COMMITTEE ON SCIENCE SPACE & TECHNOLOGY
REPUBLICANS

Opening Statement of Investigations & Oversight Subcommittee Ranking Member Jay Obernolte

As prepared for delivery

Joint Investigations & Oversight and Research & Technology Subcommittees Hearing - Securing the Digital Commons: Open-Source Software Cybersecurity

May 11, 2022

Good morning. Thank you, Chairman Foster and Chairwoman Stevens, for convening this hearing. And thanks to our witnesses for appearing before us today.

We are here today to discuss the benefits and risks of open-source software and to explore the ways that government and industry can work together to improve open-source cybersecurity. I look forward to learning more about the solutions we're trying to catalyze, and the collaborations that are already underway, to solve some of the cybersecurity challenges with open-source software. I'm hopeful that today's hearing will be a productive discussion that will help us learn from the past to improve open-source cybersecurity for the future.

At the risk of oversimplification, open-source software is essentially code that can be used, modified, and distributed by anyone. This code can comprise an entire standalone program, like an open-source web browser or operating system. It can also comprise a small component or specific function built within a larger standalone program, including proprietary and commercial products. In short, open-source software touches almost every facet of our digital ecosystem.

The ubiquity of open-source software is a function of the benefits and advantages it provides. Its open nature expands the breadth and depth of users that can contribute to, improve, and ultimately use the software. It is also flexible and can be tailored to the specific needs of the end-user without having to reinvent the wheel. Leveraging open-source software can save developers' resources, which can, in turn, be reinvested to foster novel and innovative open-source solutions.

The open nature of open-source, however, is not without inherent risk. Its open and collaborative, community-driven nature means that open-source code can be freely edited or changed. The quality and security of changes or contributions are often dependent upon the governance, structure, and policies of the relevant open-source project or community, which can make it difficult to adequately assess the quality and security of various open-source software.

Understanding when open-source has been modified, what changes have been made, and a method for verification or certification that such changes are sound would go a long way toward improving the overall security of open-source software. I'm particularly excited to learn more about Platform One and the work the Air Force is doing in this space.

The ubiquity of open-source also represents a risk. Since open-source software touches every facet of our digital ecosystem, a security vulnerability in open-source code could have a ripple effect throughout the digital economy if exploited. An example of this is the recent Log4Shell vulnerability in an open-source library. Despite being discovered more than six months ago, efforts are still underway to patch vulnerable systems. One of the pervasive issues that has hindered quick remediation is that it has been difficult to determine where the vulnerable open-source library has been used. It is so embedded in the digital ecosystem that cyber professionals are still uncovering instances of its use.

While a software bill of materials or SBOM—effectively an ingredients list for software—may not have prevented the vulnerability from being written into the open-source code in the first instance, it certainly would go a long way in helping to remediate and patch the issue on the back end. I look forward to hearing more from our experts today on how to employ SBOMs to improve open-source cybersecurity.

Finally, I think that the cybersecurity of open-source software could be improved if we can figure out a method for classifying or categorizing open-source instances that range from the critical to the non-critical.

This would help open-source communities and their contributors to prioritize the most important open-source products for heightened scrutiny. I look forward to hearing more about some of the efforts that the Linus Foundation and OpenSSF have stood up to do just this.

In closing, I think it is important to articulate plainly that open-source security is cybersecurity. Our information and communications infrastructure is only as strong as its weakest link. I'm hopeful that we can have a productive discussion today to put us on the path toward shoring up our digital infrastructure by improving the security of open-source software for the future.

Thank you, Chairman Foster, for convening this hearing. And thanks again to our witnesses for appearing before us today. I look forward to our discussion.

I yield back the balance of my time.