SPDX Governance Change Proposal: Community Specifications and Project Membership

TL;dr: The following is a summary of the background for SPDX's current governance, as well as the proposed changes to governance. For specific details, please refer to the actual proposal documents:

- **SPDX Community Specification documents**: https://github.com/swinslow/2021-08-SPDX-governance-proposal
- **SPDX Project Membership Agreement for organizations** (attached to the end of this summary)

Background

The existing SPDX governance document, available at https://spdx.dev/about/governance, was originally set up in November 2012, shortly after SPDX was formed. It defines the project's scope as focused on license and copyright information; defines the roles and responsibilities of project members, Team Leads, and the Core Team; and establishes a general basis of lazy consensus for decision-making. The SPDX spec is and has been released under CC-BY-3.0.

Over the past few years, members of the Core Team have periodically discussed updating and revising the governance to better reflect the community's practices. At the same time, recent events have also highlighted a desire for updated governance, including:

1. Recent submission of SPDX to ISO to become an official internationally-recognized standard
2. Increased visibility of SPDX in connection with the May 2021 US Executive Order regarding security and Software Bills of Materials (SBOMs)
3. Participation from new community members with perspectives of more formal standards bodies

Examples of a few of the opportunities for improving SPDX's governance include:

1. more accurately reflect the current reality and future direction of the project
2. establishing a mechanism for official membership in the project
3. using contribution processes and a license for the spec that ensure explicit patent license commitments from contributors
4. improving clarity around decision-making processes and establishing an appeals process
5. adopting a code of conduct

Proposal: Community Specifications and Project Membership

In parallel, over the past few years, The Linux Foundation has hosted and operated many additional open standards and open source software projects. Some of these projects have tended towards highly formalized standards body practices. The LF has aimed to leverage the advantages of certain practices that are particularly important for specifications, such as ensuring due process in decision-making; while at the same time avoiding procedural burdens that slow down contributions.

The specific proposal for SPDX's new governance leverages two of those efforts.

1) Community Specification

First, this proposal would establish project governance for SPDX that uses the Community Specification model for its operations.

The Community Specification model was developed by the Joint Development Foundation (JDF) as a lightweight mechanism for specification development. It continues to enable repository-based development of standards through community consensus, while also adopting explicit principles of due process, patent license grants, and other best practices for standards development.

Community Specification exists as a set of default documents that are freely available on GitHub for anyone to adapt and use. For the proposal for SPDX, we have started from the Community Specification documents and adapted them to align with SPDX's existing practices to minimize community disruption.

The Community Specification documents proposed for use with SPDX are available at https://github.com/swinslow/2021-08-SPDX-governance-proposal. (If adopted, these would be moved into an SPDX repo.) They consist of the following:

- **0_SPDX_Contributor_License_Agreement.md**:
  - By making a contribution, the contributor agrees to the Community Specification License and the SPDX Governance Policy (see items 1 and 5 below for both). They also acknowledge that they are able to make the license grants set forth in the documents, including on behalf of their employer as applicable.
  - For source code contributions, the contributor certifies to a slightly modified version of the Developer's Certificate of Origin (DCO).
- **1_Community_Specification_License-v1.md**:
  - The Community Specification License would apply to going-forward contributors to the SPDX spec. Like the existing CC-BY-3.0 license, it includes a broad copyright license grant for copyrights embodied by the spec.
  - Importantly, it also adds an explicit patent license grant for implementations of the spec. This is not addressed by the SPDX spec's current CC-BY-3.0 license. The Community Specification License helps ensure that implementors of the spec have assurances from contributors to the spec that they are not holding back patents which might apply to implementations.
  - Notably, this patent license commitment extends beyond just the contributor's own contributions. The commitments are made with regards to the spec as a whole, with triggers based on the progression from Draft to Approved status of new versions of the spec.
  - There is a mechanism for contributors, in some circumstances, to withdraw from their patent license commitments. However, in order to do so they must declare it publicly and specifically, by making a PR to the "Notices" file (see below). Such exclusion would

not be retroactive. This enables the community to understand specifically what patents are being excluded, and to have an opportunity to work around them.

- **2. Scope.md**:
  - The Scope defined in this file is used to define the boundaries of the patent license grants from the Community Specification License.
  - The draft here is intended to encompass the breadth of what SPDX will be working on. It can be updated, but changes would be forward-looking and not retroactive.
- **3. Notices.md**:
  - The Notices file lists the points of contact for Code of Conduct complaints.
  - It also includes the location where licensors and licensees can submit PRs to trigger particular provisions of the Community Specification License, including the patent exclusions mentioned above.
- **4. License.md**:
  - The License file indicates that the Community Specification License 1.0 would apply to the SPDX spec.
    - As past contributors continue to contribute to the spec going forward, their contributions (including past ones) would come under the Community Specification License.
    - For pre-existing portions of the SPDX Specification whose contributors do not contribute going forward, their past contributions would remain available under CC-BY-3.0.
  - It also indicates that SPDX software libraries and tools would continue to be provided under Apache-2.0, unless otherwise noted.
- **5. Governance.md**:
  - The Governance file lays out the processes and policies for how the SPDX working group operates.
  - It retains the Teams and Team Leads structures from existing SPDX governance, identifying specifically the Technical, Legal and Outreach teams.
  - It revises the existing Core Team into a Steering Committee, made up of (1) the Team Leads, and (2) up to two participants nominated by SPDX project members (see below).
  - The current Chair would continue for the first one-year term after the change is adopted, and subsequently a new Chair would be selected from among the Team Leads and project member representatives.
  - It establishes term lengths for Team Lead members, so that there will be regular recurring checkpoints where Team Leads may be nominated for consideration by any participant in the SPDX community, and then selected by the Steering Committee from the nominated candidates.
  - It builds upon the consensus-based decision making process by establishing appeals processes, and by clarifying the “due process” requirements for ensuring opportunities for all voices to be heard.
  - It also formalizes the practices that have developed in the SPDX project (but not documented in current governance) around the timing and process for new versions of the SPDX specification to become officially released as Approved Specifications.

