ISO/IEC DIS 18974 Self-Certification Checklist

Section 3.1.1

- ☐ We have a documented policy governing the open source security assurance of Supplied Software.
- ☐ We have a documented procedure to communicate the existence of the open source policy to all Software Staff.

Section 3.1.2

- ☐ We have identified the roles and responsibilities that affect the performance and effectiveness of the Program.
- ☐ We have identified and documented the competencies required for each role.
- ☐ We have identified and documented a list of Program Participants and how they fill their respective roles.
- ☐ We have documented the assessed competence for each Program Participant.
- ☐ We have a way to document periodic reviews and changes made to our processes.
- ☐ We have a way to verify that our processes align with current company best practices and staff assignments.

Section 3.1.3

- ☐ We have documented the awareness of our Program Participants on the following topics:

1. The open source security assurance policy and where to find it;
2. Relevant open source objectives;
3. Contributions expected to ensure the effectiveness of the Program;
4. The implications of failing to follow the Program requirements.

Section 3.1.4

- ☐ We have a written statement clearly defining the scope and limits of the Program.
- ☐ We have a set of metrics to measure Program performance.
- ☐ We have Documented Evidence from each review, update, or audit to demonstrate continuous improvement.

ISO/IEC DIS 18974 Self-Certification Checklist

Section 3.1.5

- ☐ We have a method to identify structural and technical threats to the Supplied Software;
- ☐ We have a method for detecting existence of Known Vulnerabilities in Supplied Software;
- ☐ We have a method for following up on identified Known Vulnerabilities;
- ☐ We have a method to communicate identified Known Vulnerabilities to customer base when warranted;
- ☐ We have a method for analyzing Supplied Software for newly published Known Vulnerabilities post release of the Supplied Software;
- ☐ We have a method for continuous and repeated Security Testing is applied for all Supplied Software before release;
- ☐ We have a method to verify that identified risks will have been addressed before release of Supplied Software;
- ☐ We have a method to export information about identified risks to third parties as appropriate.

Section 3.2.1

- ☐ We have a method to allow third parties to make Known Vulnerability or Newly Discovered Vulnerability enquires (e.g., via an email address or web portal that is monitored by Program Participants);
- ☐ We have an internal documented procedure for responding to third party Known Vulnerability or Newly Discovered Vulnerability inquiries.

Section 3.2.2

- ☐ We have documented the people, group or functions related to the Program.
- ☐ We have ensured the identified Program roles have been properly staffed and adequate funding has been provided.
- ☐ We have ensured expertise available is to address identified Known Vulnerabilities;
- ☐ We have a documented procedure that assigns internal responsibilities for Security Assurance.

ISO/IEC DIS 18974 Self-Certification Checklist

Section 3.3.1

- ☐ We have a documented procedure ensuring all Open Source Software used in the Supplied Software is continuously recorded across the lifecycle of the Supplied Software. This includes an archive of all Open Source Software used in the Supplied Software.
- ☐ We have open source component records for the Supplied Software which demonstrate the documented procedure was properly followed.

Section 3.3.2

- ☐ We have a documented procedure for handling detection and resolution of Known Vulnerabilities for the Open Source Software components of the Supplied Software.
- ☐ We have open source component records for the Supplied Software which track identified Known Vulnerabilities and action(s) taken (including even if no action was required).

Section 3.4.1

- ☐ We have documentation confirming that the Program meets all the requirements of this specification.

Section 3.4.2

- ☐ We have documentation confirming that Program conformance was reviewed within the last 18 months.

Next Steps

Have you self-certified to this specification? Please let us know by emailing operations@openchainproject.org. We would like to add your organization logo to the OpenChain website. This is optional, but very useful for our work.