DIGITAL SERVICE AT CMS

Establishing the first Open Source Program Office (OSPO) at a United States Federal Agency

Remy DeCausemaker, Open Source Lead, Digital Service at CMS.gov

Centers for Medicare & Medicaid Services// DEFCON // August 2024

https://github.com/DSACMS/decks/blob/main/defcon2024.pdf
opensource@cms.hhs.gov

Open Source Program Office (OSPO) at CMS

1. About CMS and Our OSPO
2. How we reduce duplicate work
3. How we reduce risk
4. Why this is important
5. How you can help

DIGITAL SERVICE AT CMS

What does the Digital Service at CMS do?

We work to transform the U.S. healthcare system by:

Improving the design of healthcare experiences

Delivering value to the government, healthcare providers, and patients

Modernizing systems

Participating in policy development

 https://github.com/DSACMS/decks/blob/main/defcon2024.pdf

How do we do it?

By hiring great talent!

We deploy **small groups** of designers, engineers, and product managers on a "tour of duty" to work alongside **dedicated civil servants**.

These **multidisciplinary teams** bring best practices and new approaches to support government **modernization** efforts.

Who we serve: The American People

65 M

Medicare Beneficiaries

(2022)

88 M

Medicaid Beneficiaries

(2022)

31 M

Healthcare.gov

(2021)

https://data.cms.gov/fact-sheet/cms-fast-facts
https://www.cms.gov/files/document/2022-medicare-trustees-report.pdf

Who we serve: Taxpayers

$ 1.7 T

CMS Budget - 12% of the federal budget

(FY 2022)

$ 829 B

Total Medicare Payments

(FY 2021)

$ 646 B

Total Medicaid Payments

(FY 2019)

https://data.cms.gov/fact-sheet/cms-fast-facts
https://www.cms.gov/files/document/2022-medicare-trustees-report.pdf

Who we serve: The Health Care System

6,244

CMS Employees

(FY 2022)

1.4M

Health Care Providers

(2022)

20%

National Health Care Spending is Medicare

(2022)

https://data.cms.gov/fact-sheet/cms-fast-facts
https://www.cms.gov/files/document/2022-medicare-trustees-report.pdf

How do we do Open Source at CMS?

Policies

How we **inbound** and **outbound** open source contributions and content

Projects

How we **solve real-world problems** by working in the open

Programs

How we **measure**, and **manage** contributors, projects, **risks**, and **opportunities**

CMS Open Source Program Office (OSPO) Functional Statement:

*"Establishes and maintains guidance, policies, practices, and talent pipelines that **advance equity**, **build trust**, and **amplify impact** across CMS, HHS, and Federal Open Source Ecosystems by working and sharing openly."*

Biden-Harris Administration Releases End of Year Report on Open-Source Software Security Initiative

AUGUST 09, 2024

Fact Sheet: Biden-Harris Administration Releases End of Year Report on Open-Source Software Security Initiative

ONCD › BRIEFING ROOM › PRESS RELEASE

August 9, 2024

Read the full report here

Today, the White House Office of the National Cyber Director, in partnership with members of the Open-Source Software Security Initiative (OS3I), is publishing a summary report on the *Request for Information (RFI)*: *Open-Source Software Security: Areas of Long-Term Focus and Prioritization*. This builds on the commitment the Administration made in the National Cybersecurity Strategy, "to invest in the development of secure software, including memory-safe languages and software development techniques, frameworks, and testing tools."

★ ★ ★ ★ ★ ★

6. **Establish the First U.S. Government OSPO:** The Department of Health and Human Services (HHS) Center for Medicaid and Medicare Services (CMS) recently established the first Open-Source Program Office at a United States Federal Agency.[xl] The function of the OSPO is to establish and maintain guidance, policies, practices, and talent pipelines that advance equity, build trust, and amplify impact across CMS, HHS, and Federal Government's open-source ecosystem by working and sharing openly.

https://www.whitehouse.gov/oncd/briefing-room/2024/08/09/fact-sheet-biden-harris-administration-releases-end-of-year-report-on-open-source-software-security-initiative-2/

“Risks” (aka Myths) of Open Source

Open source is ~~less~~ more secure.

"**Many eyes make any bug shallow**." The more people looking at a project, the faster we'll be able to identify problems and create solutions.

Open source is ~~bad~~ good for for-profit businesses.

By **lowering barriers to entry and costs of acquisition**, developers are given access to world-class industry leading tools and infrastructure used at the largest enterprises today.

~~Open Source means all data must be public.~~ Open Source means SOME data CAN be public.

Open source is not a binary, it is a spectrum, and there are layers to the stack. Being intentional about what we cannot share for privacy and security purposes, helps us determine what we can share more effectively.

Open by Default is something we ~~do not~~ already do in Federal Government.

According to **Title 17 U.S. Code § 101 and § 105**, "Copyright protection under this title is not available for any work of the United States Government" meaning, "work prepared by an officer or employee of the United States Government as part of that persons official duties.”[1][2]

https://www.law.cornell.edu/uscode/text/17
https://www.law.cornell.edu/uscode/text/17/105

What are the *actual* Risks in Open Source?

