The View from Tier 1

Supply Chain Risk Requirements in Defense Contracting

Software and Supply Chain Assurance Forum
September 23, 2026

ABOUT ME

General Atomics Aeronautical Systems, Inc.
since Jan 2020
(San Diego, California)

Supply Chain Risk & Information Security

Bureau of Internal Narcotics &
Law Enforcement (INL)
2005-2018
(Panama)

Supporting SSCA since 2022

The content and ideas presented herein are my own and do not reflect the position of General Atomics Aeronautical Systems, Inc.





WHY SCRM



Supply chains have shifted from being strategic advantages to becoming strategic targets.

Disruption ➡ Destabilization

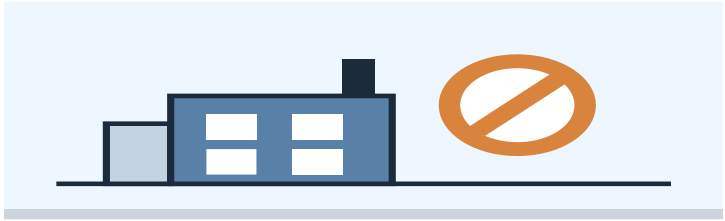
Adversaries are patient, well funded, and capable.

Advances in technology have expanded the vulnerability footprint.

Reliance upon technology has made exploitation more impactful.

THE SCRM LANDSCAPE HAS SHIFTED SIGNIFICANTLY IN THE PAST 10 YEARS. WE ARE NOW RETROFITTING COMPLIANCE REQUIREMENTS ON ESTABLISHED SUPPLY CHAINS.

STATING THE OBVIOUS



01 STATUTE

1260H

Named Chinese military companies, barred from contracts at every tier.



02 EXECUTIVE ORDER

EO 14515

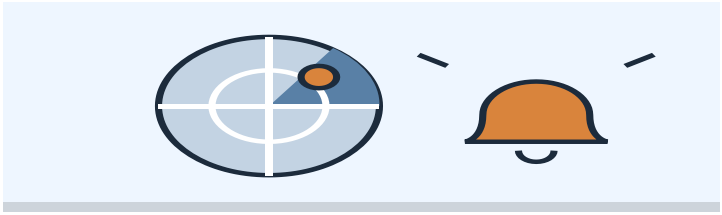
Entity and end-use screening across the supplier base, refreshed at each award.



03 MATERIAL

Raw Materials

Specialty metals and magnets held to permitted countries of melt and origin.



04 MONITORING

SCRM Alerts

Ownership changes, sanctions and adverse media trigger review of an approved supplier.



05 GEOGRAPHY

Prohibited Countries

Covered nations barred as sources of supply, manufacture, and data access.



06 CYBER

Cybersecurity

NIST SP 800-171 and CMMC verified before CUI reaches a subcontractor.



POINTS OF CONVERSATION

THE PROBABILISTIC SUPPLY CHAIN

What happens when sub-tier visibility becomes a market instead of fact

ENTITY AND ORIGIN PROHIBITIONS

An attestation chain nobody downstream can check

THE INCENTIVE STRUCTURE

What source selection actually rewards

THE SOFT TARGET PROBLEM

Contingency planning for a threat model that has changed

A PROPOSAL: COMPLIANCE READINESS LEVELS

Scaling compliance to program maturity

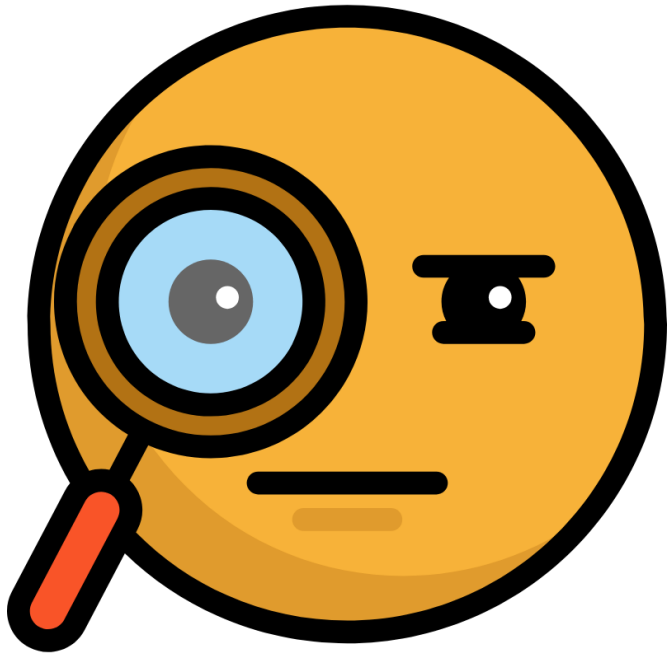
THE PROBABILISTIC SUPPLY CHAIN

94%

Confidence

- Raw material traceability has been the bane of industry.
- The best tools we have are largely AI driven and probabilistic in nature
- The result: a clean graph, a high confidence score, and no easy way to tell what that confidence is actually about.





