

CMMC 2.0

What the Change Means For Your Organization



DTC GLOBAL, LLC



November 11, 2021

Panelists



Stuart Itkin
VP Coalfire Federal



Regan Edens
DTC Global



Gregg Laroche
VP Product @PreVeil



ABOUT COALFIRE FEDERAL

Coalfire Federal provides cybersecurity services to government and commercial organizations helping them protect their mission-specific cyber objectives.

Coalfire Federal is the leading FedRAMP 3PAO, a CMMC C3PAO and CMMC RPO and offers a full spectrum of cybersecurity risk management and compliance services

ABOUT STUART ITKIN

- Coalfire Federal VP CMMC and FedRAMP Assurance
- Previously VP Product Management and Marketing at Exostar, Global CMO at CEB
- Executive roles in several cybersecurity businesses
- Lead mentor at MACH 37 cyber product accelerator



ABOUT DTC GLOBAL

Focused on DoD Cyber Threat since 2006

- ✓ Led DoD's First Cyber CI Insider Threat/FIST Program
- ✓ Operationalized +\$ 3.5B in Transformative Globally Distributed Technologies
- ✓ Cross-Discipline/Horizontal/Vertical Platform & Systems Integration

Industry Trenches ITAR/DFARS/CMMC

- ✓ Large Global Prime Contractors Supply Chain Risk to Small/Micro Businesses
- ✓ Clients: \$46.8B Market Cap, 235k Employees, 300-325k Endpoints
- ✓ Industry Thought Leaders since 2015

ABOUT REGAN EDENS

- Founder, DTC Global
- Former Board of Directors CMMC-AB
- Chartered by DoD to Manage CMMC Certification
- Chairman of Standards Management Committee



ABOUT PREVEIL

PreVeil is a simple, inexpensive and secure SaaS platform for storing and sharing CUI and ITAR data in email and files.

Designed for the enterprise, PreVeil is used by leading defense contractors for CMMC compliance, Supply Chain Collaboration and Incident Response.

ABOUT GREGG LAROCHE

- VP Product Management – PreVeil
- Numerous SaaS product leadership roles across
 - Cybersecurity
 - Identity Management
 - Large scale cloud solutions



