The Linux Foundation License Scanning and Analysis Support Program for LF projects

- Support plan summary for 2021: LF Energy
  - Notes
  - Dependencies on other LF and project teams
- Covered projects and schedule of scans
  - Cycle 1: January, April, July, October
  - Cycle 2: February, May, August, November
  - Cycle 3: March, June, September, December
- Exhibits
  - Exhibit 1
  - Exhibit 2
  - Exhibit 3

Support plan summary for 2021: LF Energy

Support to be provided by: Steve Winslow <swinslow@linuxfoundation.org>

For the projects described below, the following actions will be performed:

1. Run recurring scans, on the schedule described below, of the project’s codebases using Fossology
2. Analyze and clear licenses, notices, and copyright statements contained in the project codebases
3. Publish SPDX documents with the license conclusions and copyright statements at https://github.com/lfscanning (or a similar public location), for broader community use in their own compliance processes
4. Produce summary reports for project leads / maintainers, with limited public visibility (or optionally public at the project’s discretion) with the following:
   a. catalog and summary of licenses detected, categorized, and identifying corresponding files
   b. description of key findings, particularly relating to incompatibility with project licenses and project IP policies
   c. recommendations for remediation where necessary
   d. guidance for best practices to improve project licensing notices and add statements to files without existing notices
5. Correspond with developers to address questions about findings, where possible without providing legal advice (see “Notes” section below)
6. Upon request from the project, up to approximately two times per year (such as prior to significant releases), assist with formal IP policy approvals under the project’s charter:
   a. document the license scan findings as “license exceptions” for approval by the Governing Board or technical leadership committee, as applicable
   b. prepare summary slide deck describing the requested exceptions
   c. present to project Legal Committee or similar leadership body to describe the requested exceptions and facilitate approvals under the charter

Stretch goals: will perform where feasible, subject to available resources and time:

1. Run “red flag” pre-intake scans, for net new projects:
   a. Run Fossology scan of the incoming codebase, prior to importing into a project-controlled repository
   b. Identify any “red flag” or “high priority” issues that would be likely to present a significant problem for license compatibility
   c. Correspond with developers regarding these issues where remediation is recommended
2. Parallel to Fossology scans, also run dependency scans using WhiteSource:
   a. review and clear scanning results, researching potentially concerning findings as appropriate;
   b. flag key issues to the project leads / maintainers;
   c. work towards providing standardized reports of all dependencies; and
   d. work towards providing vulnerability findings as part of results.

Note that WhiteSource has recently been incorporated into the license scanning workflow, so some of this functionality will be subject to the continued development of the scanning workflow automation.

Notes

- The Linux Foundation is not able to provide legal advice to project community members. The support program is focused on providing transparency about identified project licenses, and where possible describing general community understandings of license requirements. However, questions about e.g. whether a license is legally okay to use must be directed to the contributor’s own legal counsel and/or a project’s Legal Committee.
- The support program utilizes various automated tools supplemented by manual reviews. However, like any other scanning tool or process, the LF cannot guarantee the completeness or accuracy of the license scanning results and does not guarantee that all possible license issues in a scanned codebase will be identified.

Dependencies on other LF and project teams
Will periodically need assistance from the project manager or similar project staff support, to coordinate on preferred methods for communications with appropriate project community members.

May periodically need LF IT assistance for configuring certain types of scans, for those that are dependent on CI/CD processes that are managed by LF IT (none presently anticipated for current projects/scan types)

Covered projects and schedule of scans

NOTE: during the TAC meeting on Dec. 8, 2020, it was stated that not all projects’ source code is currently available. It is possible that the schedule below may be adjusted to accommodate sizing or changes in timing for when the full code base is available.

Cycle 1: January, April, July, October
  - RIAPS
  - CoMPAS
  - OpenLeadr

Cycle 2: February, May, August, November
  - GXF
  - OperatorFabric
  - PowSyBi

Cycle 3: March, June, September, December
  - Seapath
  - EM2
  - OpenEEMeter

Exhibits

1. Screenshots from example SPDX document
2. Screenshots from example scan report for developers
3. Screenshots from example board decks

Exhibit 1

Screenshots from example SPDX document
SPDXVersion: SPDX-2.1
DataLicense: CC0-1.0

## Document Information

DocumentNamespace: http://fossology.lfscanning.org/repo/SPDX2TV_adlik-2020-09-01.zip_1599769241
_documentName: /srv/fossology/repository/report
SPDXID: SPDXRef-DOCUMENT

## Creation Information

Creator: Tool: spdx2
Creator: Person: steve ()
CreatorComment: <text>
This document was created using license information and a generator from Fossology.
</text>
Created: 2020-09-10T20:20:42Z
LicenseListVersion: 2.6

