OPENING STATEMENT
RANKING MEMBER ROB PORTMAN
Responding to and Learning from the Log4Shell Vulnerability

February 8, 2022

Thank you, Senator Peters. And thank you to our witnesses for joining us.

Today we will hear from organizations who each provide distinct perspectives on log4shell, a pervasive cybersecurity vulnerability in a Java software library called log4j.

Log4j is open source software meaning -- unlike proprietary software -- it is available for anyone to use and access free of charge. Open source software like log4j has unique advantages and disadvantages relative to proprietary software that we will discuss at today's hearing.

- For example, open source software may not have the same resources and number of full time employees focused on keeping it secure and up-to-date.

- On the other hand, because of the nature of open source software—everyone can see it and submit suggestions to make changes and improvements to those who manage the projects—security becomes a crowd-sourced exercise. This means security experts have many opportunities to identify and fix bugs. In fact that's how the log4shell vulnerability was discovered—by someone outside the organization that managements log4j.

Open source software is also ubiquitous in the software industry and underpins much of our economy and numerous other software products. Companies benefit from not having to re-invent the wheel when developing their products. As a result of these dependencies, a vulnerability in open source software can affect many other software products that rely on it.

The log4shell vulnerability is a particularly severe vulnerability because the code is in so many places, the vulnerability is easy to exploit requiring less than a sentence, and because it provides a high level of access. To put it in perspective, CISA Director Jen Easterly described it as "the most serious vulnerability" she has seen in her decades-long career.

This is not the first severe vulnerability in open source software either. In 2014, there was another open source vulnerability, called "Heartbleed," that allowed normally protected information to be stolen. Similar to log4j, the open source product with the Heartbleed vulnerability was widely-used, making the response challenging.

Then, in 2017, Equifax suffered a massive breach due to a vulnerability in an open source Apache Software Foundation product, called Apache Struts. Log4j is also maintained by Apache, who is here today. When I was Chairman of the Permanent Subcommittee on Investigations, I released a bipartisan report with Senator Carper on Equifax's failure to remediate the vulnerability, compromising the personal information of roughly 147 million people. I am concerned that without prompt remediation of the log4shell vulnerability, we run the risk of experiencing one or even more incidents of the same magnitude as the Equifax breach.

It's clear that issues involving the security of open source software have been around for a long time. I'm looking forward to hearing from our witnesses, who have a wide variety of perspectives, on how we can address these longstanding challenges.

This hearing builds on a previous briefing on log4j the Committee received just over a month ago from the National Cyber Director, Chris Inglis and CISA Director, Jen Easterly.

In that briefing we learned several things. First, we learned this vulnerability is widespread. Hundreds of millions of devices have the vulnerability. David Nalley, the President of the Apache Software Foundation is here and I look forward to a conversation about the disclosure and subsequent remediation of the vulnerability.

Second, we learned that fixing this vulnerability is not as easy as Apache putting out a one-size-fits-all patch. Vendors who used this vulnerable code, not knowing it was vulnerable, will have to issue their own patches for their own products. This makes the response even more complicated and time consuming. I'm glad Brad Arkin, a Senior Vice President and the Chief Security and Trust Officer of Cisco is here to provide the perspective of a company that had this vulnerability and remediated it.

And finally, we learned that because this response will be drawn out, attackers will have time to exploit the vulnerability and launch attacks. Just because a

vulnerability exists, does not mean that it's actively being used to attack an entity. But the concerning reality today is that our nation does not know how widespread attacks leveraging this vulnerability are. That is one reason it is more important than ever to pass my *Cyber Incident Reporting Act* legislation with Senator Peters—to ensure that our nation has visibility into attacks exploiting the log4shell vulnerability against critical infrastructure. I'm looking forward to hearing from Jen Miller-Osborn from Palo Alto about their work tracking and analyzing the threats stemming from this vulnerability.

Open source software is inextricably woven into every bit of software we use every day. The answer to this problem is not to stop using it. However, I think we can use this hearing to understand how we can address security risks in open source products working within existing processes and strategically investing time and money to support the open source community.

I am hopeful that we will leave this hearing with a better understanding of the risks and benefits of open source software and what the role of the Federal Government should be in supporting efforts to increase open source security.

Thank you for convening this hearing, Mr. Chairman. I look forward to the testimony of our witnesses.