Naval Facilities Engineering Systems Command
NAVFAC SOUTHEAST

NAVFAC Southeast

Cybersecurity Maturity Model Certification (CMMC)

CIO

Andrea Freeman, Command Information Officer
Joseph Ellis, Cybersecurity Division Director/Command ISSM
22 March 2023

NAVFAC SE CIO Cybersecurity POCs

CYBERSECURITY PROGRAM OVERSIGHT

CIO: Andrea Freeman
Command Information Officer
904-542-4191

CIO2 CYBERSECURITY

CIO2: Joseph Ellis - 904-542-5839
Cybersecurity Division Director
Command Information Systems
Security Manager

CIO21: Antonio Jefferson
904-542-9056
FRCS Branch Manager
Risk Management Framework (RMF)
Requests for Authority-to-Operate (ATO)

CIO PM: Venita Hollinger
Cybersecurity Contracts Manager
904-542-2490
Responsible for tracking all
construction contracts with
Cybersecurity requirements through
to step 6 of the RMF process.

CIO4 OPERATIONAL TECHNOLOGY

CIO4: Charlie Weaver - 904-542-8482
Operation Technology Division
Director

CIO41: Kevin Gaddist
904-542-8495
OT Enterprise Support Branch Manager
Control System Platform Enclave (CSPE)
Cyber Hygiene

What is the CMMC?

The Cybersecurity Maturity Model Certification (CMMC) program is aligned to DoD’s information security requirements for DIB partners. It is designed to enforce protection of sensitive unclassified information that is shared by the Department with its contractors and subcontractors.

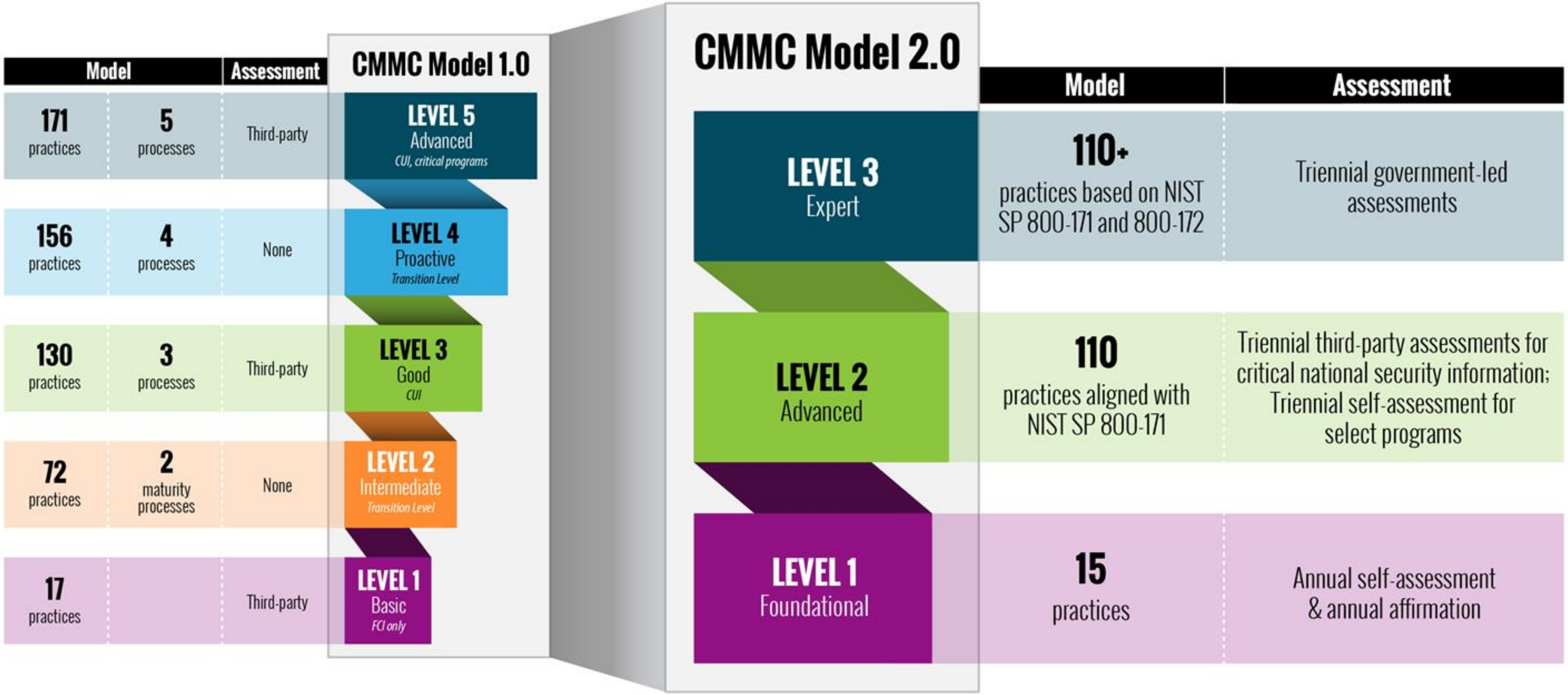
The CMMC 2.0 program has three key features:

