Chairman Peters Opening Statement As Prepared for Delivery
Full Committee Hearing: Responding to and Learning from the Log4Shell Vulnerability
February 8, 2022

I’d like to thank our witnesses for joining us to examine the vulnerability in Log4j, which our government’s top cybersecurity experts have called one of the most severe and widespread cybersecurity risks ever seen.

This bug, which can be exploited by only typing in 12 characters, can allow cybercriminals and foreign adversaries to remotely access critical American networks.

Reportedly, the Russian Federation has already taken advantage of this vulnerability to perpetrate cyber-attacks against Ukraine. While I hope that situation deescalates, we must be prepared to protect our systems from similar attacks from the Russian government and the criminal organizations they harbor, who could exploit this or other vulnerabilities to compromise American networks in retaliation for our nation’s support for Ukraine.

The weakness in log4j is just one example of how widespread software vulnerabilities, including those found in open source code, or code that is freely available and developed by individuals, can present a serious threat to our national and economic security.

In terms of the amount of online services, sites, and devices exposed, the potential impact of this software vulnerability is immeasurable, and it leaves everything from our critical infrastructure, such as banks and power grids, to government agencies, open to network breaches. We have already seen how cyber-attacks on these critical entities can have catastrophic impacts on the lives and livelihoods of Americans.

That’s why I am grateful to our private sector partners, the open source community, and the federal government who have swiftly mobilized to respond to this threat.

And, while I am grateful to the Administration for their quick action and transparency with Congress, I remain concerned that we may never know the full scope and impacts of this vulnerability, or the risks posed to our networks that the American people rely on each and every day.

That is why I will continue to monitor and track this latest cybersecurity threat, and work with my colleagues to help ensure the government is receiving timely information about cybersecurity threats, so we can formulate a comprehensive strategy to fight back against hackers and hold foreign adversaries accountable for targeting our networks.

That includes urging the Senate to pass landmark legislation that Ranking Member Portman and I authored and passed out of this Committee, to require critical infrastructure companies and civilian federal agencies to report to the Cybersecurity and Infrastructure Security Agency when they are hit by a substantial cyber-attack.

Our efforts will also ensure that critical infrastructure owners and operators are reporting ransomware payments. Our government's top cybersecurity experts would analyze this information and use it help private sector organizations that provide essential services to the American people, protect their networks.

This legislation will help our lead cybersecurity agency better understand the scope of attacks, including from vulnerabilities like Log4j, to warn others of the threat, prepare for potential impacts, and help affected entities respond and recover.

And, by modernizing the government's cybersecurity posture by passing FISMA reforms, we can help prevent online assaults against federal agencies, from foreign and domestic actors who seek to degrade our national and economic security.

I'm pleased that yesterday, Ranking Member Portman and I introduced a bipartisan package that combines these critical efforts into one bill, along with our bill to modernize FedRAMP that we hope to move forward soon.

Today, I am honored to welcome a panel of experts, who can discuss this vulnerability in greater detail, how it has been exploited, how they have worked to mitigate its impacts, and broadly discuss how we can work to secure modern software that commonly contains open source coding.

I look forward to hearing their thoughts on how to improve our government's overall ability to respond to open source vulnerabilities like log4j, and ensure we have comprehensive plans and procedures in place to prevent a cybersecurity crisis of this magnitude.