DLA
DEFENSE LOGISTICS AGENCY

The Nation's Combat Support Logistics Agency

Cybersecurity Requirements (CMMC)

WARFIGHTER ALWAYS

Overview

- **Program Goal**
- **DOJ - Civil Cyber Fraud Initiative**
- **Current Requirements**
  - DFARS 252.204-704-7012, 252.204-7019 & 252.204-7020
- **Future requirements - (CMMC 2.0)**
  - DFARS 252.204-7021
- **Contractor Resources/Key Websites**

DoD Priority: DIB Cybersecurity

- **Goal is to mitigate and reduce the risk of cyber attacks**
  - The complexity and size of the DIB offers numerous pathways for adversaries to access sensitive systems and information.
  - Implementation of the DoD mandated cybersecurity requirements on networks that process, store, or transmit sensitive unclassified information reduces the risk of cyberattacks
  - In February 2022, due to increasing geopolitical tensions, the Department of Homeland Security's (DHS) Cyber and Infrastructure Security Agency (CISA) issued a "Shields Up" advisory. Reminds the DIB to:
    - Report Cyber Incidents IAW DFARS 252.204-7012 within 72 hours of discovery to https://dibnet.dod.mil/
    - Get Assistance and Partner with:
      - DoD Cyber Crime Center's (DC3) DoD- Defense Industrial Base Collaboration Information Sharing Environment (DCISE)
      - National Security Agency's Cybersecurity Collaboration Center (CCC)
      - National Defense Information Sharing and Analysis Center (ND-ISAC)

DOJ - Civil Cyber Fraud Initiative

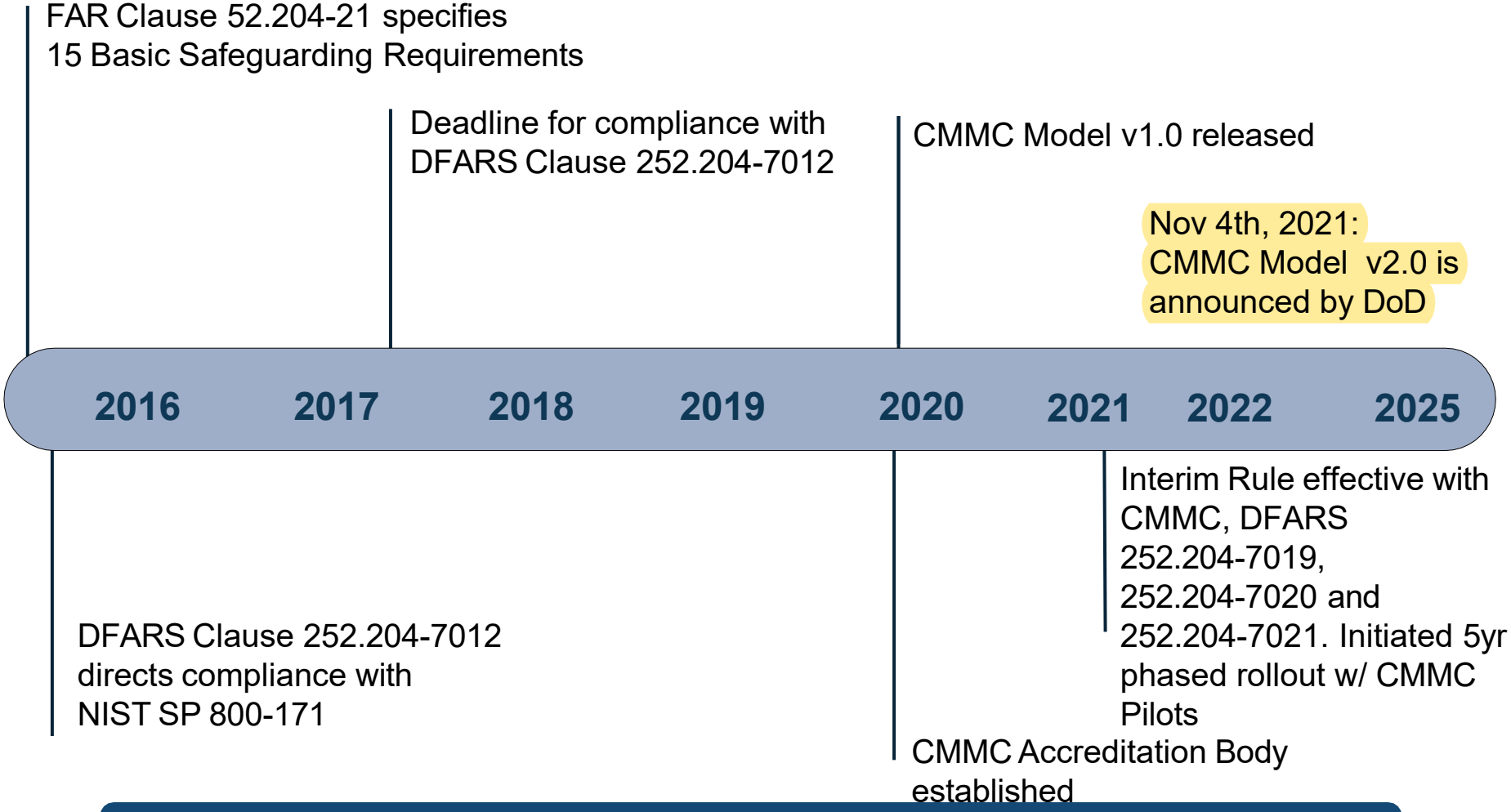
- On October 6, 2021, DOJ announced a new Civil Cyber-Fraud Initiative

