**The Open Source Security Foundation**
MINUTES OF GOVERNING BOARD (FOR PUBLIC RELEASE)
11 November 2022

A regular meeting of the Governing Board of the Open Source Security Foundation was held on 11 Nov. 2022 at 9:00 am Pacific Time at the Resort at Squaw Creek, Olympic Valley, CA and via teleconference.

**Governing Board Members In Attendance**

| Company | Governing Board Director | Present |
|---|---|---|
| Atlassian | Adrian Ludwig | ✓ |
| Coinbase | Scott Roberts | ✓ |
| Dell Technologies | John Roese | ✓ |
| DeployHub* | Tracy Ragan | ✓ |
| Ericcson | Per Beming | ✓ |
| GitHub | Mike Hanley | ✓ via teleconference |
| Google | Eric Brewer | ✓ |
| Google* | Bob Callaway | ✓ |
| Huawei | Jinguo Cui | ✓ via teleconference |
| IBM Corporation | Jamie Thomas (Chair) | ✓ |
| Intel Corporation | Arun Gupta | ✓ |
| JP Morgan Chase | Rao Lakkakula | ✓ |
| Microsoft | Mark Russinovich | ✓ |
| Morgan Stanley | Declan O'Donovan | ✓ |
| NCC Group* | Jennifer Fernick | ✓ via teleconference |
| Oracle | John Heimann | ✓ via teleconference |
| OWASP* | Andrew van der Stock | ✓ via teleconference |
| Security Community Rep. | Ian Coldwater | ✓ via teleconference |
| Sonatype | Brian Fox | ✓ |
| Wipro | Subha Tatavarti | ✓ via teleconference |

**Observers, Invited Guests, and Staff Attendance**

| Company | | Observer |
|---|---|---|
| AWS | ✓ | Debashis Das |

| | | |
|---|---|---|
| Dell Technologies | ✓ | Sarah Evans |
| Ericsson | ✓ | Phil Robb |
| Google | ✓ | Anne Bertucio |
| IBM Corporation | ✓ | Jeff Borek |
| Microsoft | ✓ | Sarah Novotny |
| Red Hat | ✓ | Vincent Dannen |
| VMWare | ✓ | Tim Pepper |
| WiPro | ✓ | Andrew Aitken |

| **TAC Representatives and Invited Guests** | | |
|---|---|---|
| TAC Representative | ✓ | Aeva Black |
| TAC Representative via teleconference | ✓ | Christopher ‘CRob’ Robinson |
| TAC Representative via teleconference | ✓ | Luke Hinds |
| TAC Representative via teleconference | ✓ | Dan Lorenc |
| TAC Representative | ✓ | Abhishek Arya |
| TAC Representative via teleconference | ✓ | Josh Bressers |
| Invited Guest | ✓ | Emily Fox via teleconference |
| Invited Guest | ✓ | Kelly Ann via teleconference |

| **OpenSSF and Linux Foundation Staff** | | |
|---|---|---|
| General Manager | ✓ | Brian Behlendorf |
| Director of Open Source Supply Chain Security | ✓ | David A. Wheeler |
| Program Director | ✓ | Jory Burson |
| Sr. Marketing Manager | ✓ | Jennifer Bly |
| SVP, GM of Projects | ✓ | Mike Dolan |
| Executive Director | ✓ | Jim Zemlin |
| Strategic Advisor | ✓ | Sam Ramji |
| Strategic Advisor | ✓ | Jerry Michalski |
| Program Manager | ✓ | Khahil White via teleconference |
| VP, Dependable Embedded Systems | ✓ | Kate Stewart |
| CTO, Linux Foundation | ✓ | Nirav Patel |

**Call to Order**

Brian Behlendorf (BB) called the meeting to order at 9:02 am Pacific Time, and Jory Burson (JB) recorded the minutes. A quorum of Governing Board Members was established for the conduct of business, and the meeting, having been duly convened, was ready to proceed with business.

**Agenda and Welcome**

BB introduced the objectives and agenda for the meeting, and reminded participants of the pre-reads that were shared with the participants prior to the meeting. There were no additional topics added.

