# 2022 TAC Security Seat Election

## Information on the TAC Security Seat Role

The TAC will elect from amongst the voting TAC members a chairperson for a term of one year. The TAC shall hold elections to select a TAC Chair annually; there are no limits on the number of terms a TAC Chair may serve.

**Responsibilities**

**The scope of this seat will include, but not be limited to:**

The role of the security SME is to work with project TSCs, the TAC and the LFNGB to improve the security of the code produced by LFN projects by

- Implementing more secure software development culture:
  - Secure software development best practices and tools (e.g. from the survey table),
  - Software development best practices and tools that decrease the vulnerabilities in LFN project code (code scanning, package upgrades),
  - Software supply chain security best practices (SBOM, code/container signing) to increase the security transparency of LFN project code,
  - LFIT security practice improvement,
  - OpenSSF badging assistance.
- Identify cross open source project security issues and provide action recommendations.
- Keep track of the The Open Source Software Security Mobilization Plan implementation and identify touch points for LFN projects.
- Providing subject matter expertise to the TAC.
- Advising the TAC on security related issues.

## Election Mechanics

- Candidates for TAC Appointment to the TAC are nominated by the existing TAC members.
- A nomination page will be created for each candidate, including a supporting statement and contact information
- Candidates must accept nomination prior to consideration.
- Failure to accept within two weeks is considered declining the nomination.
- Once the candidates' nomination period is complete, there will be a 14-day period for the TAC to contact and evaluate candidate submissions.

### Nomination Phase

The nomination phase starting 12 Oct 2022  and will conclude on  26 Oct 2022  17:00 PDT.

### Election Phase

If there are multiple nominees: A Condorcet election will be initiated by the LF using the OpaVote voting system.  All TAC members will receive an invitation to vote. In the case of multiple candidates the timing is as follows:

- The election phase will begin on with the distribution of the OpaVote poll via email
- The election phase will end four (4) full business days later in the same time zone the poll was initiated from (typically PDT).

## Information on Candidates

**Name**: Amy Zwarico

**Company: AT&T**

**Short Biography**:

Amy Zwarico is a Director Security at AT&T specializing in software and open source security.

She has PhD in Computer Science from the University of Pennsylvania and has worked in the telco industry for 25 years, beginning with BellSouth and then with AT&T, where she developed web based integrations to BSS/OSS systems, architected mobility systems, and for the past 19 years focused on application security, cloud security, applied cryptography and policy.

She has been a member of ONAP since 2017 serving on the security subcommittee (SECCOM) as a contributor and as the vice chair. She has helped drive community acceptance of Core Infrastructure Initiative (CII) badging, a prioritized approach to upgrading vulnerable packages within the ONAP code base, and inclusion of security testing in the integration pipeline. She consistently solicits feedback from the PTLs and ONAP developers to help SECCOM define realistic security goals for each release. She also is lead for the VNF security requirements.

She joined the O-RAN Alliance in 2020 and is a contributor to the Security Focus Group. She is focused on defining security controls for the O-RAN interfaces and helping the O-RAN Software Community adopt the secure development practices used by the ONAP community. She also contributed security requirements to CNTT.

She was also elected as our LFN Governing Board Member Committers Representative in 2021.

**Statement of Intent**:

If Amy is elected then she will use her Security experience to develop a “Security by Design” Development Culture, identifying cross open source project security issues and providing action recommendations.

She will provide regular feedback to the TAC about the LFN Open Source Community project security improvement plan and implementation.

She will also share trends (tools, best practices, etc.) from the Security Industry that can benefit to the LFN Open Source Community projects.

She will also communicate any new security alert that can impact LFN Open Source Community projects

-----------------------------------------------

**-----------------------------------------------**