CMMC 2.0

WHAT YOU NEED TO KNOW

A Guide to Level 2 Cybersecurity Maturity Model Certification

Property of SWICKtech

SWICKtech
Cybersecurity+IT+Compliance

WHAT IS CMMC 2.0?

The Cybersecurity Maturity Model Certification (CMMC) program serves as a method of verifying appropriate levels of cybersecurity controls. These controls must meet the specific standards in place to protect Controlled Unclassified Information (CUI), and Federal Contract Information (FCI), that may be held on the U.S. Department of Defense's (DoD) industry partners' networks.

In November 2021, the DoD introduced CMMC 2.0, which has an updated program structure and requirements. The key changes from CMMC 1.0 to 2.0 are a more streamlined model, more reliable assessments, and a more flexible implementation.

Until the rulemaking process is complete, the DoD will not approve inclusion of a CMMC requirement in any DoD solicitation. An updated timeline on this process has not yet been released.

Property of SWICKtech

CMMC IS NOT JUST FOR I.T.

Consider organization-wide efforts also...

Property of SWICKtech

Physical Building Protections

(camera systems, locked spaces, badging systems, etc.)

Company Policy Documentation

(adopting new policies that adhere to CMMC requirements)

Employee Awareness & Training

(training all necessary employees on CMMC requirements)

Personnel Security

(screening/background checks of employees and documented processes for termination)

Media Protection

(setting clear expectations for employees handling CUI)

ROADMAP TO CMMC LEVEL 2

Review existing or future contracts where CMMC is applicable

Do you currently or plan to work on government contracts?

Identify where data requiring CMMC lives

Where is the CUI and FCI stored within your organization?

Obtain an implementation partner such as SWICKtech

Who will you count on to ensure your organization is prepared for an audit?

Develop Plan of Actions & Milestones (POA&M)

Detail resources, tasks, dates, etc. associated with your milestones

Implement POA&M and CMMC controls

This will include documentation, systems, processes, and more

Identify & work with a trusted 3rd party partner (C3PAO) if applicable

If applicable refer to the CMMC-AB for an updated list of C3PAOs

Become CMMC Level 2 certified!

NOTE
Timelines are dependent on which controls may already be implemented by the organization

Property of SWICKtech

HOW CAN SWICKTECH HELP?

Our team of senior industry experts are early adopters of the CMMC program, closely following its development and rollout from day one.

SWICKtech is currently working towards becoming CMMC Level 2 certified, is a Registered Provider Organization (RPO), and has two of its own Registered Practitioners (RP) designated by the CMMC Accreditation Body (CMMC-AB).

Property of SWICKtech

WHAT CAN YOU EXPECT FROM WORKING WITH SWICKTECH TO ACHIEVE CMMC LEVEL 2?

The SWICKtech engineering and project management teams will determine the best solution to address the CMMC-required data and processes. This can range with your existing compliance and levels of of cybersecurity. Often, we begin with building a secure enclave to ensure all applications and data are hosted and accessed securely, and meet compliance requirements.

Property of SWICKtech

Our team members will assist with setting up documentation framework.

SWICKtech will run through pre-assessments needed along the way, and will work directly with that third party vendor.

A cybersecurity support agreement will address ongoing technology, support, and documentation requirements to maintain compliance.

SWICKtech will implement tools and resources required along the way.

Where applicable, SWICKtech will work with the third party partners to complete the audit for CMMC Level.

Property of SWICKtech

FAQ

1 IS MY ORGANIZATION REQUIRED TO BECOME CMMC LEVEL 2 CERTIFIED?

Once the DoD finishes defining the rulemaking process or CMMC 2.0, the requirements for each organization will be as follows: If your organization handles FCI you will need to achieve CMMC Level 1, if your organization handles CUI you will need to achieve CMMC Level 2, and if your organization handles prioritized CUI/CTI you will need to achieve CMMC Level 3.

2 WHAT TIMELINE SHOULD BE EXPECTED TO BECOME FULLY READY TO MEET CMMC LEVEL 2?

CMMC requirements are currently on hold, and a new deadline has not been set. It will take an estimated 9-24 months for the DoD to complete the new rulemaking process for CMMC 2.0. Once complete, and with the maturity model requirements revoked, the estimated timeline to achieve CMMC Level 2 is 8-12 months.