**Antitrust Policy Notice**

BB reminded the Governing Board of the Linux Foundation antitrust policy notice to which all meetings must adhere.

**Welcome and Highlights of the past year**

BB presented highlights from the past year of OpenSSF operations. BB drew attention to several OpenSSF projects and Working Groups that made significant impact and improvements over the course of the past year, including Sigstore's General Availability release, increased publication of security education and content, new features and maintenance improvements to Scorecard and SLSA, new specification development efforts, the publication of the State of OSS Security Report, and the Open Source Software Security Mobilization Plan. BB also gave an overview of the community grants made through Project Alpha-Omega as well as the OpenSSF events that were hosted in 2022.

BB then invited Jim Zemlin (JZ) to welcome the group and comment on OpenSSF's successes as well as his enthusiasm for the future. JZ shared that the LF would be investing in additional staff to advance the SBOM work and investing additional funds into census research. JZ cited insights from the State of OSS Security Report that could inform the OpenSSF's priorities in 2023.

**Scene Setting**

BB then introduced Sam Ramji (SR) to provide context and framing for the remainder of the meeting agenda. SR described his role, as well as methods used to assist the group in developing a shared strategy. SR reviewed the synthesized output from the stakeholder interviews, noting that the discussions produced four distinct visions for OpenSSF.  These visions were summarized in a pre-read document emailed to the Board prior to the meeting.

SR then invited Mark Russinovich (MRu), Tracy Ragan (TR), Eric Brewer (EB) and Jamie Thomas (JT) to describe and make a reasoned case for each of the four foundations. JT spoke to the importance of an education-focused foundation, describing a "10 Million Developer Uplift" with training, education and resources. EB spoke to the role of the foundation in producing a "Sterling Toolchain" and noted that it dovetailed nicely with education. TR spoke to the role of the Foundation as a "Funder of First Resort," noting that money is an energy we can deploy to the benefit of open source security. MRu spoke to the need for a Rapid Threat Response Center, and the potential for the foundation to grow a response team for the open source community the way large companies provide rapid response for themselves and their customers.

SR then invited an open discussion on these four positions amongst the meeting attendees. Several participants provided comments on the "four foundations'' framing. Participants noted that many issues are experienced most acutely by the end user, who may not be aware that package updates are available, for example. Participants also noted a strong connection between the "Uplift" and "Sterling Toolchain" ideas. Making end users aware of the issues, holding organizations accountable for security, and using the Linux Foundation developer community as a starting point for "Uplift" were also identified as potential opportunities.

SR asked the meeting participants to consider which of the visions were most important and compelling during the break. The group then took a 20 minute recess at 10:04 a.m.

**Envisioning Session: Strategic Vision for 2023**

BB resumed the meeting at 10:23 a.m. and SR introduced a small-group exercise to facilitate discussion. SR asked participants to help determine which of the 4 foundations, or which combination of the foundations would be most appealing to them, by distributing a percentage of 100 to each option. The participants were then dismissed into 8 breakout groups for a 20 minute small group discussion.

Jerry Michalski (JM) recalled participants to report on the small group activity. Each of the groups provided a representative to report the outcomes of the exercise. JM then facilitated a discussion of the group findings to determine common themes and preferred directions.

**ACTION:** BB will synthesize notes from the discussion and provide a readout report for the group.

The meeting went into a one hour recess for lunch at 12:02 p.m.

BB called the meeting to order following the lunch break at 1:02 p.m. BB summarized some of the takeaways from the morning sessions from his perspective as OpenSSF's General Manager. BB then invited Anne Bertucio (AB) to discuss OpenSSF's structure, emphasizing the value of prioritization and encouraging the Governing Board to focus on a few, high priority items. BB suggested that certain projects or efforts, that were not deemed to be of highest priority, could be spun out into separate efforts. Governing Board members in attendance generally agreed with the statement that they would prefer not to attempt to drive forward on all four foundations all at once, and that the group's focus should be clear and crisp. Discussion ensued on the extent to which the OpenSSF should be tightly focused vs. opportunistic (taking advantage of an unseen event or issue) on items that were not of highest priority. The group noted that the strategy it pursues will influence the shape and hiring strategy of the organization.

