Bradley M. Kuhn
+1-212-461-3245
bkuhn@sfconservancy.org
137 Montague St STE 380
Brooklyn, NY 11201–3548
USA

Re: Cybersecurity for Free and Open Source Software

1 February 2022

Joseph Biden, President of the United States
Chris Inglis, National Cyber Director
Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology
The White House
1600 Pennsylvania Avenue, N.W.
Washington, DC 20500

Dear President Biden, Deputy Advisor Neuberger, Director Inglis, et al:

Firstly, we appreciate very much that your administration has taken the issue of the log4j software vulnerability so seriously, and also appreciated President Obama's efforts to take the OpenSSL vulnerability (so-called "HeartBleed") seriously during his administration. While we at the Software Freedom Conservancy believe deeply that Free and Open Source Software (FOSS) is a better and more reliable method to develop software, we also readily acknowledge that no method of software development is perfect. (Flaws can and do occur.) However, sound planning — which includes meaningful investment in infrastructure — will not only limit potential vulnerabilities, but is also essential to respond to them adequately when they do inevitably occur.

As you likely agree, our nation's infrastructure and national security — both of which increasingly depend on software — demand this type of care and attention. While we are pleased that your administration has taken some basic steps to focus on this critical issue, we send this open letter to request necessary improvements to the current methodology that your administration is using to address the issue of software security vulnerabilities in FOSS. In short, your administration has taken a great first step — one which the for-profit software industry has embraced — but we have deep concerns. We expect the powerful technology industry to resist the mandatory steps necessary to ensure the security of FOSS. This is due to the basic fact that the necessary changes mean that companies and their shareholders will have to live with more modest profits if your administration does demands the necessary changes to ensure cybersecurity for FOSS.

Your meeting earlier this month included some important entities, but unfortunately was biased in one specific direction. Specifically, we observed that the meeting only included representatives from companies and organizations that prefer a specific form of FOSS — the form of FOSS that allows entities to change the software into their own proprietary technology. Roughly speaking, there are two forms of FOSS: *non-copylefted FOSS*, which allows vendors to take the publicly available software and make trade-secret changes; and *copylefted FOSS*, which — by contrast — is licensed in a manner that *requires* full disclosure of all source code (and the necessary means to repair vulnerabilities in that software) to customers. Non-copyleft FOSS has a fatal flaw: it can easily be incorporated into a proprietary product — including with modifications that may introduce vulnerabilities. Vendors can keep all details about those changes secret from everyone — including their customers and the government. Furthermore, a company may disclose that the software is *based on* a particular FOSS project, which perpetuates a false sense of security. Consumers will often assume that since it's labeled as FOSS, that the key benefits of FOSS de-facto apply — such as easily auditing the software themselves (or hire an third-party firm) to examine the software for vulnerabilities and/or repair discovered vulnerabilities. However, if that FOSS is not under a **copyleft license**, there are no such guarantees. Imagine what can happen when a vendor goes out of business while the customer (who could be the federal government itself) still relies on that software for essential infrastructure.

As one of the leading organizations dedicated to FOSS, we believe it is extremely important to share our expertise at this critical moment. We reiterate our sincere appreciation for your administration's interest and promulgation of Software Bill Of Materials requirements. On the surface, this is a small step in the right direction. We fear, however, that, without meaningful and informed improvements, it merely serves as camouflage and creates a false sense of security. A simple list of software included will give only vague clues as to how to repair vulnerabilities of a vendor's software. No existing SBOM formats actually require full disclosure of software source code — nor means for its modification — to the customers who receive, use, and rely on it. Having an SBOM for your non-copylefted, proprietary software is like having a list of parts that you know are under the hood of your car, but discovering that the manufacturer has welded the hood shut, and forced you to sign an agreement that they could sue you for millions of dollars if you attempt to open it. The car may look safe and secure from the outside, but there is no way to know if the car is safe, reliable and, maintainable.

We are pleased to note that many software companies do chose to use copyleft licenses responsibly and provide the necessary source code; they serve as model citizens for other companies. Interestingly, the early positive revolution of FOSS in the software industry occurred precisely because copylefted FOSS was originally the more common form of FOSS; companies who seek higher profits and control of their customers have campaigned to limit the amount of copylefted FOSS developed. The history behind this is politically intriguing and not unique to FOSS. We see tech companies wielding power in problematic ways in other areas, too. Specifically, they have spent the last few decades pressuring hobbyist creators and small businesses to abandon copyleft licenses. As a result, non-copylefted FOSS is much more commonplace now than ever before (and the reason why this is such a critical issue). We at the Software Freedom Conservancy urge your administration to carefully consider the larger context of software cybersecurity—particularly as it relates to FOSS. We also offer up our guidance and expertise, and hope you will make room for additional seats at the table as you continue discussions and make decisions of this magnitude.

At the White House Meeting on Software Security on January 13, 2002, Big Tech was well-represented, and even overrepresented since it primarily included companies that are considered anti-copyleft. (Indeed, some Microsoft executives in the past have even called copyleft licensing "against the American Way" and a "cancer" on the software industry.) Yet, it is common knowledge in the technology sector that key components of our nation's software infrastructure, such as Linux and the GNU Compiler Collection, were initially written by hobbyists and activists under copyleft licenses. Hobbyists and activists, who are the founders of FOSS, deserve a seat at the table—alongside Big Tech companies and their trade associations—as you continue to discuss these important national cybersecurity issues. The Software Freedom Conservancy is proud to serve and and give a voice to these hobbyist and activities, and we are also willing to recommend other organizations, academics, and individuals if you feel we're not an ideal fit but nevertheless do want to diversify your committees on FOSS cybersecurity.

More generally, we ask that your administration reconsider how it solicits advice on these matters from technologists, and that you not succumb to the monoculture of opinion and manufactured consent from large technology companies and their trade associations. We appreciate that in other areas, your administration has valued inclusivity and actively seeks input from experts who disagree with the status quo. We believe you are truly interested in working on meaningful solutions to this critical issue facing our nation, and thank you for your consideration of our points raised in this letter.

Sincerely,

Bradley M. Kuhn
Policy Fellow
Software Freedom Conservancy