Nominee's Full Name	Nominee's Pronouns	Nominee's Title	Nominee's Organizational	Nominee's Bio	Nominee's Candidate Statement
Arnaud J Le Hors	He/Him	Senior Technical Staff Member, Open Technologies	IBM	Arnaud Le Hors is Senior Technical Staff Member of Open Technologies at IBM, working on a range of technologies with a primary focus on Open Source supply chain security. Arnaud has been working on standards and open source for over 30 years, both as a staff member of the X Consortium and W3C, and as a representative for IBM. He has been involved in every aspect of the open technology development process: technical, strategic, political, and legal. Arnaud was editor of several key web specifications including HTML and DOM and was a pioneer of open source with the release of libXpm in 1990. Arnaud has participated in several prominent open source projects including the X Window System and Xerces, the Apache XML parser. Arnaud is the main representative for IBM at W3C and INCITS, a member of the Hyperledger Technical Oversight Committee and contributor to OpenSS.	Arnaud: "Open Source software is under attack and having dedicated my entire career to open technologies, I have a personal interest in helping the industry address this issue. This is why I have spent most of my time working on OpenSSF since September 2021 and made contributions to various projects and groups including Scorecard, Criticality Score, Sigstore, the Best Practices WG, the SLSA specification SIG, and the TAC just to name a few. I fixed bugs, improved documentations, provided feedback, guided WGs and SIGs on the OpenSSF process and adopting the appropriate license framework, and so on. I largely contributed to the development of the governance structure and process the TAC has adopted. I strongly believe in the importance of OpenSSF and my primary goal is to make OpenSSF a successfully functioning and inclusive open community so that it can deliver on its mission. In running for the TAC election, I want to bring to the TAC my extensive experience in open communities with a special interest in helping improve communication across OpenSSF and beyond as well as improve clarity as to what is going on so that interested parties can easily find their ways and help OpenSSF with its mission."
Priya Wadhwa	she/her	Engineering Manager	Chainguard	Priya has been an active member of the Sigstore community and last year became one of the Technical Steering Committee members. Priya was central to the release of General Availability of Sigstore demonstrating her leadership in open source and the ability to bring the community together to achieve something great. She continues to work hands on with Sigstore infra, cosign and many other parts of the ecosystem as well other open source projects.	I've been proud to work in open source communities for my entire career, and have had the opportunity to previously serve on the Tekton Governing Board and currently serve on the Sigstore Technical Steering Committee. From my experience helping lead these large open source projects, I've experienced firsthand how a supportive foundation can empower maintainer-driven open source projects to succeed. Continuing to do so would be my primary goal as a member of the OpenSSF TAC. I've maintained a variety of open source projects (Tekton, Sigstore, kaniko, minikube) and so I can bring an open source maintainer's perspective to the OpenSSF TAC. I consistently speak at open source conferences, continue to make contributions to a variety of OSS projects, and in doing so I've built a strong network that I believe would help me succeed as an OpenSSF TAC member.
Tim Pepper	they/them/theirs	Principal Engineer	VMware	Tim Pepper is a Principal Engineer in the Office of the CTO at VMware, the engineering lead for the company's Open Source Program Office and open source software supply chain security initiatives. Technical experience spans orchestration, distributed systems, linux distribution build/release/test/update, linux kernel and drivers, embedded systems and hardware bringup. Across almost 30 years of experience, Tim embodies the notions of full stack engineering and open source servant leader. This year Tim completes a 2-year term as an elected member of the Kubernetes project Steering Committee, and has previously served in leadership in the project's SIG Release and WG Long Term Support, and as an elected member of the project Code of Conduct Committee.	Across capacities of engineering leadership in VMware's Open Source Technology Center and software supply chain security initiatives, OpenSSF Governing Board Observer, and Kubernetes project roles, I'm at the nexus of complex open source producer/consumer interactions. I see tremendous positive work underway stitching this network of actors into a more trustworthy flow of collaborative innovation. But even more remains and I am drawn to contribute time to the TAC's mission within the OpenSSF. If elected, I will work to represent all initiatives and subprojects fairly, but I also profess an affinity the Supply Chain Integrity and Securing Software Repositories Working Groups. It is not possible for every ecosystem entity to build all open source on their own trusted process, nor will every open source project reach SLSA level 3 or "4" any time soon. Redistribution and reuse are present for the foreseeable future, if not forever. This makes incremental improvement toward more trustworthy and informed artifact exchange and consumption a keen interest area as we advance the state of the art, public policy, and industry norms. Additionally I will contribute engineering leadership in organizing, documenting, and bridging between OpenSSF Governing Board and TAC, member companies, and contributors to encourage sustainable contributor experience and transparency in our Technical Initiatives. Through my diverse background as a specializing generalist, I work to see, foresee, and mitigate issues with a bias for action and decision. Ahead of decisions I will facilitate thoughtful communication and consensus across project developers, operators, users, and also vendor stakeholders.
