SAMPLE: PLEASE UPDATE WITH YOUR CORRECT BUSINESS INFORMATION AND ENGAGEMENT DETAILS

[COMPANY NAME] Completes Key CMMC Readiness Milestone

[COMPANY NAME] recently completed a CMMC readiness review with BARR Advisory as part of our continued effort to strengthen cybersecurity, protect sensitive government information, and prepare for a formal CMMC assessment.

This milestone reflects our commitment to protecting the data entrusted to us by our customers, partners, and government stakeholders. It also helps ensure we are better prepared to meet cybersecurity requirements tied to our work in the Defense Industrial Base.

What is CMMC?

The Cybersecurity Maturity Model Certification, or CMMC, is the Department of War's cybersecurity assessment program for defense contractors and subcontractors. CMMC is designed to help verify that organizations have implemented required cybersecurity protections for systems that process, store, or transmit Federal Contract Information, or FCI, and Controlled Unclassified Information, or CUI.

FCI is non-public information provided by or generated for the government under a contract. CUI is information that requires safeguarding or dissemination controls under applicable law, regulation, or government-wide policy. Both types of information must be protected appropriately when handled in support of government contracts.

CMMC requirements may apply to prime contractors, subcontractors, and certain service providers depending on the work performed, the type of information handled, and the requirements included in the applicable contract.

What does CMMC involve?

CMMC includes three levels, with requirements increasing based on the sensitivity of the information involved and the cybersecurity risk associated with the work. For organizations pursuing CMMC Level 2, the requirements align with NIST SP 800-171 Revision 2 and focus on protecting CUI. Level 2 may require either a self-assessment or an assessment by an authorized CMMC Third-Party Assessment Organization, or C3PAO, depending on the solicitation and contract requirements.

Preparing for CMMC typically includes:

- Identifying where FCI and CUI are received, stored, processed, and transmitted;
- Defining the systems, users, locations, and service providers that are in scope;
- Implementing security controls aligned with CMMC and NIST SP 800-171;

- Developing and maintaining a System Security Plan;
- Collecting evidence that demonstrates controls are implemented and operating; and
- Preparing for ongoing monitoring, annual affirmations, and future assessments.

What this milestone means

As part of our readiness efforts, [COMPANY NAME] worked with BARR Advisory to evaluate our current cybersecurity posture, review our CMMC scope, identify potential gaps, and prepare for the next stage of our CMMC journey.

This readiness work is an important step toward formal assessment. It does not represent final CMMC certification, but it helps us better understand our environment, prioritize remediation, and prepare for the level of evidence and documentation expected during a CMMC assessment.

“Completing this readiness milestone is an important step for [COMPANY NAME] as we continue strengthening our cybersecurity program and preparing for CMMC,” said [COMPANY REPRESENTATIVE NAME, TITLE]. “It reflects our commitment to protecting sensitive information, supporting our customers’ missions, and meeting the expectations of the defense community.”

Our commitment to customers

Cybersecurity is not a one-time project. It is an ongoing responsibility. As we continue our CMMC journey, [COMPANY NAME] remains committed to improving our security program, protecting sensitive information, and supporting the customers and partners who rely on us.

Current and prospective customers interested in learning more about [COMPANY NAME]’s CMMC readiness efforts may contact [NAME] at [PHONE/EMAIL].