FedRAMP Reciprocity: A Fast Track to CMMC 2.0?

PROJECT HOSTS™
Security Compliant Clouds

www.projecthosts.com

info@projecthosts.com

Introduction

As events unfold, it's becoming abundantly clear that the war against cybercrime won't be easily won. Even the Department of Defense (DoD) — a treasure trove of cyber resources — can't single-handedly put a stop to the constant barrage of threat actors targeting government data.

Simply put, everybody has a part to play, contractors included. As foot soldiers on the frontline, DoD suppliers are an essential piece of the puzzle. Consequently, compliance with the Cybersecurity Maturity Model Certification (CMMC) program is a vital prerequisite to working with the DoD.

Here's the problem: The goalposts are moving. With updates to CMMC around the corner, contractors need to be wary of how they can achieve and maintain compliance. Fortunately, there's hope that organizations can leverage FedRAMP authorization to gain CMMC 2.0 certification.

In this white paper, we'll discuss CMMC 2.0's changes, how it overlaps with FedRAMP and what contractors can do to fast-track compliance.

Understanding CMMC 2.0

CMMC stands for Cybersecurity Maturity Model Certification. It's a comprehensive framework designed to protect information shared within the U.S. Defense Industrial Base (DIB) — a network of companies that provide goods and services to the DoD.[1]

Organizations included in the DIB process, exchange and store contract information necessary to produce the parts, systems and components required for national defense. Independent software vendors (ISVs) who provide cloud service offerings to the government also fall into this category.

The main goal of CMMC is to validate the safeguards and controls all DoD contractors use. More specifically, the aim is to enhance federal contract information (FCI) and controlled unclassified information (CUI) protection.

The DoD introduced CMMC in 2019 and launched the first iteration of the framework in early 2020. Now, the government is updating the program after many contractors objected to the complexity of the framework and assessment process.[3] The new and improved version — CMMC 2.0 — is expected to be fully implemented by 2025. However, there's speculation that it may be operational as early as 2023.

Companies without CMMC 2.0 compliance may be unable to bid for government contracts. This could result in a substantial revenue loss and, potentially, business closure.

What's new about CMMC 2.0?

The original iteration of the program included five levels of compliance. To streamline the certification process, CMMC 2.0 will reduce the number of levels down to three simplified categories:

Level 1 — Foundational: Applies to any company handling FCI.
Level 2 — Advanced: Applies to any company handling CUI.
Level 3 — Expert: Applies to companies with CUI on the DoD's highest priority programs.

Each level builds on the previous with the ultimate goal of helping organizations mitigate risk as threats evolve. The higher the level, the more "mature" the contractor's cybersecurity posture must be to adequately protect sensitive information.

CMMC vs. FedRAMP

CMMC is far from the first federally standardized cybersecurity framework. Since 2011, the Federal Risk and Authorization Management Program (FedRAMP)[4] has sought to strengthen the federal government's Cloud First strategy by enabling agencies to acquire secure cloud applications. FedRAMP is designed to provide assurance that cloud applications have been properly vetted through a process of assessment and continuous monitoring.

As a federally mandated security framework with many overlapping characteristics, FedRAMP fits neatly into the CMMC ecosystem. Like CMMC 2.0, FedRAMP compliance is assessed based on three impact levels: FedRAMP Low, FedRAMP Moderate and FedRAMP High.

Both initiatives are rooted in standards produced by the National Institute of Standards and Technology (NIST). However, FedRAMP is based on NIST 800-53, whereas CMMC uses NIST 800-171, a similar yet different framework.

Accordingly, CMMC 2.0 requires organizations to implement 14 control categories, **which include:**

- Access Control.
- Audit and Accountability.
- Awareness and Training.
- Configuration Management.
- Identification and Authentication.
- Incident Response.
- Maintenance.
- Media Protection.
- Personnel Security.
- Physical Protection.
- Risk Management.
- Security Assessment.
- Systems and Communications Protection.
- System and Information Integrity.

All of CMMC's controls — plus three others — are also outlined by NIST 800-53. Thus, it's reasonable to assume that FedRAMP authorization may position a contractor or subcontractor to also achieve CMMC 2.0 compliance via reciprocity, so long as they also implement the three remaining FedRAMP control families. These include:

- Contingency Planning.
- Planning.
- System and Services Acquisition.

Is Reciprocity Possible?

According to the NIST glossary,[5] reciprocity refers to a "mutual agreement among participating organizations to accept each other's security assessments" which allows parties to reuse resources and eliminate duplicative work. In other words, reciprocity allows you to utilize your validated assessment for one framework and apply it toward compliance with another.

There are numerous benefits to reciprocity. Streamlining the requirements between CMMC and FedRAMP would likely ease the burden on contractors, and mitigate a shortage of assessment organizations who are necessary to complete the process. Reciprocity would also minimize redundant effort and cost associated with re-assessing for a standard once a company has already been authorized.

The good news is that CMMC 2.0 has made it easier for reciprocity to become a reality. In its prior iteration, the most significant challenge was converting the five compliance levels to the three FedRAMP levels. Now, with three compliance categories in CMMC 2.0, there's a clearer path between the two programs.

A similar sticking point was the inability of organizations to use plans of action and milestones (POAM). For instance, under the FedRAMP program, an ISV can be found FedRAMP compliant without having fully implemented all controls, so long as they have a specific action plan for doing so in the next six months. CMMC 1.0, however, did not allow such flexibility. The new iteration affords companies the leniency to implement POAMs under certain circumstances.

Perhaps the most promising sign that reciprocity will be possible is that the Pentagon already practices it. Indeed, the government's internal auditors give organizations credit for implementing FedRAMP controls. However, the DoD has yet to disclose how such a system would work under the CMMC 2.0 program.

Compliance as a Service

Although it's not set in stone, it appears likely that FedRAMP reciprocity is more than just a pipe dream for government contractors. Thus, organizations can best prepare for their CMMC 2.0 requirements — which could go into effect as soon as 2023 — by becoming FedRAMP-authorized.

That said, compliance still isn't easy. It takes time, money and manpower to do it on your own. Fortunately, that's where compliance as a service comes into play.

Take Project Hosts, for example. Our turnkey compliance services ease the burden on organizations as they work through the assessment process, ultimately reducing the cost and time needed to earn a FedRAMP authorization.

ISVs who connect their cloud applications to our platform-as-a-serving offering, the General Support System, instantly offload 80% of FedRAMP security controls to us. Why? Because the GSS is already FedRAMP authorized. This means assessors only need to evaluate the remaining controls at the software level, speeding up the process and taking the load off your shoulders.

ISVs who connect their cloud applications to our platform-as-a-serving offering, the General Support System, instantly offload 80% of FedRAMP security controls to us.

Why? Because the GSS is already FedRAMP authorized.

Get started with Project Hosts

As the DIB anxiously awaits further updates on CMMC 2.0, forward-thinking businesses know that compliance doesn't happen overnight. With compliance services delivered by Project Hosts, you can get ahead of the game and make sure you're set up for success when CMMC 2.0's requirements go into effect.

Whether by reciprocity or not, Project Hosts is here to help. Contact our team for more information about our turnkey compliance as a service offering.

Sources

1. https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/15/fact-sheet-department-of-defense-releases-new-report-on-safeguarding-our-national-security-by-promoting-competition-in-the-defense-industrial-base/
2. https://isoo.blogs.archives.gov/2020/06/19/%E2%80%8Bfci-and-cui-what-is-the-difference/
3. https://dodcio.defense.gov/CMMC/
4. https://www.fedramp.gov/
5. https://csrc.nist.gov/glossary/term/reciprocity