

CYBERSECURITY MATURITY MODEL VERIFICATION

LBMC

INFORMATION SECURITY

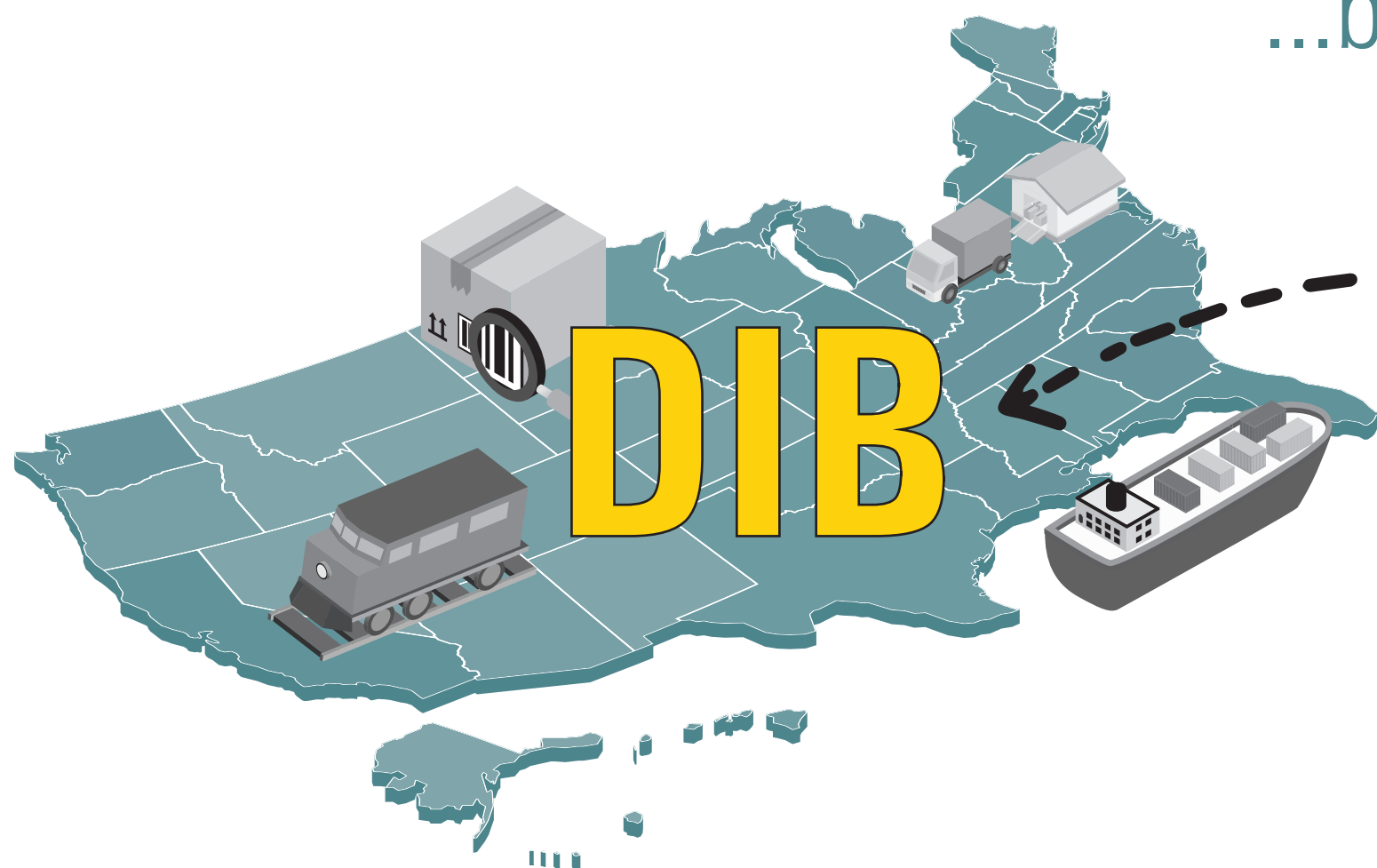
The Cybersecurity Maturity Model Certification (CMMC) accreditation framework impacts the U.S. Department of Defense (DoD) contractors, supply chain, solution providers, and systems integrators.

What is the Cybersecurity Maturity Model Certification (CMMC)?

CMMC is the Cybersecurity Maturity Model Certification, which is in development to help protect the Department of Defense's supply chain from cybersecurity related threats. The DoD is including the requirement for certification against the CMMC maturity model in future contracts, which includes subcontractors as well.



...but why do we need it?



The supply chain, referred to in DoD circles as the **Defense Industrial Base** or DIB, could potentially be the target of our adversaries because vendors in the DIB may have sensitive or confidential information related to the nation's security. The idea is that without Cybersecurity serving as a secure foundation, functions are at risk across all aspects of the nation's defense industrial base.

Global cyber-attacks on the DoD supply chain from foreign adversaries, industry competitors, and international criminals are at the forefront of US national security concerns. Countries like China, Russia, and North Korea exfiltrate over \$600 billion in the US (1% global GDP), according to Ellen Lord, Undersecretary of Defense for Acquisition and Sustainment. Even today, these bad actors are using the COVID-19 pandemic as cover for their nefarious actions while organizations are distracted as they extend their business operations from physical offices to individuals' homes.



