

Sandia's Open-Source Process

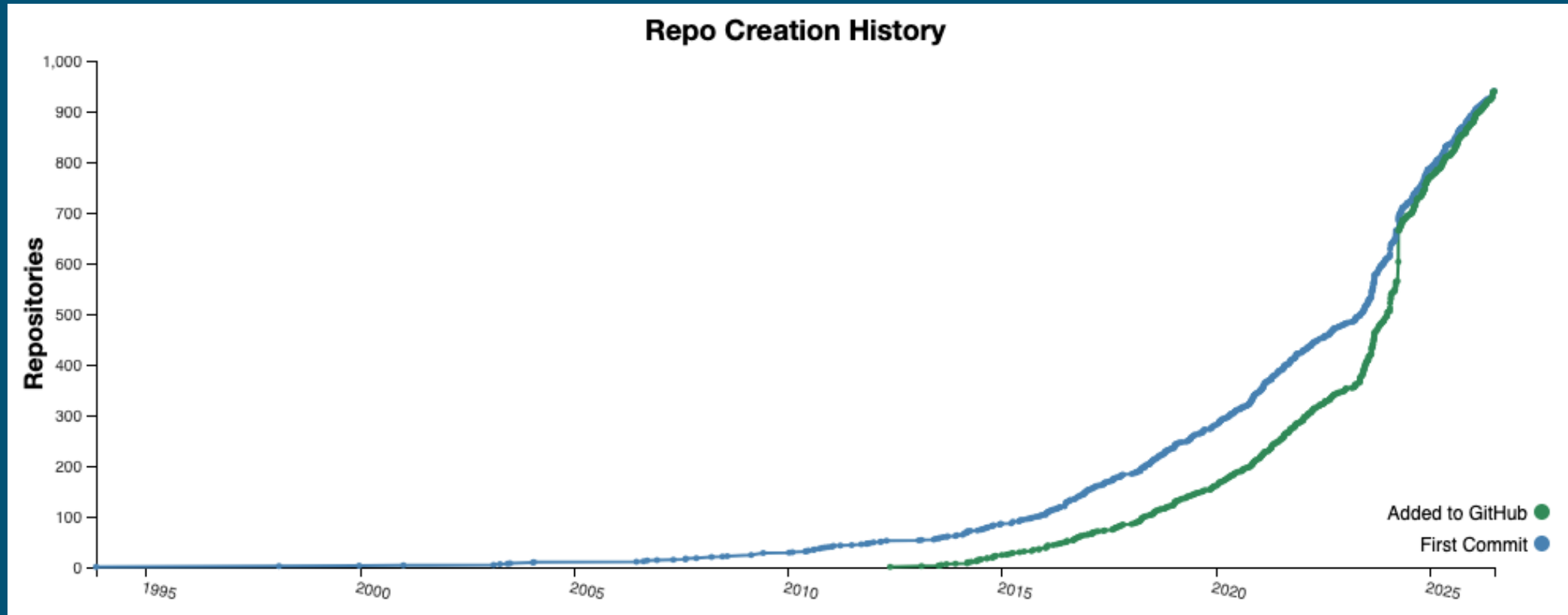
Jason M. Gates

PVPMC OSS Summit — August 4, 2026

Sandia's OSS Footprint

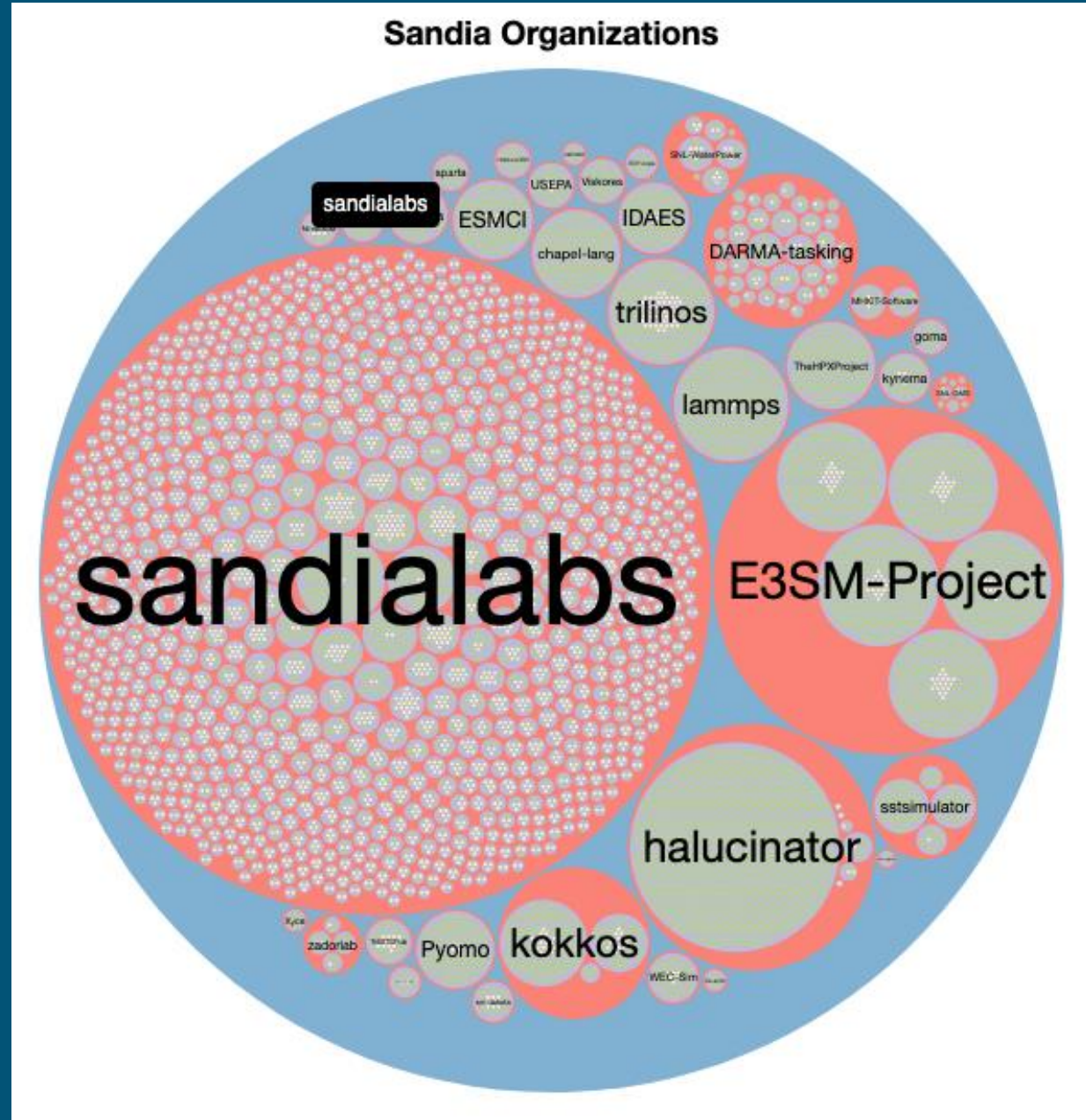


