Testimony for the Record from the

GovCon Small Business Coalition

House Committee on Small Business Committee

"Main Street Under Attack: The Cost of Crime on Small Businesses"

December 2, 2025

GOVCON SMALL BUSINESS COALITION

December 8, 2025

The Honorable Roger Williams
Chairman
House Committee on Small Business
U.S. House of Representatives
Washington, DC 20515

The Honorable Nydia Velázquez
Ranking Member
House Committee on Small Business
U.S. House of Representatives
Washington, DC 20515

Chairman Williams, Ranking Member Velázquez, and Members of the Committee:

The GovCon Small Business Coalition represents small and midsize contractors advocating for policies that support business growth and strengthening of the defense industrial base. The Coalition respectfully submits the following comments on the prohibitive costs associated with CMMC compliance to small businesses. We believe the Cybersecurity Maturity Model Certification (CMMC) 2.0 final rule , which entered its first implementation phase on November 10, 2025, requires increased costs to small businesses, thus decreasing the number of small businesses bidding on defense work.[1] Fewer bidders can result in less competitive pricing for these projects.

Impact of CMMC 2.0 on Small Businesses

We agree that assured cybersecurity is vital to national security because the threat from sophisticated, state-sponsored cyber actors is real. Our coalition strongly supports efforts to raise cybersecurity standards across the defense supply chain and civilian agencies. However, the implementation of CMMC 2.0 imposes significant costs and uncertainties that will shrink the nation's industrial base by disproportionately impacting small firms.

On June 20, 2025, the Small Business Administration (SBA) Office of Advocacy issued a letter to the Department of Justice's (DOJ) Anti-Competitive Regulations Task Force and the Federal Trade Commission (FTC), highlighting that small businesses nationwide view CMMC compliance as an obstacle that prevents participation in federal contracting for many small businesses, and urging the Department of Defense (DoD)/Department of War (DoW) to reengage with the small business community to address these concerns.[2] As noted in the letter, "small manufacturers have submitted

[1] Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), 90 Fed. Reg. 43560 (Sept. 10, 2025)
[2] U.S. Small Bus. Admin., Office of Advocacy, Comment Letter: Comments on DOJ's Request for Information — Anti-Competitive Regulations Task Force (June 20, 2025), https://advocacy.sba.gov/wp-content/uploads/2025/06/Comment-Letter-DOJ-RFI-on-Anticomp-Regs-Task-Force.pdf

cost data to Advocacy that portray the impacts of Level 2 certification compliance to be…between $150,000-800,000 in upfront costs plus $5,000-7,500 every month in consulting expenses. When adding in costs to maintain their systems over time, many small businesses have said that they will pay $1-2 million or more in compliance costs. These estimates do not account for any changes in the compliance standards, which would likely add even more costs." CMMC 2.0 is likely to shrink small business participation in federal contracting and raise overall procurement costs, as firms pass new cybersecurity compliance expenses into their overhead estimates and rates.

We supported the Section 886, CMMC Certification Assessment support, in the House-passed National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2026 (H.R. 3838) directing the DoD/DoW, SBA, and Internal Revenue Services (IRS) to report to Congress on the resources available to small businesses to achieve CMMC compliance.[3] We encourage the House to require the DoD/DoW to provide resources to help small businesses achieve CMMC compliance, thereby securing the defense industrial base.

CMMC is not a resource for providing cyber protection, but rather a cyber process that implements a set of best practices through compliance. Unfortunately, attackers constantly evolve their tactics at a faster pace than the government can change policy, or companies can implement those changes. As noted in the December 2, 2025, hearing, AI is increasing common cybersecurity threats to small businesses. Cyber criminals utilize AI to operate and launch cyberattacks at large and broad scales. We support the recommendation raised during the hearing to consider small businesses who do business with the federal government part of our critical national infrastructure (CNI). Being classified as CNI enables small businesses to receive prioritized federal cybersecurity support: threat intelligence, incident-response assistance, and access to resilience resources.

[3] Text - H.R.3838 - 119th Congress (2025-2026): Streamlining Procurement for Effective Execution and Delivery and National Defense Authorization Act for Fiscal Year 2026, H.R.3838, 119th Cong. (2025), https://www.congress.gov/bill/119th-congress/house-bill/3838/text.

GOVCON SMALL BUSINESS COALITION

Conclusion

The strength of America's defense industrial base depends on the vitality of small businesses. Yet rising compliance costs risk stagnating or shrinking that base, especially given the fact that current monetary based size standard decisions are not keeping pace with the economic realities of industry cost increases. If not addressed, this challenge threatens to weaken competition, limit innovation, and undermine national security.

Thank you for the opportunity to submit the Coalition's testimony. We look forward to working with the Committee to advance policies that support America's small businesses and strengthen those who provide critical goods and services to the federal government.