Timestamp	Email Address	Full Name	Pronouns	Title	Organizational Affiliation	Bio	Candidate Statement	Notified?	Reason for denial	
1/5/2022 6:00:36	aarya@google.com	Abhishek Arya	He/Him	Principal Engineer and Manager, Google Open Source Security Team	Google	Abhishek Arya is a Principal Engineer and head of the Google Open Source Security Team. His team has been a key contributor to various security engineering efforts inside the Open Source Security Foundation (OpenSSF). This includes the Supply Chain Security Framework and Tools (SLSA, Sigstore), Security Risk Measurement Platform (Scorecards, AllStar), Vulnerability Management Solutions (OSV) and Package Analysis pipeline. Prior to this, he was a founding member of the Google Chrome Security Team and built OSS-Fuzz, a highly scaled and automated fuzzing infrastructure that fuzzes all of Google and Open Source.	I lead the Google Open Source Security Team. I have been involved in OpenSSF since the early days of incubation. I have helped nurture several projects in OpenSSF. This includes Supply Chain Security Framework (SLSA), Security Risk Measurement Tools (Scorecards, AllStar, Criticality Score), Vulnerability Management (OSV-Schema) and Package Analysis. These projects are now thriving well, with strong community involvement: -SLSA - Helped establish Steering Committee and processes (with members from Citi, VMWare, Intel, Datadog, ActiveState, LF, Google). -Scorecards - Core contributor, reviewer, got external contributors on-board (Naveen, Chris). -OSV-Schema - Schema launched and refined with community feedback. On-going collaboration with GitHub on using this in GitHub Security Advisories. -Alpha-Omega - Collaboration with Microsoft, helped with project plans. -Fuzzing - OSS-Fuzz fuzzing service for the community, serves 500+ OSS projects. I will bring in an interesting perspective from the open source security problems we see at Google. I will also help fill in existing gaps by identifying new initiatives we can start in OpenSSF (e.g. have moved fuzzing industry discussions to OpenSSF security tooling wg).			
1/13/2022 16:48:21	aeva.online@gmail.com	Aeva Black	they/them	Open Source Hacker	Microsoft	Aeva Black is a dot-com veteran, an open source hacker, and a queer and non-binary geek with twenty years' experience spanning roles as a developer, team and project lead, and startup executive. Today, they work in Azure's Office of the CTO, focusing on improving the security of open source software and digital privacy. Before joining Microsoft, Aeva worked at IBM, HP Cloud, and several startups. They created the OpenStack Bare Metal project, and have contributed to MySQL, Ansible, and many other open source projects over the years. Aeva currently serves on the Board of the Open Source Initiative, and as an alternate on the Board of the CNCF. They previously served on the Confidential Computing Consortium's Outreach Committee, the Kubernetes Code of Conduct Committee, the OpenStack Technical Committee, and the board of the Consent Academy.	While security in open source projects has been a consistent thread throughout my career, it has been a specific focus of mine for the past few years. Some of you may already be familiar with my work on the security landscape survey, gitbom, my contributions to CNCF TAG-Security, or my work within the Confidential Computing Consortium. I'd like to continue that work by supporting the OpenSSF. If I am elected, I will bring my experience as a leader in other open source communities, as well as current connections to other Foundations, to support the growth of OpenSSF's technical projects and working groups. For the Foundation to succeed in its mission, we must think and act broadly – not only looking after our own interests, or our favorite ecosystem, or today's employer, but the whole of open source. We must engage constructively with each other, following accepted norms of practice in public forums, to work towards the public good. The stakes today are too high to do otherwise. Because inclusivity and community safety are also matters of security, I believe it is important for the leadership in every organization to consider how their policies may impact marginalized communities. To that end, I will continue to raise awareness when I believe a decision could jeopardize community safety, and I will work to create policies that foster inclusive and welcoming community spaces. Thank you for your consideration.			