3 WHAT CONSIDERATIONS DOES MY ORGANIZATION FACE AS WE ARE WORKING TOWARDS FULL COMPLIANCE WITH NIST 800-171/CMMC?

Any organizations handling FCI/CUI are required to meet the existing requirements outlined in DFARS. FCI organizations must meet FAR 52.204-21 and CUI organizations must meet DFARS 252.204-7012, which includes NIST 800-171. Failure to meet the above requirements can be pursued by the federal government under the False Claims Act (see page 13). Organizations can pursue and bid on contracts without meeting these requirements, but must achieve compliance and meet the requirements before executing any work. Organizations may lose bids if their current score for NIST 800-171 self-assessment is not available in Supplier Performance Risk System (SPRS).

Property of SWICKtech

FAQ

4 IF DFARS / CMMC-AB IS NOT READY FOR CMMC LEVEL 2 AT LARGE, WHAT IS THE CONCERN?

It takes time to implement the extent of changes and policies required. SWICKtech encourages to get started as soon as possible as this may be a multi-year endeavor.

5 DO WE NEED TO MAKE OUR ENTIRE COMPANY CMMC LEVEL 2 COMPLIANT OR ONLY PART OF IT?

The people handling any kind of CUI / FCI data need to be in a controlled CMMC Level 2 environment. Most of the time this is not all employees. Where appropriate, we can create a secure enclave to build out the military security grade environment needed for those people. This can help make the solution more affordable and attainable.

6 WHAT IS A SECURE ENCLAVE?

A turn-key solution, purpose-built for the secure, compliant handling of data subject to CMMC, DFARS, FAR, ITAR, and similar that hosts a dedicated environment, isolated from the IT infrastructure for the rest of the business. It's an assessment-ready system accompanied by documented baselines, policies, and procedures.

7 WHAT DOCUMENTATION IS REQUIRED FOR CMMC LEVEL 2?

While final guidelines are not yet available for CMMC 2.0, CMMC Level 2 environments will focus on the NIST 800-171 framework. A complete System Security Plan (SSP) and POA&M will be the minimum to get started.

Property of SWICKtech

FAQ

8 WHAT RESPONSIBILITIES BELONG TO MY ORGANIZATION VERSUS SWICKTECH'S THROUGHOUT THE PROCESS AND ONWARD?

CMMC certification is a joint journey. Various technologies and vendors will need to be involved along the way. SWICKtech will help through the entire process, and you'll need to consider 1-2 dedicated team members to champion building the required documentation and implement the changes to daily processes. SWICKtech will help lead on documentation processes upon request as well.

9 WHERE WILL THIS LIVE DIGITALLY?

Microsoft Azure Government and GCC High will be used to host secure enclave environments. Microsoft Azure Government provides security, protection and compliance services at a world-class level. Microsoft advises Azure Government services handle data subject to certain government regulations and requirements, such as highly rated FedRAMP, NIST 800-171 (DIB), ITAR, IRS 1075, DoD L4, and CJIS. Even more, the service provides the highest level of security and compliance by physically isolated datacenters and networks, located in U.S. only. Meaning, Azure Government is an isolated instance of Azure, operated by screened U.S. persons only, which is not connected to Azure Commercial Data Centers whatsoever.

10 WHAT DO WE NEED TO DO IN THE MEANTIME WHILE WE WORK TOWARDS CMMC LEVEL 2?

A great place to start is to have the organization complete the NIST 800-171 questionnaire and submit it to SPRS, resulting in a score for the company, as required in DFARS 252.204-7012.

Property of SWICKtech

GLOSSARY

Certified Third-Party Assessor Organization (C3PAO)

Refers to organizations (generally cybersecurity or accounting firms) which have CPs and CAs on staff to perform assessments. The C3PAO is the entity that contracts with Defense Contractors seeking CMMC Maturity Level certification. The C3PAO is the first line of quality control for audits.