- software.sandia.gov
- 940 open-source repositories



Sandia's OSS Footprint

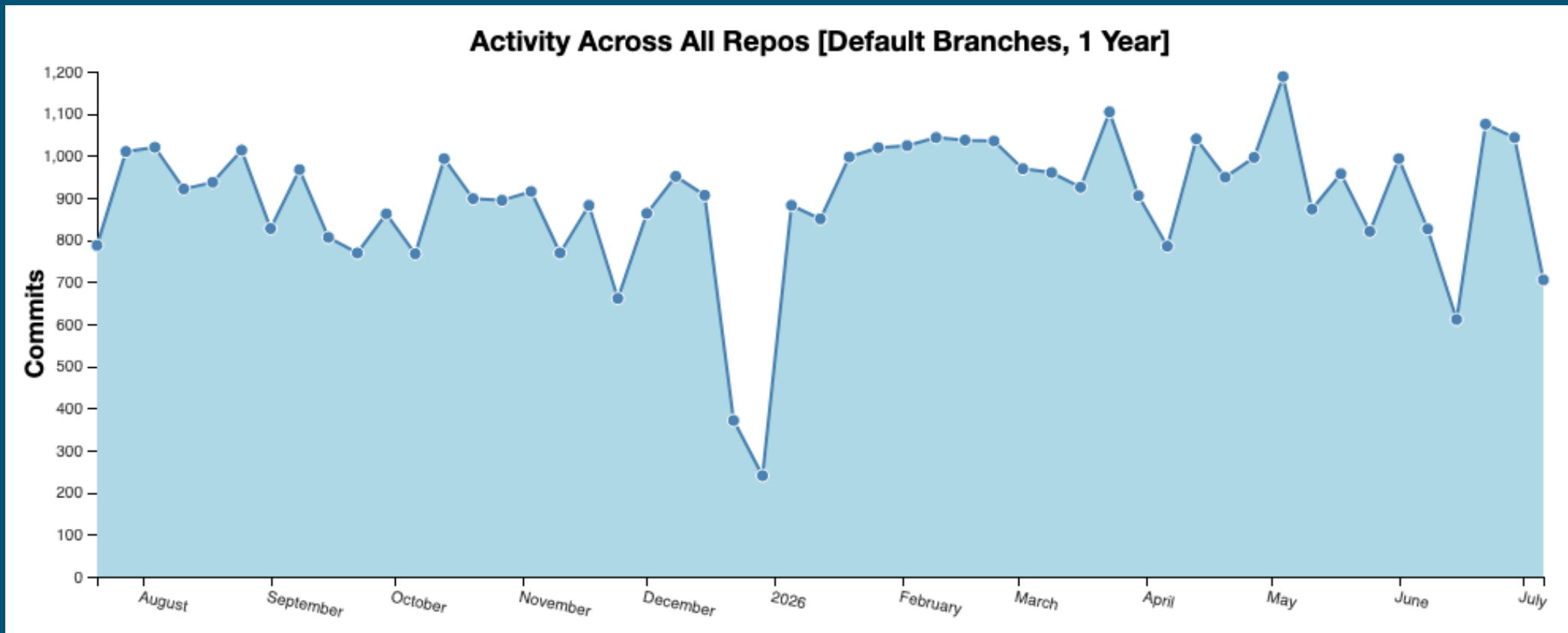
- software.sandia.gov
- Dozens of organizations

