Need Funds for Your CMMC Program?

Federal and State Grant Funding for CMMC Readiness in Defense Manufacturing

A White Paper for Defense Industrial Base Decision Makers

David W. Koran, CMMC Registered Practitioner

March 2026

Summary

The Cybersecurity Maturity Model Certification program is no longer a planning exercise; it is a present contractual requirement with measurable financial consequences for every manufacturer in the Defense Industrial Base. As of November 10, 2025, the Department of Defense has authorized contracting officers across every military branch to embed CMMC Level 1 and Level 2 self-assessment requirements into solicitations as a condition of contract award. Phase 2, beginning November 10, 2026, will extend that mandate to include third-party certification by a Certified Third-Party Assessment Organization (C3PAO) for contracts

involving Controlled Unclassified Information (CUI). The operational implication is clear: manufacturers that cannot demonstrate compliance will be ineligible to compete.

For small and medium-sized manufacturers (SMMs), the financial burden of CMMC Level 2 readiness is significant. Industry estimates for the full scope of readiness activities, including gap analysis, technical remediation, policy development, and system security plan documentation, range from $35,000 to well over $100,000 depending on organizational complexity and current security posture. These costs arrive at a time when operating margins in precision manufacturing remain thin and capital allocation decisions carry lasting consequences.

This paper examines the structure of federal and state funding mechanisms available to offset CMMC implementation costs. From the NIST Hollings Manufacturing Extension Partnership (MEP) network to the Office of Local Defense Community Cooperation's Defense Manufacturing Community Support Program, to state-level initiatives in Connecticut, New York, Massachusetts, Georgia, and a growing number of additional states, a defined architecture of public funding exists. The central argument of this paper is that CMMC implementation costs, when structured properly and paired with grant funding, function not as an expense to be absorbed but as a subsidized capital investment that strengthens a firm's long-term competitive position within the defense supply chain.

The Regulatory Landscape: 2026

The transition from voluntary self-attestation to enforceable third-party verification is already underway. When the 48 CFR Final Rule took effect on November 10, 2025, CMMC stopped being theoretical. Contracting offices at NAVAIR, NAVSEA, the Army Corps of Engineers, and Air Force Global Strike Command have all issued solicitations that include explicit CMMC Level 2 language. In early February 2026 alone, NAVSEA published requirements for submarine support and ship self-defense systems that listed CMMC Level 2 certification as a core capability requirement, with contractors expected to undergo C3PAO assessment every three years for the life of the contract. NAVAIR has issued similar language for antenna systems and weapons programs, with provisions allowing offerors to contest the assigned CMMC level only through written justification.

The phased rollout operates on a defined timeline. Phase 1, running from November 2025 through November 2026, requires self-assessments posted to the Supplier Performance Risk System (SPRS) for both Level 1 (Federal Contract Information) and Level 2 (CUI) contracts. Phase 2, beginning November 10, 2026, will mandate

C3PAO-assessed Level 2 certification for applicable contracts. Phase 3 adds Level 3 requirements for higher-sensitivity programs. By November 2028, every DoD contract involving FCI or CUI, with the exception of commercial off-the-shelf items, must include the appropriate CMMC level as a condition of award.

The enforcement pressure is not limited to the DoD itself. Prime contractors are now driving compliance requirements down through their supply chains independent of the federal timeline. Lockheed Martin has directed all suppliers to document their CMMC status in SPRS and has framed compliance as a prerequisite for uninterrupted business operations. Boeing has issued similar guidance, encouraging suppliers to begin preparation for Level 2 certification immediately rather than waiting for requirements to appear in individual solicitations. For SMMs operating as subtier suppliers, the practical effect is that the compliance deadline may arrive well before the DoD's own Phase 2 trigger.

The Funding Architecture

A structured network of federal and state funding programs exists specifically to reduce the financial burden of cybersecurity compliance for manufacturers. These programs are not hypothetical, nor are they speculative. They are appropriated, administered, and actively issuing awards. Understanding the architecture of available funding is a prerequisite for responsible capital planning in the current regulatory environment.

The MEP National Network

The NIST Hollings Manufacturing Extension Partnership program is the primary federal vehicle for delivering cybersecurity readiness services to small and medium-sized manufacturers. Established in 1988, the MEP National Network operates through 51 centers, one in every state and Puerto Rico, each functioning as a public-private partnership. The model is built on a cost-share structure: federal appropriations fund approximately half of each center's budget, with the balance provided by state and local governments and client fees. Congress funded the MEP program at $175 million for fiscal year 2026, despite an executive branch proposal to eliminate the program entirely.

