THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

DIGITAL SERVICE AT CMS

CHAOSS OSPO Metrics WG: Repo Maturity Models, Metrics, Templates, & Linters with CMS.gov OSPO

Digital Service @ Centers for Medicare/Medicaid Services
Remy DecauseMaker, Isaac Milarsky, Natalia Luzuriaga

CMS Open Source Program Office (OSPO)

Remy DeCausemaker
Open Source Team Lead

Aayat Ali
UX Designer

Natalia Luzuriaga
US Digital Corps Fellow

Isaac Milarsky
US Digital Corps Fellow

CodingItForward Fellow ‘24
Full-Stack Developer

CodingItForward Fellow ‘24
Full-Stack Developer

CodingItForward Fellow ‘24
Full-Stack Developer

DIGITAL SERVICE AT CMS

What does the Digital Service at CMS.gov do?

The Digital Service at the Centers for Medicare & Medicaid Services transforms the U.S. Healthcare system by deploying design, engineering, product, and policy experts on a 'tour of duty' alongside dedicated civil servants.

We bring industry best practices and fresh approaches government modernization, to help solve some of the most complex problems facing healthcare today.

CMS Open Source Repository Baselines Overview: repo-scaffolder

Open Source Repository Maturity Models

- Where is our project on our Open Source Journey?
- **https://github.com/dsacms/repo-scaffolder/blob/main/maturity-model-tiers.md**

Repository Templates

- What files are required/recommended for healthy repository hygiene?
- **https://github.com/DSACMS/repo-scaffolder/tree/main/tier3/{{cookiecutter.project_slug}}**

Outbound Checklists

- What steps should our project take to release the repository publicly?
- **https://github.com/dsacms/repo-scaffolder/blob/main/tierX/checklist.pdf**

Cookiecutter

- How do we know what Maturity Model Tier our project should be in? What files are required in that Tier?
- `cookiecutter https://github.com/DSACMS/repo-scaffolder --directory=tierX`

Repolinter Configs

- What files or information is missing from our repo?
- **https://github.com/DSACMS/repo-scaffolder/blob/main/tier1/{{cookiecutter.project_slug}}/repolinter.json**

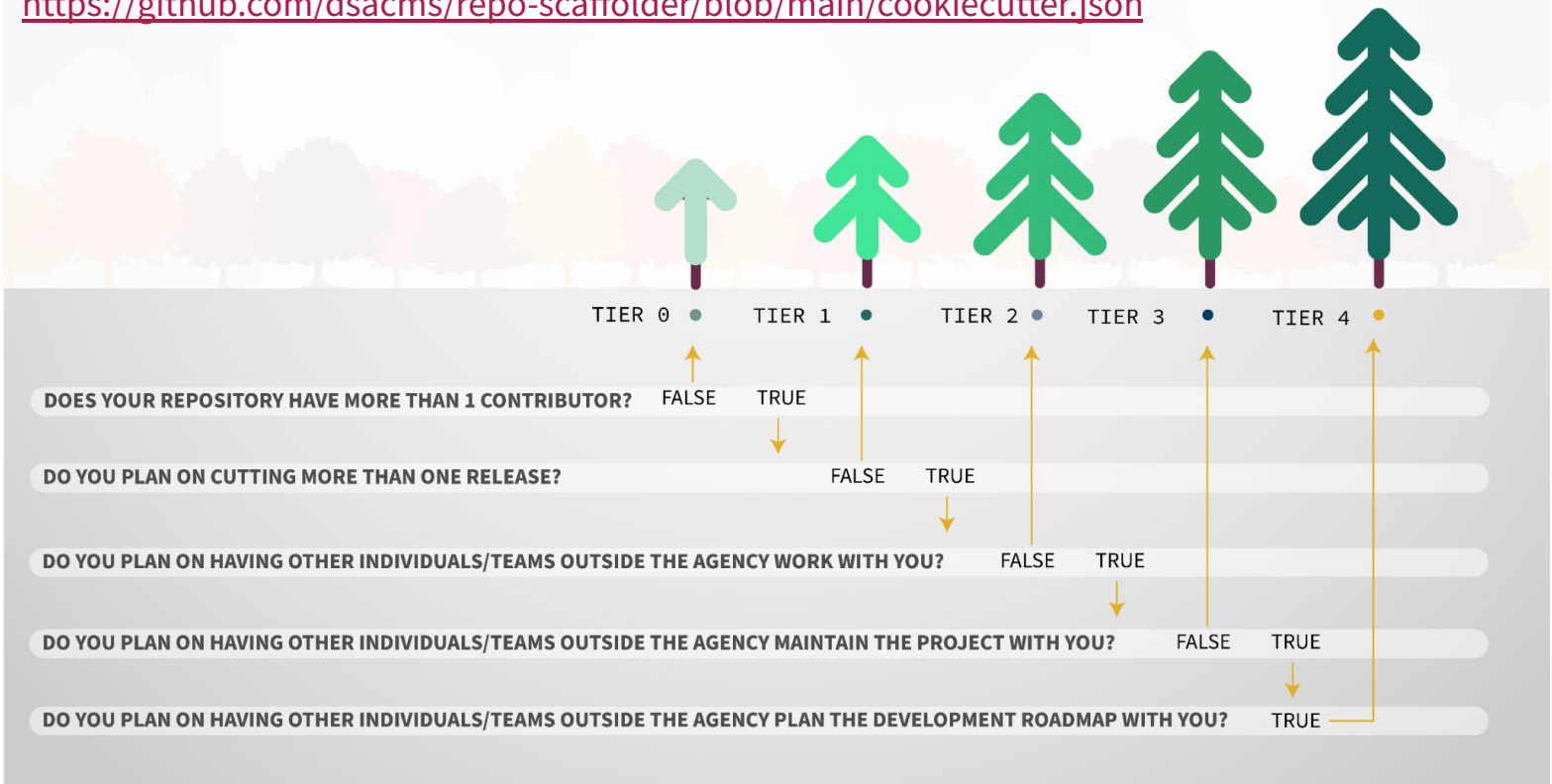
CMS Open Source Repository Maturity Model (v2)

