CMMC

WHAT YOU NEED TO KNOW

CATALYST CONNECTION℠
POWERING POTENTIAL

CATALYSTCONNECTION.ORG

BANK OF AMERICA

WHAT IS CMMC?
CYBERSECURITY MATURITY MODEL CERTIFICATION

If you are a defense contractor, the Department of Defense (DoD) is requiring that all companies submitting a bid on defense contracts will need to prove that they are certified in a basic level of cybersecurity standards.

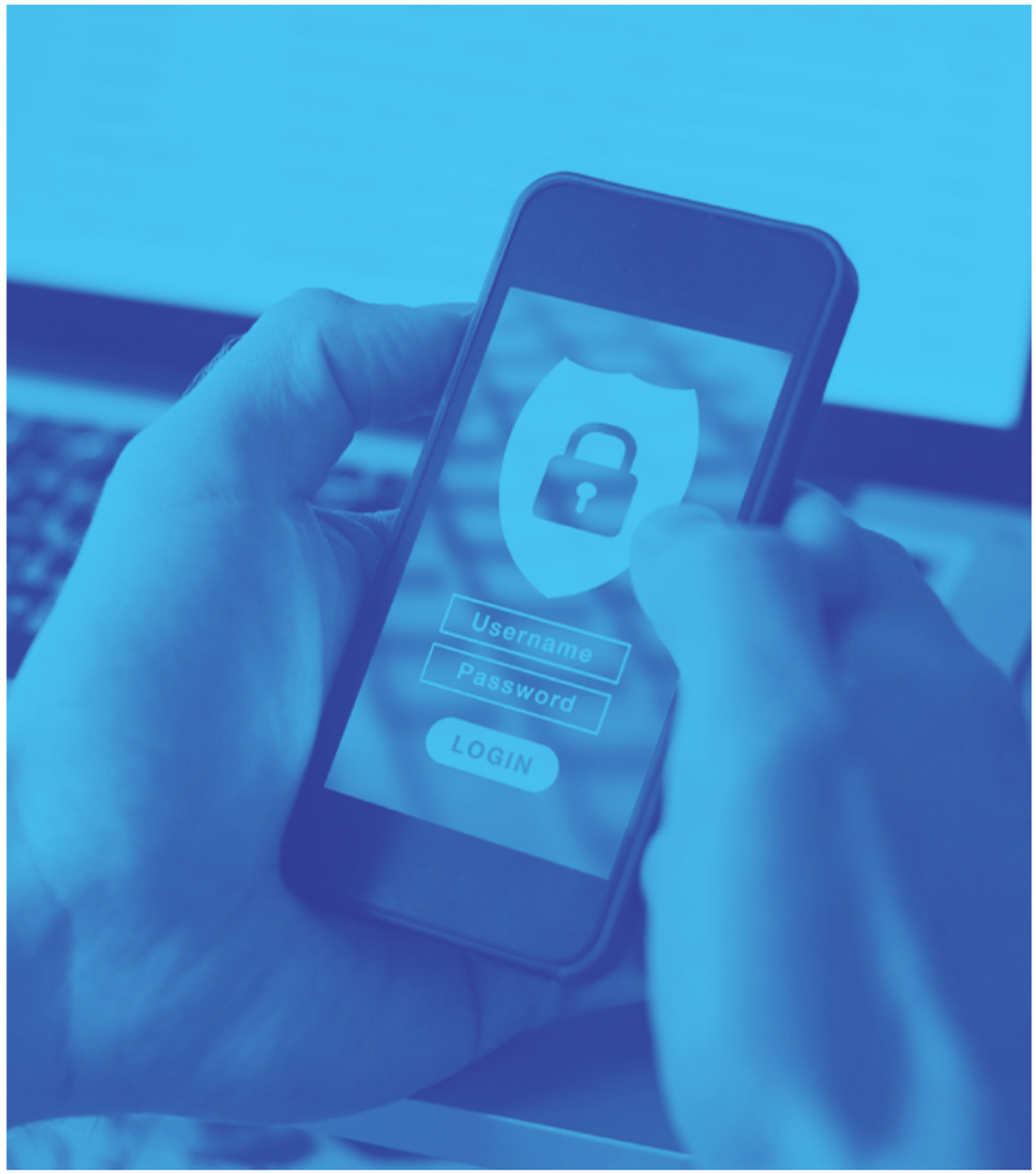
The Cybersecurity Maturity Model Certification (CMMC) is a unified standard that was designed to address cybersecurity issues for Department of Defense (DoD) contractors.