Overdifferentiation

- Unnecessarily duplicating work
- Unnecessarily dividing your resources

Examples

- “Not Invented Here Syndrome”

Proliferation

- Unnecessarily duplicating communities and projects
- Unnecessarily dividing your addressable market

Examples

- License Proliferation
- Event/Conference Proliferation

Fragmentation

- Unnecessarily dividing your community of contributors

Examples

- Hostile Forks
- Internal Forks

How does our OSPO provide value to the Agency?

Save us Money

Save us Time

Accountability for Contract Performance

Engine for Talent

Reduce Duplicate Work

Reduce Duplicate Costs

Reduce Security Risk

Reduce Continuity Risk

 https://github.com/DSACMS/decks/blob/main/defcon2024.pdf

How we reduce duplicate work

Repository Maturity Models & Cookiecutter Configs

DIGITAL SERVICE AT CMS

CMS Repository Cohort Definitions: Maturity Model Tiers

Level	Name	Purpose	Description
Tier 0	**Private Repository**	Experimental, Historical	Project is **private**, usually with a single developer. Typically **working projects**, example code, and **early prototypes**.
Tier 1	**One-Time Release**	Publication for Informational, Accountability, Transparency Purposes	Project released publicly, but ***without planned future activity*** or maintenance from original author(s).
Tier 2	**Close Collaboration**	Collaboration with smaller, mostly internal teams	Project within a team or Operational Division (OpDiv), Internal Repo for ***Innersource-style work.***
Tier 3	**Working in Public**	Collaboration in the open with smaller, semi-open teams	Project developed Open Source by CMS or a CMS contractor, public website hosted on GitHub, tool or utility used in CMS official business by the public. ***Limited external contribution, CMS-led (by choice or by statute).***
Tier 4	**Community Governance**	Collaboration broadly in public	Project donated to or stewarded by an external community, open standard that welcomes public input, mature open source project that purposefully develops an ***open governance structure***.

 https://github.com/DSACMS/decks/blob/main/defcon2024.pdf

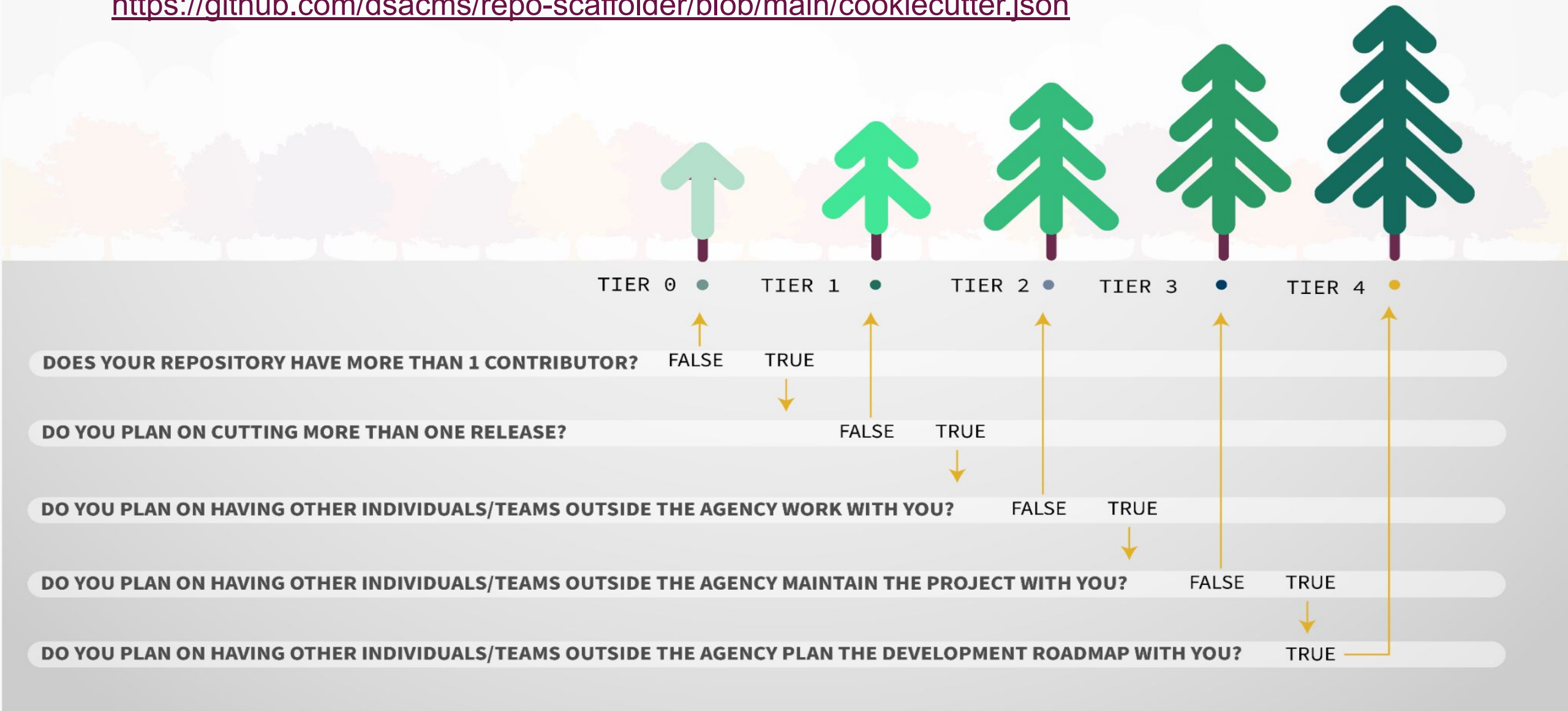
CMS Open Source Repository Maturity Model (v2)