Section 1642 of the National Defense Authorization Act for Fiscal Year 2021 authorized the Secretary of Defense, in consultation with the NIST Director, to provide financial assistance to MEP Centers specifically for the purpose of helping manufacturers address CMMC and NIST SP 800-171 requirements. In practice, this means that MEP Centers

are positioned to deliver cybersecurity readiness services, including gap analysis, policy development, network architecture review, and implementation support, through cost-share projects that reduce the direct financial exposure for the manufacturer. The Vermont Manufacturing Extension Center (VMEC), for example, has partnered with Norwich University Applied Research Institutes (NUARI) to deliver cybersecurity readiness services that include drafting comprehensive cybersecurity strategies, facilitating employee training, and building organizational capability around NIST SP 800-171 compliance requirements.

The cost-share model is a critical structural feature. A Government Accountability Office study found that because client fees give manufacturers a financial stake in the outcome, the positive impact on their businesses is measurably greater than in fully subsidized programs. At the same time, the public funding component ensures that smaller manufacturers, those with limited capital reserves and thin margins, can access services they would otherwise be unable to afford. For a manufacturer facing a $60,000 to $100,000 CMMC readiness project, a properly structured MEP cost-share engagement can reduce the out-of-pocket investment by 50 percent or more.

OLDCC and the Defense Manufacturing Community Support Program

The Office of Local Defense Community Cooperation (OLDCC), operating under the Office of the Under Secretary of Defense for Acquisition and Sustainment, administers the Defense Manufacturing Community Support Program (DMCSP). Authorized by Section 846 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, the DMCSP is a competitive grant program designed to support long-term community investments that strengthen national security innovation and expand the capabilities of the defense manufacturing ecosystem.

From fiscal years 2020 through 2023, the DMCSP allocated $110 million to 23 designated Defense Manufacturing Communities. These awards have supported more than 5,366 defense businesses and 100,000 workers. Among the program's documented outcomes, 452 companies have received cybersecurity capability enhancements, and over 1,143 small and medium-sized companies have received guidance on entering the defense sector. Individual awards have reached $5 million per consortium, with total project values exceeding $11 million when non-federal matching funds are included.

The DMCSP model operates through regional consortia rather than individual company grants. A consortium may include state and local governments, academic institutions, defense manufacturers, workforce organizations, and nonprofit organizations. The lead organization submits proposals on behalf of the consortium. This structure means that individual manufacturers typically access DMCSP benefits through their regional

consortium's service offerings rather than through direct grant applications. Connecticut, for example, has leveraged DMCSP funding to accelerate the adoption of advanced manufacturing technologies, including cybersecurity capabilities, across its defense supply chain.

It is important to note that DMCSP funding has not been appropriated for every fiscal year. No funding was available for fiscal year 2025, and designations are only considered during open competition periods when program funding is available. Manufacturers should monitor OLDCC announcements and coordinate with their regional economic development organizations to ensure awareness of future funding cycles.

State-Level Case Studies

State governments with significant defense manufacturing sectors have recognized that CMMC compliance is an economic competitiveness issue, not solely a cybersecurity matter. Several states have created targeted funding programs to support their manufacturers through the compliance process. Four programs with defined funding structures illustrate distinct models of state-level intervention.

Connecticut: The Cybersecurity Adoption Program (CAP)

Connecticut's defense manufacturing sector generates an estimated $41.7 billion in GDP for the state. The concentration of aerospace and defense production along what is informally known as "Aerospace Alley" creates a significant economic interest in ensuring that Connecticut manufacturers can meet CMMC requirements and retain their positions in the DoD supply chain.

The Connecticut Office of Manufacturing created the Cybersecurity Adoption Program (CAP), administered by the Connecticut Center for Advanced Technology (CCAT) and funded through the Department of Economic and Community Development's Manufacturing Innovation Fund. The program provides matching grants of up to $35,000 per company on a 50/50 cost-share basis, meaning the state will match dollar-for-dollar up to that ceiling. The funding is structured in two tiers: up to $10,000 may be applied toward the initial cybersecurity readiness evaluation, and the remaining $25,000 is dedicated to remediation activities including implementation of technical controls, policy development, and infrastructure hardening.