When do Contractors Need to be Certified?

In late 2020, a few DoD contracts were chosen to be the first ones that will require CMMC certification. Between 2021 and 2025, new requests of proposals (RFP) will gradually begin requiring CMMC certification. By October 2025, all DoD contractors and suppliers will have to be certified.

The Bottom Line

Within five years, every DoD contractor and supplier will need to be audited and certified by an approved third-party auditor. Preparing for this audit can take a company six months to two years. As such, many small and medium sized businesses grapple with finding the proper staff and financial resources it takes to ensure they're meeting security regulations. Therefore, finding the right CMMC compliance solution needs to be a priority for small-to-midsize DoD contractors.



IT'S TIME TO LEVEL UP IN CYBERSECURITY

An organization aiming to obtain contracts for the Department of Defense will be required to complete the CMMC certification via a third-party assessor.

In order to create a unified standard for cybersecurity, a selection of controls will be combined. They include: NIST SP 800-171, NIST SP 800-53, ISO 27001, ISO 27032, and others. Through CMMC, auditors can verify that required security controls, processes and procedures are being implemented by DoD contractors, versus allowing contractors to self-certify, which was allowed with NIST 800-171.

In an effort to reinforce NIST 800-171 requirements, CMMC emphasizes auditing and monitoring processes in order to detect any incidents that may occur. There are five levels of cybersecurity within CMMC which range from basic skills to advanced knowledge. Keep reading to learn more about each level.

CMMC LEVELS

In the very near future, a CMMC requirement from Level 1 to 5 will be specified in Sections L and M of every RFP. Having proof of certification at that level will be a requirement to even submit a bid. This means that every prime and subcontractor who works for the DoD will be required to certify, at a minimum, at Level 1. Putting a policy in place can help make the process easier if contractors wish to obtain a higher level of certification in the future. The CMMC levels are as follows:

Level 1: Basic Cyber Hygiene: implementation of 17 controls
Level 2: Intermediate Cyber Hygiene: implementation of 72 controls (includes Level 1 controls)
Level 3: Good Cyber Hygiene: implementation of 130 Controls (includes Level 2 controls)
Level 4: Proactive: implementation of 156 Controls (includes Level 3 controls)
Level 5: Advanced/Progressive: implementation of 171 Controls (includes Level 4 controls)

CMMC was designed to help organizations achieve continuous improvement. Each level builds on the previous one, which provides a clear path for increased capacity and maturity.

CMMC TIMELINE

DoD is moving quickly on CMMC. Keep this timeline on-hand in order to remember important dates and developments.