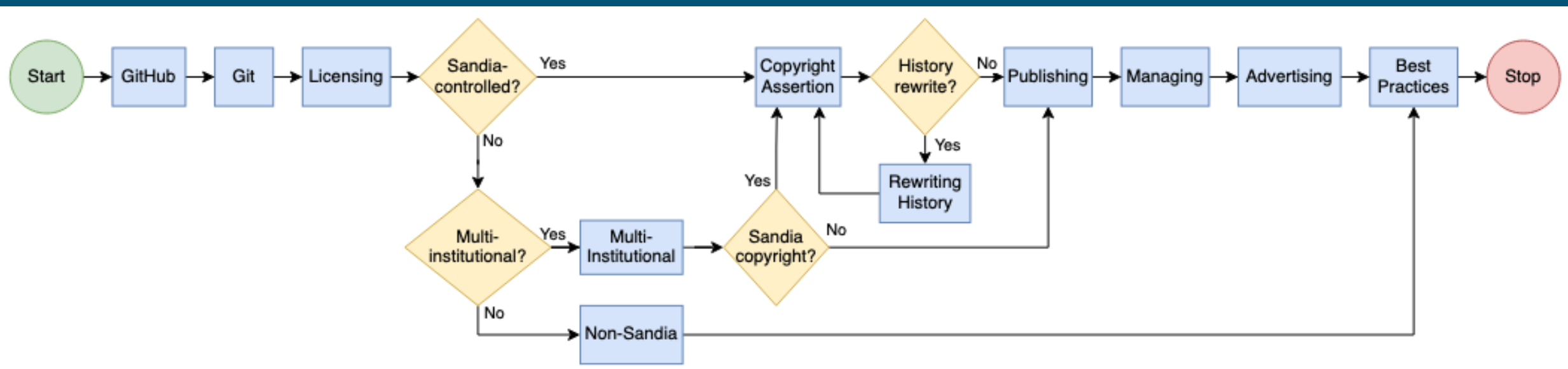


Sandia's OSS Footprint



- software.sandia.gov
- ~1K commits/week







Managing Access to Your Repository:

- Familiarize yourself with GitHub's documentation for how to [manage teams and people with access to your repository](#) and the [permissions associated with each role](#).
- Protect the main development branch of the repository by requiring a Pull Request (PR) with at least one approval before merging. See GitHub's documentation on [protected branches](#) and [managing branch protection rules](#) for details.
 - Due to a confusing quirk with GitHub permissions, individuals without **Write** access will still be able to approve PRs, but the PR cannot be merged until it's been approved by someone with **Write** access.
- Instruct all your collaborators to use a [fork, branch, and PR workflow](#).



For Sandia-Controlled OSS:

- Ensure that only Members of the [sandialabs organization](#) (who must be Sandian) have **Write** access or above. Any Outside Collaborator (non-Sandians) must be limited to **Triage** or **Read** role/access.
- Temporary Sandians may be an **Admin** on a repo only if a regular Sandian is also **Admin**.
- Student interns and contractors should not be granted **Admin** access to a repo.
 - Student Interns and Contractors may have the **Maintain** role, and often this is all that's needed to handle the day-to-day running of a project, but you'll still need someone on the team as an **Admin**. See the GitHub documentation for [the permissions for the different roles](#).



For Multi-Institutional OSS:

- [Use teams](#) to organize your project membership.
- Consider creating teams for the following:

Purpose	Contains	Permissions	Organization Members
Team leads	At least one lead from each institution	Admin	✓
Core developers	Team members from any institution making regular contributions	Write	✓
Outside collaborators	Those who frequently interact with the project in ways other than direct contributions	Triage	✗

- Anyone, including those not included in the teams above, can submit changes via the [fork, branch, and PR workflow](#).