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

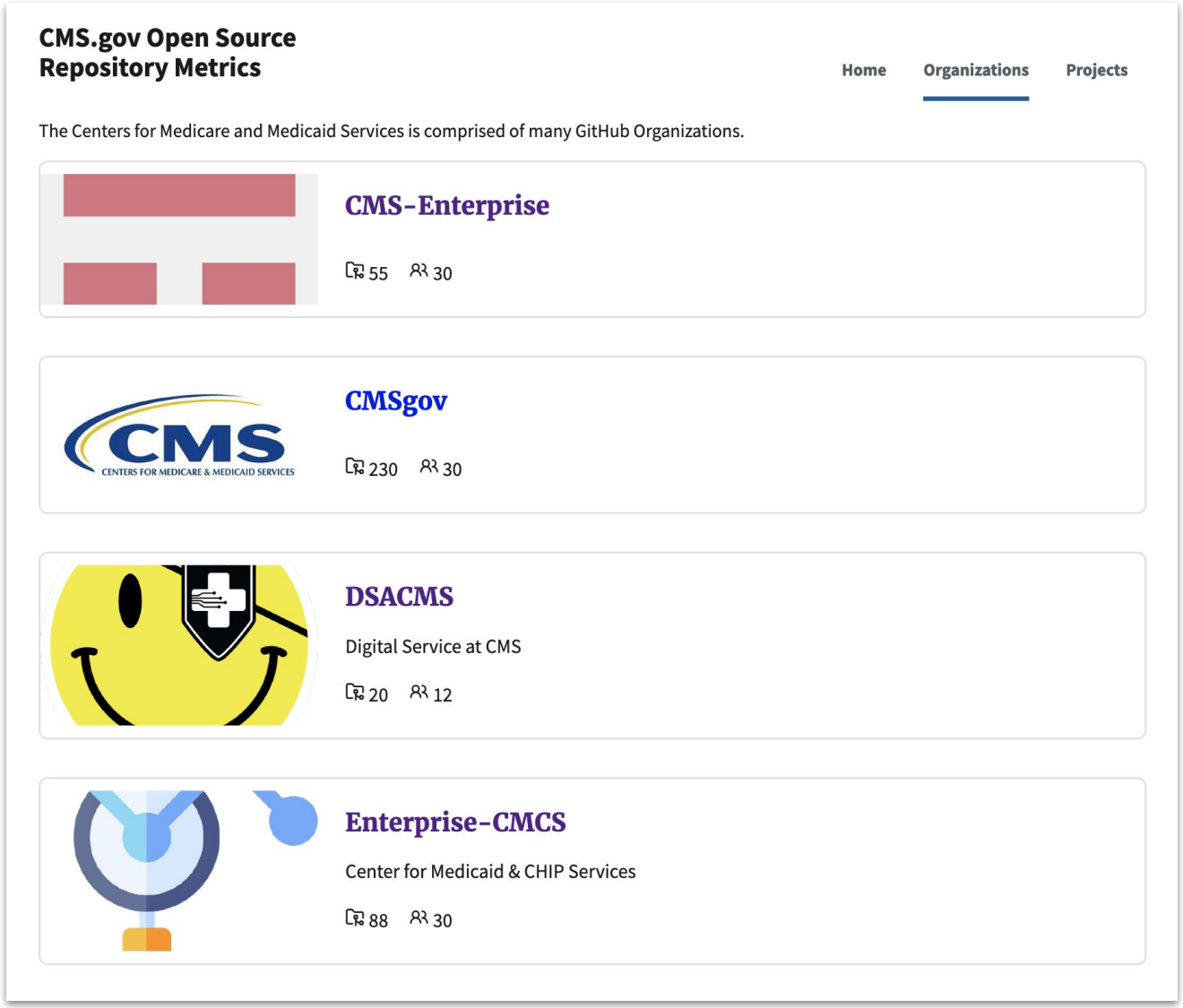


How we reduce risk

Outbound Repository Checklists, Metrics, and Linters

DIGITAL SERVICE AT CMS

CMS.gov Open Source Repository Metrics Front-end



Report for metrics

project type midsize

Repo Stats

Stars	Forks	Issues	Watchers	Pull Requests
5	2	17	3	113

Summary Table

Metric	Latest	Previous	Diff	% Diff
Commits	568	538	30	5.4%
Issues	17	15	2	12%
Open Issues	7	6	1	15%
Closed Issues	10	9	1	11%
Open Pull Requests	11	9	2	20%
Merged Pull Requests	95	87	8	8.8%
Closed Pull Requests	7	7	0	0%
Forks	2	2	0	0%
Stars	5	5	0	0%
Watchers	3	3	0	0%