Public Repo on GitHub!
https://github.com/dsacms/repo-scaffolder/blob/main/maturity-model-tiers.md

File	Tier 0	Tier 1	Tier 2	Tier 3	Tier 4
LICENSE	M	M	M	M	M
SECURITY.md	N	M	M	M	M
README.md	M	M	M	M	M
CONTRIBUTING.md	R	R	M	M	M
MAINTAINERS.md	N	N	R	M	M
GOVERNANCE.md	N	N	N	R	M
CODEOWNERS.md	N	N	R	M	M
COMMUNITY_GUIDELINES.md	N	N	M	M	M
CODE_OF_CONDUCT.md	N	N	M	M	M

cookiecutter command-line tool v2: Tier-selection config

https://github.com/dsacms/repo-scaffolder/blob/main/cookiecutter.json



Outbound Review Checklists

Tier1 - “One-Time Release”
https://github.com/DSACMS/repo-scaffolder/blob/main/tier1/checklist.pdf

Tier2 - “Close Collaboration”
https://github.com/DSACMS/repo-scaffolder/blob/main/tier3/checklist.pdf

Tier3 - “Working In Public”
https://github.com/DSACMS/repo-scaffolder/blob/main/tier3/checklist.pdf

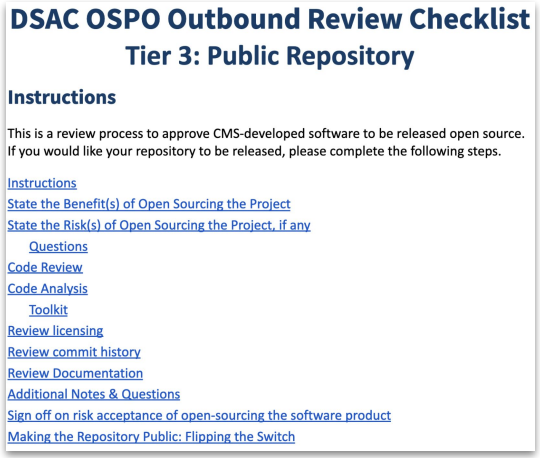
Tier4 - “Open Governance”
https://github.com/DSACMS/repo-scaffolder/blob/main/tier4/checklist.pdf

Coming Soon!