## Package Information

PackageName: adlik-2020-09-01.zip
PackageFileName: adlik-2020-09-01.zip
SPDXID: SPDXRef-upload2741
PackageDownloadLocation: NOASSERTION
PackageVerificationCode: 45359c0bc3c3ee7e2b7a0f6b1cbceb613c15c99114b
PackageChecksum: SHA1: 0e8a52216834eae030adbad2ed634a75da8d1d4
PackageChecksum: MD5: 589d8bfa86741a0ad65eab529e76f204
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageLicenseComments: <text> licenseInfoInFile determined by Scanners: 
- nomos ("3.6.0-rc2-13-gfcb13c8ef".fc1b3b) 
- monk ("3.6.0-rc2-13-gfcb13c8ef".fc1b3b) </text>
Exhibit 2

Screenshots from example scan report for developers

Key findings and recommended actions:
Summary of findings:

Finding #1
Priority: **Very High**
On December 5, commit [redacted] in [redacted] replaced the prior Apache-2.0 code with code now containing AGPL-3.0+ license headers with [redacted] copyright notices. AGPL-3.0+ is a strong copyleft license. Either [redacted] needs to replace the AGPL-3.0 notices with Apache-2.0, or else these files need to be removed from the repo.
52 files (show files)

Finding #2
Priority: **Medium**
Some package.json files incorrectly list the project's license as "ISC". These should be corrected to "Apache-2.0"
1 file (show files)

Finding #3
Priority: **Low**
This file is missing most of the Apache-2.0 license notice (including any reference to Apache-2.0). It should be replaced with either the full standard Apache-2.0 license notice, or with a short-form ID:
SPDX-License-Identifier: Apache-2.0
1 file (show files)
License summary:

**Project Licenses:**
- Apache-2.0 7871
- Apache-2.0 AND CC-BY-4.0 14
- CC-BY-4.0 223

**Needs review:**
- Apache-2.0 (ASF header) 91

**Copyleft:**
- AGPL-3.0+ 52
- Apache-2.0 AND CC-BY-4.0 AND CC-BY-SA-4.0 3
- CC-BY-SA-4.0 4
- MPL-2.0 28

**Wrong license statement:**
- ISC (wrong license statement) 1
- Incomplete license statement 1

**Attribution:**
- (BSD-3-Clause OR GPL-2.0) AND BSD-2-Clause 7
- Apache-2.0 AND BSD-3-Clause AND MIT 2
- BSD-2-Clause 307
- BSD-2-Clause AND BSD-3-Clause 4
- BSD-2-Clause-FreeBSD 16
- BSD-3-Clause 6242
- BSD-3-Clause AND MIT 1
- BSD-3-Clause AND Public domain statement 18
- BSD-3-Clause OR GPL-2.0 48
- ISC 40
- MIT 409

**Other:**
- Google Patents Notice (GRPC) 1
- Google Patents Notice (Golang) 69
- OASIS IPR Notice 12
- Public domain statement 2
- Cross licensing 1
Spreadsheet with detailed findings:

<table>
<thead>
<tr>
<th></th>
<th>File</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OpenColorIO/docs/ociotheme/layout.html</td>
<td>BSD-2-Clause</td>
</tr>
<tr>
<td>2</td>
<td>OpenColorIO/docs/ociotheme/page.html</td>
<td>BSD-2-Clause</td>
</tr>
<tr>
<td>3</td>
<td>OpenColorIO/docs/ociotheme/static/ocio.css_t</td>
<td>BSD-2-Clause AND MIT</td>
</tr>
<tr>
<td>4</td>
<td>OpenColorIO/THIRD-PARTY.md</td>
<td>BSD-3-Clause AND LicenseRef-ICC-0.2 AND Zlib</td>
</tr>
<tr>
<td>5</td>
<td>OpenColorIO/ext/sampleicc/src/include/iccProfileReader.h</td>
<td>LicenseRef-ICC-0.2</td>
</tr>
<tr>
<td>6</td>
<td>OpenColorIO/ext/sampleicc/src/include/iccProfileReader.h</td>
<td>LicenseRef-ICC-0.2 AND X11</td>
</tr>
<tr>
<td>7</td>
<td>OpenColorIO/src/OpenColorIO/md5/md5.cpp</td>
<td>Zlib</td>
</tr>
<tr>
<td>8</td>
<td>OpenColorIO/src/OpenColorIO/md5/md5.h</td>
<td>Zlib</td>
</tr>
</tbody>
</table>

Exhibit 3

Screenshots from example board decks