G1VE TECHNOLOGIES

# Mission Assurance in a Kill-Web Era: The Three Moves for the Next 90 Days

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP

Sep 8, 2026

**Original source**

https://www.linkedin.com/pulse/mission-assurance-kill-web-era-three-moves-next-90-w-b--5q5ve/

## I. Opening Imperative

Here is the line in the sand for September 2026: the mission-assurance construct the United States Department of War inherited from the 2018–2022 cycle is operationally obsolete against the threat picture we are flying into. On September 24, 2025, the United States Department of War publicly rolled out the Cybersecurity Risk Management Construct and admitted in its own press release that mission assurance must be assured "in every domain: air, land, sea, space, and cyberspace".

That release was not a press event. It was an admission that the prior frame — one largely authored for industrial-age bases, single-service MAAs, and static install lists — cannot defend a force where the kill web spans satellites in MEO, subsea cables, contract manufacturer MES lines, and a small commercial LEO constellation that any adversary can read-in to in a weekend.

...My thesis for this issue is deliberately polarizing:

- We are running a 20th-century mission-assurance defense against a 21st-century kill web.

The 2018–2022 MA construct was built around the assumption that the principal threat to mission readiness was localized disruption — weather, an isolated IED, a single failed contractor, a degraded utility feed. The 2026 threat includes contested logistics across the first and second island chains, supply-chain poisoning inside primes and subs at the firmware and solder-paste layer, AI-enabled reconnaissance of the United States Department of War installations, and synchronized cyber-physical attacks timed to a crisis flashpoint.

The reflective, cyclic, after-action MA model can no longer keep pace. The rest of this article sets the requirement and then hands you the three moves to make in the next 90 days.

## II. What Mission Assurance Now Means

Mission assurance in 2026 is no longer a checklist inside a single PEO's program office. It is an enterprise operating discipline anchored in four artifacts that every senior leader should be able to recite from memory:

1. The Mission Assurance Risk Management System (MARMS), the United States Department of War's risk register that directly supports Secretary Pete Hegseth in prioritizing mission-essential assets and functions across components (DTIC — MARMS Budget Justification PB 2025).
2. The United States Department of War Mission Assurance Construct, the whole-of-department framework that aligns MARMS to the United States Department of War's force-readiness reporting.
3. The Mission Assurance Senior Steering Group (MASSG), the United States Department of War-level body that adjudicates cross-component MA risk; MASSG convenes under the authority delegated from the Office of the Under Secretary of War for Acquisition & Sustainment per the standing directive issuance at.

4. The 2026 Status of Mission-Ready Force posture, the foundation of the Force Readiness Reporting system as currently refreshed by the Office of the Under Secretary of War for Acquisition & Sustainment in coordination with the Under Secretary of War for Policy.

If you cannot fluently connect those four artifacts to a current list of risk-mapped assets, you are not doing mission assurance — you are doing compliance theater. Two downstream signals are non-negotiable in 2026:

1. Every installation must tie its risk-mapped capability directly to one or more of the 55 National Critical Functions maintained by the Cybersecurity and Infrastructure Security Agency ; that 55-function anchor is now the lingua franca between the United States Department of War, the DIB, and the broader federal critical-infrastructure community.
2. The Defense Continuity and Mission Assurance portfolio, which sits properly inside the Office of the Under Secretary of War for Acquisition & Sustainment is now the connective tissue to U.S. Northern Command / NORAD & US Northern Command , to the homeland-defense mission, and to every continuity-of-operations plan a Combatant Commander is forced to execute under crisis.

Anyone who tells you mission assurance is still "the A&S MA team's problem" is briefing a 2019 chart.

## III. COCOMs at the Decisive Edge

Combatant Commanders are the operational arbiters of whether mission-assurance doctrine survives contact with reality. Six of them are now operating with FY26 force-structure demands that MA cannot ignore. USINDOPACOM remains the pacing theater. Admiral Paparo's FY27 posture statement, on the record to the Senate Armed Services Committee, makes the case that the command executed more than 100 joint exercises in 2025 to sustain deterrence of the PRC and the DPRK (Paparo FY27 USINDOPACOM Opening Statement). Every one of those exercises is an MA stress event against distributed logistics, throughput, and island-chain infrastructure, and the COCOM cannot win those fights without prime and sub contracting teams that have already been MAPped and risk-registered.