- Tier2 - “Close Collaboration”
  - innersource patterns!

https://github.com/DSACMS/decks/ossna24-baseline.pdf

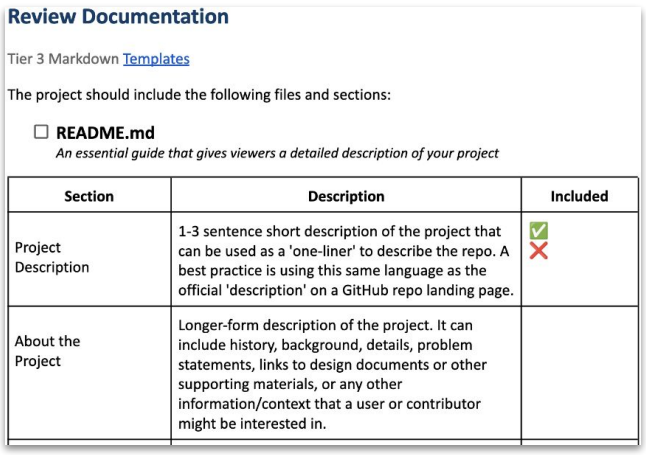
Outbound Review Checklists



DSAC OSPO Outbound Review Checklist
Tier 3: Public Repository

Instructions

This is a review process to approve CMS-developed software to be released open source. If you would like your repository to be released, please complete the following steps.



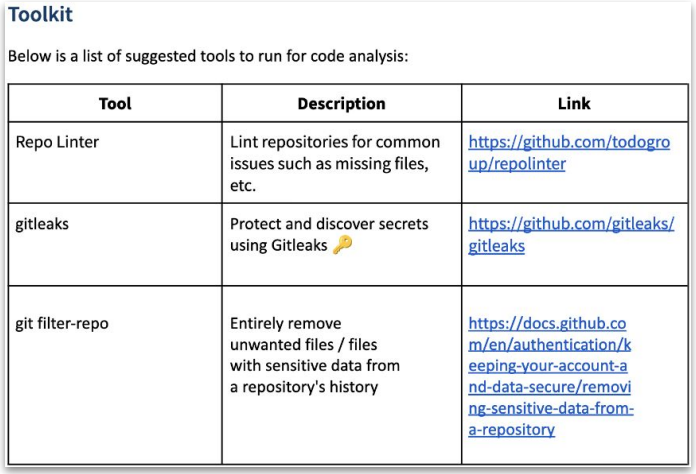
Review Documentation

Tier 3 Markdown Templates

The project should include the following files and sections:

☐ **README.md**
An essential guide that gives viewers a detailed description of your project

Section	Description	Included
Project Description	1-3 sentence short description of the project that can be used as a 'one-liner' to describe the repo. A best practice is using this same language as the official 'description' on a GitHub repo landing page.	✅ ❌
About the Project	Longer-form description of the project. It can include history, background, details, problem statements, links to design documents or other supporting materials, or any other information/context that a user or contributor might be interested in.	



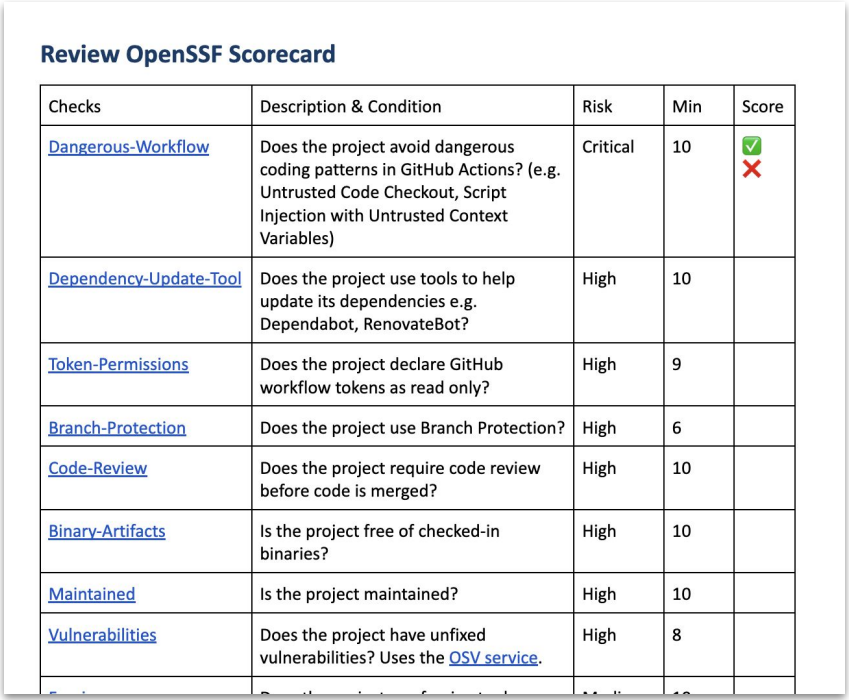
Toolkit

Below is a list of suggested tools to run for code analysis:

