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

Chairwoman Eddie Bernice Johnson (D-TX)

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. Thank you everyone for joining us for this joint subcommittee hearing. I especially want to thank Chairs Foster and Stevens, as well as Ranking Members Obernolte and Feenstra, for their leadership on the important issue of open-source software cybersecurity.

Cybersecurity is a perennial problem. It is one we have frequently examined here in the Science Committee. Nearly one year ago, we held a hearing on ways to improve the cybersecurity of software supply chains. Our expert witnesses spoke of a need to improve the security of open-source software to protect the entire software supply chain.

Their foresight was astute. At the end of last year, a vulnerability called Log4Shell (log-four-shell)was found in a piece of crucial and widely used open-source software. Thousands of organizations and systems were affected, and the work of protecting those systems is still ongoing. One leading cyber company called this software exploit "the single biggest, most critical vulnerability ever." It is clear that we must dedicate more resources to securing open-source software.

Our government agencies have been working hard to support this goal. NIST, in particular, has released extensive guidance for the successful development of secure software. An executive order from last May pushed the agency to do even more. They have released a definition of critical software that can guide the focus to the most important pieces of open-source software. And just last week, NIST issued updated guidance on supply chain risk management, completing a two-and-a-half-year process for how best to handle software in the supply chain.

But NIST cannot solve this problem alone. This is a key moment for government to partner with industry. Our expert witnesses can provide perspectives on open source informed by their time spent working for industry, non-profits, the military, and the civilian government. Their insights will help us understand both the technical challenges and the underlying culture of the open-source community.

Armed with that understanding, we can steer resources towards where they will do the most good. We can also map out the complex ecosystem of those who produce open-source software,

and provide training and other resources to help make it secure. We can find more ways for agencies like NIST to collaborate with industry experts and other folks developing and maintaining open-source software across the country.

We will also look to the future. Open source is a critical part of many developing technologies. It enables the growth of artificial intelligence and makes the technology accessible to a wider range of people. Yet the dangers posed by open-source software exist here as well. Bad actors will inevitably try to manipulate open-source datasets to control AI. This is a frightening possibility as AI becomes a bigger part of all our lives.

The risks of open source should not outweigh its benefits. Properly resourced and made secure, open-source software can do a lot of good for a lot of people.

I welcome the recommendations of our expert panel to guide us in that goal.

Thank you, and with that I yield back.