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

Chairwoman Haley Stevens (D-MI)
# of the Subcommittee on Research and Technology

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 this joint hearing of the Subcommittee on Research and Technology and the Subcommittee on Investigations and Oversight. I would like to thank my esteemed colleagues, Chairman Foster and Ranking Member Obernolte, for leading this timely and needed hearing.

A supply chain is only as strong as its weakest link – and the times when the weakest link happens to be cybersecurity, we see devastating ripple-effects and wide-ranging aftershocks. We can no longer operate off yesterday's mindset and only view supply chain cybersecurity as an IT problem. In order to strengthen America's collective cybersecurity, we must examine all the vulnerable links in the chain. I am proud to be here today to encourage Congress to explore various avenues the government can engage the open-source community to identify and remedy vulnerabilities.

One year ago, President Biden released an Executive Order called "Improving the Nation's Cybersecurity." This executive order tasked the National Institute of Standards and Technology to create essential standards for critical software, software supply chain risk management, among other tasks. In the coming days, NIST is expected to publish its final piece of guidance required by the executive order, but the agency's work to secure the Nation's software is far from finished.

One aspect of supply chain security we need to take an in-depth look at is the open-source vulnerability landscape. Many leading companies and organizations don't recognize how many aspects of their critical infrastructure depend on open source. Open-source software code is available to the public, for anyone to use, modify, or inspect. Many elements of NIST's software guidance can be applied to open-source software, such as the secure software development framework. However, they do not address many of the unique challenges inherent in the open-source software ecosystem, from inadequate resourcing to vulnerability detection and mitigation.

A vibrant open-source ecosystem is an engine for U.S. competitiveness and growth. This ecosystem benefits Americans every day, including in my home state of Michigan. During the pandemic, open-source applications tracked open hospital beds and helped Michiganders access food for their families when schools were closed. But there is real risk if we leave critical open-source software vulnerable to attack. As both the Heartbleed and Log4J (*pronounced log-4-J*) incidents have revealed, open-source software issues can be a threat to our Federal agencies and businesses across the country.

There is good work underway, but still much more the U.S. scientific enterprise can do to secure open-source software repositories. Last year, I introduced the *NIST for the Future Act*, which is part of the *America COMPETES Act* that we will hopefully send to the President's desk soon. This bill would require NIST to expand its current efforts by assigning severity metrics to vulnerabilities in open-source software and producing voluntary guidance to help entities that maintain this software to secure it.

The National Science Foundation has played an important role in funding many open-source software and data repositories. NSF is planning to award grants to help secure elements of the open-source ecosystem as part of its new program "*Pathways to Enable Open-Source Ecosystems*," or POSE. I am encouraged by these efforts, which will be further bolstered once we enact and fund the *NSF for the Future Act* that is also in COMPETES.

Securing open-source software is fundamentally a resource problem. I believe the Federal government can play a role identifying vulnerabilities, providing resources where industry might not, and driving long-term structural security improvements throughout the open-source ecosystem. These efforts are most effective when done in coordination and collaboration with the private sector.

I welcome the recommendations of this expert panel on how to improve the coordination between the public and private sector on securing the open-source ecosystem, and any additional recommendations you may have for this Committee to consider.

I want to again thank the witnesses for being here today to help us tackle these challenging issues. I yield back.