U.S. – China Economic and Security Review Commission
Written Testimony
"U.S.-China Competition in Global Supply Chains"

June 9, 2021

Jennifer Bisceglie
CEO, Interos Inc.

Commissioners Borchoff, Goodwin, and other members of the Commission, thank you for the invitation and opportunity to speak with you today on safeguarding U.S. defense-critical supply chains as it relates to military readiness.

Interos is a company I founded 17- years ago to evaluate risks in the global economy and the business partnerships, alliances and distribution networks that make up our supply chains. This company is built on my 30 years in the global supply chain industry, having helped multiple US-based companies create maximum advantage from different skillsets, labor pools and competitive business arrangements with partners around the world.

During those years, I've watched risk concerns in the supply chain move from quality to physical security, to resiliency and now to product integrity and the role of the digital connection, i.e., cyber. Over the last few years, we have seen supply chain crises increase exponentially with COVID, SolarWinds, the Suez Canal blockage, and most recently with Baby Formula. As Interos noted in its 2018 report for the Commission, the federal supply chain is reactive. Meaning, until we as a country adopt a centralized government role for supply chain risk management (SCRM), we will continue to suffer consequences of supply chain disruptions whether it be in our Federal IT networks, which was my testimony in 2018, or the discussion of military readiness.

Before addressing specific areas of today's hearing, I would like to stress that the principles of the 2018 report remain true today, and whether it is 5G, blockchain, the Internet of Things, or any other emerging technology, an underlying foundation for national security – both physical and digital - is an understanding of who the stakeholders are, where vulnerabilities lie, and having a strategy for managing the associated risk. The solution cannot be solely focused on the latest tools and technologies – cultures need to change, and money needs to be spent to educate people on their role in traditional risk management.

Given our position in the market, Interos has had the opportunity to work with public and private sector organizations spanning multiple industry verticals and the situation is always the same – if the organization doesn't take a focused and comprehensive approach to risk management, prioritized by senior leadership - there will be unnecessary exposure and invariably negative impact.

To further illustrate and outline the current federal posture for supply chain risk management:

1) Federal government laws and policies do not currently address risk management comprehensively. Rather, SCRM has been addressed in a somewhat disjointed manner across the various types of federal information systems, across initiatives designed to protect critical infrastructure or high-value assets and across national security systems as a further subset of federal information systems. Additionally, SCRM is held separate from cyber – and the 2 topics are in reality inseparable.
2) In the current SCRM ecosystem, responsibility for risk management is held at different levels within agencies, resulting in SCRM offices that function largely as under-resourced stovepipes,

often lacking executive sponsorship or oversight, and only catering to the needs and procurement policies of individual programs.

3) Policy needs to be instituted to support effective unclassified information sharing to end the redundant efforts within agencies and to maximize the investment in SCRM programs.

Moving to address the topic areas for today's hearing, I will further outline the current state of our global supply chains, out interconnectedness with China, and the landscape of federal supply chain risk and resiliency.

1. How reliant are U.S. defense contractors on second and third tier suppliers from China? For what sorts of components is reliance or exposure greatest? Where is our dependence greatest? For areas where it is impossible to answer these questions, what obstacles prevent use from understanding the answer?

In a single word, very. Interos recently took a look at just how reliant the US and the UK are on the Shenzhen region:

- 8,900+ US distinct entities buy directly from suppliers in the Shenzhen region.
- This number grows to over 76,000 entities when indirect suppliers at the second tier are included, and 195,700 at the third-tier level.
- 130+ distinct UK entities buy directly from suppliers in the Shenzhen region.
- The number grows to over 11,900 entities when indirect suppliers at the second tier are included, and 29,400 at the third-tier levels.

2. What is the role of industry in mapping supply chains for critical materials and components used in U.S. defense systems? How should the U.S. government engage with industry in this area, and what does industry need (or not need) from the government to implement more robust solutions for achieving supply chain visibility? Where is private-public coordination most needed in securing supply chains critical to national security?

Industry is fully capable of mapping and monitoring supply chains for critical materials and components used in U.S. defense systems – anymore this is the cost of doing good business. Specifically, after the experiences of the past 2.5 years – from a pandemic to cyber breaches to a ship going sideways in a canal, not knowing is not good enough for business anymore. If the US government would request supply chain mapping and monitoring, as a part of normal business for industry, the flow down of this transparency would be included in the cost of the program and the shift would occur in delivery of the service. To be honest, as the world's largest buyer, as long as the US government asks for securing the supplier chains critical to national security – and is willing to pay for it – it will occur.

3. What are countries like Canada, Germany, and the United Kingdom doing to build more resilient and transparent supply chains? What types of requirements are in place in those countries to try and give their governments more visibility into companies' supply chains? In your work with executives, how do they view concentration in their supply chains? What challenges do they face in diversifying their supply chains?

All of these countries have the same or similar challenges to securing and diversifying their supply chains as the US does – so size and scale may change but the problem remains the same.

