ARCHER

Archer CMMC Management

Free Friday Tech Huddle

November 12, 2021

All lines are muted upon entry to this call.

Please use the Q&A panel for questions.

An RSA Business

Upcoming Events

November 17 – Virtual Product Roadmap

- *11:00 a.m. ET; 10:00 a.m. CT; 8:00 a.m. PT*

November 19 – Free Friday Tech Huddle

- *Archer Exchange Release Overview & Archer Documentation Request Tracking App-Pack Updates*

December 10 – Free Friday Tech Huddle

- *Archer Platform Release Overview and Archer Audit Management Use Case Updates*

December 15 – Virtual Product Roadmap – Americas

- *11:00 a.m. ET; 10:00 a.m. CT; 8:00 a.m. PT*

December 16 – Virtual Product Roadmap – APJ

- *Dec. 16: 11:00 p.m. ET (New York); 9:30 a.m. IST (India); 12:00 p.m. SGT (Singapore); 1:00 p.m. JST (Japan); 3:00 p.m. AST (Sydney)*

Registration required

ARCHER

Agenda

- **Overview of the new "CMMC 2.0" changes**
- **Demo of the new Archer CMMC Management use case**
- **Q&A**

As the CMMC Churns…

Cybersecurity Maturity Model Certification (CMMC) 2.0

Matthew A. Titcombe, CISSP

CMMC Provisional Assessor #17

m.titcombe@peakinfosec.us

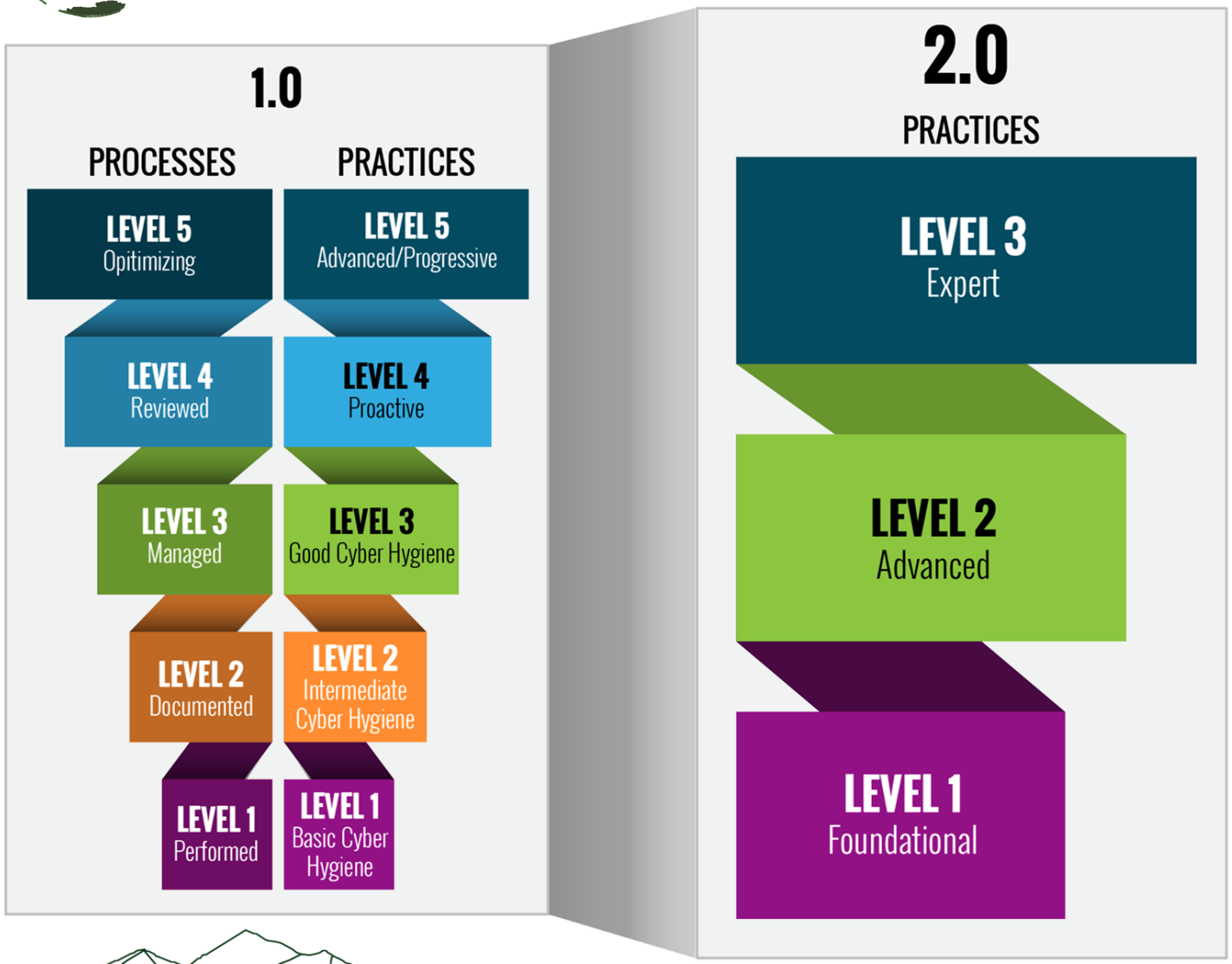
https://peakinfosec.com

Bottom-Line Up Front (BLUF)

- CMMC is not dead
- No changes to DFARS clauses -7019 & -7020
- CMMC version 1.02 Level 3 = CMMC 2.0 Level 2 = NIST SP 800-171
- Compliance to NIST SP 800-171/CMMC 2.0 Level 2 still required TODAY under DFARS clause -7012
- Level 1 (Federal Contract Information) is now Self-Attestation
- NIST SP 800-171/CMMC 2.0 Level 2 is split for Certification/Self-Attestation
- Overall timeline for when the new changes go into effect at 9-24 months out
- DoD to incentive NIST SP 800-171/CMMC 2.0 Level 2 certified firms in the interim
- Dept of Justice is still looking for new False Claims Act participants

In short, get NIST SP 800-171 Compliant

CMMC 2.0



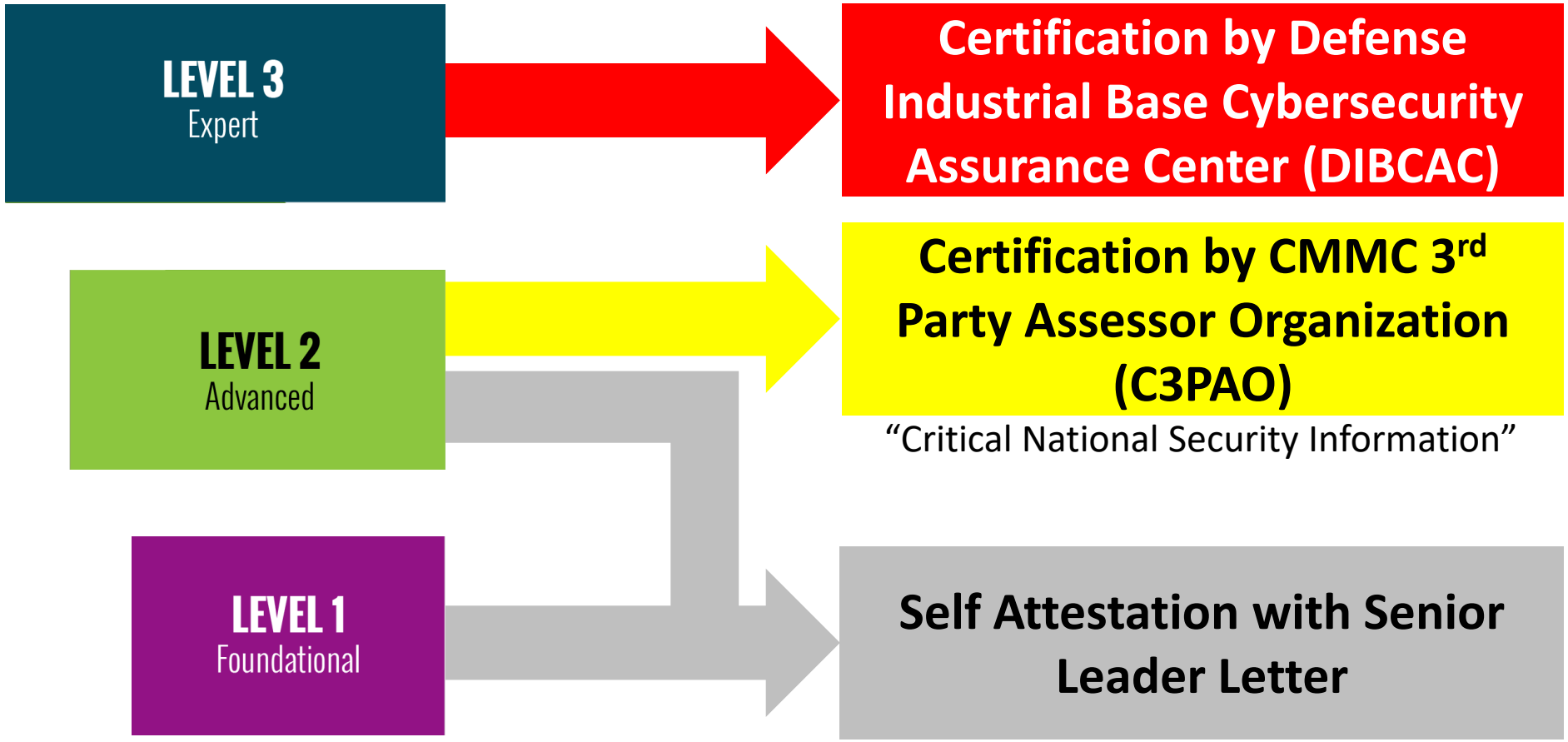
Controlled Unclassified Information (CUI) + FCI