https://dsacms.github.io/metrics

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/tier2/checklist.pdf

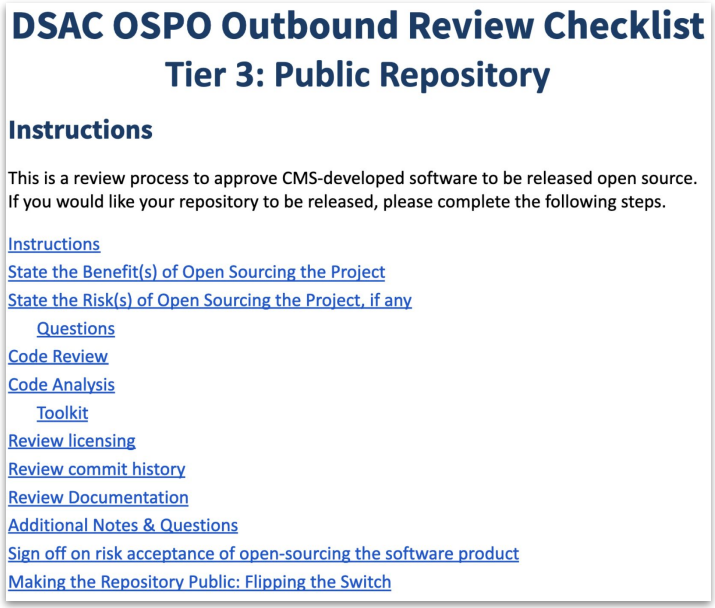
Tier3 - Working In Public

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

Outbound Review Checklists: Tiers 1-4

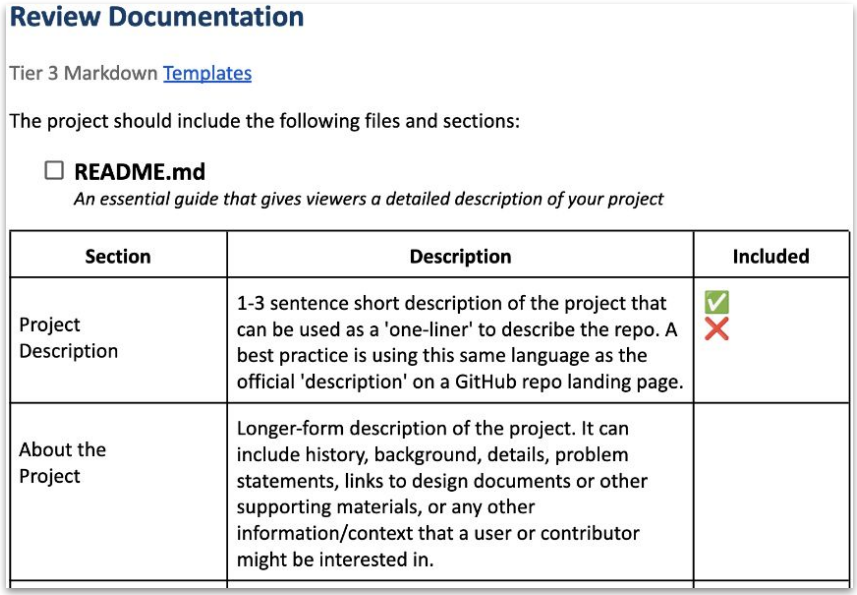


DSAC OSPO Outbound Review Checklist
Tier 3: Public Repository

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.

Instructions
State the Benefit(s) of Open Sourcing the Project
State the Risk(s) of Open Sourcing the Project, if any
  Questions
Code Review
Code Analysis
  Toolkit
Review licensing
Review commit history
Review Documentation
Additional Notes & Questions
Sign off on risk acceptance of open-sourcing the software product
Making the Repository Public: Flipping the Switch



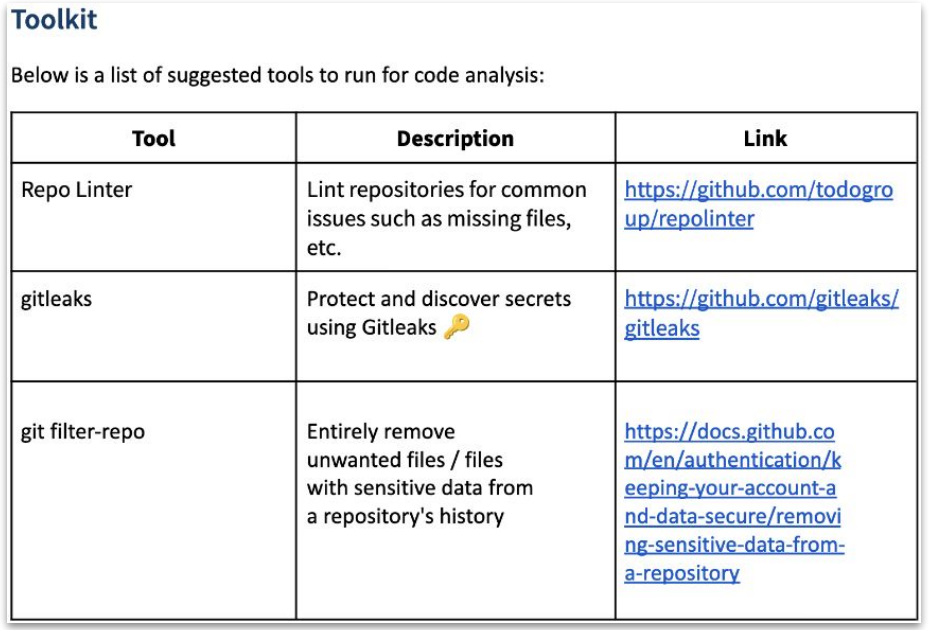
Review Documentation

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.	