Unfortunately, when we all started offshoring manufacturing back in the 1990s, we all simply got lazy and left supply chains very global, single threaded and fragile. The good news is, via the education of the past almost 3 years, we all realize that sometimes a global and unknown supply chain is not necessarily resilient - nor does it support National Security and military readiness. We now have the option to change. The challenge is going to be a strong enough desire, the right leadership and the available funding as security comes at a cost. But so does not being secure.

4. What challenges do companies face in mapping and monitoring their supply chains? What solutions or technologies, like artificial intelligence, can companies utilize to better map their supply chains?

While businesses are experiencing an average cost of $184M per instance of supply chain disruption, Interos' recent study showed: (1) Only 11% of organizations monitor supplier risk on a continuous basis and (2) Only 19% have technology (automated/intelligent solutions) in place to gain visibility into interdependencies within their supply chain.

The good news is that there are technologies, including such offered by Interos, that offer continuous mapping and monitoring of supply chains using artificial intelligence. Specifically, the Interos platform ingests real-time data from a wide array or sources both public and commercial. New data is continuously ingested to provide supply chain awareness and our platform utilizes cutting edge technologies, including artificial intelligence, to sift through these large quantities of data. This technology allows us to not only map with accuracy, but also provide expert guidance across multiple risk factors including financial risk and geopolitical risk.

It's worth noting, on average, using Interos' technology results in a reduction of over 8000 hours – almost a full man year – that used to be used for manual supplier assessments. This cannot – nor should it be - replicated by humans. National security and military readiness requires the adoption of the latest technologies and capabilities to get ahead of the negative impact vs always being in response and clean up mode.

5. Can you discuss how different tiers of suppliers may present different threats to U.S. national security? How far down the supply line should companies map?

This is a great question and a hard one, knowing that the malicious actors are 100% augmented by the normal dynamic business process, creating a constantly changing and uncontrollable extended supply chain network. In this, there really isn't a limit of tiers that we should be talking about, we should be mandating that the cost of doing business with the US Government is the requirement for supply chain mapping of your next tier supplier, and flow that down for ongoing illumination, as well as the continually monitoring of the network. Once this expectation is set, the US Government can begin to expect – and to receive – a more secure and operational resilient supply chain.

6. In its work with the Department of Defense, what types of vulnerabilities has Interos identified in supply chains providing critical goods for the military? How might China take advantage of these vulnerabilities, and what would that mean for military readiness?

The vulnerabilities identified are extensive and continuously changing based on what's happening in the world; everything from financial instability to cybersecurity, geopolitical and restricted entities, and now the rise of Environmental, Social, Governance (ESG) and sustainability.

7. The Commission is mandated to make recommendations to Congress. Do you have other policy recommendations would you make based on the topic of your testimony? Specifically, what are several first steps the government should be taking to improve supply chain security?

Interos recommends 4 steps:

Embrace an Adaptive SCRM Process – Military readiness and national security have increased reliance on the private sector and commercial off-the-shelf products. These products have increasingly complex and globalized supply chains, many of which include commercial suppliers which source from China. These supply chains morph over time as companies develop new technologies and partner with new suppliers, thus effective SCRM policies must be able to adapt as well. It's not the supplier we know, it's the embedded and other unknown industry partnerships that potentially cause us harm.

Promote Supply Chain Transparency - Supply chain transparency increases our national security posture by enabling the federal government to source responsibly and securely, and by improving the government's ability act with a ready military at the moment needed – as well as the ability to proactively de-escalate when the opportunity presents itself. The government should partner with industry to push for transparency on the part of all tiers of suppliers according to the level of risk management rigor required (not all programs and suppliers present the same level of risk).

Centralize Federal SCRM Efforts - The U.S. government lacks a consistent, holistic SCRM approach – and does not realize the forever connection of the physical and cyber supply chain as seen in the separate authorities of the DoD, DHS CISA and the SEC. The conflicting and confusing laws and regulations result

in loopholes, duplication of effort, and inconsistently applied policies. Congress and the Executive Branch should encourage information sharing and the consolidation of common federal supply chain risk management efforts.

Craft and Implement Forward-Looking Policy - Future risks will involve software, cloud-based infrastructures, and hyper-converged products, not just hardware and physical weapons. A supplier's business alliances, investment sources, and joint research and development (R&D) efforts are also sources of risk that are not routinely evaluated in traditional SCRM. Identifying these risks and addressing them creatively will be important to the success of federal policy efforts.

In summary, the threat that China poses to U.S. federal supply chains is real, is significant and is growing. Our reliance on China as a supplier will remain high. The time to address the supply chain threat and risk to our Nation's national security ad military readiness is now, not after a major incident, the scale of which we may not yet have envisioned, is realized. I thank you, again, for inviting me here today and will be pleased to take your questions during the remaining time and look forward to future dialog with the Commission.