

July 16th, 2026

To Our Suppliers:

CMMC Phase II Suspension – Stay the Course

On July 13, the Department of War suspended the transition to CMMC Phase II while it reviews the program. Existing cybersecurity requirements remain in place, including Phase I self-assessment requirements.

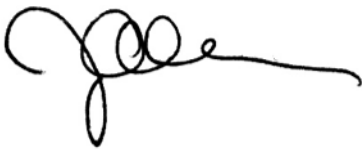
While the assessment timeline has changed, the underlying cybersecurity requirements have not. Suppliers that receive, or expect to receive, Controlled Unclassified Information (CUI) should continue implementing NIST SP 800-171 and be prepared to complete a CMMC Level 2 (Self) assessment when required.

Actions to Continue

1. Closing identified security gaps, including open Plans of Action and Milestones, and keeping your System Security Plan and supporting evidence current.
2. Maintaining current SPRS Cyber Reports and required affirmations. Before scheduling or cancelling a C3PAO assessment, confirm the applicable requirement with your Elbit America buyer.

Organizations that remain focused on maturing their cybersecurity programs will be better positioned when the revised assessment timeline is announced. Elbit America will continue enforcing the cybersecurity requirements contained in our purchase orders and will update our supplier guidance as additional direction is provided by the Department.

This pause is an opportunity to strengthen your program – not a reason to delay it.



Jason Allen
Vice President, Supply Chain
Elbit Systems of America, LLC.