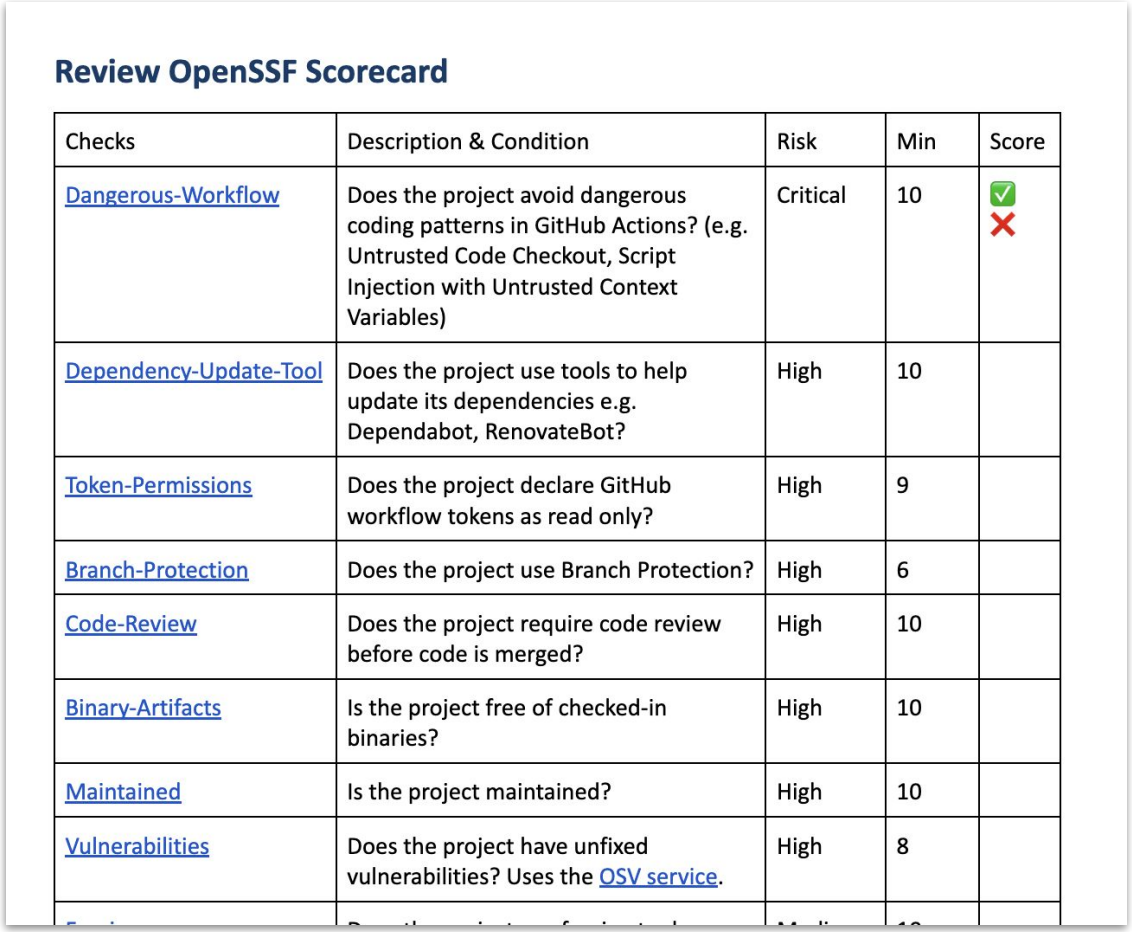
Toolkit

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

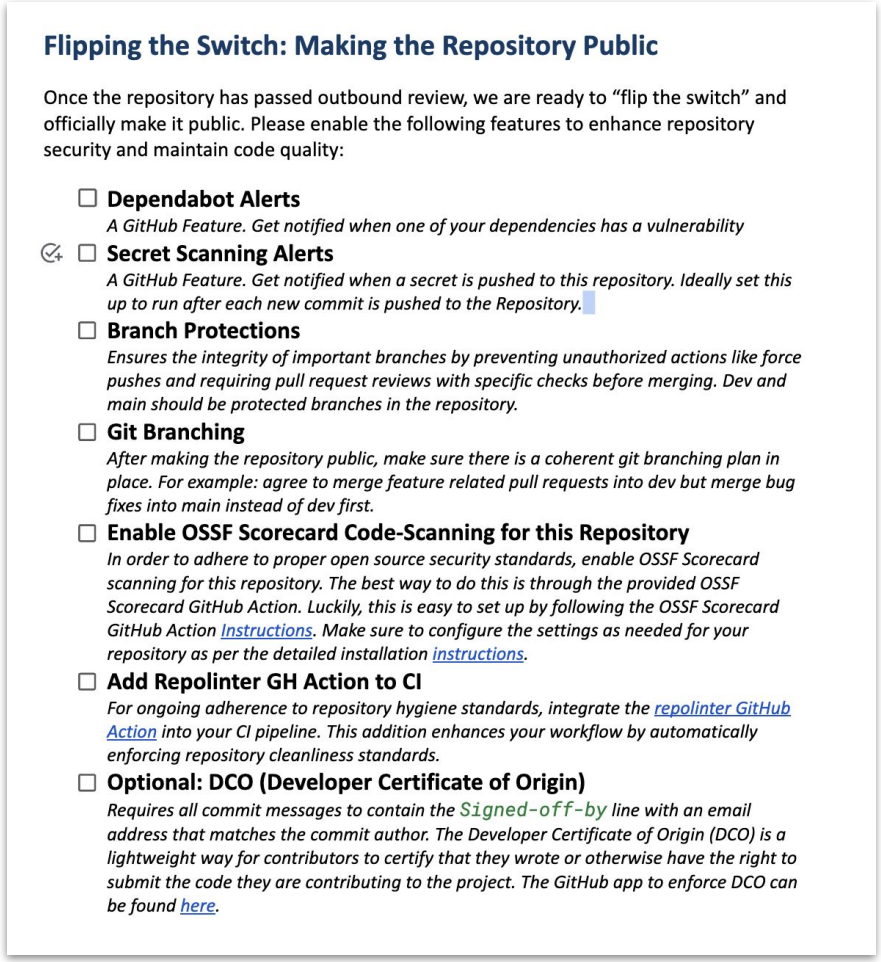
https://github.com/DSACMS/repo-scaffolder/blob/main/tier3/checklist.pdf

Tier 4: Reviewing 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

CMS Open Source Repo Metrics Back-end

STEP 1

Fetch Metrics

Check the project-stracked.json file

STEP 2

Fetch Metrics

For each $repo in each $ORG in projectstracked.-json

- Fetch Metrics From Augur
- Fetch Metrics From Github

For each $ORG in projectstracked.json

- Fetch Org Metrics From Augur
- Fetch Org Metrics From Github

STEP 3

Generate Elements & Assemble Report

For each $REPO in each $ORG in projectstracked.json

- Generate Weekly Metrics Repo Tables
- Generate Repo reports (markdown)
- Generate Repo Graphics (pygals)

For each $ORG in projectstracked.json

- Aggregate Weekly Metrics Org Table
- Generate Org reports (markdown)
- Generate Org Graphics (pygals)

STEP 4

Generate front-end (Liquid)

STEP 5

Publish Static Generated Front End (GitHub)

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

Repo: https://github.com/DSAMCS/metrics

CMS Open Source Repository Maturity Model: Repolinter

https://github.com/todogroup/repolinter

Repolinter is a tool maintained by the TODOGroup for checking repositories for common open source issues, using pre-defined rulesets. This can be run stand-alone as a script, pre-commit in your IDE, or post-commit or within CI/CD systems!