1/14/2022 12:52:36	bcallaway@google.com	Bob Callaway			Google	Bob Callaway is the technical lead and manager of the supply chain integrity group in Google's Open Source Security Team. He and his team directly contribute to critical secure supply chain projects and drive communication & adoption of best practices throughout the open source ecosystem. Bob is a member of the Technical Advisory Council for sigstore, a Linux Foundation / OpenSSF set of projects focused on improving transparency and UX of software supply chains. Before joining Google in 2021, Bob was a member of Red Hat's Office of the CTO where he was responsible for emerging technology strategy with strategic partners (including IBM) and a principal architect at NetApp where he focused on contributions to OpenStack and storage automation projects. He holds a PhD in Computer Engineering from NC State University where he also serves as an adjunct assistant professor in the ECE department.	I am running for a position on the Technical Advisory Council of OpenSSF. For the past 10 years of my career, I have been involved in various open source communities in professional roles focused on upstream development, partner strategy and ecosystem engagement. I currently lead the Supply Chain Integrity group within Google's Open Source Security Team, where we directly contribute to critical projects and drive communication & adoption of secure software supply chain best practices. I also am a founding member of the sigstore TAC where we have built an exploding community of vendors, individuals and users focused on improving transparency of the supply chain and dramatically improving the UX for consumers and producers of OSS software. As part of the OpenSSF TAC, I would bring a breadth of experience and industry & academic connections to bear to help accelerate the impact of the various working groups. I am thrilled to see the OpenSSF grow as both a forum for discussing best practices and as an sponsoring organization for projects that are laser-focused on helping OSS communities adopt them.			
1/5/2022 5:12:47	christopher.robinson@int	Christopher Robinson (CRob)	He/Him	Directory of Security Communications	Intel	Christopher Robinson (aka CRob) is the Director of Security Communications at Intel Product Assurance and Security. With 25 years of Enterprise-class engineering, architectural, operational and leadership experience, Chris 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.	I have been involved in Open Source security for nearly a decade. I started off as an enterprise consumer of open source software and grew in my admiration and love of the movement to solve critical business problems. As my use and interest deepen I joined a commercial open source supplier, and ultimately worked with the Red Hat Product Security team for nearly seven years. While there we were founding participants in the OpenSSF and I was able to contribute as a member and ultimately am helping lead several OSSF Working Groups. Today in my current role with Intel, I still get to contribute both to community efforts as well as help educate and steer internal policy to leverage open source methodologies. During my tenure with the OpenSSF I have had the privilege to work the Developer Best Practices working group and the Vulnerability Disclosures working group. I also am able to participate with the Tooling working group to help coordinate activities amongst the assorted projects more smoothly. I have also had the privilege or working with the OpenSSF's Public Policy Committee, helping shape messaging and approaches to global government activities that interact with open source software communities. Over the last year I've also worked with the TAC in coordinating town halls or cross-project efforts in addition to speaking on behalf of the foundation at events like FOSS Backstage and BlackHat USA. I feel I bring passion, energy, and humour to vital work of helping make open source software more secure and giving developers access to training and tools that help them improve their practices and their software. I have deep connections throughout the industry with both commercial organizations (aka "vendors") as well as relations with OSS devs and projects.			
1/6/2022 6:36:23	lorenc.d@gmail.com	Daniel Lorenc	He/Him	CEO	Chainguard	Dan has been working on and worrying about containers since 2015 as an engineer, manager, founder and CEO. He started projects like Minikube, Skaffold, and Kaniko to make containers easy and fun, then got so worried about the state of OSS supply-chains he partnered up with Kim and others to found the Tekton and Sigstore projects to make it easier to build and use containers securely, as well as SLSA to create a common language for software security and supply chain integrity. He has been involved with the Cloud Native Computing Foundation, chaired the Continuous Delivery Foundation technical oversight committee, and sits on the governing board and technical advisory committee for the Open Source Security Foundation. He's now a founder and CEO at Chainguard, a startup focused on software supply chain security.	I've been directly involved in open source security efforts for the last 5 years, both at Google and at my new company, Chainguard. I'm passionate about making the secure way the easy way, and believe that open source communities are key to overall software supply chain security. We need to work together in the OpenSSF across funding, education, and development of new technologies to get maintainers the support they need, onboard the next generation of OSS contributors, and make it easier for projects and communities to develop software securely. I believe that companies leveraging open source software have both a vested interest and an obligation to help here. I've had the privilege of serving on the OSSF TAC since it's formation, and have led several working groups and projects. I plan on continuing to contribute and lead these efforts, and would love the opportunity to continue to represent our contributors on the TAC.			