- NIST SP 800-172 Rev 1
- NIST SP 800-171 Rev 2

Federal Contracting Information (FCI) Only

- NIST SP 800-171 Rev 2
- DFARS Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
- 48 CFR § 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems

CMMC 2.0 Details – 3rd Party Assessments

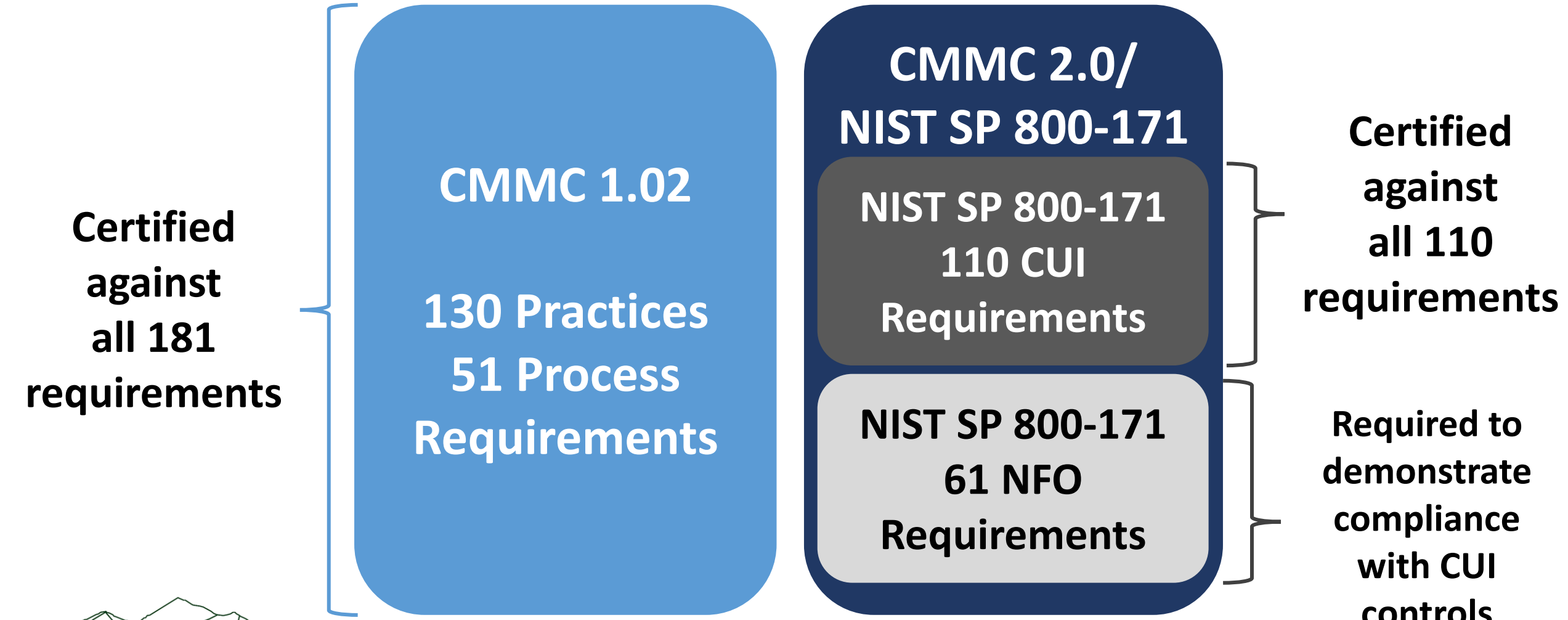


CMMC 2.0 Details – Level 2

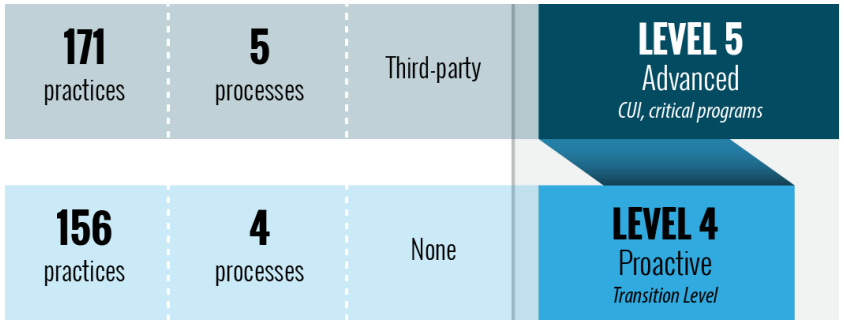
130 practices	**3** processes	Third-party	**LEVEL 3** Good *CUI*	**LEVEL 2** Advanced	**110** practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs

- **Requirements**
  - CMMC v1.02 "Delta 20 Practice" & Maturity Level requirements are gone
  - Back to the core: Compliance with 32 CFR Part 2002 – Controlled Unclassified Information (CUI) & NIST SP 800-171 Rev 2
- **3rd Party Assessments**
  - *Initially*, the bulk majority of OSC's will self-attest compliance
  - Some OSC's who process CUI that is "Critical National Security Information" will have to be certified by a CMMC 3rd Party Assessor Organization (C3PAO)
  - "Critical National Security Information" is a wholly made-up term by DoD
- **POA&Ms**
  - DoD is looking to enforce POA&Ms as a part of the contract vehicle

CMMC 2.0 Details – Non-Federal Organization (NFO) Controls



CMMC 2.0 Details – Level 3



LEVEL 3
Expert

110+
practices based on NIST SP 800-172

Triennial government-led assessments

- **Requirements**
  - CMMC v1.02 Level 4+5 Practices & Maturity Level requirements are gone
  - NIST SP 800-171 Rev2 + NIST SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171
- **3rd Party Assessments**