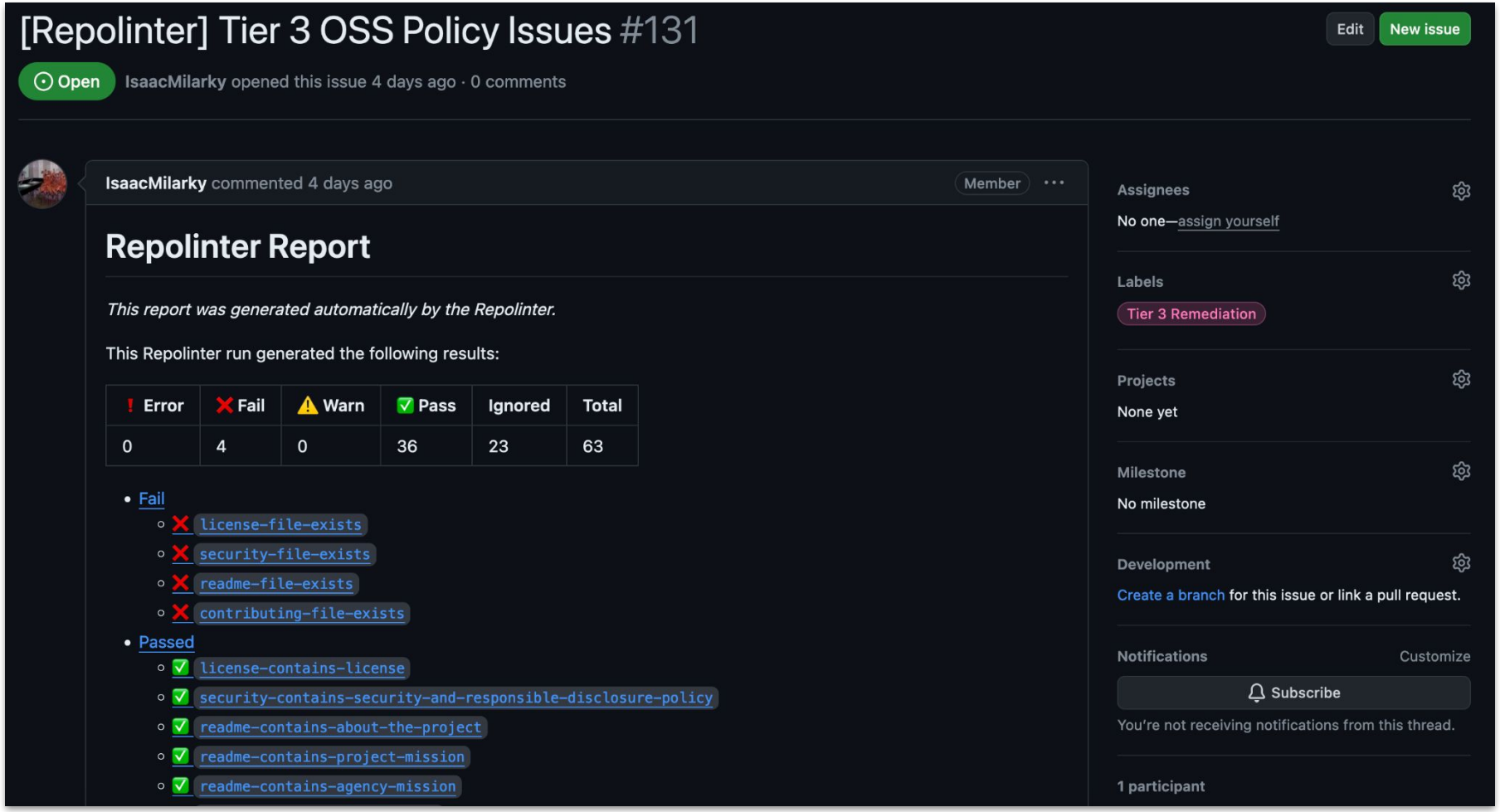
✔ = Pass
✖ = Fail
⚠️ = Warn

Thanks to Chan and Satwic at the Comcast OSPO, we now have repolinter.json configs and rules that map to each Tier of our Open Source Repository Maturity Model!

```
✔ license-file-exists: Found file (LICENSE.md)
✔ security-file-exists: Found file (SECURITY.md)
✔ readme-file-exists: Found file (README.md)
✔ contributing-file-exists: Found file (CONTRIBUTING.md)
✔ maintainers-file-exists: Found file (MAINTAINERS.md)
✖ codeowners-file-exists: Did not find a file matching th
⚠ governance-file-exists: Did not find a file matching th
✖ community-guidelines-file-exists: Did not find a file m
✖ code-of-conduct-file-exists: Did not find a file matchi
✔ license-contains-license: Contains license (LICENSE.md)
✔ security-contains-security-and-responsible-disclosure-p
✖ readme-contains-about-the-project: Doesn't contain Abou
```

https://github.com/DSACMS/repo-scaffolder/blob/main/tier3/%7B%7Bcookiecutter.project_slug%7D%7D/repolinter.json

CMS Open Source Repository Maturity Model: Repolinter



[Repolinter] Tier 3 OSS Policy Issues #131

Edit | New issue

Open | IsaacMilarky opened this issue 4 days ago · 0 comments

IsaacMilarky commented 4 days ago — Member

Repolinter Report

This report was generated automatically by the Repolinter.

This Repolinter run generated the following results:

! Error	❌ Fail	⚠️ Warn	✅ Pass	Ignored	Total
0	4	0	36	23	63

- Fail
  - ❌ `license-file-exists`
  - ❌ `security-file-exists`
  - ❌ `readme-file-exists`
  - ❌ `contributing-file-exists`
- Passed
  - ✅ `license-contains-license`
  - ✅ `security-contains-security-and-responsible-disclosure-policy`
  - ✅ `readme-contains-about-the-project`
  - ✅ `readme-contains-project-mission`
  - ✅ `readme-contains-agency-mission`

Assignees: No one—assign yourself

Labels: Tier 3 Remediation

Projects: None yet

Milestone: No milestone

Development: Create a branch for this issue or link a pull request.

Notifications: Customize — Subscribe — You're not receiving notifications from this thread.