CMMC Accreditation Body (CMMC-AB)

A private sector, non-profit organization. The DoD has granted the CMMC-AB official responsibility for some aspects of the CMMC rollout.

CMMC Certified Practitioner (CP)

A cybersecurity professional who has been sanctioned to work on an assessment team (but not lead an assessment) by the CMMC-AB. This is the entry level assessor qualification.

CMMC Licensed Training Provider (LTP)

Organizations approved by the CMMC-AB that are authorized to offer CMMC training courses using CMMC official curriculum.

Controlled Unclassified Information (CUI)

Information that the government creates or possesses, or that an entity creates or possesses for or on-behalf of the government. It also needs to fit into a category that the United States Federal Government identifies as needing special safeguarding or dissemination controls.

Cybersecurity Maturity Model Certification (CMMC/CMMC 2.0)

The CMMC will encompass multiple maturity levels that ranges from “Basic Cybersecurity Hygiene” to “Advanced/Progressive”. The intent is to incorporate CMMC into Defense Federal Acquisition Regulation Supplement (DFARS) and use it as a requirement for contract award.

CMMC 2.0 is the most recent CMMC update, which introduced key changes that build on and refine the original program requirements.

GLOSSARY

Defense Federal Acquisition Regulation Supplement (DFARS)
A published supplement to the Federal Acquisition Regulation (FAR) which adds additional guidance and requirements for DoD contracts.

Defense Industrial Base (DIB)
The worldwide industrial complex that enables research and development, as well as design, production, delivery and maintenance of military weapons systems/software systems, subsystems, and components or parts, as well as purchased services to meet US Military requirements.

Department of Defense (DoD)
An executive branch of the United States Federal Government. Its mission is to provide combat-credible military forces needed to deter war and protect the security of our nation. The DoD (specifically the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) is the government agency that is responsible for creating the CMMC model.

Federal Acquisition Regulation (FAR)
An almost 2000 page document (as of 2019) which is used to standardize policies and procedures for any contract made with the United States Federal Government (including Department of Defense). Federal contractors have to follow this regulation during bidding and performance on contracts.

Federal Contract Information (FCI)
Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

GLOSSARY

NIST SP 800-171
A 113 page document published by the National Institute of Standards and Technology (NIST). It provides "recommended security requirements for protecting the *confidentiality* of CUI... when the CUI is resident in a nonfederal system and organization." This document lists 110 security requirements with guidance on how to implement them. These requirements are re-stated in CMMC levels 1-3.

Plan of Action and Milestones (POA&M)
A document created by a cybersecurity professional which identifies missing security requirements and lays out a plan to resolve them. This document is expected to contain mid-or-high level tasks and milestones to reach a certain cybersecurity goal. POA&Ms are one of the key ways to show process maturity. They should show that you have properly funded and allocated resources to your remediation efforts. They should show progress (completion of tasks and milestones) over time.

Registered Practitioner (RP)
A person who delivers a non-certified advisory service informed by basic training on the CMMC standard.

Registered Practitioner Organization (RPO)
Organizations that provide advice, consulting, and recommendations to their clients. They are the "implementers" and consultants, but do not conduct Certified CMMC Assessments.

System Security Plan (SSP)
A document (or several documents) created by a cybersecurity professional which describes the information system of an organization. This document is expected to be very detailed and in-depth about the network, devices connected to the network, software in use, clouds in use, and security requirements that have been implemented (or not).

DISCLAIMER

CHRISTIAN DOCTRINE & FALSE CLAIMS ACT

The Christian Doctrine states that contracts with the U.S. government are not all-encompassing and may not reflect all the obligations and responsibilities of the contracting parties. Meaning, the contractor will still be held accountable for any omissions, intentional or otherwise.

Under the Christian Doctrine, even if an organization does not have the CMMC requirement in their current contracts, if they are handling any of the covered data (FCI or CUI), they still have a legal obligation to comply. Just because a contractor did not explicitly say there is CUI or FCI in a contract- by signing the contract you are agreeing to the minimum requirements, like DFARS and CMMC, set forth by the DoD.

This law states that any clause considered “a deeply ingrained strand of public procurement policy” should be read into any contract as a matter of law.