INFERENCE, NOT VERIFICATION

- **Built from proxy signals (digital exhaust)**
  Customs records, SEC filings, corporate registries, historical trade data
- **Is any of it related to your contract?**
  The data reflects patterns across the market, not verified facts about your supply chain
- **The output is a score**
  Confidence in a calculated relationship, presented as if it were an observed one

FAILURE MODE 1: FALSE POSITIVES

- **A phantom relationship**
  Stale trade data, a shared address, name collisions, not in your supply chain
- **The real cost**
  Wasted investigation hours, damaged supplier relationship, and a flag that looks bad in a future audit even if it was never true.



FAILURE MODE 2: FALSE NEGATIVES

- **One missing tier 2**
  Breaks, or worse yet, loses the entire downstream inference. Everything below it gets reconstructed by the model or completely omitted.

- **The adversarial advantage**
  A structure built to not appear in the data these tools scrape produces a map that looks cleanest exactly where the risk is highest.



THE CONFIDENCE TRAP

The Dashboard

- Score-based, looks precise
- Invites over-trust by the people using it
- A confidence number nobody can audit

The Sales Pitch

- Real gaps hidden behind confidently espoused capabilities
- Large technology investments should equal superior results
- Rewards the right words, not the right facts

Is this more compliance theater?



If you know what data a tool scrapes, you know exactly what to avoid appearing in.

A sophisticated actor doesn't hide from your supply chain map. They manipulate it.

THE ADVERSARIAL ADVANTAGE

TAKEAWAY

A probabilistic map is a triage tool. It is not attestation-grade evidence.



THREE RULES, ONE SHAPE

1

Section 1260H

Align Aerospace and AVIC. Entity Prohibition, June 30 2026. Goods and Services Prohibition, June 30 2027.

2

DFARS 252.225-7052

Chinese-origin rare earth magnet restrictions.

3

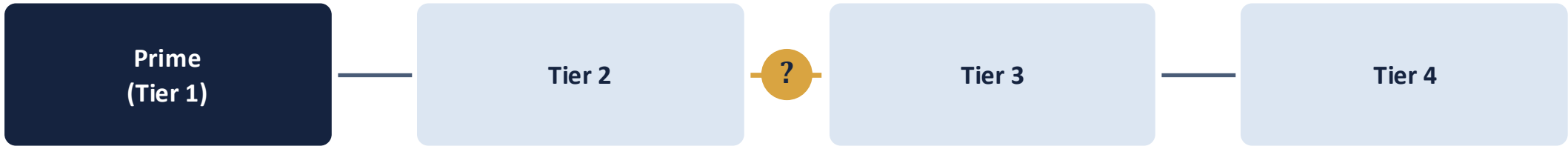
Executive Order 14415

Securing America’s Defense Supply Chains and Ensuring Domestic Acquisition of Critical Materials

Requires BOM-level, n-tier country-of-origin tracing, without the regulatory backing to make it happen.

LET’S TALK PROHIBITIONS

AN ATTESTATION NOBODY CAN CHECK



Each tier attests to the tier below it.

No tier can independently verify two tiers down. The chain looks solid. It's actually a relay of trust with no referee.

WHERE THE LIABILITY LANDS

Who Can Verify

- Limited visibility past tier one
- Limited resources to investigate further
- Often no tooling at all

Who Carries the Risk

- The prime, contractually and legally
- False Claims Act exposure for a claim it cannot independently confirm

The risk sits with the party least able to verify the fact.

WHEN THE RULE ARRIVES AFTER THE PART IS ALREADY QUALIFIED

1. **Sole sourced and qualified years ago**

   A part selected under a completely different regulatory landscape.

2. **A new restriction lands on it today**

   No grandfathering, no transition period.

3. **Requalification isn't a sourcing decision**

   It's a multi-year engineering and testing effort, assuming an alternate source even exists.



O&M

THE TIGHTEST MONEY IN THE PROGRAM

Sustainment runs on operations and maintenance dollars, not procurement or RDT&E.