- Government will use False Claims Act (FCA) to prosecute DoD contractor cybersecurity misrepresentations

- "The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches."

  - Department of Justice, Office of Public Affairs,

CMMC Regulatory & Implementation Timeline



CMMC implementation effective on November 30, 2020, per the interim rule

Current Cybersecurity Requirements

DFARS 252.204-7012

- Implement NIST 800-171
- Have a NIST- conformant SSP
- Work on POA&M
- Obtain medium assurance certificate

DFARS 252.204-7019

- At a minimum conduct NIST 800-171 Basic (self) Assessment in accordance with NIST 800-171A
- Post Basic Assessment information to SPRS
- Preparation for potential DIBCAC Medium & High Assessments

DFARS 252.204-7020

- Ensure applicable subcontractors also have results of a current assessment posted in SPRS prior to awarding a subcontract
- Requires contractors to provide access to its facilities, systems, and personnel when necessary for DoD to conduct or renew a higher level assessment

Current Cybersecurity Requirements

DFARS 252.204-7019

Notice of NIST SP 800-171 DoD Assessment Requirements

- Details located in Interim Rule DFARS Case 2019-D041.
- Applies to all DoD actions that involve CUI/CDI* with two exceptions:
  - Exclusively Commercial Off The Shelf (COTS) items
    - COTS designation made by US Government
  - Actions below the micro-purchase threshold
- The contracting officer will include in solicitations and contracts.

•Requires contractors to implement the NIST SP 800-171 standards and complete an Assessment (Basic, Medium or High).

•Contractors must ensure the results of the Assessment are posted in the Supplier Risk Management System (SPRS). Must not be older than three years.

- EFFECTIVE **November 30, 2020**

* Identified by use of Tech STOs: RD002, RD003 and/or RQ032 in the item description

DFARS 252.204-7019
Interim Rule Compliance Steps

1. Become familiar with the NIST requirements (Review Rev.2 Handbook and/or Self-Assessment Handbook).
2. At a minimum, conduct a Basic (Self) Assessment.
3. Use the DoD Scoring Template to calculate the score.
   - You may receive a negative score.
   - Negative score is acceptable under the Basic (self) Assessment.
4. Upload your score to the Supplier Risk Management System.
   - Register at the Procurement Integrated Enterprise Environment (PIEE) https://piee.eb.mil/piee-landing For registration issues, contact the PIEE Help Desk (866-618-5988).
   - Upload score at https://www.sprs.csd.disa.mil/
     For uploading issues, email basic company data such as company name, address, cage code, etc., along with the score to webptsmh@navy.mil.