  - All OSCs will be audited by the Defense Industrial Base Cybersecurity Assurance Center (DIBCAC)-–C3PAOs will not certify level 3
- **POA&Ms**
  - DoD is looking to enforce POA&Ms as a part of the contract vehicle

CMMC 2.0 Details – Plans of Action & Milestones (POA&M)

- **"allow companies to receive contract awards with a POA&M in place to complete CMMC requirements"**
  - IOTW, POA&Ms for non-compliant requirements may be allowed…
- **"specify a baseline number of requirements that must be achieved prior to contract award, in order to allow a remaining subset to be addressed in a POA&M within a clearly defined timeline"**
  - "Minimum Viable Security Product" standard at contract award
  - Predefined timeline for the remaining non-compliant controls based on risk
- **"specify a small subset of requirements that cannot be on a POA&M in support of achieving a CMMC certification"**
  - Contracts cannot be awarded if these show up
- **"Highest weighted requirements cannot be on POA&M list" and "DoD will establish a minimum score requirement to support certification with POA&Ms"**
  - Likely closely aligns to SPRS scoring

CMMC 2.0 Pincer Movement

Compliant

"Sr. Leader Letter of Attestation"

Contractually Enforced POA&Ms

DoD's Intent

- "allow companies to receive contract awards with a POA&M in place to complete CMMC requirements."
- "specify a baseline number of requirements that must be achieved prior to contract award, in order to allow a remaining subset to be addressed in a POA&M within a clearly defined timeline."
- "specify a small subset of requirements that cannot be on a POA&M in support of achieving a CMMC certification."