Daniel Appelquist	He/Him	Mr	Snyk	Daniel a background in open source and open standards participation, leadership and governance. He was a startup founder and dot-com CTO, which brought him from the US to Europe. Before joining Snyk, he worked for large companies (notably Vodafone, Telefonica and Samsung), the UK Government as well as smaller companies. He co-chairs the W3C Technical Architecture Group (one of the W3C's two elected leadership groups) where he worked on initiatives such as Securing the Web https://www.w3.org/2001/tag/doc/web-https and the Security & Privacy Self-Review https://www.w3.org/TR/security-privacy-questionnaire/. He was Samsung's board representative for the JS Foundation, where he helped to create the OpenJS Foundation. He also co-founded Open Web Docs, an organization supporting development of web developer documentation. He is an appointed member of the UK Government Open Standards Board.	I bring extensive experience in open source and open standards organizations, with a strong focus on user needs and tangible benefits. I have a track record of driving results and tangible outputs in my work with W3C and other open source organizations. As someone based outside the US, I offer international experience and focus as well as government policy experience. Since joining Snyk, I have been actively engaged in the Best Practices, End User, and Tooling working groups, and have worked to bring additional engagement from my employer to OpenSSF groups and projects. I am currently working on OpenSSF work items such as the SCM best practices and the SBOM everywhere implementation plan, as well as planning a joint workshop with W3C, OWASP, and OpenJS Foundation on web developer security. If elected to the OpenSSF TAC, I would bring my experience driving consensus across diverse technical organizations. I would also put energy towards delivering on our stated "Public Good" value, drawing on my experience spearheading work on the Ethical Web Principles at W3C. I am also passionate about promoting diversity and inclusion in how we work and how we work with the developer community. I believe that security plays an essential role in ensuring a healthy and trustworthy ecosystem for all. The work we do at OpenSSF is vital to achieving this goal.
Marina Moore	she/her	PhD candidate	NYU Tandon School of Engineering	Marina has been prolific in the open source security space in both the CNCF and OpenSSF, including TUF and Sigstore projects. I have learned a lot from her talks, blog posts and academic papers. She would be an incredible asset to the TSC and also be an excellent bridge to the academic world.	I would bring my perspective as both a maintainer and academic to the OpenSSF TAC. I am a maintainer of numerous security-focused open source projects, including the OpenSSF's Sigstore project where I am a root key holder. I am also a PhD candidate doing research in the space of software supply chain security. As part of this research I have interacted with many open source community members to learn more about the needs of the community and ensure my research can have a real, practical impact on the security of the ecosystem. OpenSSF is in a unique position to facilitate collaboration between academics and open source projects by making data about projects available to academics and sharing lessons back out to the open source community.
Christopher (CRob) Robinson		Director of Security Communications	Intel Corporation	Christopher Robinson (aka CRob) is the Director of Security Communications at Intel Product Assurance and Security. CRob is a 42nd level Dungeon Master and a 25th level Securityologist. He has worked at several Fortune 500 companies with experience in the Financial, Medical, Legal, and Manufacturing verticals, and spent 6 years helping lead the Red Hat Product Security team as their Program Architect. He is a leader within several Open Source Security Foundation (OpenSSF) efforts and is a frequent speaker on cyber, application, and open source security. CRob has been a featured speaker at Gartner's Identity and Access Management Summit, RSA, BlackHat, DefCon, Derbycon, the (ISC)2 World Congress, and was named a "Top Presenter" for the 2017 and 2018 Red Hat Summits. CRob was the President of the Cleveland (ISC)2 Chapter, and is also a children's Cybersecurity Educator with the (ISC)2 Safe-and-Secure program. He holds a Certified Information Systems Security Professional (CISSP) certification, Certified Secure Software Lifecycle Professional (CSSLP) certification, and The Open Group Architecture Framework (TOGAF) certification. He is heavily involved in the Forum for Incident Response and Security Teams (FIRST) PSIRT SIG, collaborating in writing the FIRST PSIRT Services Framework, as well as the PSIRT Maturity Assessment framework. CRob is also the lead/facilitator of the Open Source Security Foundation (OpenSSF) Vulnerability Disclosures and OSS Developer Best Practices working groups as well as a Technical Advisory Committee (TAC) member.	CRob have been involved in upstream open source security for nearly a decade, and is proud to be a trusted member of our community. CRob has been involved with the OpenSSF since its inception as a contributor, working group/SIG lead, and as a current TAC member. He is passionate about helping improve the security posture of open source software for maintainers and vast downstream ecosystem of consumers. Continuing to be part of the TAC, CRob can contribute his experiences in cyber and application security, as well as providing organization, leadership, and mentorship to our assorted groups, projects, and members. Helping shape our technical direction and execution has been exciting and he is hopeful to see us continue to make security simpler, more accessible, and part of our core daily activities for all contributors, maintainers, and consumers!