Connecticut CAP Eligibility Requirements

Criterion	Requirement
Business Type	Manufacturing company or allied service provider
State Registration	Registered with the Secretary of State for at least three years
Employee Count	Between 3 and 300 employees within Connecticut
Revenue Source	More than 50% of revenue from manufacturing or allied services
Match Structure	50/50 cost share, up to $35,000 lifetime maximum
Minimum Project Value	$5,000
Third-Party Requirement	Must engage a third-party vendor or service provider

The CAP is a rolling grant, meaning applications are accepted on a continuous basis rather than through competitive funding cycles. This is a significant practical advantage for manufacturers who need to begin work within a defined timeline. For a manufacturer facing a $70,000 CMMC readiness project, the CAP grant effectively reduces the company's direct financial exposure by $35,000, transforming the economics of the entire engagement.

New York: Cybersecurity Manufacturing Initiatives Grant

New York operates a dedicated Cybersecurity Manufacturing Initiatives Grant administered through the NY Manufacturing Extension Partnership, with FutureSense (AIM) serving as the grant administrator. The program is structured in two phases: Phase 1 funds personalized cybersecurity readiness evaluations that identify gaps against NIST SP 800-171 requirements, and Phase 2 provides funding for implementation and remediation of those gaps. The manufacturer's direct financial contribution is $1,500, with the grant covering the remaining project costs. Applicants sign a contract agreement directly with a service provider approved by the grant administrator, and the program includes access to in-person cybersecurity awareness events held at multiple locations across the state.

New York has also benefited from federal DMCSP awards. In the most recent funding cycle, the Department of Defense designated two separate New York consortia, each receiving $5 million: the New York Consortium for Space Technology Innovation and

Development, and the New York State Microelectronics Defense Manufacturing, Supply Chain, and Workforce consortium. While these awards target specific technology sectors rather than CMMC readiness directly, they reflect a broader pattern of federal investment in New York's defense manufacturing ecosystem that creates additional pathways for manufacturers seeking compliance support.

Massachusetts: Manufacturing Cybersecurity Program

The Massachusetts Manufacturing Cybersecurity Program (MCP), administered through the Massachusetts Manufacturing Accelerate Program (MMAP) under MassTech Collaborative, provides up to $30,000 in capital cost share for cybersecurity infrastructure improvement projects. The program is designed specifically for manufacturers located within the Commonwealth and targets the capital expenditure side of cybersecurity compliance, covering hardware, software, and infrastructure upgrades required to meet federal cybersecurity standards. For manufacturers whose CMMC readiness gap is primarily technical rather than procedural, this program addresses the most capital-intensive portion of the compliance investment.

Georgia: OLDCC-Funded Cybersecurity Grants and GaMEP

Georgia's defense contracting sector generates approximately $7.2 billion annually and includes roughly 4,000 contractors statewide. The Georgia Department of Economic Development (GDEcD), through its Center of Innovation for Aerospace, has administered cybersecurity grants funded by the DoD's Office of Local Defense Community Cooperation (OLDCC). These grants target small and mid-sized defense contractors and require that applicants hold active defense contracts or have held one within the preceding six months. The program reflects a direct federal-to-state funding pathway that leverages OLDCC resources for manufacturer-level cybersecurity compliance.

In parallel, the Georgia Manufacturing Extension Partnership (GaMEP) at Georgia Tech provides CMMC readiness services including gap evaluations, training on NIST SP 800-171 requirements, and project implementation support. NIST awarded GaMEP $457,663 specifically to develop and deliver a CMMC training program for small and medium-sized manufacturers, with pilot deployments extending to MEP Centers in Iowa, Missouri, and North Carolina. GDEcD has also partnered with the Technology Association of Georgia (TAG) to form the Georgia Defense Industrial Base Task Force, which coordinates cybersecurity webinars, resources, and cross-sector support for the state's defense manufacturers.

Additional States with Active or Emerging Programs

The four programs described above are not exhaustive. A growing number of states have established or are developing cybersecurity funding mechanisms relevant to defense manufacturers. The following states have active programs, delivered primarily through their MEP Centers, that provide cost-share or grant-funded cybersecurity readiness services: Virginia (GENEDGE, which leads the MEP National Network's Eastern Region cybersecurity collaborative and operates the DEFENDCUI-VA program for DoD supply chain manufacturers); Texas (TMAC at the University of Texas at Arlington, which holds multiple federal grants for DoD supply chain cybersecurity services and guided the first manufacturer in the nation through a CMMC 2.0 Level 2 Joint Surveillance Voluntary Assessment); Maryland (MD MEP, a designated Go-To Collaborative Center for cybersecurity that has provided technical assistance and funding to manufacturers since 2018); Arizona (Arizona MEP, which has delivered phased CMMC readiness engagements including policy development, network mapping, and tabletop exercises); and California (CMTC, which leads the Western Region MEP cybersecurity collaborative serving the Northwest, Southwest, and Mountain states).