Current Cybersecurity Requirements

DFARS 252.204-7020

NIST SP 800-171 DoD Assessment Requirements

- When it is necessary for DoD to conduct or renew a higher-level Assessment (Medium or High), contractors must provide the Government access to its:
  - Facilities, Systems, Personnel, Etc.
- Requires contractors ensure that subcontractors have a current Assessment posted in SPRS prior to awarding a subcontract.
  - Subcontracts that involve contract performance on CUI information only.
- Provides additional information on how a subcontractor can conduct and submit an Assessment when one is not posted in SPRS.
- Requires the contractor to include the requirements of the clause in all applicable subcontracts.
- EFFECTIVE November 30, 2020

Future Cybersecurity Requirements

In support of FY21 NDAA S.1648 the Department laid out a set of programs for implementation to help protect the DIB

- **The Cybersecurity Maturity Model Certification (CMMC)**
  - Program incorporates a unified set of cybersecurity requirements into the acquisition processes via contracting language and provides DoD with a mechanism to ensure that contractual cybersecurity requirements are fulfilled
- **The CMMC framework**
  - Maps cybersecurity practices and maturity processes
  - Builds upon existing regulations and adds verification of implementation of cybersecurity requirements
  - Uses authorized/accredited CMMC Third Party Assessment Organizations (C3PAOs), government, and contractors (self) to conduct assessments of DIB contractors' unclassified networks

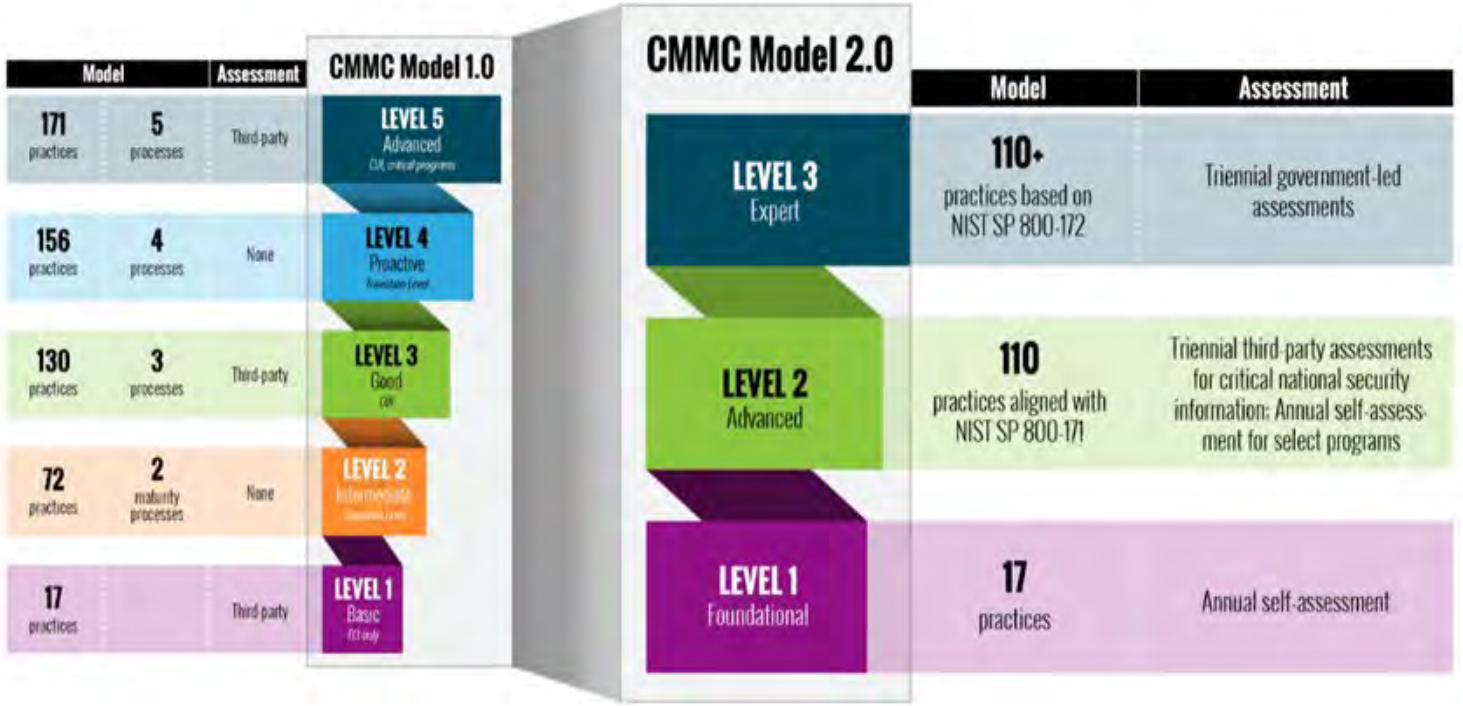
Future Cybersecurity Requirements - Update