Nominee's Full Name	Nominee's Pronouns	Nominee's Title	Nominee's Organizational	Nominee's Bio	Nominee's Candidate Statement
Zach Steindler		Principal Engineer	GitHub	I've been interested in helping secure open source for several years, starting with helping PyPI implement MFA and API keys back in 2019. Once the OpenSSF formed, I started participating by being one of the co-facilitators / co-writers for stream 10 in the OSS Mobilization Plan. Since then, I've been most active in the Security Software Repos working group, which dovetails nicely with my role at GitHub as the program manager for providing provenance of npm packages using Sigstore. We're working on sharing what we've learned on that project to help more CI/CD systems and more package managers provide provenance. Recently, I've also been participating in stream 9: SBOMs everywhere to help open source projects increase transparency in an interoperable way. There's so much to do in securing open source, but it's clear to me we need tools that are easy for developers and aren't tied to a single ecosystem	The energy across the membership of the OpenSSF is incredible. There's over a dozen working groups and workstreams that are either blazing new trails, or paving paths to enable mass adoption of new security capabilities for open source. To that end, I think the most import thing the TAC can do is aggressively unblock and enable those workstreams to move forward. That doesn't mean greenlighting everything, but that does mean focusing on operations: ensuring prompt feedback to requests, driving the TAC body to a decision, and thoroughly communicating results to ensure transparency. I have not previously served on a TAC, but I think my experience on non-profit boards and organizing tech events will help the TAC with its operations.
Jonathan Meadows	he / him	Managing Director Citi - Head of Cloud, App Sec & Supply Chain Engineering	Citi	Jonathan Meadows heads up the Cloud, Application Security and Supply Chain Engineering groups at Citigroup. Jonathan has extensive software engineering experience in the financial services industry and an in-depth knowledge of cyber security. Jonathan has co-authored the CNCF's Secure Software Factory Reference Architecture. He also created the CNCF Software Supply Chain Working Group, OSSF End User Working Group and the FS-ISAC Supply Chain Working group. He currently chairs both the end user and FS-ISAC groups. Jonathan is also a member of the governing board of the OSSF and has followed the foundation since the early days. His main focus is on working with end users across multiple industries to socialize the emerging threats associated with supply chain security, whilst providing actionable guidance and capabilities that allow end users to protect themselves.	I passionately believe that the only way to address the growing threat of supply chain vulnerabilities and open source security is to work collaboratively with peers in the industry and the OSSF. Hence ensuring that Citi were amongst the early large industries to join the OSSF where I now sit on the governing board. I believe by joining the TAC I would be able to bring my breadth of experience from a technical end user perspective providing an end user voice to the technical discussions and help tailor our work and priorities to align with the specific needs of consumers. This will help ensure that we at the OSSF continue to deliver value where it is most needed to reduce the risk of supply chain compromise. From a personal perspective I have a history of working in the open source community from creating the CNCF Financial Services working group, CNCF Supply Chain Working Group and the OSSF End User working group which I now chair. Additionally I believe in working openly and collaborating with others and hence set up a team at Citi to build and open source the FRSCA project which we contributed to the OSSF last year. This is along with co-authoring the CNCF supply chain best practices guide amongst other contributions.
Thomas Nyman	he/him	Senior Security Technology Specialist	Ericsson	Thomas Nyman is Senior Security Technology Specialist at Ericsson where he works primarily in the areas of hardware and platform security for critical telecommunications infrastructure. Thomas has 10 years of experience working with systems security both in industry and academia. Before joining Ericsson, he worked in the R&D organization for Trustonic, a company originally formed to commercialize an Arm technology called TrustZone that enables hardware-isolated trusted execution environments in smartphones, connected vehicles, and Internet-of-Things devices. He holds a PhD in Computer Science from Aalto University, Finland, where he worked on systems security research in the areas of mobile and embedded platform security. His PhD thesis was on the topic of hardware-assisted defenses against run-time attacks. Thomas currently leads the C/C++ Compiler Options Hardening Guide initiative part of the OpenSSF Best Practices for Open Source Developers working group.	Open source code, best practices, and tooling have become indispensable building blocks for the digitalized society in nearly all industry sectors, including for critical infrastructure such as mobile networks. At the same time, digitalization creates significant risks through increased exposure to cyberattacks. Because of its importance to vital societal functions, the cybersecurity of open source software, including the open source supply chain is an obligation that should be shared by the volunteers, as well as the organizations that benefit from, and contribute to open source. I have only recently become an active member of the OpenSSF community through the C/C++ Compiler Options Hardening Guide initiative. However, throughout my previous academic career I have been a firm believer in that research output, including source code should be freely available to the research and open source communities to build further upon, and have been contributing to the body of open source code throughout the various research programs I have had the opportunity to be a part of. During my academic career, one of the defining experiences for me as a young researcher was the opportunity to interact with various industry experts who were able to provide insights on the practicability of solutions, surprising challenges, and open problems related to joint systems security research. If elected, now that I'm in such a position in industry myself I hope to be able to contribute insights on the cybersecurity challenges and opportunities with open source in the telecommunications sector, as well as my previous experience with technologies for trusted execution and confidential computing, which are often less well understood outside the organizations that develop proprietary software for such environments, but where software security, nevertheless is paramount to the security of the system as a whole.