Witness Statement

Hearing on "Microelectronics: Levers for Promoting Security and Innovation"

U.S. House of Representatives
House Permanent Select Committee on Intelligence
Subcommittee on Strategic Technology and Advanced Research

Rayburn House Office Building
Room 2359

Dr. Lisa J. Porter

20 July 2021

Chairwoman Speier, Ranking Member Stewart, and Members of the Subcommittee, thank you for the opportunity to participate in this important hearing regarding levers for promoting security and innovation in the microelectronics industry.

While people often equate the microelectronics industry with foundries and fabless design houses, the value chain of the industry is highly complex and global in scope, with a vast network of thousands of suppliers performing specialized tasks at many different levels of the lifecycle (e.g., specialty gases and chemicals, silicon wafers, Electronic Design Automation (EDA) software, lithography tools, packaging, and test). The international division of tasks and the interdependencies among the thousands of participants has enabled the growth of the global industry to more than $470B.[1]

In recent years, the global nature of the industry has raised concerns regarding the security of the chips being produced, and of the supply chain that produces them. There are those who would argue for the creation of "trusted" onshore foundries, and for limiting all actors in the supply chain to only those who can be "trusted". Such a perspective is not only naive, but also dangerous. Fortunately, this industry can learn from similar mistakes made by the cybersecurity industry in years past – mistakes that they are now rectifying through widespread adoption of Zero-Trust approaches. The pursuit of "trusted foundries" and "trusted supply chains" – like "trusted networks" – is the opposite of a Zero-Trust approach – it actually makes us more vulnerable to the things we are trying to protect ourselves from. "Zero-Trust" and "trust" cannot co-exist as goals.

Executing the entire semiconductor manufacturing lifecycle inside the U.S. is simply infeasible. But even if we could somehow recreate the entire value chain within our borders - walling ourselves off from the rest of the global enterprise – security is not guaranteed. Perimeter defense methods that assume you can build a secure perimeter around your network or foundry or supply chain and guarantee that everything inside can be "trusted" have repeatedly failed us – Edward Snowden was a stark reminder of this almost 10 years ago; recent cyberattacks launched through access to U.S. company software (e.g., SolarWinds) have served to reinforce the lesson.

[1] This was the total for 2018; the World Semiconductor Trade Statistics Market Forecast predicts approximately $450B in 2021.

The Zero-Trust philosophy assumes that everything in a complex system (e.g., supply chains, networks, software) either has been or will be compromised, regardless of location. It advocates for the use of data-driven, quantitative risk assessment and management techniques. And importantly, its focus is on resilience – ensuring that when a risk materializes, its impact is minimized (not eliminated). It is important to note that not all risks are malicious in nature – often, unintentional human mistakes, or significant weather events or natural disasters, can produce negative consequences, if resilience has not been emphasized.

If we look at this complex global industry through the lens of Zero-Trust, then, what is needed? First and foremost, the establishment of quantitative, measurable security standards along the entire lifecycle should be a major focus of our efforts. The DoD has recently begun such work in collaboration with the commercial sector through its emphasis on quantifiable assurance in programs that leverage the fact that the data that commercial fabs already collect for quality control can also be used for security standards, but this work needs to be broadly supported and accelerated. In the recent past, the DoD tried to obtain what it needed by using "trusted foundries", which left it vulnerable to the flawed perimeter-defense approach, as well as unable to access state-of-the-art capabilities available to the rest of the world. During the past few years, the DoD has pivoted to a Zero-Trust approach to accessing microelectronics that aligns its incentives with those who will be driving the demand signal for this industry over the next decade – to include the telecom, medical, automotive, and IoT industries – and who will also want the means to quantitatively assess risk in their supply chains and their chips. Success here will require the development of data collection and analysis methods applied along the entire lifecycle, in a manner that does not introduce significant throughput impact or prohibitive cost penalties. Collaboration among government and commercial sector stakeholders to – (1) establish standards, (2) develop tools and methods for assessing compliance with those standards, and (3) develop methodologies for assessing residual risk once standards are employed – is an activity whose benefits would accrue to all.

Second, while geography does not guarantee security, the fact that a single location – TSMC in Taiwan – currently accounts for the majority of the global foundry market does not reflect a resilient supply chain. This lack of resilience should be of concern to the dominant customers of the market, and the U.S. government (USG) should work closely with those customers to better understand the impediments to diversifying their source of advanced chips. If a clone of TSMC were constructed in the U.S. or another allied nation, would that be sufficient for those customers to port over a significant portion of their work to that foundry? If not, what more is required, and is there an appropriate role for the USG to help enable that? One likely impediment is workforce. Foundries have no value without a skilled workforce. The US should carefully consider incentives to attract the best and brightest from within its borders as well as from around the globe to pursue careers in this industry. It is important to note that this is not just about advanced engineering degrees – highly trained technicians are extremely important to the success of this industry.

Finally, concerns about "U.S. leadership" in this industry are often raised, separately from the security concerns addressed above. The U.S. is currently a leader in several critical areas of this industry, to include the design of chips, EDA software, RF chip design and manufacturing, and specialty tooling. Furthermore, DARPA is still recognized as a global leader of cutting-edge innovation in this domain. Before taxpayer dollars are spent to enhance the U.S. leadership posture, it is imperative that the

goals are clearly defined – what does success look like, and how will it be measured? It is worth noting that those who define the standards of an industry are the ones who have the most influence over it, and for a country with less than 5% of the world's total population, influence over what gets built and to what standards is a significant means of exerting influence, and hence, leadership. Thus, the pursuit of quantitative, measurable security standards, and the tools and methods needed to enforce them, may go a long way towards addressing both security and leadership concerns facing the U.S. with regard to this industry.

In closing, it is worth emphasizing that the nature of this global, complex, intertwined industry is such that government intervention can distort the market in ways that are hard to predict, leading to unintended and undesirable consequences. Any attempts by the USG to influence this complex market should focus on the incentives of the demand signals driving the market (e.g., via standards), and extreme caution should be exercised before any subsidies are provided to the supply side. The government, by its very nature, is ill-suited to pick winners and losers in the market; any subsidy targeting a specific part of such a complex value chain – or even worse, specific companies within the chain – will weaken the competitive forces of a free market that correct for poor performance and poor alignment with the market demand. Furthermore, intervention through the use of export controls to try to prevent technology transfer often backfires in two important ways: (1) it incentivizes others to build indigenous capability and (2) it shelters our companies from international competition, while limiting their access to the global markets. The aerospace industry provides a cautionary tale to any who would propose using export controls to enhance our global leadership posture in this or any technology industry. While export controls usually do provide a short-term advantage, and timelines for others to develop indigenous capability may be long, there is no finish line. Whatever choices we make, it is important that we take the long view, as our adversaries have been doing. And we must not let our fears lead us into the trap of emulating the tactics of nations whose principles are contradictory to our own. We must play to our strengths, which include our culture of innovation, our free market principles, our entrepreneurial spirit, our respect for intellectual property, and the rule of law. It is these strengths, taken together, that will enable us to maintain a leadership position in this important global market.