Tool	Description	Link
Repo Linter	Lint repositories for common issues such as missing files, etc.	https://github.com/todogroup/repolinter
gitleaks	Protect and discover secrets using Gitleaks 🔑	https://github.com/gitleaks/gitleaks
git filter-repo	Entirely remove unwanted files / files with sensitive data from a repository's history	https://docs.github.com/en/authentication/keeping-your-account-and-data-secure/removing-sensitive-data-from-a-repository

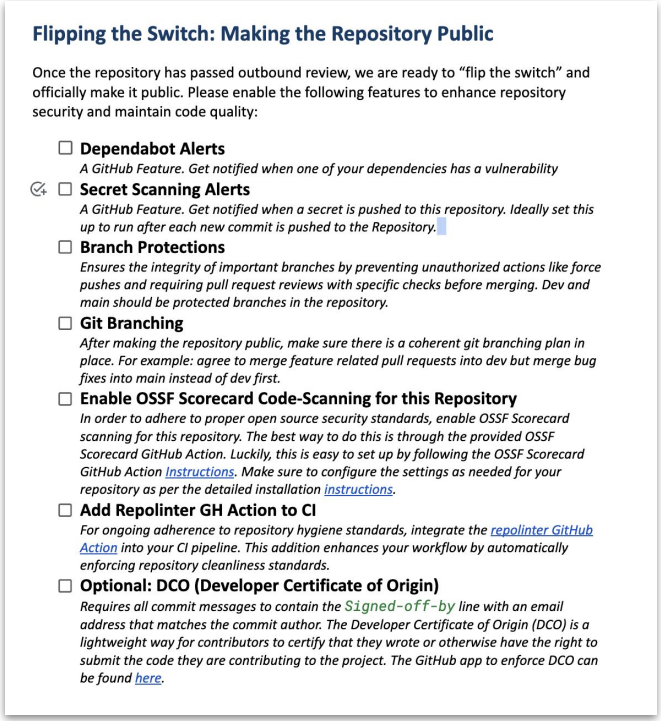
https://github.com/DSACMS/repo-scaffolder/blob/main/tier3/checklist.pdf

Tier 4: Review OpenSSF Scorecard



Review OpenSSF Scorecard

Checks	Description & Condition	Risk	Min	Score
Dangerous-Workflow	Does the project avoid dangerous coding patterns in GitHub Actions? (e.g. Untrusted Code Checkout, Script Injection with Untrusted Context Variables)	Critical	10	✅ ❌
Dependency-Update-Tool	Does the project use tools to help update its dependencies e.g. Dependabot, RenovateBot?	High	10	
Token-Permissions	Does the project declare GitHub workflow tokens as read only?	High	9	
Branch-Protection	Does the project use Branch Protection?	High	6	
Code-Review	Does the project require code review before code is merged?	High	10	
Binary-Artifacts	Is the project free of checked-in binaries?	High	10	
Maintained	Is the project maintained?	High	10	
Vulnerabilities	Does the project have unfixed vulnerabilities? Uses the OSV service.	High	8	



Flipping the Switch: Making the Repository Public

Once the repository has passed outbound review, we are ready to "flip the switch" and officially make it public. Please enable the following features to enhance repository security and maintain code quality:

