U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Opening Statement

Chairman Bill Foster (D-IL)
of the Subcommittee on Investigations and Ovesight

Joint Subcommittee Investigations and Oversight & Research and Technology Hearing:

Securing the Digital Commons: Improving the Health of the Open-Source Software Ecosystem

May 11, 2022

Good morning, and welcome to our members and witnesses. Thank you for joining us for this important hearing on open-source software security. Cybersecurity is certainly an evergreen issue, and today we're focusing on an important and often overlooked corner of the ecosystem.

Open-source software is software that's freely available for anyone to use or modify. It's the hidden workhorse of the digital ecosystem, and it's a part of software ranging from standalone browsers to complex commercial operating systems.

It's also common in scientific research. For instance, Fermilab – where I worked for many years as a physicist – recently announced the development of open-source software to support the control electronics of quantum computers. Even if you're not working with a quantum computer, it's safe to say that anyone who has used a computer has relied on open-source software, whether they knew it or not.

And yet, despite its importance, open source only draws attention when something goes wrong. In 2014 the Heartbleed vulnerability in OpenSSL prompted a surge of concern and action to save open source on the part of industry and government alike. Good work was done in response to that vulnerability, but interest waned and, in many ways, we find ourselves in the same situation now that we were in back then.

This past winter, the open source community was once more rocked by a dangerous vulnerability. The Log4j project and its vulnerability, called Log4Shell, reminded everyone of the dangers of neglecting open-source software. The sheer breadth of organizations affected by a vulnerability in a single piece of software drove home just how much everyone relies on open source.

This hearing is not meant to look back at the hows and whys of Log4j – others, including other Congressional committees, have already done an admirable job of that. Instead, this hearing will look forward. We will explore how industry and government can cooperate to make sure open source has resources commensurate with its importance. Those resources are not just financial,

but also include technical capabilities, volunteer efforts, and administrative and organizational contributions.

This hearing is also an opportunity to look at some of the dangers of open source that are looming on the horizon. Open-source software is not just in traditional computers; it's in our drones, our AI models, and yes, even quantum computers. We need to fully understand how open-source resources are used in developing technologies to properly assess the risks that those uses represent.

It is important to remember that no software is ever completely secure. Just as, for instance, Windows and iOS will certainly be hacked in the future, there will also be other open-source software vulnerabilities. Rather than seeking perfection, our goal is instead to structure how we think about open source, how we identify the most critical pieces of open-source software, and how we secure that software against intrusion.

If we do that, we will be able to mitigate both the risk of future vulnerabilities and the damage caused when vulnerabilities are exploited.

In a world where our technology so often comes with hidden drawbacks or motivations, open-source software is often a charmingly utopian exception. At its best, it is simply people creating software out of passion, and sharing out of a desire for others to benefit from the fruits of that labor. It empowers people of all backgrounds and levels of technical ability to build upon the work of others and find or make software suited to their needs.

There is something wonderful about that. I hope that through our conversation with our witnesses here today we can contribute to the future of safe and secure open-source software.