Cybersecurity Maturity Model Certification (CMMC) 2.0

- November 4, 2021 – DoD announced an updated strategic direction of the Cyber Maturity Model Certification (CMMC) program: “CMMC 2.0”
- DoD is pausing active CMMC pilots until 2.0 has gone through the appropriated rulemaking process (estimated: 9-24 months).
  - Use of 252.204-7021 in solicitations and contracts is paused
- Reduces assessment cost, relieving some impact to small and medium-sized businesses
- Simplification: less barriers to become certified, reducing levels from 5 down to 3
- Level 1 & parts of Level 2 will be an annual contractor self-assessment.
- More available at: https://www.acq.osd.mil/cmmc/
- DFARS 252.204-7012, 7019 and 7020 requirements will remain unchanged (current requirements)

CMMC 1.0 vs 2.0

KEY FEATURES OF CMMC 2.0



Source: https://www.acq.osd.mil/cmmc/

Cybersecurity Requirements

In summary, it is important to:

- Stay vigilant and be proactive of possible cyber attacks.
- Continue preparations for the future requirements of CMMC 2.0 as soon as possible. DO NOT wait until final implementation of CMMC 2.0
- Use DFARS 252.204-7019 & 7020 as a precursor to the future requirements of 252.204-7021.

Contractor Resources

- Supplier Performance Risk System (SPRS) - https://www.sprs.csd.disa.mil/
- Email address for posting summary level scores in SPRS for Basic assessments - webptsmh@navy.mil.
- The official requirements in DFARS 252.204-7019 and 252.204-7020 can be found on the official OSD DFARS website - https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm
- Project Spectrum is a nonprofit effort funded by the DoD Office of Small Business Programs to help educate the Defense Industrial Base (DIB) on compliance with this requirement - https://www.projectspectrum.io/.
- PTAC - https://www.dla.mil/SmallBusiness/PTAP/.
- The NIST SP800-171 DoD Assessment Methodology - https://www.acq.osd.mil/dpap/pdi/cyber/index.html.
- FCA – False Claims Act - see DOJ Announcement at: https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative

Additional Key Websites

- NIST 800-171 Handbook - https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf
- National Archives CUI Registry - https://www.archives.gov/cui
- DOD INSTRUCTION 5200.48 CONTROLLED UNCLASSIFIED INFORMATION (CUI) - https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF
- DoD CUI Program - https://www.dodcui.mil/
- CMMC 2.0 information - https://www.acq.osd.mil/cmmc/
- CMMC FAQ - https://www.acq.osd.mil/cmmc/faq.html
- CMMC Accreditation Body - https://www.cmmcab.org/
- DLA Master List of Technical and Quality Requirements (Tech STOs) -https://www.dla.mil/HQ/Acquisition/Policy-and-Directives/
- "Shields Up" Advisory - https://www.cisa.gov/shields-up