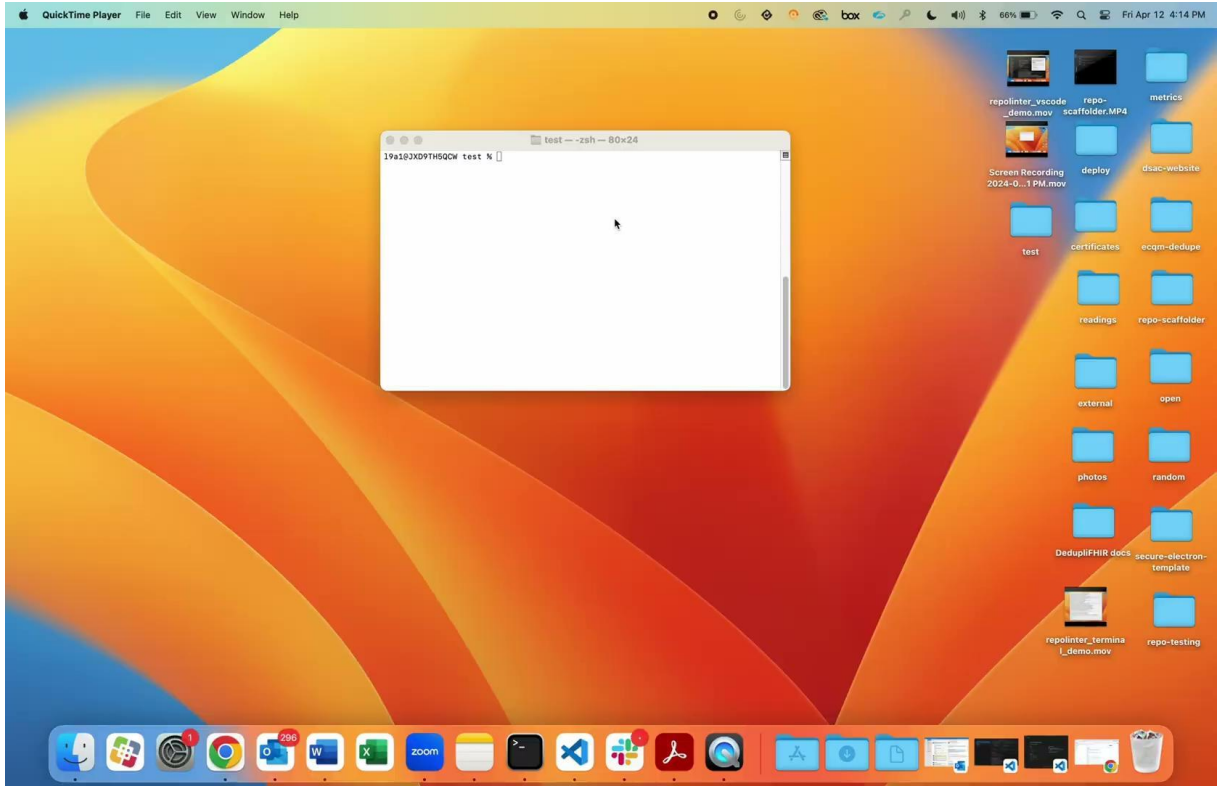
- ☐ **Dependabot Alerts**
  A GitHub Feature. Get notified when one of your dependencies has a vulnerability
- ☐ **Secret Scanning Alerts**
  A GitHub Feature. Get notified when a secret is pushed to this repository. Ideally set this up to run after each new commit is pushed to the Repository.
- ☐ **Branch Protections**
  Ensures the integrity of important branches by preventing unauthorized actions like force pushes and requiring pull request reviews with specific checks before merging. Dev and main should be protected branches in the repository.
- ☐ **Git Branching**
  After making the repository public, make sure there is a coherent git branching plan in place. For example: agree to merge feature related pull requests into dev but merge bug fixes into main instead of dev first.
- ☐ **Enable OSSF Scorecard Code-Scanning for this Repository**
  In order to adhere to proper open source security standards, enable OSSF Scorecard scanning for this repository. The best way to do this is through the provided OSSF Scorecard GitHub Action. Luckily, this is easy to set up by following the OSSF Scorecard GitHub Action Instructions. Make sure to configure the settings as needed for your repository as per the detailed installation instructions.
- ☐ **Add Repolinter GH Action to CI**
  For ongoing adherence to repository hygiene standards, integrate the repolinter GitHub Action into your CI pipeline. This addition enhances your workflow by automatically enforcing repository cleanliness standards.
- ☐ **Optional: DCO (Developer Certificate of Origin)**
  Requires all commit messages to contain the `Signed-off-by` line with an email address that matches the commit author. The Developer Certificate of Origin (DCO) is a lightweight way for contributors to certify that they wrote or otherwise have the right to submit the code they are contributing to the project. The GitHub app to enforce DCO can be found here.