Important Dates

Mid 2020

3rd party auditors applied for accreditation

Late 2020

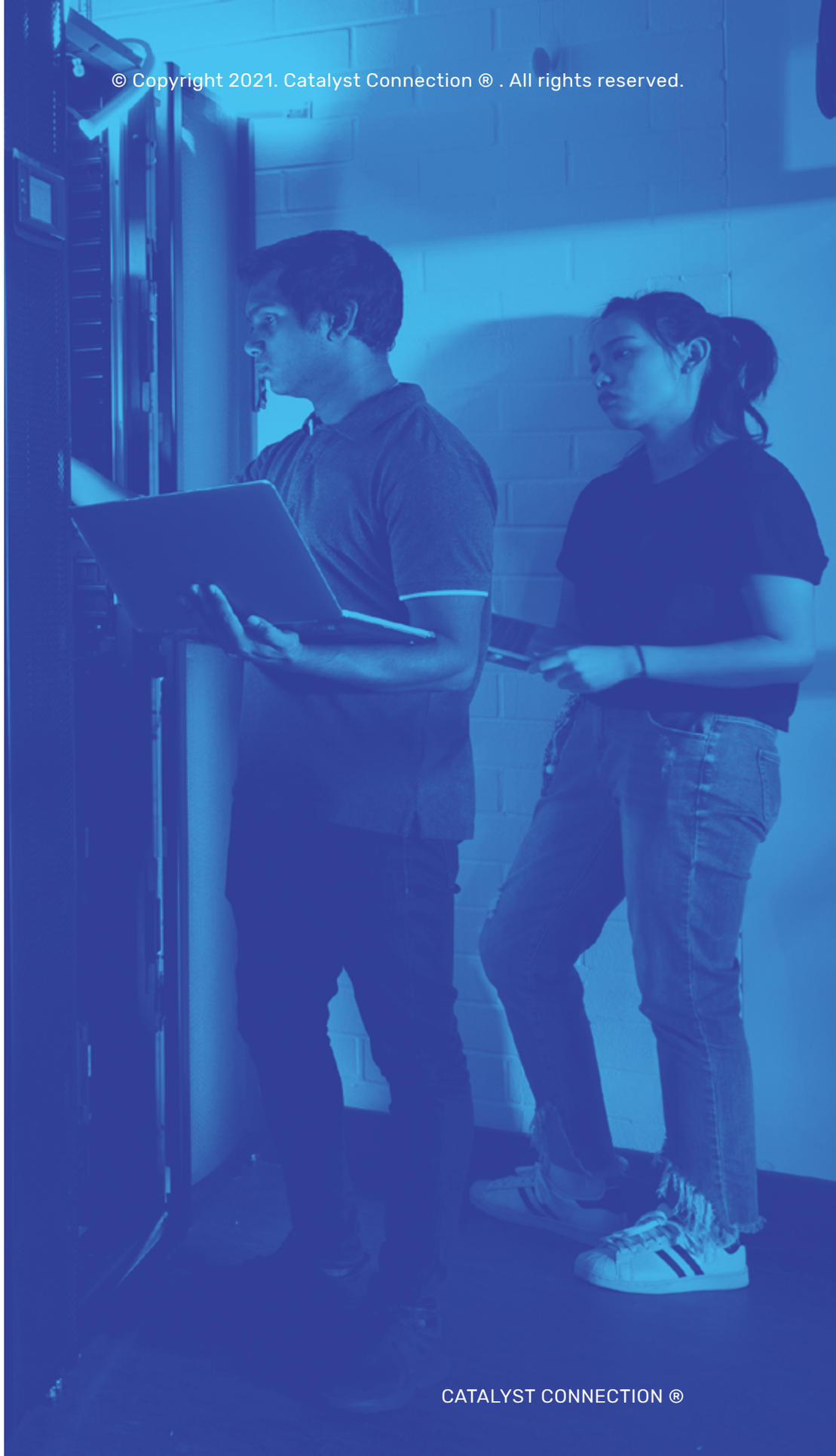
Ten DoD contracts were chosen to be the first ones that required CMMC certification. These contracts impacted 100 - 150 suppliers each.

Nov. 30, 2020

DFARS was modified to require submission of cybersecurity self-assessment for contract award. Suppliers handling controlled unclassified information (CUI) must post their self-assessment score and an estimated date for executing their Plan of Action and Milestones on the Supplier Performance Risk System (SPRS).

2021-2025

New RFPs gradually begin requiring CMMC certification. With this tight timeline, it's crucial that contractors avoid delays that may put CMMC certification and business development activities at risk. DoD contractors need to decide the CMMC level they'd like to achieve and where they currently stand with NIST 800-171 controls.



GAINING SUCCESS WITH CMMC

Similar to any compliance initiative, the success of CMMC is determined and supported by careful planning and interpretation of CMMC requirements at an organizational level. By paying attention to guidance provided by compliance experts, core business processes can avoid any major disruptions.

Here are five tips for improving your success rate with CMMC.

