Securing the Backbone: The Defense Industrial Base

PHOTO BY: Air Force Staff Sgt. Marco Gomez

By Ryan Caughill, President, Western New York Council, Navy League of the United States.

> *“You can’t fight tomorrow’s war with yesterday’s plans.”*

In the summer of 2018, I completed my internship at Moog Inc., one of the United States’ premier defense contractors. My role was in Environmental Health & Safety, but my mission went deeper: I was tasked with modernizing and guiding emergency management planning across an organization that was deeply integrated into the Defense Industrial Base (DIB), and yet, lacked a dedicated emergency management function.

Like my time later at M&T Bank, this experience left a lasting impression. It showed me that even companies at the forefront of defense technology can have blind spots when it comes to continuity, resilience, and crisis preparedness.

[While this article isn't just about my singular experience, but a holistic and general overview,] that's what makes the Defense Industrial Base one of the most paradoxical critical infrastructure sectors in America: incredibly advanced, but dangerously lacking.

The Backbone Behind the Uniform

The Defense Industrial Base is more than just tanks, missiles, or aircraft. It's an expansive network of over 100,000 private companies that provide products, services, logistics, and technologies to support the U.S. military.

This includes:

- Weapons systems and munitions
- Aerospace components and military-grade software
- Advanced electronics and cyber capabilities
- Research and development institutions
- Transportation and supply chain networks
- Small manufacturers producing critical, often irreplaceable, parts

Some of these are Fortune 500 giants. Many are small, family-owned machine shops in rural communities. All are vital.

But here's the problem: there is no unified resilience standard across the DIB. And that's a problem hiding in plain sight.

The Vulnerabilities No One Wants to Talk About

During my time at Moog, I saw firsthand how emergency management often sits outside the core of DIB corporate culture. Not out of apathy, but due to the sheer scale and

complexity of operations. Many companies have excellent safety and security programs, but few have comprehensive crisis management systems. Fewer still have trained emergency managers or business continuity professionals guiding cross-functional coordination across cyber, physical, and operational risks. This isn't to say they don't exist, I've met some, and they do a really great job.

That makes this sector vulnerable in ways most people don't understand.

The DIB is:

- Extremely decentralized: A single failed supplier can halt delivery of critical weapons platforms.
- Highly classified: Cyber breaches can compromise national defense secrets, yet many companies, especially smaller ones, lack mature cyber defenses.
- Logistically fragile: Long-lead items, global supply chains, and just-in-time manufacturing leave little room for error.
- Resource-limited: Many smaller firms simply don't have the bandwidth or expertise to build robust resilience programs.

Worse yet, we take it for granted that these companies – because of what they do – are already hardened. That's not always true.

Why This Sector Isn't Taken Seriously – Until It's Too Late

The Defense Industrial Base occupies an odd place in the national consciousness. We respect the military. We fund the military. But we rarely consider who makes the military work.

The supply chains, R&D labs, fabrication shops, and logistics hubs that build and sustain America's warfighting capability are not invincible. And yet, the DIB isn't regularly treated

like critical infrastructure in the traditional emergency management sense , even though it underpins our strategic deterrence, military readiness, and wartime surge capacity.

That disconnect has consequences. If a natural disaster, ransomware attack, insider threat, or geopolitical disruption strikes a key node in this ecosystem, the effects won't be immediate headlines. They'll show up months or years later when a military platform is delayed or compromised.

In an age of strategic competition with China and resurgent threats in Europe and the Middle East, that delay could mean the difference between deterrence and disaster.

Strengthening the Arsenal of the Republic
If we want the DIB to remain viable, competitive, and secure, we must elevate resilience as a strategic imperative, not an afterthought.

At the Federal Level:

- The DoD must go beyond cybersecurity compliance and require holistic emergency management, business continuity, and crisis communications programs for Tier 1 and Tier 2 contractors
- Congress should fund regional DIB resilience initiatives and technical assistance hubs to help small firms build preparedness capacity
- DIB firms must be integrated into DHS-FEMA and CISA exercises, not treated as isolated contractors

In the Private Sector:

Contractors should invest in full-time emergency managers or resilience officers, especially at multi-site operations
Continuity of Operations plans (COOP) must be tested regularly and integrated across functions – especially cyber, facilities, HR, and production

Leadership should prioritize exercises and scenario planning, particularly for cyber-physical convergence threats

Across the Supply Chain:

Vendors must be mapped and tiered by criticality, with redundancy plans in place for sole-source dependencies.
Smaller manufacturers should be given access to resilience toolkits and grant-supported planning assistance.

For the Defense Community:

Collaboration must improve across DoD, DHS, and the intelligence community to identify emerging threats to the DIB
Emergency management professionals should be embedded, or a partner, in acquisition planning and supplier vetting
The public and political class must recognize that defense readiness includes domestic resilience

Resilience is Readiness

The Defense Industrial Base is one of the quietest, but most consequential, sectors in the nation's infrastructure portfolio. You don't see it in parades. But it's there in every missile defense test, every jet engine, every encrypted radio, and every armored vehicle.

If we allow it to weaken, structurally, logistically, or digitally, we erode not just our defense capability, but our credibility.

We cannot afford to wait for crisis to realize that the arsenal of our Republic isn't just built on innovation or budgets.

It's built on resilience.

These challenges aren't theoretical, they're unfolding in real time. Delays in the F-35 rollout, the Navy's struggles and eventual cancellation with the Littoral Combat Ship (LCS) program, and schedule slippages in the next-generation

aircraft carriers, guided missile frigates, and Columbia-class ballistic missile submarines all point to a sector under immense strain. While these issues stem from a mix of design complexity, funding cycles, and industrial bottlenecks, one thing is clear: the Defense Industrial Base cannot afford additional disruption.

A well-funded, well-placed crisis management function, integrated at both the facility and enterprise level, won’t solve design flaws or procurement hurdles, but it can absorb shock, accelerate recovery, and ensure continuity when disaster strikes. In a sector already grappling with compounding risks, crisis management isn’t a luxury, it’s a strategic buffer against the unpredictable threats of 21st century warfare.