https://github.com/DSACMS/repo-scaffolder/blob/main/tier4/checklist.pdf

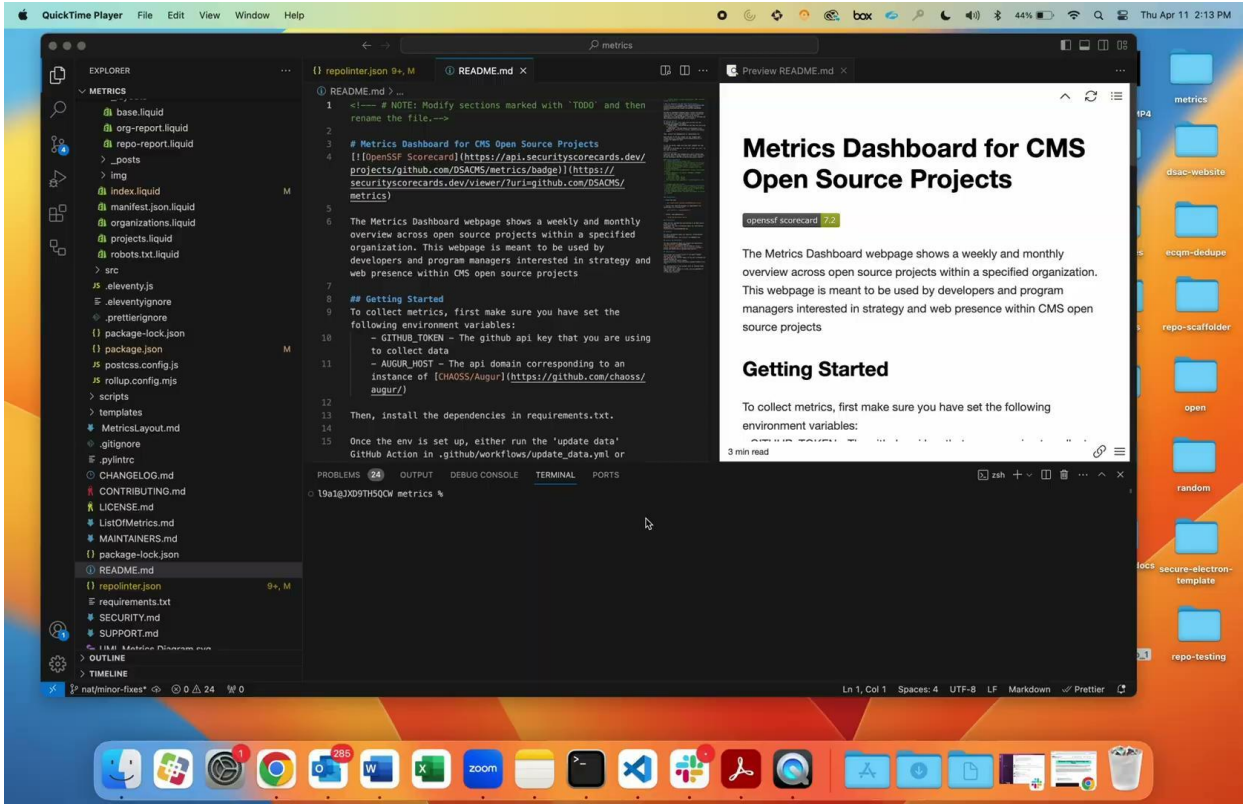
https://github.com/DSACMS/decks/ossna24-baseline.pdf

repo-scaffolder: Determining Tier

repo-scaffolder: Creating a Repository

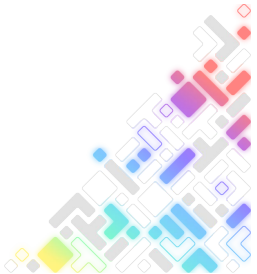


repolinter: running Tier 3 repolinter.json



CMS.gov Open Source Repository Metrics

https://dsacms.github.io/metrics/



Interested in learning more?
Come to our talks at OSPOcon tomorrow!

Repository Cohorts: How OSPOs Can Programmatically Categorize All Their Repositories with Microsoft OSPO
Thursday 11:00-11:40 @ Level 4 Room 447-448

Establishing a Baseline:
Repository Maturity Models, Templates, Checklists & Metrics
Thursday 4:10-5:00 @ Level 4 Room 447-448

Big shoutout to CHAOSS.community, TODOgroup.org, USDigitalResponse.org, digitalcorps.gsa.gov!!! We are hiring for 2025 fellows!

THE LINUX FOUNDATION

OPEN SOURCE SUMMIT

NORTH AMERICA