

BOF Days

February 10 - 12, 2026

<https://cass.community>

**The
Consortium
for the
Advancement
of Scientific
Software
(CASS)**



<https://cass.community/news/2026-02-10-cass-bof-days.html>

CASS: Stewardship and Advancement of the Scientific Software Ecosystem

- **Inward-facing activities:** Strengthening software products
 - Improve development practices, sustainability, quality, and trustworthiness
 - Enhance user experience and integration within the broader ecosystem
- **Outward-facing activities:** Community engagement and discovery
 - Curate and evolve the software portfolio
 - Help teams connect with and grow their user communities
 - Enable the broader community to discover and adopt useful software

CASS Members

CORSA

Partnering with foundations to provide sustainable pathways for scientific software

FASTMATH

Stewardship, advancement, and integration for math and ML/AI packages

PESO

Stewarding, evolving and integrating a cohesive ecosystem for DOE software

RAPIDS

Stewardship, advancement, and integration for data, visualization and ML/AI packages

S4PST

Stewardship, advancement and engagement for programming systems

STEP

Stewardship, advancement of software tools for understanding performance and behavior

Sponsored by the
Department of
Energy, Office of
Advanced Scientific
Computing Research

Engage with CASS!

- Learn about CASS:
 - <https://cass.community/about/>
- Join the CASS Announcement list (low-volume):
 - <http://eepurl.com/iRiSnY>
- Find out more about our **software products**
 - Catalog: <https://cass.community/software/>
 - Collected as part of the [Extreme-Scale Scientific Software Stack](#) (E4S)
- Participate in **CASS Working Groups**
 - Impact Framework, Integration, Metrics, Software Ecosystem, User-Developer Experience, Workforce
 - <https://cass.community/working-groups/>

OSSF Scorecards & best practices

CASS BoF Feb 2026

The Panel

- (Host) Vicente Bolea @ Kitware
- Luc Berget-Vergiat @ SNL
- Jason Gates @ SNL
- James Willenbring @ SNL
- Roscoe Bartlett @ SNL
- William Allen @ Kitware
- Jonathon Anderson @ RICE university

Agenda

- **0'-10' : Introductions**
- **10'-30': Software Security for HPC**
- **30'-50': OSSF Scorecards and how to use them**
- **50'-70': OSSF Scorecards Automation**
- **70'-90' : Future works and further discussion**

We will try our best for the last 5 mins of each sections to be open for audience interaction.

◆ Software Security for HPC

- **Short presentation by Roscoe A. Bartlett**
- **Conversation**
 - What makes securing HPC environments fundamentally different from traditional enterprise or consumer systems?
 - How do you manage security risks from the massive open source dependency chains in HPC software stacks?
 - How do you balance community-driven open source benefits with security challenges from volunteer-maintained projects in HPC?

OSSF Scorecards (and best practices) and how to use them

- **Short presentation by Luc Berget-Vergiat.**
- **Short presentation by Jason M. Gates.**
- **Questions:**
 - Why did you particularly adopted OSSF Scorecard and its best practices, are there alternatives? Is this a sellers market?
 - Are OpenSSF Scorecard's security metrics aligned with the needs of HPC open source projects? Is its criteria appropriate for all software, if not can we customize it? Would it defeat its purpose?
 - Is there a HPC OSS that would not benefit from adopting these projects?
 - What is your experience with the OSSF Scorecard upstream team?

OSSF Scorecards Automation

- **Short presentation by William Allen**
- **Conversation:**
 - Do we all agree that scorecards need to be periodically run in CI pipelines to avoid regressions?
 - Should Scorecard report expire after a given time? For instances, settings of the repository are not immutable.
 - Tools such as CodeQL and Dependabot help automating this, LLMs further helps correcting low hanging fruit issues, what is your experience with existings tools?
 - Scorecard.dev provides a viewer of the score, is this enough? Could this displayed as metrics natively in gitlab/github/cdash?

Further discussion and future work

- What future improvements or features would make OpenSSF Scorecard and similar security tools more effective for HPC OSS projects?
- Will we see a future where HPC centers would require a minimum OpenSSF Scorecard score for OSS?
- Do you expect a lite|core version of Scorecards that could be universally adopted?
- Is there anything that OpenSSF scorecards could learn from previous successful similar projects (SPDX/SBOM)?
- In a dystopic future where LLMs produces and consume most of the OSS software, is there a place for OSSF Scorecards?

Conversation with the audience

- What are your experiences with OpenSSF Scorecard and best practices?
- Thank you!