Yocto and the Linux Foundation

By Julie Baker
Application Security/Cybersecurity Expert
https://www.linkedin.com/in/julie-baker-1ab89a

February 11, 2025

Open source software has been the foundation of software development for decades now. I doubt there is an application or an operating system in use today that does not have some open source libraries or components. I know many utilize a high percentage of open source components. There are many benefits to open source software - https://www.geeksforgeeks.org/introduction-to-open-source-and-its-benefits/. These are very utopian ideals, but then there is human nature, which leads to the fact that there are also significant security risks that go along with its use – https://owasp.org/www-project-open-source-software-top-10/. These are both well-known to those of us in application security, and I will not spend time on those very real issues here. Instead, I want to focus on specific concerns regarding the open source project Yocto[i].

Late last year, the State of South Carolina upgraded its election systems to EVS 6.3.0.0. As part of this update, DS300 tabulators were purchased, and these run a Yocto image. The ESS EVS 6300 Certificate and Scope of Conformance.pdf[ii] only mentioned Yocto once in the document. I expected more information about the image, especially regarding updates, versions, and anti-virus protection. But there is nothing in the conformance document about this. I became curious and decided to do some research into Yocto.

What I discovered about Yocto is concerning. Yocto is an open source project. Open source projects emphasize openness and collaboration amongst their members, and they have historically followed a decentralized model. Members often share code, ask and answer questions, and help and support each other as part of the community. Security is usually a collaborative effort, but Yocto now has a security team, a new and welcome development.

Additionally, “Without fanfare, Yocto Project touches most people’s lives without their knowledge,” notes Richard Purdie, lead Architect at Yocto Project. “At least half the world’s internet traffic passes through routers built using Yocto. Add in mobile phone masts, software in cars, and software inside core server components. Billions of devices around us are relied upon daily, making it a key piece of easily overlooked critical infrastructure software.”[iii] Even if Yocto was not being used to generate software for ES&S election infrastructure, it is critical because it is ubiquitous.

How open source communities work sounds quite idyllic, and it can be. However, it is not so idyllic when there is a direct push from the U.N. and globalist governments like Germany and China to centralize, govern, and monitor these open source communities and projects. This is done through direct funding grants, membership fees, participation in leadership, and everyday community collaboration, all under the guise of sustainability and the public good. It sounds like USAID, only this funding is to subvert critical open source communities and software. There has been an increase in momentum for this centralization and governance in the past three years because the critical nature of these communities and what they produce has come to the attention of the “powers that be.” The fact that ES&S is generating software for critical election infrastructure using tools from an open source project with these issues increases the likelihood that the software has been compromised.

The Evidence

1. Yocto is a project under the umbrella of the Linux Foundation, a non-profit group established in 2000 to support Linux development and open-source software projects.[iv] Umbrella projects are allocated resources from the Linux Foundation parent and receive funding from membership dues. Yocto is also in partnership with other open source projects like OpenEmbedded and provides financing for those open source projects as well.[v]

2. Some of the Yocto participating organizations (ones that were willing to make their participation public) include Meta, Huawei (Chinese company), Dell, AWS, KCE Group Services (Venezuelan company), Linaro (Chinese CEO, non-profit), and others.[vi] I am assuming that ES&S since they use Yocto, is also a participating organization. However, they have decided not to publicize this.

3. Yocto received an infusion of funding in 2023 from the Sovereign Tech Fund[vii] , now known as the Sovereign Tech Agency - this "is a funding program initiated by the German Federal Ministry for Economic Affairs and Climate Action, aimed at supporting the development and maintenance of open-source software and digital infrastructure. Established in May 2022, it focuses on enhancing technological diversity and resilience in the open-source ecosystem."[viii] This is fully supported by the U.N. as well – they appear to be hand in glove to centralize and manage open source.