- **Tiered Model**: CMMC requires that companies entrusted with national security information implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also sets forward the process for requiring protection of information that is flowed down to subcontractors.

- **Assessment Requirement**: CMMC assessments allow the Department to verify the implementation of clear cybersecurity standards.

- **Implementation through Contracts**: Once CMMC is fully implemented, certain DoD contractors that handle sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award.

The CMMC 1.0 vs 2.0 Model



Model		Assessment	CMMC Model 1.0
171 practices	5 processes	Third-party	LEVEL 5 Advanced *CUI, critical programs*
156 practices	4 processes	None	LEVEL 4 Proactive *Transition Level*
130 practices	3 processes	Third-party	LEVEL 3 Good *CUI*
72 practices	2 maturity processes	None	LEVEL 2 Intermediate *Transition Level*
17 practices		Third-party	LEVEL 1 Basic *FCI only*

CMMC Model 2.0	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-171 and 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Triennial self-assessment for select programs
LEVEL 1 Foundational	15 practices	Annual self-assessment & annual affirmation

Model 2 simplifies the CMMC standard for companies, while safeguarding critical Department of Defense information

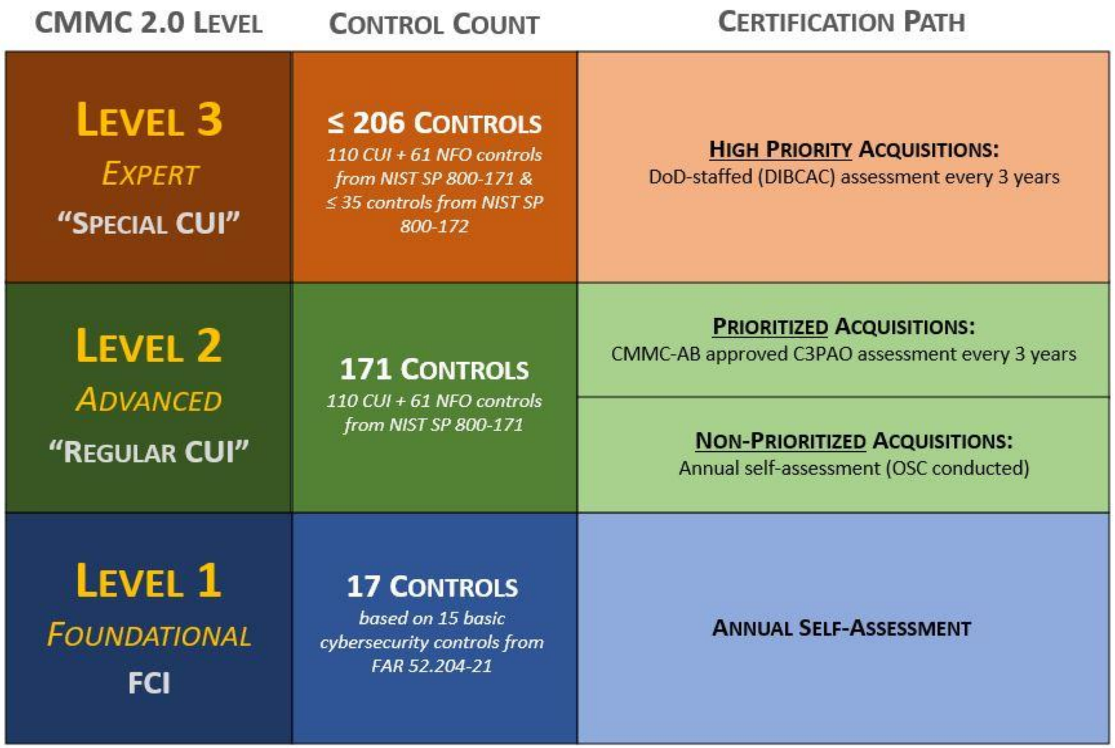
What is the difference between NIST SP 800-171 compliance and CMMC?

