Safeguarding the Federal Software Supply Chain- United States House Committee on Oversight and Accountability

Good afternoon, Mr. Chairman and members of the subcommittee. My name is Jennifer Bisceglie, Founder and CEO of Interos Inc. Thank you for inviting me to testify as a subject matter expert on supply chain risk management, with today's focus on securing the Federal Software Supply Chain.

My company, Interos, is built on almost 30 years of personal experience in global supply chain and IT implementation experience. Over the past 19 years, since I started Interos, I have seen the discussions turn from a lack of understanding of the issue; to simple compliance and resiliency intended to ensure business operations continue even if supply chains were interrupted; and now to product integrity and software pedigree to preempt and protect from intentional malicious attack.

Interos has been working this issue for multiple Federal agencies as well as the world's largest commercial customers, firsthand, for 19 years. Our initial response was to set up the first Supply Chain Risk Management global threat information Center back in 2012, which offered services and capabilities to help both the public and private sector organizations implement supply chain risk frameworks, conduct supplier audits, and conduct open-source research to identify potential threats with current or future suppliers – this was simply to (1) understand there was an issue to be concerned about, (2) how to evaluate the issue and provide a commensurate response, and (3) most importantly, educate and train the people involved as removing the fear of such a borderless and often invisible attack left most customers inert.

At the same time, and to support our customers, we began the buildout of what is now the world's largest business relationship graph. Using artificial intelligence, Interos is responsible for mapping and continuously monitoring the business relationships, business dealings and supply chains of more than 300 million businesses around the world and the billions of relationships between them.

I will first share some of our observations and then follow those with some recommendations.

- According to Mandiant, the leading threat intelligence company, supply chain attacks through software are up 700% year over year.
- According to Lineja, a leading software bill of material company that uses technology to allow customers to govern software bills of materials (SBOMs) at an enterprise-wide level, 88% of all supply chain dependencies are invisible to developers

All this being the case, we're still struggling with finding a common definition for supply chain risk management as well as a standard way to measure the challenge. Also, we tend to separate hardware from software from service supply chains, which will continue to create artificial silos and increase the available attack vector for both the intended and unintended enemy. When in actuality, all we're talking about is simply who is doing business with each other and what risks those relationships might entail.

The definition of manufacturing lines vs cyber security vs software bills of material extends deep into the supply chain as both physical and digital working arrangements are increasingly and unwittingly reliant on globally sourced, commercially produced, information technology and communications hardware, software, and services.

To Interos, any 'type' of supply chain security will mandate transparency of where things are coming from, where they are going to, and who has access to them along the way. That should be the definition of supply chain risk management for hardware, software or services.

Our second observation is that supply chain risk management must be viewed as an investment versus an expense. Interos has worked with multiple Federal mission critical organizations – including being the selected technology for the only true supply chain risk management shared service in the world, currently hosted in the US Navy - to help them provide the transparency and pedigree of what is coming into various offices in the Navy – as well as the ongoing monitoring of said national security systems – in a proactive and information sharing way. By investing in the technology and training needed, the US Navy has been able to expand to multiple programs as well as other agencies – including Missile Defense Agency and the DoD CIO. What cannot be stressed enough, by using technology to complement the needed cultural shift at the leadership level, change is happening, and pockets of supply chain security are being realized. However, none of this is happening through a funded program of record. We're still handling supply chain security across the Federal Government in a 'rob Peter to pay Paul' fashion.

Now to our recommendations: From our perspective, Congress can take four steps to better protect our Nation's critical infrastructure.

First, awareness and education have to start at the top in order to be adopted by those actually executing the mission. In our experience, the level of awareness of the challenge varies across federal agencies, as does their level of attention to managing their supply chain risk. Awareness and education are critical to communicate that supply chain risk impacts everyone within the federal infrastructure.

Second, fund the program, assign someone within each agency to own the issue, and measure the success. In 2020, GAO published ***GAO-21-171***, which was titled ***'Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks'*** – unfortunately there is little enforcement behind this report. Without the top-down support within the agency, without an owner of the concern, and without funding, these programs are being bootstrapped and implemented in various non-standard fashions – which is not conducive to effective protection. On the positive, the ***Federal Information Security Modernization Act (FISMA) of 2023*** does begin to move us in the right direction – in stressing cataloging, coordination and moving towards a risk tolerance-based approach that can be flexible based on the event and impact of an occurrence. And, of course, ***EO 14028, Executive Order on Improving the Nation's Cybersecurity,*** which aligned much of the cybersecurity community and provided such collaboration and frameworks as the common Supply-chain Levels for Software Artifacts (SLSA) framework as part of the Open-Source Security Foundation.

Third, make supply chain security for hardware, software and services, be the cost of doing business not only with the Federal Government, but also between private sector organizations. How many more examples of the ripple effect of our business connections and how easily disturbances can be shared – everything from NotPetya and the Target Breach to Log4j, MoveIt, SolarWinds – not to mention we're also target for countries such as China, Russia and Iran. Why do we let public and private sector organizations continue to fund service-based supplier risk assessments and not leverage technology and continuous monitoring? We've now seen multiple approaches prioritized for software security – including CISA's Security By Design – yet we treat it as a compliance activity vs a risk-based decisions that needs continuous monitoring and adjusting. Truly being able to not just implement but achieve the desired outcomes of such Executive Orders such as EO 13873, "Securing the Information and

Communications Technology and Services Supply Chain," and EO 14034 "Protecting Americans' Sensitive Data From Foreign Adversaries" takes advancement to at least the level of the enemy we're fighting against vs spending the resources fighting against ourselves.

Finally, implement contractual language that works and will be used such as EO 14028, "Improving the Nation's Cybersecurity, Section 3.5. In addition, there are multiple industry associations working on standards for supply chain risk management, such as those in the room today. Doing as much as possible via internal policy changes and contractual language as a way to inform suppliers of how to do business with you and to mitigate risks coming into your organization is a much less expensive way to approach the problem than regulation and legislation.

In conclusion, the solution needs to be viewed as an investment in national security, not just another expense, and needs to include upskilling the people buying and using software supply chain security requirements – not just putting a requirement in a contract. It's the use of the SBOM – to KNOW/PREVENT/FIX as Google likes to say – that will make the difference for the Federal software supply chain, this country's security posture and our global competitiveness.

Thank you for the opportunity to present our views. I look forward to answering any questions.