COMMITTEE ON SCIENCE SPACE & TECHNOLOGY
REPUBLICANS

Opening Statement of Research & Technology Subcommittee Ranking Member Randy Feenstra

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

May 11, 2022

Thank you, Chairman Foster and Chairwoman Stevens for holding today's hearing. And thank you to our expert witnesses for your participation here today. I look forward to the discussion and learning more about ways to improve open-source software security.

Open-source software is a key component of modern software development. Over the past two decades, open-source software has become widely adopted, and has a vast number of applications from powering small personal devices to supercomputers.

Open-source software is largely created by volunteers on their own time who often do not receive any sort of compensation for their work, but rather work on projects they are passionate about that may be useful to others.

It is collaborative in nature, as it is available for anyone to use, modify, and share for better usability and accessibility.

Additionally, open-source software is often available free of charge, which allows users to have access to technological capabilities that they may not be able to otherwise.

While open-source software offers many benefits, there are also risks involved in using this type of software. One of the main challenges of open-source software is the lack of dedicated resources for security and internal vulnerability checks. If open-source software has a security vulnerability, it could cause widespread harm to all users.

What's more, because open-source software is typically part of another software component, it may be tough to determine when and where patching may be needed.

Critical technologies such as artificial intelligence often have their own unique challenges when it comes to open-source software security. For example, large datasets are used to train artificial intelligence systems to improve their accuracy. If malicious actors manipulate or poison these datasets the models will be corrupted and could produce inaccurate or harmful outcomes.

Federal science agencies are actively working to address some of the ongoing challenges to open-source software security. The National Institute of Standards and Technology (NIST) has developed standards and best practices that apply to open-source software. NIST also produced guidance for managing compromised cyber supply chains and fixing vulnerabilities.

On May 12, 2021, the President issued an Executive Order on “Improving the Nation’s Cybersecurity” to enhance the security and integrity of the software supply chain. This Executive Order required NIST to create new security standards for software, including open-source software.

The National Science Foundation (NSF) also recently launched a new program called “Pathways to Enable Open-Source Ecosystems” (POSE) to harness the power of open-source development for the creation of new technology solutions. Additionally, many NSF-funded research projects produce open-source software, hardware, or data platforms that promote further innovation.

It is important that security risks to the open-source ecosystem are adequately addressed and that the necessary resources are dedicated to bolstering cybersecurity.

Improving our nation’s cybersecurity is particularly important to me, as my district has recently been targeted by malicious cyberattacks to our agriculture supply chain.

I hope we can have a productive discussion today about improving security in open-source software without compromising its benefits. I once again want to thank our witnesses for being here to discuss this important topic, and I look forward to hearing your solutions.

I yield back.