CMMC – is **designed to enforce** protection of sensitive unclassified information that is shared by the Department of Defense with its contractors and subcontractors. Requirements are based on NIST SP 800-171 guidelines.

NIST SP 800-171 - provides recommended security requirements for protecting the confidentiality of sensitive unclassified information residing in a nonfederal system and organization.

The major differences between these are:

- CMMC compliance does **not** necessarily mean NIST SP 800-171 compliance
- CMMC Level 1 is the lowest level of certification
- CMMC Level 2 & 3 requires application of NIST SP800-171 and associated NIST SP800-172 controls

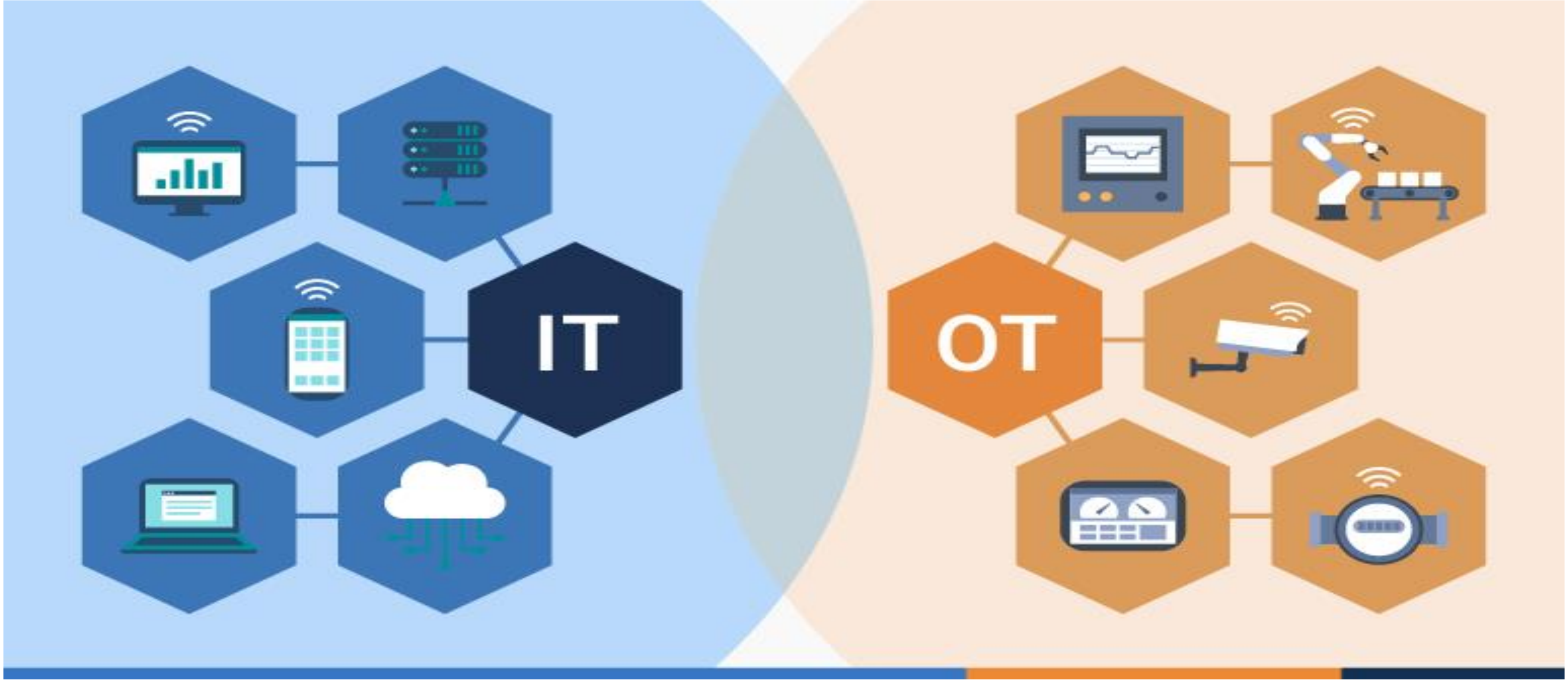


CMMC 2.0 Level	Control Count	Certification Path
Level 3 *Expert* **"Special CUI"**	**≤ 206 Controls** *110 CUI + 61 NFO controls from NIST SP 800-171 & ≤ 35 controls from NIST SP 800-172*	**High Priority Acquisitions:** DoD-staffed (DIBCAC) assessment every 3 years
Level 2 *Advanced* **"Regular CUI"**	**171 Controls** *110 CUI + 61 NFO controls from NIST SP 800-171*	**Prioritized Acquisitions:** CMMC-AB approved C3PAO assessment every 3 years **Non-Prioritized Acquisitions:** Annual self-assessment (OSC conducted)
Level 1 *Foundational* **FCI**	**17 Controls** *based on 15 basic cybersecurity controls from FAR 52.204-21*	**Annual Self-Assessment**

Source: https://www.complianceforge.com/cmmc-compliance/

Difference between CMMC and UFGS 25-05-11

Non-Government Environment **Government Environment**



CMMC
NIST SP800-171/172

UFC 4-010-06
UFGS 25-05-11

Protection of Government Data a MUST!

CMMC FAQs

What is the relationship between National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 and CMMC?