1/13/2022 6:14:48	josh.bressers@anchore.c	Josh Bressers	He/Him	VP of Security	Anchore	Josh Bressers is passionate about security and active in the open source community. As the Vice President of Security at Anchore he manages the Infosec team and guides security features for the company's products and acts as a public security advocate. Before Anchore, Josh was with Elastic where he built the product security team, managed supply chain security, and created an application security program focusing on realistic requirements. Josh was an early hire to the Red Hat Security Response Team where he coordinated vulnerability disclosures, eventually becoming the CVE CNA for all OSS projects. He later founded the Red Hat Product Security Team focusing on application security. Josh is active in the OpenSSF, hosts the Open Source Security Podcast and the Cypherconn Hacker History Podcast. Josh is also a co-founder of the Global Security Database project, a Cloud Security Alliance working group exploring the future of security vulnerability identifiers.	The OpenSSF is too important to fail. It needs enthusiastic leaders and curious members that want to help drive the industry forward. The aftermath of the Log4j shows us open source is more important and pervasive than ever. I do not believe the OpenSSF as an organization today is as effective as it needs to be. Rather than watch from the sidelines, I will use my election to the TAC to focus on making it more efficient and ensure its priorities are aligned with the goals of the OpenSSF. The TAC appears to struggle with making decisions, responding to requests, and following through. The election timelines set by the charter were not met, self nomination opening and the close of nominations was unnecessarily short. There have been several contributor requests which have not received any response from the TAC. The TAC should be using accepted open source tooling such as mailing lists, Slack, and GitHub issues to set the standard. I believe leadership is best accomplished by leading by example. I intend to contribute with the leadership of the TAC to ensure the OpenSSF is a successful organization by following the process defined in the OpenSSF charter and ensuring reasonable requests are responded to in a timely manner. This will be done by being the change that is needed and encouraging other TAC members to do the same. I'd be honored to assume this role and will work diligently to create a cohesive and productive community.			
1/13/2022 8:37:35	jhutchings1@github.com	Justin Hutchings	he/him	Director of Product Management	GitHub		I am running for the Technical Advisory Council for OpenSSF, because software security is one of the most important challenges of our generation. I currently lead Product Management for GitHub's Supply Chain Security team and work on products like Dependabot, our open source Advisory Database, and the dependency graph. These features are many developers only exposure to supply chain security, so I'm very interested in how to raise the security standards across the industry by promoting security tools and best practices that we're incubating in the OpenSSF as they mature. I have proudly served the last year on the OpenSSF Board of Directors for the last year. Prior to joining GitHub, I worked at Microsoft where I worked to build a number of standards and open source projects including Linux Foundation projects like AllJoyn or OCF/Iotivity, the IEEE Printer Working Group, and the USB-IF.			
1/5/2022 13:31:50	lhinds@redhat.com	Luke Hinds	he/him	Security Engineering Lead	Red Hat	I am an open source security engineer who lives in the south west of the UK. I have lots of experience running vulnerability programs for large open source projects as well as a developer who has founded / co-founded several successful open source projects.	I was one of the original members to help bootstrap the OpenSSF. Having served one term on the TAC, I think it's important that we get some continuity, so therefore I am putting myself forward for one more term. Currently I am active in the following communities: * One of the founding members of https://sigstore.dev * Lead and Developed the https://keylime.dev project alongside MIT * Kubernetes Security Response Team member (where I manage the bug bounty program and handle embargoed CVEs) * Board member on the confidential computing consortium In the past I have held other open source security roles, such as: * Elected project team lead of the OpenStack Security Group * Security Vulnerability Manager for OpenDayLight Project My days are filled with either writing or reviewing code for security projects or triaging vulnerabilities. This I believe makes me a good candidate for the TAC as I understand the pressures of being a maintainer on a large project and the stresses of dealing with vulnerabilities. I work in the Office of the CTO , Red Hat, where I lead a team of engineers focused on emerging technologies in the open source security space. My team developed projects such as https://enarx.dev and many more.			
