Eclipse IP Management Modernization

Sharon Corbett
MODERNIZATION

WELCOME

- Eclipse IP - About
- Issue Statement
- Objectives/Benefits
- License Compliance
- Self Service
- New Process Overview
- Futures
- Best Practices
- OSCM
- Wrap Up
Eclipse Intellectual Property Management

> Eclipse IP Policy (Board Approved)
  ○ Defines mechanism for accepting and licensing the intellectual property developed and leveraged by Eclipse projects

> Legal Agreements
  ○ Formal - ECA, Committer Agreements, Working Group Participation Agreements

> Due Diligence Review Process
  ○ Provenance, License Compatibility, Scanning for Anomalies
  ○ IP Ticket (CQ)

> Commercial Adoption (Confidence/Safe)

> High Bar, Rigorous, Well Respected
What’s at Issue?

- Significant changes over time
- Cannot support agile development nor continuous delivery
- Impossible to scale to modern day technology (Node.JS, Electron, NPM, etc.)
- Burdensome - Lack of Automation
The Time has Arrived ...

> Bring Eclipse IP Policy and Process in line with contemporary expectations!
Eclipse IP Governance Approach (Redefined)

- Revise the IP Review requirements for third party content

- Update IP Policy
  - Change due diligence approach for third party content
  - Streamline Definitions
    - Project content
    - Third party content
    - Official Release=Distributed Content (NOT git commits, milestone, nightly, etc.)

- IP Advisory Committee Review

- Board Approval (October 21, 2019)
Objective

- Focus on **License Compliance Model only** for third party content (leveraged only; not otherwise produced or managed by Eclipse projects)

- Reduce burden/lower barriers

- Shift focus to other areas of high value

- Trust “other” sources of information

- Remain **WELL RESPECTED and RISK FOCUSED**
Objective

- Remove gate based on IP delays (faster service)
- Increase project velocity
- Provide flexibility and predictability
- Reduce administrivia
- Parallel IP (standard)
- New projects bring history (no review)
Objective

▪ Removal of Type A/B Stigma (Release vs Project)
▪ Allow project teams to adopt license compatible third party content during development cycle
▪ IP team certification prior to formal release
▪ Provide training/education
▪ Engagement with broader intellectual property community (leadership)
License Compliance Model

- Eclipse Foundation will stop performing deep copyright provenance reviews of Third Party Content

- Focus on license compatibility (standard) and licensing compliance

- Licenses driven by Board Approved Whitelist

- Leverage and trust “other” third party license sources (eg. ClearlyDefined)

- Enable projects to validate license compliance during development (trust but verify)
Applies to Third Party Content ONLY!
New Model

Project Content
- Provenance
- License
- Scan

Third Party Content
- License Compatibility Verification
Self Service Validation

Project Team | Eclipse IP Team

BoM
A
B
C
D

License Service

ClearlyDefined
License Whitelist
Overrides

IP Team Review

BoM
A (EPL-v2.0)
B (MIT)
C (Apache-2.0)
D (?)
Engagement with the IP Team

> IP Ticket (CQ) request only when/if required

> IP Ticket (CQ) if the dependency contains cryptography (declaration model)

> Projects must engage prior to a formal release for final IP clearance!
WHAT?
CQ REQUIREMENT FOR THIRD PARTY CONTENT ONLY WHEN/IF REQUIRED!
What does this really mean for me?

> Project onus will be fairly lightweight
> Compliance Report will identify any IP violations
> Projects are relieved of the responsibility to request IP review for every third party package requirement
> Projects should take care to only introduce dependencies that are subject to compatible licenses
Again, what does this really mean for me?

> NO piggyback/reuse CQs

> NO CQ before Adding to Orbit

> NO CQ before you start leveraging a certain library

> Periodic checks to ensure projects are on the right path
## Tracking Dependencies

<table>
<thead>
<tr>
<th>Current Process</th>
<th>New Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking via IP Tickets (CQs) Submitted by Committers</td>
<td>Tracking via Bill of Materials Ideally generated from build; e.g. Maven, Gradle, NPM dependency list, etc.</td>
</tr>
<tr>
<td>IP Log Generated (IP Tickets/CQs)</td>
<td>IP Log Generated (Bill of Materials)</td>
</tr>
<tr>
<td>IP Log Review</td>
<td>IP Log Review</td>
</tr>
<tr>
<td>IP Log Approval</td>
<td>IP Log Approval</td>
</tr>
<tr>
<td>Project Release</td>
<td>Project Release</td>
</tr>
</tbody>
</table>
Next Steps

> Prototype development/testing
  ○ Several projects in experimental drive

> Implementation roll out prior to end of year
  ○ Current infrastructure
  ○ Updates to documentation, committer handbook, front end systems, etc.

> Futures:
  ○ Build level Integration/automation
  ○ Automate an end-to-end system
  ○ Replace IPzilla
  ○ Security vulnerabilities
Community Engagement
IP Best Practices

> Include copyright and license headers on source files

> Include license text file in repository

> Include notice file (third party content information, versions, licenses, any other information in order to comply with license terms, etc.)

> Include contributing file (formal or non-formal)

> Identify project license on Github landing page (readme)
Trust Other Sources

> Leverage other sources of license data

> Donate our curated license data

> Crowd source with the greater community
Open Source Compliance Movement

SPDX - open standard for communicating software bill of material information (components, licenses, copyrights and security references) [https://spdx.org/](https://spdx.org/) (Adoption)

ClearyDefined - crowd sourced OSI Initiative to help FOSS projects; the project focuses on source location, clarifies applicable licensing and address security vulnerabilities [https://clearlydefined.io/about](https://clearlydefined.io/about) (Engagement)


Reuse Software - choose license, add copyright and license information to each file, confirm REUSE Compliance [https://reuse.software/](https://reuse.software/)

OpenChain - Its specification identifies the key requirements of a quality open source compliance program and show organizations how to meet the requirements [https://www.openchainproject.org/](https://www.openchainproject.org/)
THANKS!

Contact: emo-ip-team@eclipse-foundation.org

Helpful Links:

https://www.eclipse.org/legal/
https://www.eclipse.org/legal/licenses.php