Compliance with NIST standards are levied as contractual requirements via inclusion of clauses such as FAR 52.204-21 and DFARS 252.204-7012. The relationship between CMMC and the NIST standards is that CMMC requirements will result in a contractor self-assessment, or a third-party assessment, to determine whether the applicable NIST standard (as identified by the DFARS clause) has been met. The FAR clause states the basic safeguarding requirements for CMMC Level 1 compliance. Under CMMC 2.0, a Level 2 assessment will be conducted against the NIST SP 800-171 standard and a Level 3 assessment will be based on a subset of NIST SP 800-172 requirements.

Will prime contractors and subcontractors be required to maintain the same CMMC level?

If contractors and subcontractors are handling the same type of FCI and CUI, then the same CMMC level will apply. In cases where the prime only flows down select information, a lower CMMC level may apply to the subcontractor.

Would it be safe to say that customer data is CUI and administrative data is FCI?

The definition of FCI is in FAR 52.204-21 and CUI in 32 CFR Part 2002, respectively. The DoD CUI Quick Reference Guide, located at https://www.dodcui.mil, includes information on CUI. In addition, the Defense Counterintelligence and Security Agency (DCSA) provides answers to Frequently Asked Questions at: https://www.dcsa.mil/Portals/91/Documents/CTP/CUI/21-10-13%20CUI%20FAQ%20FINAL.pdf. These FAQs describe the difference between FCI and CUI as follows: “Both CUI and FCI include information created or collected by or for the Government, as well as information received from the Government. However, while FCI is any information that is ‘not intended for public release,’ CUI is information that requires safeguarding and may also be subject to dissemination controls.”

Source Documents

- **Cybersecurity Maturity Model Certification:** https://dodcio.defense.gov/CMMC/

- **NIST SP 800-171 Rev. 2:** Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

- **NIST SP 800-172:** Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171

- **UFC 4-010-06:** Cybersecurity of Facility-related Control Systems

- **UFGS 25-05-11:** Cybersecurity For Facility-related Control Systems

Questions?