1 participant

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**

Why this is important

Open Source Health and Software Supply Chain Security

DIGITAL SERVICE AT CMS

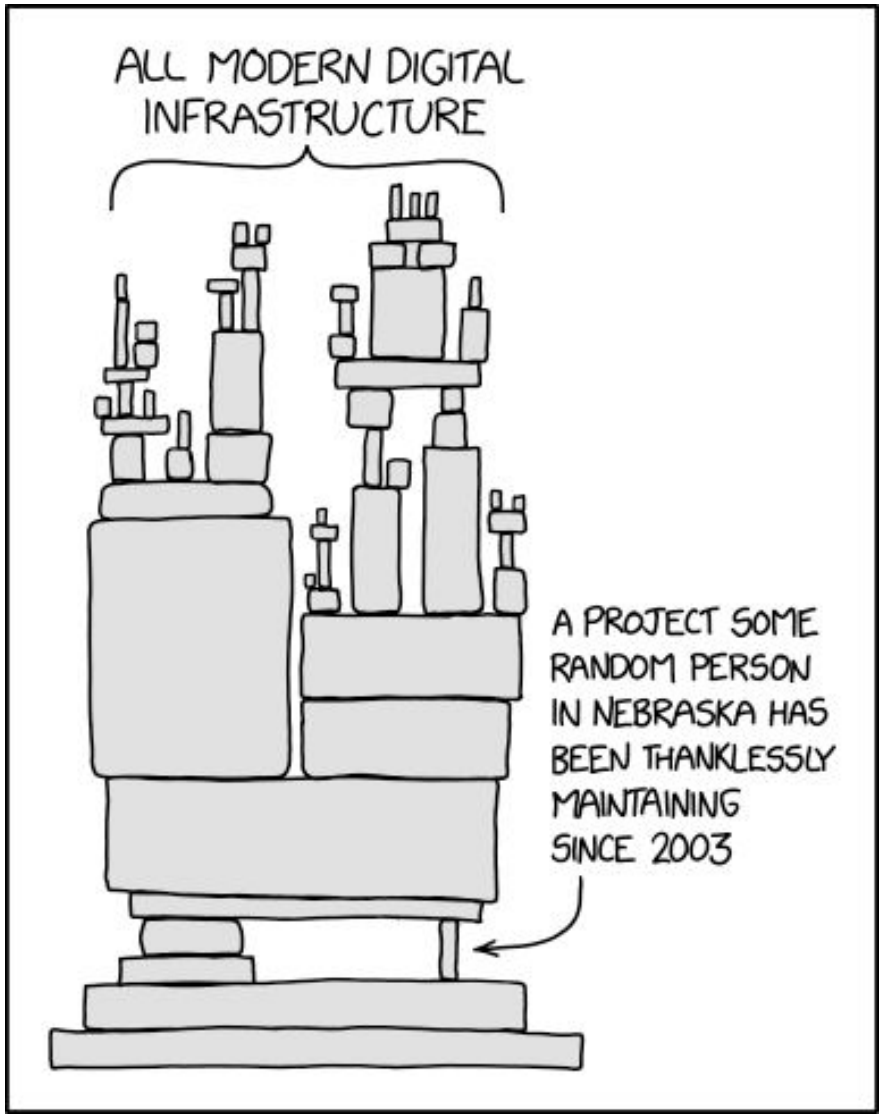
The OSS Supply Chain and XZ

Thanks to XKCD, Open Source software supply chain vulnerabilities like those seen in the recent XZ vulnerability are being referred to as a "Nebraska problems" or, when a component of software that is critical to much of the world is inadequately funded, maintained, or staffed.

Stakeholders must pay attention to the critical projects that they depend on, and support programs that fund, hire, and train maintainers.

CISA writes on their blog that *"every technology manufacturer that profits from open source software must do their part by being responsible consumers of and sustainable contributors to the open source packages they depend on."*

See: https://github.com/DSACMS/ospo-guide/blob/main/resources/XZ_Supply_chain_attack.md



https://xkcd.com/2347

How you can help

Early Career Talent Pipeline, Vulnerability Disclosure Programs, Bugbounties, and Contributions

DIGITAL SERVICE AT CMS

Early Career Talent Pipeline at the Digital Service

Digital Service at CMS.gov DIGITAL SERVICE AT CMS	**Up to 4 year tour of duty** for established professionals in **Engineering, Product management, Design, and Data science**. GS-13+	https://cms.gov/digital-service-cms
DigitalCorps at GSA.gov UNITED STATES DIGITAL CORPS	**2 year tour of duty** for **early-career** technologists, eligible to convert to full-time, career positions in the competitive service at their agency. GS-9 to 12, + **50% recruitment Incentive**.	https://digitalcorps.gsa.gov
Civic Digital Fellowship at CodingItForward.com CIVIC DIGITAL FELLOWSHIP	**Paid 10 week summer internship** program for **currently enrolled** undergrad, grad, bootcamp students **or recent graduates**.	https://www.codingitforward.com
Urban Alliance URBAN ALLIANCE	**6 month part-time to full-time Program** that provides skills training, mentoring, and **paid internships** to high school seniors that keep them connected to school or the workforce.	https://urbanalliance.org

Acknowledgements & Attributions

Our repository hygiene and baseslines work began as a collaboration between the United States Digital Service (USDS.gov), The Department of Health and Human Services (HHS.gov), The Digital Service at the Centers for Medicare & Medicaid Services (CMS.gov), and USDigitalResponse.org.

CMS would like to thank General Services Administration (GSA)'s 18F team, the Consumer Financial Protection Bureau (CFPB), and the Office of Management and Budget (OMB) and the Cybersecurity and Infrastructure Security Agency (CISA) for their inspirational work in the use of Free/Open Source Software in the Federal Government.

Our work continues to be guided by contributions from the CHAOSS OSPO Metrics Working Group and TODOGroup.org members.

And Thank you to all the Open Source contributors sending PRs, filing issues, and advocating for this important work across the Ecosystem!

#HackThePlanet

Questions or Comments?

https://cms.gov/digital-service/open-source-program-office

https://github.com/DSACMS/decks/blob/main/defcon2024.pdf

Open Source Questions?
opensource@cms.hhs.gov

Digital Service Questions?
DigitalService@cms.hhs.gov

Help Answer the Call!

Digital Service at CMS.gov
https://cms.gov/digital-service

DigitalCorps Fellowships
https://digitalcorps.gsa.gov

CodingItForward Summer Internships
https://codingitforward.com