# *open source* feedback on implementing guidance for NIS 2 security measures

(Source doc) Joint submission by OpenSSF, FSFE, NLnet Labs, GitHub and CPANSec

## Questionnaire

### 1. What type of entity are you representing?

- [ ] An entity in scope of these implementing rules
- [ ] An entity in scope of NIS2 but not in scope of these implementing rules
- [ ] Other

**Please specify:** We are a number of industry and civil society organizations with an interest in supporting the open source software ecosystem. This is a joint response by OpenSSF, FSFE, NLnet Labs, GitHub and CPANSec.

### 2. What do you think of the ENISA guidance?

- 1 I like it
- 2
- 3 I do not like it

### 3. Which sections of the guidance do you find most challenging to implement?

These are corresponding to the chapters of the Annex of the implementing regulation.

- [ ] 1. Policy on the security of network and information systems
- [ ] 2. Risk management policy
- [ ] 3. Incident handling
- [ ] 4. Business continuity and crisis management
- [ ] 5. Supply chain security
- [ ] 6. Security in network and information systems acquisition, development and maintenance
- [ ] 7. Policies and procedures to assess the effectiveness of cybersecurity risk management measures
- [ ] 8. Basic cyber hygiene practices and security training
- [ ] 9. Cryptography
- [ ] 10. Human resources security
- [ ] 11. Access control
- [ ] 12. Asset management
- [ ] 13. Environmental and physical security

**Please explain:**

General recommendation on chapter 5.1 guidance

It would be helpful to clarify that where the guidance refers to suppliers, it does not include open source projects that have been obtained outside of the procurement process, where no contractual relationship exists between the regulated entity and the open source project beyond adherence to a standardized copyright license, or where the contractual relationship is with an *open source software steward* (Regulation 2024/2847, Art. 3(14) "provides support on a sustained basis for the development and ensures the viability of those products") when contractually imposing technical or methodological requirements of a cybersecurity risk-management measure would not be appropriate, applicable or feasible considering the nature of the contractual relationship. This will align the expectations of open source stewards under the CRA with the supply chain security rules in the context of NIS2.
Instead, the guidance should include a separate chapter on supply chain security for open source dependencies, incorporating elements from the "tips" section starting in line 1941, that guides entities in responsibly using and nurturing the open source projects they rely on, without assuming that the NIS2 Directive imposes any obligations on those projects.

Specific recommendations on chapter 5.1 guidance:

- **5.1.2** We suggest adding to the examples of evidence the case where an entity has documented its use of open source software as a means to diversify sources of supply and limitation of vendor lock-in.
  We further note that the selection of a supply chain based on secure development procedures is constrained by e.g. the programming languages used. Instead, if selection based on secure development procedures is not possible, entities should consider investing in hardening the security posture of the supply chain, especially in an open source context (contribute and fund the work, including this in budget planning).
- **5.1.7** We believe lines 1943-1962 are solid content for a "supply chain policy for OSS", as suggested above in response to 5.1 and could be moved to the guidance for that section. We have the following suggestions for improvement:
  - **Risk assessment (line 1945):** Add "The risk assessment should be done in coordination with its open source project or associated Open Source Software Steward (Regulation 2024/2847, Art. 3(14)), at the expense of the supplier or service provider using the component, and in such a way that subsequent risk assessments done by third parties benefit from this work."
  - **Community collaboration (line 1948):** replace "for peer reviews [..] best practices" (addressed in previous item) with "to ascertain whether adequate resources are available to support sustainable maintenance efforts and contribute such resources where appropriate, including to guarantee future availability of security patches".
  - **Updates (line 1951):** replace "to the latest versions" with "to address all known and patched security vulnerabilities", in order to take into account that updating to the latest version is not always best practice from a security perspective. We suggest adding a footnote with a reference to SP 800-161r1-upd1, p. 2: "Updates to software deployed across enterprises often fail to update the smaller COTS components with

known vulnerabilities, including cases in which the component vulnerabilities are exploitable in the larger enterprise software."

- **Licensing (line 1953):** Delete this line and the corresponding footnote, it does not have any security relevance.
- **Code reviews (line 1954):** We suggest to add that suppliers don't necessarily need to perform security audits (and the resulting remediation efforts) themselves, but that they can fund existing initiatives that perform open source security audits at scale (e.g. Sovereign Tech Agency, Alpha-Omega, OSTIF). Additionally, suppliers and service providers should make any code reviews reusable for others to align with manufacturer obligations under Article 13(6) CRA.
- **Dependencies (line 1956):** We welcome this important element of the guidance. Dependency resolution can quickly become surprisingly challenging, and having a requirement to keep the automated tooling updated is a critical step in this effort.
- **Zero trust (line 1959):** Delete or move to a different place in the document, it is a different subject to OSS entirely.
- **Documentation (line 1961):** This element of the guidance is unclear. It should be re-worded as follows to create a clear requirement on suppliers to contribute to supply chain security for its open source dependencies: "Require the supplier or provider to provide clear documentation and policies for using open source libraries, including guidelines for evaluating and integrating, along with evidence of efforts to ensure sustainable maintenance of their dependencies by nurturing the open source projects they rely on, such as by referencing their public (code) contributions." We note that NIST SP 800-161r1-upd1, Section CM-8 paragraph (10) on p.95 provides an example of such a requirement specifically relating to SBOM generation.

## 4. Are there additional standards that should be included in the ENISA guidance? If yes, which ones?

-

## 5. What kind of support do you expect from ENISA in the future?

- Standards should be open and implementable with Open Source Software, if there is the expectation that they are to be adopted. We ask ENISA to support such adoption by only referencing standards that are publicly available, or by making summaries of relevant parts publicly available for this purpose. Open Standards are the foundation of cooperation in modern society. They allow sharing all kinds of data freely, prevent vendor lock-in and other artificial barriers to interoperability, and promote choice between vendors and technology solutions.
- To support further alignment between NIS2 and CRA and to reduce overlapping risk assessment efforts by NIS2 entities and other users of the same open source projects, ENISA should encourage the Commission to develop the concept of security attestation of free and open source software under Article 25 CRA to foster collaborative and complementary risk assessment efforts.
- We would welcome the opportunity to enter into a dialogue with ENISA to further elaborate on these points and to support open source supply chain security.