Tablets, Trust, and the Supply Chain: Why Domestic Production Can't Wait

Tablets are everywhere. Soldiers use them in the field, pilots use them in cockpits, and commanders use them to track missions. These devices help run our military. But here's the problem: most of the key parts inside tablets, chips, circuit boards, and displays come from overseas. In many cases, they come from China.

That's not just a supply issue. It's a security risk. If we can't trust the origin of these parts, we can't fully trust the tablets themselves. Right now, we're handing our adversaries leverage they should never have.

A tablet looks simple from the outside, but it's anything but simple inside. Each one contains processors, memory, sensors, and displays sourced from all over the world. One weak link in that chain, and the whole device is at risk.

These aren't just "consumer electronics" anymore. The same tablets that track shipments in warehouses are also used to interface with aircraft or missile defense systems. The line between civilian and military use has blurred. And that makes them a target.

The military depends on tablets in more ways than most people realize. They run avionics interfaces, help track global logistics, support interoperability and tactical operations, enable command-and-control, and even support missile defense. A disruption in supply could ripple across all of these.

And it doesn't stop at defense. Tablets are everywhere in civilian life, too. They're in hospitals, banks, utility systems, and transportation hubs. If adversaries cut off supply or compromised these devices, the fallout wouldn't just hit our military. It would affect every American.

If an adversary controls part of your supply chain, they have options, and this is something that should be concerning inside the United States. These companies can drive up costs, restrict shipments, or embed hidden risks that no test will catch until it's too late. A single compromised part can open the door to sabotage or surveillance.

That's not a chance we can afford to take. The more dependent we become, the more leverage we give away. And in a crisis, that dependency could cost us dearly.

This isn't theoretical, it's already happening. Chinese companies dominate big chunks of the supply chain, from processors to printed circuit boards. Investigations have already found banned suppliers inside DoD tablets.

Meanwhile, U.S. factories keep closing, workers move on, and our ability to produce shrinks. Once that capability disappears, it's hard to bring back. Every year we wait, the more complex the problem becomes.

The good news is, we have a foundation. Companies like Intel, Micron, Texas Instruments, SkyWater, and GlobalFoundries still lead in advanced chips. Trusted manufacturers like Jabil, Sanmina, Benchmark, and Plexus already assemble electronics here in the U.S. PCB makers like Calumet, Greensource, and TTM are investing in advanced circuit board technologies.

But here's the catch: these pieces don't yet form a whole chain. We've got the parts, but we don't have the system that ties them all together at scale. Without that, we'll always fall short.

We can fix this. But it requires action before it's too late. We can start by buying from trusted sources, as the government should stop rewarding the cheapest bidder if there is any risk to overall security. Separately, we need to create a real demand in the case the DoD orders 500,000 tablets and critical infrastructure orders even more. There has to be a real possibility that production at this volume can happen here at home.

To get started, we need to prove that a system can work by funding demonstrators who can build an entirely domestic tablet to demonstrate its feasibility. Using frameworks like IPC-1791 and IPC-1792 so suppliers know what "trusted" really means. Lastly, investing in the people who can make all of this happen domestically by building workforce pipelines. This country needs engineers, technicians, and operators, so don't just build factories, but staff them as well.

Tablets are just one example. The same risks exist in radios, vehicles, and even aircraft carriers. In fact, over 6,500 Chinese-made parts have been found in the Ford-class carrier. That's unacceptable.

If we can fix the tablet problem, we can apply the same playbook everywhere: tear down supply chains, find the gaps, build demonstrators, create demand, and enforce standards. Done right, this approach not only strengthens national security but also creates jobs and strengthens our economy.

Now Is The Time For Action

There is no reason to hide the reality that this can't be a problem for the next generation to solve. It's a problem for us, right now, and the solution can start today.

- **For policymakers:** put trusted sourcing into law and require in buyer flow-downs, fund demonstrators, and drive demand across sectors.
- **For industry:** invest in capacity, adopt standards, and align commercial and defense production.
- **For the public:** understand that the same device in your hand also powers our military. Security starts with knowing the stakes.

The window is closing. If we wait, the risks will only grow. It’s time to move from awareness to action. Readiness must replace risk.

Jim Will, Executive Director, U.S. Partnership for Assured Electronics