- **6. Contributing.md**:
    - This file simply clarifies that different SPDX repos may have different contribution processes, which will be documented in their respective CONTRIBUTING.md files.
- **7. Code of Conduct.md**:
    - Finally, this file adopts the Contributor Covenant Code of Conduct for the project.

2) Project Membership

Second, the proposal is to establish a mechanism for companies, non-profits, and other organizations to become members of the SPDX project.

Initial discussions centered around establishing a legal entity within the Joint Development Foundation (JDF). However, after reviewing the JDF structure and materials, the Core Team felt that they included complexity that was not applicable to SPDX and therefore did not want to proceed with utilizing the JDF structure.

Instead, this proposal is to establish a simple structure for organizations to join the SPDX Project as members within The Linux Foundation's own legal entity. This mirrors the structure used by many other LF projects.

Membership is not required in order to participate in the technical development of the SPDX specification, license list, tools or any other materials. Membership is also not required for contributors to participate on the Steering Committee or as a Team Lead.

Membership gives two primary benefits to members:

- have their logo displayed in appropriate places on the SPDX website, to express their support of the SPDX project; and
- nominate a person from their organization to potentially participate as one of the two SPDX Member Representatives on the Steering Committee.

As described earlier, the Steering Committee is made up of (1) the Team Leads; and (2) up to two Member Representatives selected by the Team Leads from member nominees.

To become a member, an organization would sign the Membership Agreement which is being shared along with the Community Specification documents.

Membership in the SPDX Project itself would be no-cost. However, because this structure requires project members to also be members of the Linux Foundation, organizations would need to join the Linux Foundation if they are not already LF members. Associate membership in the LF may be available at no charge to non-profits and governmental entities.

THE LINUX FOUNDATION

THE SPDX PROJECT
Membership Agreement

Thank you for your interest in supporting the SPDX Project (the "Project") as a member. The mission of SPDX is to increase transparency and reduce redundant work in managing software by providing a common format for organizations and communities to share metadata about software, thereby streamlining and improving security and compliance activities. The scope of the Project is to support the development and promotion of open standards for communicating software bill of material information, including provenance, license, security, and other related information.

Governance and intellectual property policies for the Project are documented in the Project's governance repository at https://github.com/spdx/governance.

Members are entitled to:

1. have their logo displayed on the Project website and informational materials where appropriate;
2. participate in Project general meetings, initiatives, events and any other activities;
3. during each cycle to select an SPDX Member Representative to serve on the SPDX Steering Committee, nominate one person from their organization as a candidate for selection; and
4. identify themselves as supporting members of the SPDX Project and community.

The SPDX Project is established as a project of The Linux Foundation (the "LF") and membership in the Linux Foundation is required. Members will comply with all such policies as the LF Board of Directors or the Project's Steering Committee may from time to time adopt with notice to members.

Please have this Membership Agreement (the "Agreement") executed by an authorized representative of the member company named below ("Member"). A countersigned copy will be returned to you by email for your records when your eligibility for membership has been confirmed. If you have any questions about membership, please contact membership@linuxfoundation.org.

Contact Information: If you are an existing LF Member, all notices from the LF relating to your participation will be sent to the individuals already on file with the LF under those categories unless you designate different individuals in Exhibit A.

Membership Term:

The initial term of membership will continue until the last day of the calendar year in which you join the Project. At the first renewal and renewal anniversaries thereafter, your membership will automatically renew on a calendar-year renewal cycle. You may cancel your membership upon request by emailing membership@linuxfoundation.org.

[REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

Name of Member Company: _____

Membership Level: General

Consolidated Employees (*if applicable*)**:** not applicable

PR/Logo Usage: Do we have your permission to:

...display your logo on the Project's website (Yes or No)? _____

...announce your participation via press release (Yes or No)? _____

Preferred method(s) for receiving invoices (*PDF or Hard Copy*): not applicable

Is a Purchase Order (PO) required (*Yes or No*)? not applicable

If Yes, please provide the following details:

Name: not applicable

E-mail: not applicable

By signing below, the Member acknowledges and agrees that, when signed and accepted by the LF, this Agreement represents a binding contract between the parties and commits the applicant to these terms and obligations:

Authorized Representative of Member:	Accepted:
	THE LINUX FOUNDATION
_____	
(Print Member Name)	
_____	_____
Signature	Signature
_____	_____
Name	Name
_____	_____
Title	Title
_____	_____
Date	Date

Exhibit A

Primary Project Contact

(for all notices)

Name: _____

Title: _____

Phone No: _____

E-mail: _____

Primary Technical Contact

Name: _____

Title: _____

Phone No: _____

E-mail: _____

Primary Marketing Contact

Name: _____

Title: _____

Phone No: _____

E-mail: _____

Primary PR Contact

(For approving press releases or quotes with respect to the Project)

Name: _____

Title: _____

Phone No: _____

E-mail: _____

Legal Contact

(This contact should be your primary in-house attorney for open source matters with respect to the Project. If you do not have in-house counsel, please leave this blank.)

Name: _____

Title: _____

Phone No: _____

E-mail: _____