- Nobody budgeted for an emergency requalification three years ago, because the rule didn't exist three years ago.
- The compliance deadline and the engineering timeline are running on two completely different clocks.
- The program office is stuck in the middle without the money to close the gap.

TAKEAWAY

The new-build problem and the legacy problem are the same failure, wearing two different uniforms.





THE INCENTIVE STRUCTURE

A CASE STUDY – CYBERSECURITY AS PROXY

Price and schedule are hard discriminators in a source selection. Cybersecurity posture is closer to a pass or fail gate. Here's what a rational bidder does with that math.

THE BRIDGE, AS DESIGNED

1

DFARS 252.204-7012

Requires implementation of NIST SP 800-171.

2

The POA&M

A documented, good-faith path to close remaining gaps over time.

3

Not a loophole

A reasonable bridge for the reality that nobody hits all 110 controls on day one.



WHERE THE BRIDGE BECAME A PARKING LOT

1. **No real cost to an open line item**

   Nothing forces the gap to actually close.

2. **Nobody checking the timeline**

   A temporary bridge became a permanent address.

3. **A form, not a forcing function**

   Compliance on paper, not necessarily in practice.



THE RATIONAL BIDDER'S MATH

Bidder A

- Real MFA across the environment
- Functioning logging and monitoring
- A staffed incident response capability
- Higher price

Bidder B

- A thin POA&M with no real closure plan
- Minimum viable paperwork
- Lower price

Bidder B wins the award.

CMMC EXISTS BECAUSE THIS ALREADY HAPPENED ONCE.

The government built an entire certification regime to force what self-attestation didn't.

A QUICK ASIDE

This is not a CMMC issue, so I'll stop the argument there. What I don't want anyone to take from this is that I'm arguing for or against CMMC. The point was the incentive structure. If anyone wants to keep talking CMMC, I'm happy to continue that in a sidebar, because going down that rabbit hole here means I never get to my next slide.

TAKEAWAY

Show me the incentive structure, and I'll tell predict the behavior with 100% accuracy.



THE SOFT TARGET PROBLEM

ARE WE REALLY ADDRESSING THE PROBLEM

DCMA asks for a contingency plan. The war didn't wait for the paperwork.

207 DAYS AND COUNTING



Feb 28, 2026

US and Israeli strikes on Iran begin.

Mar 1, 2026

Iranian drone strikes hit AWS data centers in the UAE and Bahrain.

Apr 7, 2026

A ceasefire is announced.

Jul 8, 2026

The ceasefire collapses; attacks resume in the Strait of Hormuz.

Sep 23, 2026

Intermittent escalation continues.

THE THREAT MODEL THE RULE ASSUMES

What Contingency Planning Assumes

- A discrete incident
- Against your own environment
- A failover you fully control

What Actually Happened

- A coordinated strike
- Against shared infrastructure
- A published target list naming the providers everyone sits on

The agencies asking us to develop contingency plans against the same infrastructure they rely upon.

Not a gotcha. A reason to build the answer together.

TAKEAWAY

A plan for an outage is not a plan for an act of war against infrastructure everyone assumed would just be there.



A Proposal: Compliance Readiness Levels

Rapid prototyping needs a P-Card and basic hygiene. Instead, it gets the same apparatus built for Full Rate Production. There's already a model for fixing that.



WE'VE DONE THIS BEFORE

1

Technology Readiness Levels

A published scale for how mature the technology is.

2

Manufacturing Readiness Levels

A published scale for how ready the production process is.