Who does CMMC apply to?

Three hundred thousand companies are involved in the Defense Industrial Base (DIB) to some extent, whether they are contracting directly with the DoD or are subcontractors to larger firms. Regardless of the relationship to the DoD, all contractors will need to achieve at least Level 1.

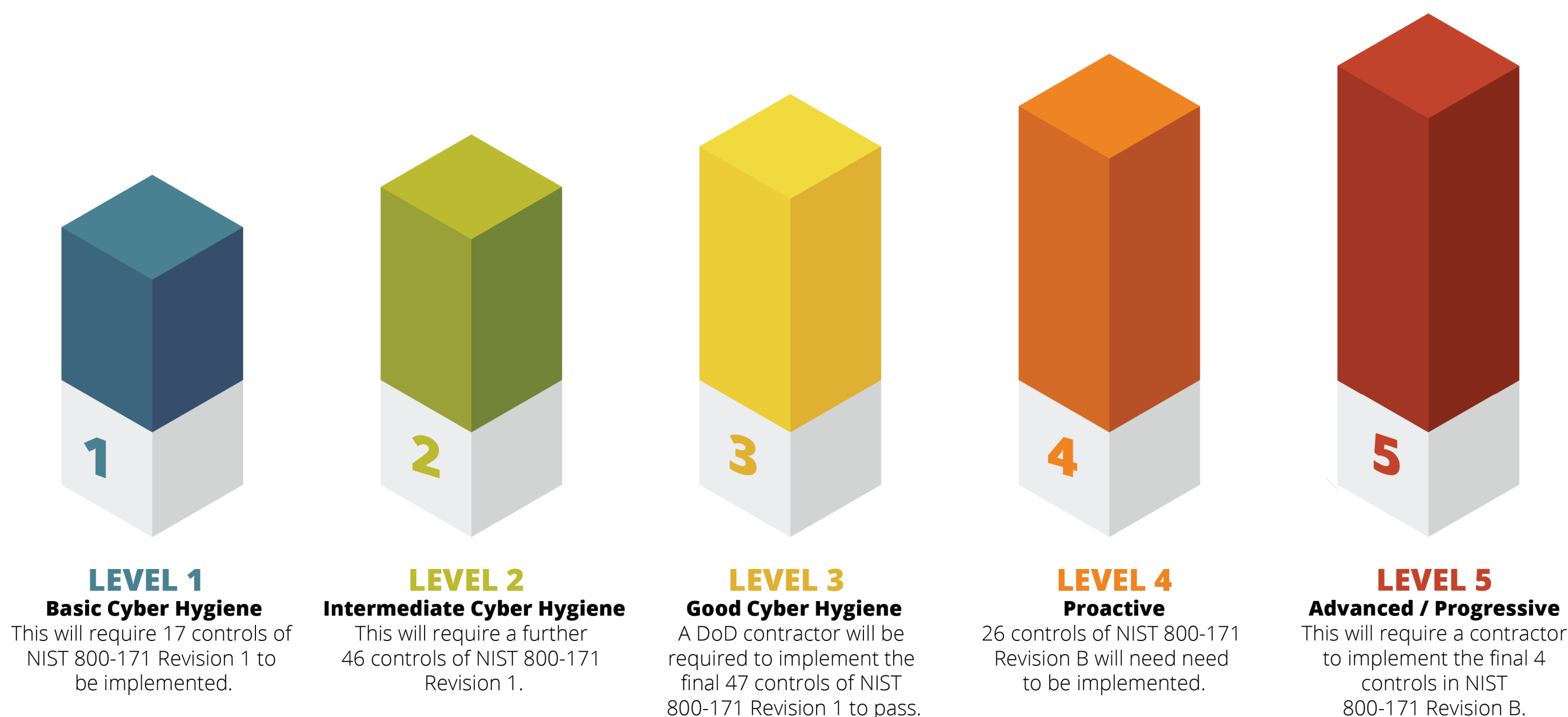
What is the CMMC Certification Process?

The CMMC initiative is largely being driven by the DoD Office of the Under Secretary of Defense for Acquisition. Generally, the certification process will flow similarly to many other certification or cybersecurity assessments, such as ISO or FedRAMP.

First, an accreditation body was put together in order to form the rules and framework around the entire assessment and certification process. Assessment bodies must then apply to the accreditation body to accredit their organization to be able to perform CMMC assessments and then train and certify their workforce to perform the assessment work. After an assessment body completes these processes, they will be able to perform CMMC assessments to certify clients.



What are the 5 Certification Levels?



When is CMMC going to be required?

CMMC is something you may need to worry about if you are a contractor or vendor to the DoD, or subcontractor to a DoD contractor. However, the DoD and CMMC accreditation body have indicated that the DoD will be deploying the requirement in new contracts over a period of years. The CMMC requirement is not expected to be inserted into active contracts. Even though you may not have to worry about it right this minute – it's never too early to start considering your security posture.

2021 Pilot  **2025** Fully Required

...have questions?

LBMC can help your organization prepare for and obtain CMMC certification. Contact us now or click the links to the right for our CMMC resources.

[Website](#)

[Blog](#)

[Podcast](#)