4. The Linux Foundation probably provides much funding for Yocto since Yocto is under its umbrella. However, it is hard to tell, given the lack of transparency in the finances of these non-profits. There are some areas of concern about the Linux Foundation:

    a. The Linux Foundation has aligned its goals to the U.N. Sustainable Development Goals[ix]

    b. The Linux Foundation believes open-source communities need assistance becoming "sustainable" (ensuring appropriate funding). Therefore, they "suggest that open source work is consolidated under a single banner, such as an Open Source Program Office (OSPO) at companies. Finally, we suggest incorporating contribution monitoring into the organization's pipeline. We developed a toolkit to help improve data capture and monitoring."[x]

    c. The U.N. is pushing for establishing OSPOs – Open Source Program Offices – OSPOs for Good to "champion OSPOs as a global network for good" and 'enablers of global cooperation.'[xi]

    d. The Sovereign Tech Agency, mentioned above as a source of Yocto funding, is very tightly associated with the United Nations and its goals. The United Nations hosted the 2nd annual OSPOs for Good conference at its headquarters. The Linux Foundation and Sovereign Tech Agency were participants/speakers.

    e. There is a definite push to centralize/govern open source communities under the auspices of the U.N. and an effort to get governments, like Germany, more involved to make sure this happens for the sustainability of critical open source technologies. Also, centralization and monitoring are needed for security – to prevent another xz utils incident, which was stopped from going global by sheer "luck." Never let a crisis go to waste.

    f. Jim Zemlin – executive director of the Linux Foundation and Board member: "Jim has been recognized for his insights on the changing economics of the technology industry, and he is a regular keynote speaker at industry events. He advises various startups, including Splashtop, and sits on the boards of the Global Economic Symposium, Open Source For America, and

Chinese Open Source Promotion Union."[xii] Based on this description, the executive director has strong ties to Chinese and globalist endeavors.

g. China has been increasing its influence in open source – "Today, China's open source community has become a driving force behind some of the most influential projects in the cloud-native ecosystem."[xiii] The article mentioned Kubernetes, but as you will see below, it also includes the Linux Foundation.

h. Two board members are Chinese – Peixin Hou (Huawai) and Xin Liu (Tencent), representing Chinese-owned companies. Other board members include people from large multinational companies, including Microsoft, Ericsson, Oracle, Intel, Sony, and others.

i. Platinum member companies (which provide a large part of the funding through annual membership fees) include Ericsson, Huawei, and other large multinational companies. Platinum member companies, given the large membership fees (500k per year), very likely have a lot of influence over how things are run.

j. Gold member companies ($100k per year) - Ali Baba Cloud (Chinese), Blackrock, Webank (Chinese)' and others.

Getting out of the Linux business

What are a few of the specific projects receiving that funding? Here's four that have an entirely unknown amount of funding:

- "**LF Public Health**" - tasked with creating vaccine passport systems.
- "**LF Energy**" - tasked with climate change related initiatives.
- "**The Overture Maps Foundation**" - tasked with creating a Google Maps alternative.
- "**The Open Metaverse Foundation**" - tasked with creating a Facebook/Meta "Metaverse" competitor.

This is worth repeating: We do not have detailed financial information on these sub-foundations. They don't provide individual annual reports for each (as they are all under the "Linux Foundation" umbrella) and there doesn't appear to be *any* source of documentation, publicly available, to figure out those details.

The fact is, some of these projects may receive many times what the Linux kernel receives. Others may receive a tiny fraction of that amount. We simply don't have

Very interesting article that I found as I was doing research on this – worth a read. See excerpt above.

Shared post - Linux Foundation decreased Linux spending to 3.2% in 2022.

---

[i] "The Yocto Project is an open source collaboration project that provides templates, tools and methods to help you create custom Linux-based systems for embedded system deployments in connected edge devices, servers, or virtual environments, regardless of the hardware architecture."i An embedded system is a small computer that's built into a larger device or machine to control it and allow the user to interact with it. ES&S is using a Yocto project image on its DS200 and DS300 tabulators – the computers that count the votes.

[ii]https://www.eac.gov/sites/default/files/voting_system/files/ESS%20EVS%206300%20Certificate%20and%20Scope%20of%20Conformance.pdf
[iii] https://www.yoctoproject.org/blog/2023/10/10/sovereign-tech-fund-boosts-yocto-project/
[iv] Linux Foundation - Wikipedia
[v] https://www.yoctoproject.org/blog/2023/10/10/sovereign-tech-fund-boosts-yocto-project/
[vi] https://www.yoctoproject.org/about/participants/
[vii] https://www.sovereign.tech/tech/yocto
[viii] https://www.linuxfoundation.org/blog/sovereign-tech-fund-boosts-yocto-project
[ix] Sustainability | Linux Foundation
[x] Understanding the State of Open Source Funding in 2024
[xi] OSPOs for Good 2024 | Office for Digital and Emerging Technologies
[xii] Leadership | Linux Foundation
[xiii] https://www.computerweekly.com/news/366608127/The-rise-and-rise-of-open-source-in-China