



CMMC & SBIR/STTR

Navigating CMMC in the Department of War's (DoW) Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs



On July 13, 2026, the DoW announced the immediate suspension of the Cybersecurity Maturity Model Certification (CMMC) Phase II requirements, originally scheduled for November 10, 2026. All CMMC Phase I (Level 1 and 2 self-assessment) requirements remain firmly in place.

CMMC ensures companies protect sensitive information when working on government contracts and requires contractors handling Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) implement adequate cybersecurity practices to protect the defense industrial base.

KNOW WHERE YOU STAND

APPLYING FOR AN AWARD

Check the topic's projected CMMC level requirement on the DoW SBIR/STTR Innovation Portal (DSIP) Topics and Topics Q&A page.

Carefully review all CMMC requirements – compliance is required prior to award.

ALREADY HAVE AN AWARD?

You are responsible for the requirements **currently on your funding agreement.**

Review all funding agreements and **contract modifications** for CMMC requirements.

TIPS TO GET READY

1 Plan Beyond a Single Award
Establish cybersecurity practices that support future Department of War opportunities.

2 Use Technical and Business Assistance
Leverage TABA funding to strengthen your cybersecurity and business capabilities.

3 Take Advantage of Free Resources
Leverage Project Spectrum and other DoW cybersecurity resources to support your compliance efforts.

4 Stay Informed
Monitor solicitation updates and evolving CMMC guidance throughout the acquisition process.

REFERENCES

CMMC Marketplace, including C3PAOs
DoW CIO – CMMC FAQ

DoW Implementation Guidance
DoW CUI Program