1. **Assess your current operations for compliance with NIST 800-171.** If you're new to compliance with Federal government and DoD procurement, reviewing this information provides context that's important to know. Your assessment should cover all 14 families and 110 security requirements. It can be an internally led effort or executed by a third-party, but with CMMC eliminating self-certification, building a relationship with a third-party now is recommended.
2. **Identify the right CMMC level for your organization.** The majority of small- and mid-sized companies will only require a Level 1 certification. However, any organization that handles CUI will require a Level 3 certification.
3. **Carefully read through contracts and RFPs for cybersecurity requirements.** It's very important to read through all of the details. CMMC requirements will be stated in Sections L and M of RFPs. If you have questions, look to procurement or compliance experts.
4. **Don't skip scoping your boundary.** Incorrectly scoping your boundary can create more work that can jeopardize your chances of achieving compliance. An experienced advisor can help you identify where your CUI or Federal Contract Information (FCI) is stored and processed.
5. **Document, document, document. Document your System Security Plan (SSP) and your Plan of Action & Milestones (POAM).** Your SSP describes your system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. Your POAM identifies your deficiencies with NIST 800-171 and maps out how you will close these gaps. Documenting every policy and procedure and collecting evidence of implementation is critical for being able to demonstrate compliance with CMMC and achieving your goal CMMC level.

“THERE’S NO SILVER BULLET SOLUTION WITH CYBER SECURITY, A LAYERED DEFENSE IS THE ONLY VIABLE DEFENSE.”

–JAMES SCOTT,

INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY

CMMC COMPLIANCE SERVICES

It’s never too early to begin your CMMC certification efforts. As your trusted consulting and training partner, our team of experts at Catalyst Connection has your back in making sure your small-to-mid-size manufacturing organization has everything you need to complete CMMC compliance requirements. Here are some things we can help with:

- Consulting with your leadership team and employees on everything they need to know about CMMC compliance
- Securing mini grants for your business to help offset certification costs
- Helping you conduct a NIST SP 800-171 self-assessment, and develop your SSP and POAM
- Identifying a 3rd party cybersecurity expert to help your team execute its POAM and prepare for your CMMC audit

Summary

Partnering with Catalyst Connection can provide your manufacturing organization with insights, expertise, and extra funding to help you better understand and achieve your target level of DoD’s cybersecurity requirements. Please reach out to our team to get started with a consultation.

CMMC

WHAT YOU NEED TO KNOW.

AUTHOR

Catalyst Connection

Catalyst Connection is a private not-for-profit organization headquartered in Pittsburgh, Pennsylvania. We provide consulting and training services to small manufacturers in southwestern Pennsylvania, accelerating revenue growth, and improving productivity. Through active collaboration with our clients and the manufacturing community, we contribute to the growth, vibrancy, and ongoing robustness of manufacturing in our region.

Catalyst Connection is supported, in part, by the Commonwealth of Pennsylvania, Department of Community and Economic Development, and by the National Institute of Standards and Technology's Hollings Manufacturing Extension Partnership.

Connie Palucka, NPDP
Vice President, Consulting
Catalyst Connection
412.918.4259
cpalucka@catalystconnection.org

Mark Sewell
Senior Consultant, Manufacturing
Catalyst Connection
412.480.7862
msewell@catalystconnection.org

FOLLOW US

/CatalystConnection /company/Catalyst-Connection

/madeinSWPA /user/CatalystConnection

CATALYST CONNECTION℠
POWERING POTENTIAL

BANK OF AMERICA

Catalyst Connection | 4501 Lytle Street, Suite 301, Pittsburgh, PA 15207 | **WWW.CATALYSTCONNECTION.ORG**

Catalyst Connection's funding sources:

- NIST MEP
- US DOD
- ARC
- PA DCED, PA L&I
- Local Foundations

CATALYST CONNECTION℠
POWERING POTENTIAL

BANK OF AMERICA

INFO@CATALYSTCONNECTION.ORG | 412.918.4300
4501 LYTLE STREET, SUITE 301, PITTSBURGH, PA 15207
CATALYSTCONNECTION.ORG