contact and ENISA</i>
	Article 14.3	A manufacturer shall notify any severe incident having an impact on the security of the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA . The manufacturer shall notify that incident via the single reporting platform established pursuant to Article 16.	<i>establish an EU National CSIRT contact, report "severe" vulns to EU National CSIRT contact and ENISA</i>
	Article 14.8	After becoming aware of an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, the manufacturer shall inform the impacted users of the product with digital elements, and where appropriate all users, of that vulnerability or incident and, where necessary, of any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured, machine-readable format that is easily automatically processable. Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.	<i>notify end-consumers of "severe" vulnerabilities</i>