Aug. 14, 2026

The Honorable Pete Hegseth
Secretary of War
U.S. Department of War
1000 Defense Pentagon
Washington, D.C. 20301-1000

RE: Department of War's Request for Information on reforming the Cybersecurity Maturity Model Certification (CMMC) program; Docket No. WHD-2026-0001; RIN 1235-AA50 (91 Fed. Reg. 9932, February 27, 2026)

Dear Secretary Hegseth:

The National Small Business Association (NSBA) appreciates the opportunity to respond to the Department of War's Request for Information on reforming the Cybersecurity Maturity Model Certification (CMMC) program. NSBA is the nation's oldest small-business advocacy organization, a nonpartisan association representing 65,000 members in every state and industry, including manufacturers, technology firms, and other small businesses that make up the defense industrial base (DIB). Our comments here draw on input from across that membership, including the Small Business Technology Council (SBTC), NSBA's council representing 6,000 small firms in the SBIR/STTR pipeline, and individual small-business contractors and manufacturers who have raised these issues directly with us.

We commend the Department's decision to suspend Phase II requirements and we welcome the establishment of the CMMC Reform Task Force. The following recommendations reflect our general views on how program reforms can best serve small businesses that exist in, or are attempting to enter, the DIB.

A Framework Should Fit the Business, Not the Other Way Around

NSBA's position on CMMC has never been that small businesses should be exempt from cybersecurity obligations. Our concern is that a uniform certification mandate treats every contractor as if it carries the same risk profile and the same balance sheet, when in reality the DIB includes everything from six-person specialty manufacturers that touch CUI only through an occasional technical data package, to SBIR-funded technology firms doing continuous, CUI-intensive R&D, to businesses far outside the tech sector that hold a single defense contract. A framework calibrated to the risk actually presented will do more for security than a flat certification gate that applies the same cost regardless of exposure.

NSBA recommends the Task Force build its replacement framework around tiered assurance: annual, evidence-backed self-assessment and executive affirmation as the default posture for small and mid-sized contractors with limited or episodic CUI exposure, with mandatory third-party or government-led assessment reserved for objectively defined higher-risk categories, such as mission-critical programs, high-volume or highly sensitive CUI processing, or contractors with a demonstrated history of security incidents.

Help Small Businesses Build Compliance Infrastructure

A recurring theme across our membership is that the most burdensome cost isn't the security control itself, but the expectation that each of thousands of small contractors independently stand up a bespoke compliance environment. We recommend that the Department pursue shared infrastructure instead: whether through a NIST- or DoW-administered portal small businesses can use to handle protected data without replicating government-grade security independently, or through a competitively selected commercial platform that small contractors can affordably adopt off the shelf. Either path is preferable to the current default of thousands of one-off, expensive builds, particularly given that even large, well-resourced firms have recently shown that bespoke security architecture is no guarantee against sophisticated intrusion.

Eliminate Duplicative Verification

Small businesses report spending significant time reformatting and resubmitting the same compliance evidence to multiple prime contractors, customer portals, and assessors, even when nothing about their systems has changed. The Task Force should establish a single, authoritative evidence and status record that primes and Department components are required to accept, rather than layering their own bespoke verification demands on top of a contractor's official assessment status. Standardized evidence templates and published control mappings would further reduce the interpretive guesswork that currently drives up consulting costs without producing any additional security.

Match Compliance Cost to Contract Value

For a small business competing for a modest-dollar or intermittent defense contract, a fixed six-figure certification cost can exceed the value of the opportunity itself. NSBA recommends the Department evaluate compliance cost relative to covered contract value rather than as a flat requirement, and, consistent with recommendations we've made previously, incorporate equitable adjustment mechanisms into small-business fixed-price contracts so that new compliance costs imposed after award don't fall entirely on the contractor.

Give Small Businesses a Stable Target

Finally, whatever framework the Task Force ultimately proposes, NSBA urges the Department to resist further last-minute shifts once a path is set. Many of our members have already spent years preparing for a Phase II deadline that has now been suspended; others are unsure whether to keep investing in current self-assessment obligations while third-party requirements are paused and False Claims Act exposure continues. That uncertainty carries its own cost, distinct from the cost of any given control. A revised framework, once finalized, should come with a clear, adequately long implementation runway and a firm commitment to stability, so small businesses can plan and invest with confidence rather than bracing for the next revision.

Conclusion

NSBA appreciates the Department's willingness to pause and rethink an approach that could have pushed capable small businesses out of the defense supply chain. We support strong, enforceable cybersecurity requirements, and we believe the recommendations above would achieve that goal more efficiently, and more fairly, than the framework Phase II would have imposed. We would welcome the opportunity to participate in any small-business working group, pilot program, or further consultation the Task Force convenes as it finalizes its recommendations."

Respectfully,

Todd McCracken
President & CEO
National Small Business Association
1156 15th Street NW, Suite 1100
Washington, D.C. 20005