To protect themselves, it is important for all contractors and sub-contractors to be thorough in their DoD contracts. By signing a contract with the federal government, contractors are attesting they meet requirements whether they are included in the contract or not.

Compliance gaps, intentional or not, could cost you money and/or contracts. It’s imperative for each contractor in the DIB supply chain to assess their framework for such gaps. As a Registered Provider Organization (RPO) SWICKtech can help you meet cybersecurity and compliance requirements.

NEED HELP GETTING STARTED?

CONTACT SWICKTECH TO LEARN MORE, AND GET STARTED ON YOUR JOURNEY TO CMMC COMPLIANCE TODAY!

(414) 257-9266

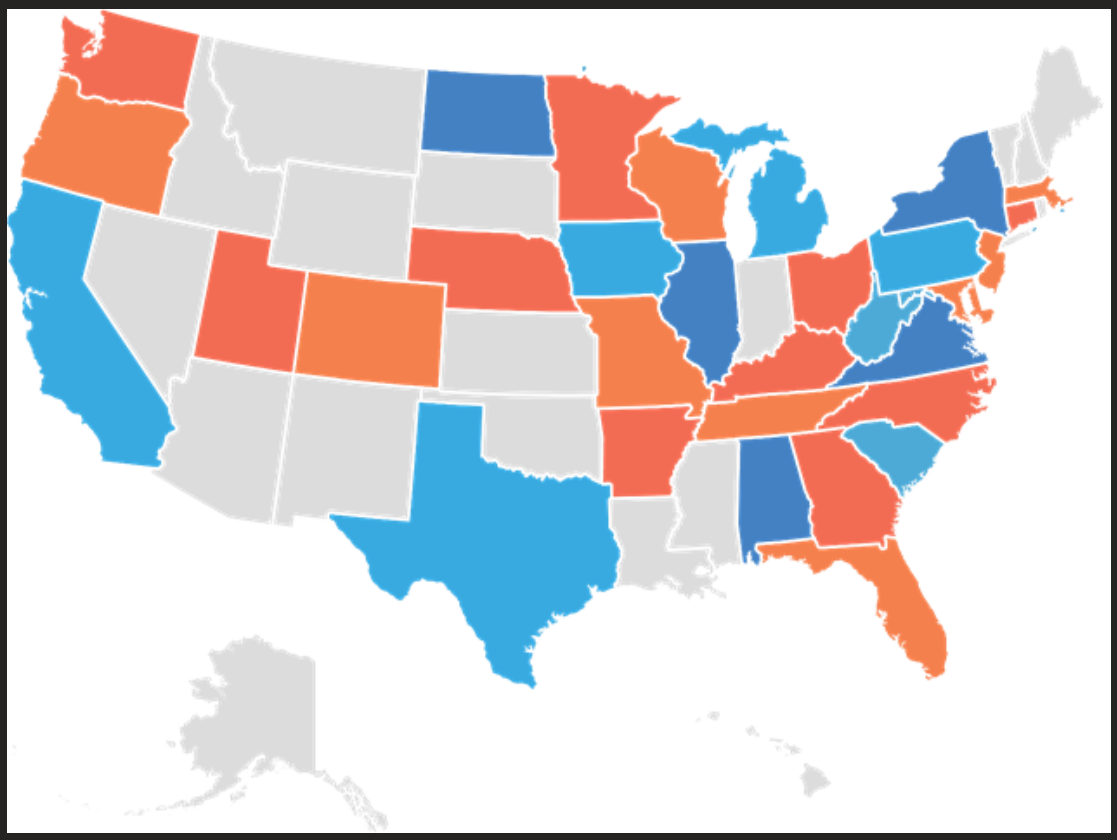
SWICKTECH.COM/GOVERNMENT-COMPLIANCE

SOLUTIONS@SWICKTECH.COM

SWICKtech

Cybersecurity+IT+Compliance

Where are SWICKtech's clients loctated?



SECURITY IS IN OUR DNA

ZERO BYTES LOST UNPARALLELED DATA SECURITY

WORLD CLASS CUSTOMER SERVICE NET PROMOTER SCORE

Learn More at SWICKtech.com