Retiring OSS:

- If, at some point, your open-source repository will no longer be maintained, indicate to prospective users that this is the case:
 - Update the README.md file in the repository root to indicate the change in status.
 - [Archive the repository.](#)



Documentation:

- Create community health files
 - [Starting an Open-Source Project](#)
 - [Your Code of Conduct](#)
 - [How to Contribute to Open Source](#)
 - [Building Welcoming Communities](#)
 - [Customizing Your Repository](#)
 - [Building Communities](#)
 - [Adding a Security Policy to Your Repository](#)
 - [Security Guidelines for New Projects](#)
 - [Guidelines for open-source software development](#)
- Register with the OpenSSF [Best Practices Badge Program](#)
- Add copyright and license information to source files (see [SPDX Tutorial](#))
- Include [all four types of documentation](#)



Collaboration:

- Adopt [Conventional Commits](#)
- Adopt [Conventional Comments](#)



Continuous Integration:

- Secure your GitHub Actions with [StepSecurity](#)
- Use [pre-commit](#) and [pre-commit.ci](#)
- Automatically format your code
- Use linting tools
- Scan for security vulnerabilities (e.g., [CodeQL](#), [CodeFactor](#), etc.)
- [Scan for secrets](#) added to the repository
- Run automated testing
- Automate releases (e.g., [Semantic Release](#))
- Automatically assess your open-source practices with the OpenSSF [Scorecard](#)



Template Repositories:

- At a high level, the files themselves are **strongly recommended**
- The details within the files are **suggestions**
- Both generic and Python-specific templates available

Sandia Open-Source Software | Python Templates

This repository contains Python-specific template files to serve as guidelines for Sandians working through [our open-sourcing process](#). They are meant to be used in place of the generic templates found in [sandia-open-source-software/general-templates](#).

The following templated supplementary files can be found in the [templates](#) directory:

- [README](#)
- [Code of conduct](#)
- [Contributing guidelines](#)
- [Security guidelines](#)
- [Issue templates](#)
- [Pull request template](#)
- [License](#) and [Copyright](#)

Additionally, there are some files to help with automating adherence to your policies:

- [Pre-Commit configuration](#)
- [GitHub Actions workflows](#)
- [Python project configuration](#)
- [ReadTheDocs configuration](#)
- [Test coverage configuration](#)
- [Python Semantic Release templates](#)

The `templates` directory also contains a bare-bones [package](#), along with sample [documentation](#), [examples](#), and [unit tests](#), to give you an idea of how to set up each.

Monitoring



Daily Monitoring

- ✗ [3 members of `sandialabs` are not Sandians](#)
- ✗ [The `outside\\_collaborators.csv` file in the repository is outdated](#)
- ✗ [The `sandians.csv` in the repository is outdated](#)

Weekly Monitoring

- ✗ [29 repositories have one or more administrators who are not US citizen Sandia regular employees](#)
- ✓ [No repositories have outside collaborators with elevated permissions](#)
- ✗ [3 repositories are missing a SCR#](#)

Monthly Monitoring

- ✗ [549 repositories are missing SNL topics](#)
- ✗ [5 repositories are private](#)

Monitoring



Daily Monitoring

✗ [3 members of `sandialabs` are not Sandians](#)

Only Sandians are allowed in the organization

✗ [The `outside\\_collaborators.csv` file in the repository is outdated](#)

✗ [The `sandians.csv` in the repository is outdated](#)

We keep track of all collaborators

Weekly Monitoring

✗ [29 repositories have one or more administrators who are not US citizen Sandia regular employees](#)

There are restrictions on who can have **Admin** permissions

✓ [No repositories have outside collaborators with elevated permissions](#)

Outsiders can only have **Read** or **Triage**

✗ [3 repositories are missing a SCR#](#)

All OSS repos require a Sandia Copyright #

Monthly Monitoring

✗ [549 repositories are missing SNL topics](#)

Topics are used for categorization on software.sandia.gov

✗ [5 repositories are private](#)

All OSS repos must be public

Monitoring



Daily Monitoring

- ✗ [3 members of `sandialabs` are not Sandians](#)
- ✗ [The `outside\\_collaborators.csv` file in the repository is outdated](#)
- ✗ [The `sandians.csv` in the repository is outdated](#)

Weekly Monitoring

- ✗ [29 repositories have one or more administrators who are not US citizen Sandia regular employees](#)
- ✓ [No repositories have outside collaborators with elevated permissions](#)
- ✗ [3 repositories are missing a SCR#](#)

Monthly Monitoring

- ✗ [549 repositories are missing SNL topics](#)
- ✗ [5 repositories are private](#)

Automatically notify repository **Admins**, providing instructions to remedy the issues themselves



Sandia's Open-Source Process



Outline:

- Sandia's OSS Footprint
- Sandia's OSS Process
- Managing OSS
- Best Practices
- Monitoring