Several board members offered suggestions related to operational efficiency, noting that with the large membership and leadership base, OpenSSF resources could be more effectively marshaled by developing and empowering committees, which could alleviate pressure on the TAC and Board. Participants also agreed that the TAC should be further empowered and supported to develop OpenSSF's technical opinions and position on tools, best practices, and technical direction. TAC chairperson Bob Callaway (BC) aked if the group would agree that the TAC appears to be executing mostly on activities that fit the "Sterling Toolchain" and "Uplift" foundations, and participants agreed by consensus that is the case. Meeting participants from the TAC noted that, while there are many people who attend OpenSSF working group meetings, it has been challenging to activate those attendees to work on deliverables. TAC representatives requested more staff support for organizing the working groups and their deliverables, as well as for developing the toolchain and technical vision.

**Technical Vision, TAC Role, and Staffing**

BB then asked BC to lead a discussion of questions posed by the Technical Vision, TAC Role, and Staffing pre-read sent to Governing Board members prior to the meeting. BC shared a graphic indicating a spectrum that the TAC might operate on, from an advisory role to an active, hands-on product-oriented role. Discussion ensued regarding staffing requirements to support a more active and technically particular TAC, and what the organization would need to look like in order to support an authoritative technical body. JM then led the full group in a discussion of what would be "in scope" or "out of scope" for the TAC given the directive to develop technical leadership and tooling. It was further clarified that the purpose of identifying "out of scope" items was to determine what was not a responsibility of the TAC, though those items may be owned by other roles or functions in the organization.

JM thanked everyone for the discussion and the group took a refreshment break at 2:27 p.m.

BB called the meeting to order at 2:36 p.m. BB asked the group if there was general consensus among participants to approve the TAC's request for additional staff resources, in particular filling a CTO role. Hearing no objections, BB directed staff to develop a job description for the key roles. Board members also requested a hiring committee to review the job descriptions and assist with sourcing.

> **ACTION:** Develop and share job descriptions for the CTO and technical program manager roles.
> **ACTION:** Create scope and resolution to charter a board-level hiring committee

**Envisioning Session: What Does Success Look Like in 2023?**

SR asked meeting participants to return to their breakout groups for further small group discussion. SR asked the group to do a visioning exercise to tell the story, "What was successful in 2023?" based on what success would look like if the organization operated to its purpose successfully next year. The participants were dismissed for 15 minutes of small group discussion.

JM recalled participants for large-group discussion at 3:08 p.m., asking each group to provide their "success headlines." Each group presented for approximately 3 minutes what was discussed in the small group discussion.

JM then facilitated a short discussion about the aspirational nature of our work, noting that the headlines provided by the groups did not exist in conflict with each other or the four foundation identities discussed earlier in the meeting.

BB noted that the outcomes for today will be consolidated into operational documents and a 2023 budget proposal. BB thanked everyone for their participation in discussions.

> **ACTION:** BB will share a budget ahead of the Dec. 2 meeting.

BB asked for closing comments. Several participants noted their appreciation for the challenging but productive sessions, and thanked the staff and facilitators. Other Governing Board members suggested meeting twice a year in person would be more ideal, to which there was general approval.

BB and Sarah Novotny (SN) concisely summarized the day's key conclusions, noting that the Board has agreed 1) that the TAC should be technically opinionated and should further develop its vision and requirements for a "Sterling Toolchain"; 2) that of the four foundations, "Sterling Toolchain" should take the primary focus, with a secondary focus on "Uplift"; 3) that "Rapid Response" and "Funding" should be enabled in a more opportunistic manner; 4) that the staff should proceed with role development for a CTO and program management hires; and that 5) the Board should hold in-person meetings twice a year.

**Adjournment**

BB called the meeting to a close and the meeting of the Governing Board adjourned at 3:40 PM Pacific Time.