1/13/2022 6:59:52	moshe@apiiro.com	Moshe Zioni	He/Him	VP Security Research	Apiiro	Listed in "27 influential penetration testers in 2020" by Peerlyst. Moshe has been researching security for over 20 years in multiple industries, specializing in penetration testing, detection algorithms and incident response; a constant contributor to the hacking community and has been co-founder of the Shabbatcon security conference for the past 6 years. Expresses views and presents research on stages and at conferences worldwide and always enjoys healthy conversations on revolving security aspects and believing in tutoring as a key to shifting security mindsets.	Apiiro has been innovating and propelling discussions around next-steps of supply-chain security and vision towards holistic and innovative approaches to tackle issues around it. Since our inception, two years ago, we've been introducing novel concepts that through contextual-risk knowledge-building practices we can successfully spot important and malicious intent through the SDLC lifecycle. Myself, as leading the Security Research of Apiiro, I'm promoting those concepts through different media and organizations today (OpenSSF WGs, Open Source Solutions, regularly speak at conferences and meetups (BlackHat, OWASP and other conferences) to make those notions a familiar subject, educate and lead those conversations with government, financial and other industries to promote and constitute education mechanisms throughout them. OpenSSF TAC is the perfect place for me to contribute and collaborate with global leaders that also take those subjects to heart and promote a healthy conversation about immediate and long-term topics that can be beneficial to better security posture and enterprise/public SDLC elements' resilience, which I would be honored and believe I have a lot of passion and knowledge to contribute to the advisory council.	Done; But, responded with contributions t	~~not yet a contributor~~	Reinstated
1/14/2022 15:20:54	estesp@gmail.com	Phil Estes	he/him	Principal Engineer, Container Runtime Strategy	Amazon Web Services (AWS)	Phil Estes is a Principal Engineer in the Container Compute organization at Amazon Web Services (AWS) and helps define AWS's container runtime strategy across Linux and container offerings at AWS. Phil is the current chair of the OCI's Technical Oversight Board (TOB) and a founding maintainer of the CNCF graduated container runtime project, containerd. For the past seven years Phil has been working upstream in various container runtime and cloud native communities on topics like security (user namespaces, apparmor) and multi-platform support and worked on implementations of core features such as these initially in the Docker engine, as well as early work on OCI's runc and currently in the containerd project.	I would like to continue working on the TAC as I believe open source security and the secure supply chain are both critical areas for the cloud native/container communities but also of critical importance to cloud and platform providers like my current employer. I would like to both be involved in the important work of the TAC to set technical direction for the OpenSSF and to be a connector to a significant group of interested parties inside AWS to the various working groups and initiatives already begun and those that are yet to be defined within the OpenSSF. The first 18 months of the OpenSSF have already produced some great efforts and increased awareness across our industry to the critical importance of this work. I would love to be a participant and representative in continuing and expanding that work across the cloud native communities for which I'm a part and also for which my employer and other platforms are key consumers.			

Timestamp	Email Address	Full Name	Pronouns	Title	Organizational Affiliation	Bio	Candidate Statement	Notified?	Reason for denial	
1/14/2022 18:24:54	hey@auggie.dev	Stephen Augustus	he/him	Head of Open Source	Cisco	I have been active in the LF/CNCF ecosystem for several years in multiple capacities. One of my primary contributor/maintainer roles is as Chair for Kubernetes SIG Release, leading the Release Managers team, responsible for operationalizing Kubernetes releases. Acting as a liaison to our Security Response Committee, our team is responsible for helping to responsibly disclose and remediate security vulnerabilities. Additionally, we are actively driving security-related improvements to community infrastructure, including the usage of tools like dependabot, scorecard, image vulnerability scanning. My teams have delivered proposals to the Kubernetes Community on implementing a software bill of materials for the project, as well as image signing, and artifact provenance. In terms of contributions, we are one of the largest projects in the cloud native ecosystem, trusted advisers/colleagues of several of the active OpenSSF project maintainers, and look forward to collaborating even more deeply with the OpenSSF community this year.	As the OpenSSF technical contact and Head of Open Source at Cisco, I believe that securing our communities is paramount to the long-term sustainability of all software projects, and by extension, all businesses. In my roles as a Kubernetes Steering Committee member, SIG Release Chair, CNCF TAG Contributor Strategy Chair, and TODO Group Steering Committee member, I draw unique experience on: - operationalizing software projects - maintaining open source communities - balancing open source and corporate interest - understanding the importance of open source software as a critical, but oft-overlooked component of product delivery In a previous life, I have held SRE, DevOps, production engineering, field engineering, and solutions architecture roles, and I bring those experiences to every facet of my work in the community. As a TAC member, I would deliver a wealth of knowledge and interlock between the myriad foundations and companies that we interact with, ensuring that the solutions that we deliver and maintain are easy to implement, well-maintained and documented, and helping to drive some of the most critical infrastructure in the world.			