Non-Compliant

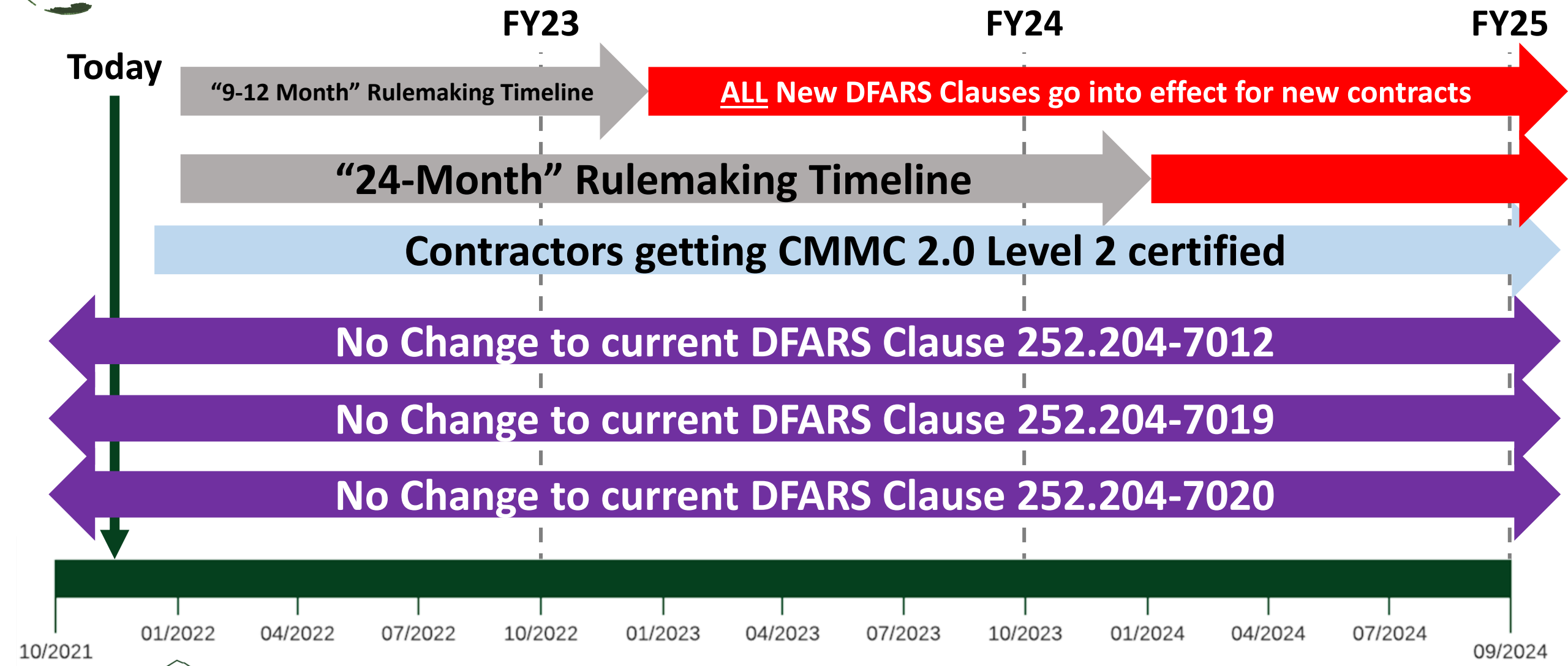
"Critical National Security Information" + Market Pressures

3rd Party Certification

Department of Justice (DOJ) announced on October 6, 2021 the launch of a "Civil Cyber-Fraud Initiative" to use the False Claims Act (FCA) to target govt contractors who allegedly put information or systems at risk. DOJ will focus on bringing actions against contractors who allegedly have knowingly:

1. Provided deficient cybersecurity products or services to the United States;
2. **Misrepresented their cybersecurity practices**; or
3. Failed to monitor and report cyber breaches.

Notional Timeline



As the CMMC Churns…

References

- Key CMMC Sites
  - National Archives & Records Administration Controlled Unclassified Information (CUI) Homepage
  - DoD Cybersecurity Maturity Model Certification (CMMC) Home Page
  - CMMC Accreditation Body (CMMC-AB)
- Key References
  - NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
  - NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information
  - NIST SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171

Key Acquisition References

- 32 CFR Part 2002 – CONTROLLED UNCLASSIFIED INFORMATION (CUI)
- 48 CFR § 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems
- DFARS Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.
- DFARS Clause 252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements
- DFARS Clause 252.204-7020 NIST SP 800-171 DoD Assessment Requirements.

- Other Key Sites
  - DoD Procurement Toolbox Cybersecurity FAQS
  - DoD CUI Program
  - Security Awareness Hub || DoD CUI Mandatory Training
  - Security Awareness Hub || Insider Threat Awareness
  - Security Awareness Hub || DoD Security Principles
  - CUI Supply – Cyber Security Compliance, CUI Supplies


ARCHER