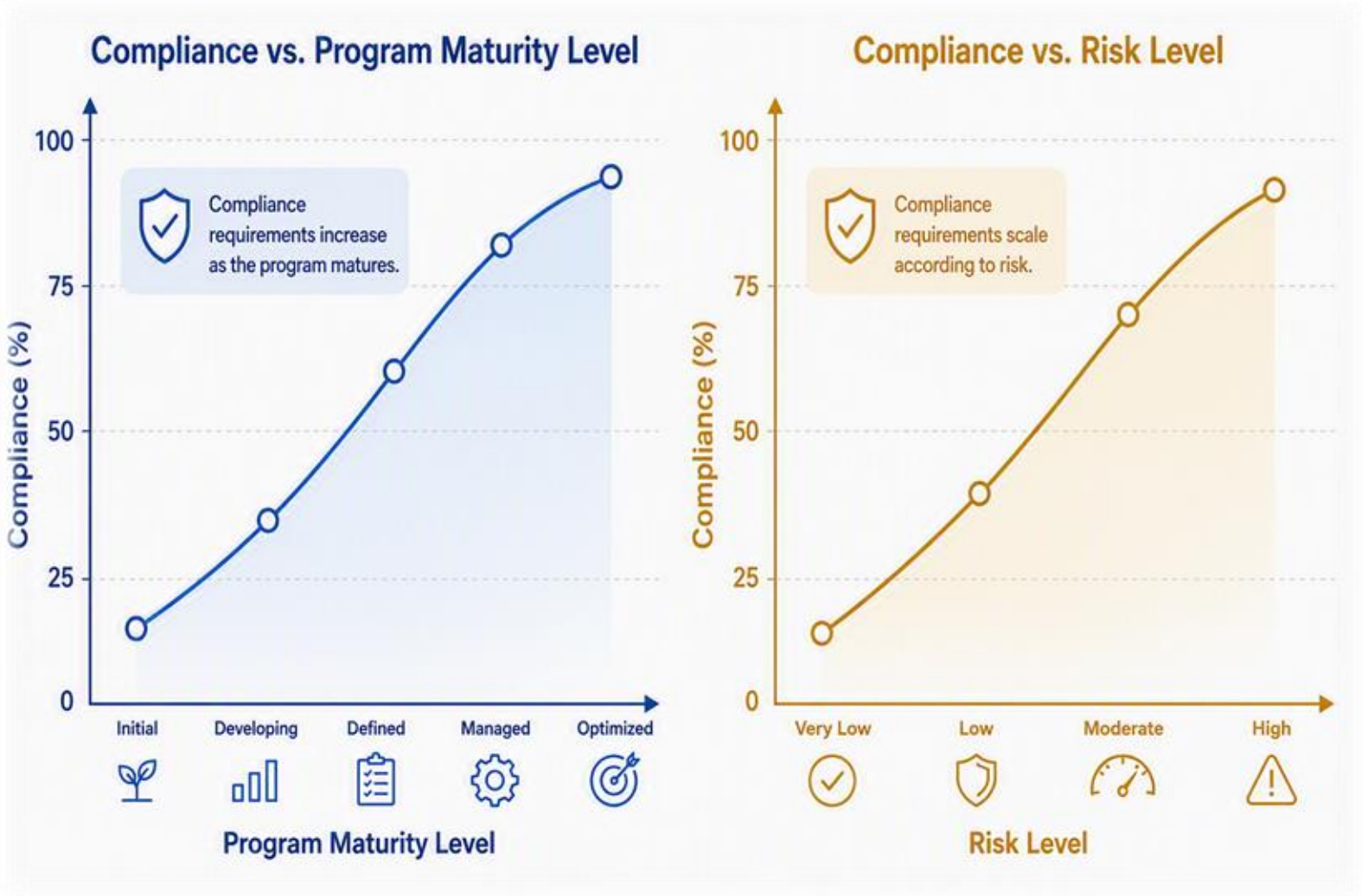
3

The missing scale

Compliance is the one dimension that still doesn't scale with program maturity or level of risk.



TWO SCALES


Compliance vs. Program Maturity Level
Compliance requirements increase as the program matures.
Compliance (%)
100
75
50
25
0
Initial
Developing
Defined
Managed
Optimized
Program Maturity Level
Compliance vs. Risk Level
Compliance requirements scale according to risk.
Compliance (%)
100
75
50
25
0
Very Low
Low
Moderate
High
Risk Level

DIFFERENT RISK, SAME BURDEN

A $2M Subcontractor

- Machines a single part that is labeled as CUI
- No compliance or IT staff
- Less than 10 employees
- Wondering why they keep receiving cybersecurity questionnaires about their Overtime (OT)

A $200M Subcontractor

- In possession of multiple Technical Data Packages that it flows through their sub tier supply chains. All of it labeled as CUI
- Dedicated compliance and IT staff
- Absorbs the cost and moves on

Guess who leaves the defense industrial base first.

WHAT DO WE REALLY NEED

1

A real workability impact statement

Current regulatory impact assessments assume that all subcontractors have access to the same level of expertise and resources.

2

Quit being ambiguous on purpose

Refusing to provide clear guidance on definitions and expectations then telling contractors to figure out with their PCO.

3

A shared verification schema

A new rule, a new questionnaire. Even if the agency already has the answer. The epitome of inefficiently and bureaucracy.

4

A reasonable-diligence safe harbor

While the authoritative data sources for entity prohibitions are still maturing.

If I had the pen, I wouldn't ask for less compliance.

I'd ask for compliance that survives contact with the people who have to build it.

That's the view from Tier 1.


THANK YOU