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

[COMPANY NAME] Achieves CMMC Level 2 Compliance After C3PAO Assessment

[COMPANY NAME] has successfully achieved Cybersecurity Maturity Model Certification (CMMC) Level 2 following the completion of an independent assessment conducted by an authorized Certified Third-Party Assessor Organization (C3PAO). But what does that mean for us as an organization—and for you as our customer?

At [COMPANY NAME], maintaining strong processes and procedures for data security is our top priority. To validate that our systems and controls are properly designed and implemented to protect sensitive information and meet CMMC requirements, we engaged BARR Advisory, an authorized C3PAO, to perform a formal assessment.

The successful completion of this assessment has resulted in [COMPANY NAME] achieving CMMC Level 2 certification, demonstrating our compliance with the cybersecurity requirements established by the U.S. Department of War.

In this blog post, we'll explain what it means to be CMMC certified and what this milestone represents for our organization and our customers.

WHAT IS CMMC?

CMMC is a cybersecurity framework developed by the U.S. government aimed at protecting sensitive government information and reducing risk across the Defense Industrial Base (DIB).

The framework outlines security requirements for organizations that handle Federal Contract Information (FCI)—communications related to government contracts, such as contract details, RFPs, and other collaborative documents—and Controlled Unclassified Information (CUI)—sensitive but unclassified government information, such as technical schematics, research data, and procedural documents, that could pose a national security risk if exposed.

Organizations that work with the Department of War and handle FCI or CUI, or that could impact the security of that information, must comply with CMMC.

WHAT DOES CMMC COMPLIANCE INVOLVE?

To align with CMMC requirements, organizations must prove that they have implemented cybersecurity practices established by the Department of War based on the level of risk associated with their work. These practices are designed to form the foundation of a strong cybersecurity program that can effectively protect sensitive government information.

Those foundations include:

- Identifying and protecting sensitive government information, including FCI and CUI;
- Implementing security controls aligned with established standards, such as NIST SP 800-171;
- Enforcing strong identity and access management practices;
- Maintaining a proactive approach to risk management and system security;
- Monitoring systems and processes to detect and respond to potential threats; and,
- Developing and maintaining comprehensive security documentation, including a System Security Plan (SSP).

WHAT DOES THIS MEAN FOR [COMPANY NAME]?

The CMMC framework includes three levels of compliance, each with increasing requirements and validation expectations. As part of our commitment to protecting sensitive government information, [COMPANY NAME] sought and achieved CMMC Level 2 certification.

To achieve this certification, we partnered with BARR Advisory as our C3PAO to complete our formal CMMC Level 2 assessment.

“Achieving CMMC Level 2 certification marks a significant milestone for [COMPANY NAME],” said [COMPANY REPRESENTATIVE NAME, TITLE]. “This accomplishment reinforces our commitment to safeguarding sensitive information and provides our customers with confidence that we meet rigorous cybersecurity standards required for government and defense-related work.”

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