Manufacturers in any state should contact their local MEP Center as a first step. Even in states without a dedicated state-funded grant program, the MEP cost-share model provides a structured mechanism for reducing the direct financial burden of CMMC readiness work. A current directory of all 51 MEP Centers is maintained at nist.gov/mep.

Strategic Financial Planning

The single most common mistake manufacturers make when pursuing grant-funded CMMC readiness is committing to a project before securing grant approval. This error is not merely procedural; it is disqualifying. The Connecticut CAP, for example, explicitly states that projects already underway are ineligible for funding. If a manufacturer has signed a proposal, executed a contract, or made a deposit with a service provider, that project cannot receive grant support. The same principle applies across most federal and state cost-share programs: grant funds are intended to enable new work, not to reimburse completed projects.

The practical implication is that readiness planning must be sequenced in a disciplined manner. A manufacturer should begin with an internal scoping exercise to identify the nature and volume of CUI within its environment, the systems that process, store, or transmit that information, and the approximate gap between current security posture and the 110 controls specified in NIST SP 800-171. This preliminary work does not

constitute a grant-funded project, and it provides the foundation for a well-defined project scope that can be submitted with a grant application.

Once the scoping exercise is complete, the manufacturer is in a position to approach the appropriate funding source, whether that is a state-level program like the Connecticut CAP or a federal MEP cost-share engagement, with a defined project scope and realistic budget. The grant application is submitted. In some programs, receipt of an automated acknowledgment permits the manufacturer to begin work immediately while the grant is being processed. In others, work must not commence until the grant is formally approved. The specific rules of the applicable program must be understood and followed precisely.

From a capital allocation perspective, the readiness phase should be treated as a structured investment with a defined return. The return is not abstract: it is the preservation of contract eligibility for DoD work that may represent a substantial portion of the firm's annual revenue. For manufacturers where defense contracts represent 30 percent, 50 percent, or more of total revenue, the cost of noncompliance is not the cost of the readiness project itself but the loss of the revenue stream that compliance protects. When grant funding reduces the direct financial exposure by 50 percent or more, the risk-adjusted return on the investment becomes difficult to argue against.

Conclusion

CMMC implementation costs are real, and for small and medium-sized manufacturers, they are material. That much is beyond dispute. What is too often overlooked, however, is the extent to which those costs can be offset through existing federal and state funding mechanisms. The MEP National Network, the OLDCC's Defense Manufacturing Community Support Program, and state programs in Connecticut, New York, Massachusetts, Georgia, and beyond collectively form an infrastructure of financial support that is available, appropriated, and actively distributing funds.

The manufacturers who will navigate this transition most effectively are those who approach CMMC implementation as a capital investment rather than a compliance expense. A capital investment has a defined scope, a structured funding plan, a qualified professional performing the work, and a measurable return. In this case, the return is the preservation and expansion of a firm's eligibility to compete for DoD contracts at a time when noncompliant competitors are being excluded from the market.

As smaller firms exit the defense supply chain due to inability or unwillingness to invest in compliance, the manufacturers who have made that investment will find themselves

in a stronger competitive position: fewer qualified competitors bidding on the same work, stronger relationships with prime contractors who are actively seeking certified subtier suppliers, and a security posture that reduces operational risk beyond the compliance requirement itself.

The grant funding architecture described in this paper does not eliminate the cost of CMMC readiness. It does, however, reduce the manufacturer's direct financial exposure to the point where the investment becomes not only manageable but strategically advantageous. The firms that recognize this dynamic, and act on it within the available funding windows, will be the ones that retain their position in the defense manufacturing ecosystem for the decade ahead.

About the Author

David W. Koran is the founder and Managing Partner of David Koran & Associates, a CMMC compliance consulting firm serving Defense Industrial Base contractors and their legal counsel. A CMMC Registered Practitioner and Associate Member of the ABA Section of Public Contract Law, he brings over 30 years of IT and cybersecurity experience to the firm's readiness, implementation, and enablement practice. His work focuses on helping small and medium-sized manufacturers navigate CMMC scoping, remediation planning, and documentation development in preparation for third-party certification.