USEUCOM is re-tooling for sustained posture along the eastern flank in coordination with NATO allies; USNORTHCOM owns the homeland-defense seam, the ballistic-missile warning backbone, and increasingly the cyber-physical convergence around United States Department of War installations; USAFRICOM is balancing violent-extremist organization containment against great-power competition on the continent; USCENTCOM is operating forward sustainment nodes under persistent surveillance; USSOUTHCOM just published its 2026 posture statement, which puts defending the homeland and counter-narcotics as the command's #1 mission, stating explicitly that "I am honored to highlight the priorities, activities, and investments of USSOUTHCOM's #1 mission to defend the homeland" (SOUTHCOM 2026 Posture Statement). USSPACECOM and USTRATCOM are now functionally fused operationally — the SASC FY26 posture hearing for both commands is on the record at (SASC FY26 STRATCOM/SPACECOM Posture Hearing). The proof point for that integration is contract action: on 29 July 2026, Space Systems Command awarded task orders worth $1.6

billion to SpaceX for 18 Falcon 9 launches supporting the Space Based Sensing and Targeting Layer (SSTL) — the kind of commercial-integrated kill-web architecture the MA construct must now span (SSC — Space-Based Sensing & Targeting Task Orders). Over the 2023–2025 window, the Space Force spent nearly $124 million on commercial space data and services (Air & Space Forces — Commercial Data Spend) — a fact GAO itself has flagged in GAO-26-107959 as an opportunity area for the United States Department of War.

## IV. Critical Infrastructure As The New Kill Web

The United States Department of War has been quietly running on an industrial-age map of its own installations, and that map is wrong. The Mission Assurance Construct's Day-1 inputs must now include the Cybersecurity and Infrastructure Security Agency 's 55 National Critical Functions (NCFs) as the binding functional layer between any given United States Department of War install and the broader national critical-infrastructure stack on which it depends.

The NCF set was issued in 2019 and refreshed since; it spans functions as varied as "Supply Water," "Manage Wastewater," "Provide Medical Care," "Generate Electricity," "Transport People and Goods," "Produce and Provide ICT Services," and "Provide Satellite Navigation and Timing." Every single one of the 55 NCFs touches a United States Department of War mission somewhere, and the United States Department of War does not yet have authoritative NCF-down mapping for every MA Risk Category across every installation.

The CRS product on Critical Infrastructure released in March 2026 makes the same observation:

- The Cybersecurity and Infrastructure Security Agency 's NCF framework is the de facto cross-sector risk-analysis lens and the United States Department of War is being asked to align its own dependences accordingly (CRS — Critical Infrastructure: Emerging Trends (R48878)).

...For the warfighter, the takeaway is sharper:

- A PNT disruption that takes GPS timing off the wire for six hours is now a kill-web event, not a nuisance.
- A regional water utility failure at a CONUS training base is now a readiness event, not a facilities ticket.
- A subsea cable severance on a routing the Theater IPR office depends on is now a mission-assurance event, not an intel curiosity.

The MA Construct was not built to do this analysis at machine speed. We are rebuilding it now, and FY26 dollars must follow.

---

## V. DIB Exposure And The Dirty Tax

The Defense Industrial Base is the transmission system by which mission risk moves from the public sector into the private sector and back again — the dirty tax on every program of record that nobody wants to put on a slide. Three regulatory arcs shape the FY26 environment, and PMs who do not understand all three are signing contracts they cannot defend:

1. The CMMC 2.0 final rule at 32 CFR Part 170, effective 16 December 2024; the companion DFARS rule that flowed the clause into contracts was to take effect on 10 November 2025; and then on 13 July 2026 the United States Department of War/ Office of the DoW Chief Information Officer announced an immediate suspension of CMMC Phase II, freezing further implementation phases — itself a real-world demonstration of mission-resilience requirements bending the procurement bureaucracy. The Office of the DoW Chief Information Officer is the authoritative source for the live program state.
2. The U.S. Department of the Treasury Outbound Investment Security Program — The final rule was issued 28 October 2024 and is effective 2 January 2025, covering U.S. investment flows into covered national-security technologies in countries of concern Every prime that has a venture arm, and every sub with a non-U.S. capitalization event, sits inside this regime.
3. The FY26 NDAA at Sections 1545 and adjacent provisions mandates an annual report on Mission Assurance Coordination Board (MACB) activity, including cybersecurity risks to covered assets — the same body that, under MARMS, adjudicates cross-component MA risk.

The DIB-tier NCF exposure is therefore not theoretical: at least 28 of the 55 NCFs have a direct DIB-tier ingress path that the PM and the prime must jointly sign for.

## VI. Who Owns Mission Assurance In 2026

The org chart is the org chart until a crisis proves otherwise. As of this issue, mission assurance is owned by a chain that runs from the Secretary of War Pete Hegseth and the Chief of Staff to the Secretary of War, through Office of the Under Secretary of War for Acquisition & Sustainment as the principal staff assistant for acquisition and sustainment, into the Office of Strategic Services for the irregular and sensitive-operations seam, across to the DIB Task Force for the industrial-base threat picture, and laterally into the DoW Super Intelligence Office - SIO (formerly CDAO) for the AI-enabled risk-management tooling that now sits on every classification level.

The Defense Continuity and Mission Assurance office, properly placed under Office of the Under Secretary of War for Acquisition & Sustainment , is the operational continuity seam to U.S. Northern Command / NORAD & US Northern Command and to the Federal continuity community. The Under Secretary of Defense for Policy owns the policy alignment and the COCOM engagement; the Defense Intelligence Agency , National Security Agency , U.S. Cyber Command , Defense Information Systems Agency , and DFAS each own a slice of the intelligence, cryptologic, network, and fiscal backbone that MA has to map over. USSOCOM runs MA for the SOF enterprise in parallel.

Two facts about ownership matter most:

1. The DoW Super Intelligence Office - SIO (formerly CDAO) mission-resilience AI portfolio — including the United States Department of War AI Inventory and the federation/OTA prototypes such as the publicly acknowledged Thunderforge, CHIMES, and federation-prototype work — now publishes-enables the risk register that MARMS ingests; everyone

from the PEO on down must read both the program-of-record inventory and the OTA sidecar together.

2. The FY26 NDAA explicitly requires the United States Department of War to assess its own dependence on foreign entities of concern for critical infrastructure it owns — meaning SECWAR Pete Hegseth , the Chief of Staff to SECWAR, and Office of the Under Secretary of War for Acquisition & Sustainment now co-own a market-data and supply-chain illumination task that no single component can run alone. If your MA risk register is not signature-block-current to these positions and these artifacts, it is a binder, not a register.

---

## VII. Thought-Provoking Close: The Three Moves for the Next 90 Days

This is the call to action. Three moves, in order, for the next 90 days, no exceptions —

1. Move One for PEOs and PMs: Stand up a Mission-Resilience Cell on every PM-led install that supports a COCOM war-room, and tie that cell to the relevant NCFs from the Cybersecurity and Infrastructure Security Agency . Use the existing MARMS vocabulary and exercise the cell quarterly against a real adversary-scripted kill-web scenario.
2. Move Two for COCOMs and the MACB: Wire every DoW Super Intelligence Office - SIO (formerly CDAO) -listed AI tool on your network into your MA risk register before the FY26 NDAA Section 1545 Mission Assurance Coordination Board annual report is due; the CRS summary on those provisions is at. No tool, no AI capability and no model-card goes operational without a MACB-tagged MA risk entry.
3. Move Three for Senior Leaders and Acquisition: Pressure-test every prime's CMMC posture against the actual 10 November 2025 DFARS clause path — not the suspended Phase 2 muzzle that landed on 13 July 2026; and pair that pressure test with the U.S. Department of the Treasury outbound-investment regime effective 2 January 2025, because the supply-chain illumination gap between CMMC and outbound is exactly where adversaries will land.

That is not advocacy; it is field-tested risk management. If you are sitting in a session where these three moves are not on the agenda as the first three items, send me a DM — I will bring the slides, the NCF map, and the FY26 MACB template, and we will walk through the gap together.

Mission readiness is no longer a quarterly deliverable; it is a daily operating discipline.

---

## ✨ Call to Action: Step Into the Arena ✨

Most professionals will read about the future. A select few will shape it.

If you are serious about staying ahead of the curve in Artificial Intelligence, Regulatory Compliance, and Enterprise Risk, this is where you need to be.

📩 Subscribe to Securing Our Future to gain direct access to:

1. Strategic foresight on AI Governance & Ethical Deployment
2. Real-world applications across National Security & Mission Assurance

3. Advanced GRC, TPRM, and Regulatory Compliance frameworks
4. Emerging Fintech and Risk Intelligence innovations

⚔️ The landscape is shifting—fast. The gap between those who understand and those who execute is widening.
This is built for professionals responsible for decisions that carry consequence—not commentary.
📅 Ready to operationalize these insights and move beyond theory?
👉 https://calendly.com/g1ve-technologies
Let us translate insight into measurable, defensible outcomes—and build capability, not just conversation.

---

## 🔍 About the Author

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP is a National Security-aligned Artificial Intelligence Strategist/Tactician and Governance, Risk, and Compliance (GRC) Authority/Subject Matter Expert with over a decade of experience operating at the intersection of National Security, National Defense, Critical Infrastructure, Cybersecurity, AI Governance, Mission Assurance, Mission-Critical Systems, and Predictive Funding/Grant Intelligence.
As Managing Partner at G1VE Technologies, LLC and a Strategic Board Advisor, W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP architects and operationalizes enterprise-scale risk, compliance, and AI governance ecosystems across both Public and Private Sector environments—including Fortune 500/1000 organizations and Federal-aligned missions, where failure is not an option.
His work is centered on delivering Decision Advantage, strengthening Operational Resilience, and enabling organizations to navigate high-stakes, high-uncertainty environments with precision and confidence.
📡 Connect with W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP here to stay at the forefront of:

- Artificial Intelligence
- National Security
- GRC
- Cyber Risk
- Regulatory Strategy
- Mission Assurance