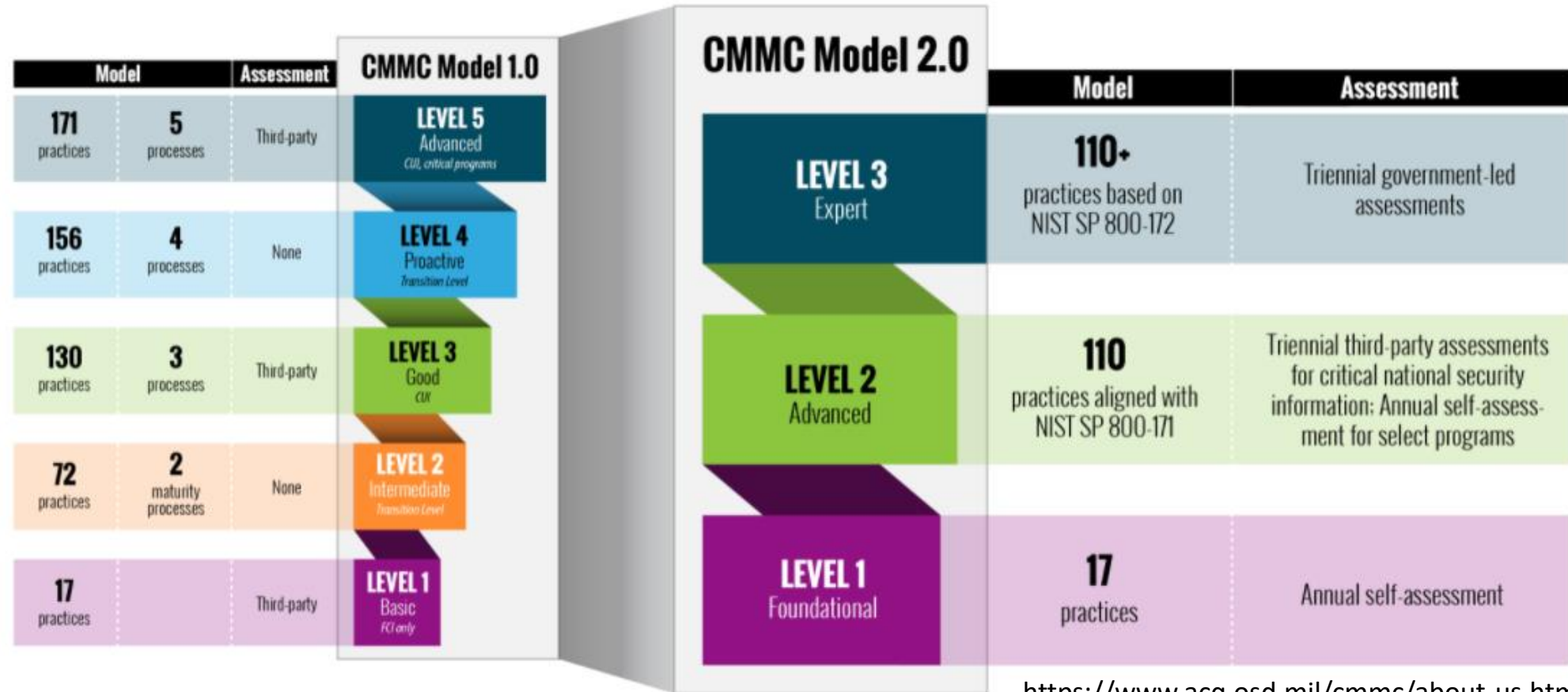
CMMC 2.0 Update

CMMC 2.0: What we know

- CMMC is not dead; It's changed
 - Exams have not been cancelled
- DFARS 252.204-7012 is still the law of the land
 - Compliance with CMMC 2.0/NIST 800-171 still required today
 - No changes to clauses 7019 / 7020
- Expect more aggressive enforcement from DoD
 - Civil Cyber-Fraud Initiative will create more False Claim Act Participants
 - Expect more aggressive requirements from primes

CMMC 2.0: What's changed

CMMC 2.0 model is streamlined: 3 versus 5 levels



<https://www.acq.osd.mil/cmmc/about-us.html>

CMMC 2.0: What's changed

CMMC 2.0 requirements mirror NIST SP 800-171 and NIST SP 800-172

- CMMC 1.02 unique practices (20 delta controls) eliminated
- CMMC 1.02 maturity processes eliminated
- CMMC 2.0 level 2 aligned with NIST SP 800-171
- CMMC 2.0 level 3 will include a subset of NIST SP 800-172 controls

CMMC 2.0 assessments change

- CMMC 2.0 Level 1 – self-assessment, entity and corporate officer attestation
- CMMC 2.0 Level 2 - bifurcated
 - Prioritized Acquisitions with CNSI: 3rd party assessment prior to award
 - Non-Prioritized Acquisitions: Self-assessment, entity and corporate officer attestation
- CMMC 2.0 Level 3 – assessed by government

CMMC 2.0: Level 1



- Requirements
 - No change
 - Still bound to 15 Information Security Requirements in 48 CFR § 52.204-21
 - NIST 800 SP 800-171 maps “FAR 52” 15 requirements to 17 practices
- C3PAO Assessments
 - Not required
 - OSC self-assess and self-attest (at the entity and individual level)
- POAMs (Plans of Action and Milestones: Not required)

CMMC 2.0: Level 2



- Requirements
 - CMMC V1.02 Delta 20 practices and Maturity Level requirements removed
 - Compliance with 32 CFR Part 2002 (Controlled Unclassified Information) & NIST SP 800-171 R2
- C3PAO Assessments – Bifurcated
 - Initially, majority of OSCs will self-assess and self-attest
 - OSCs with CUI that is CNSI (Critical National Security Information) must be certified by a C3PAO
- POAMs (Plans of Action and Milestones)
 - Limited scope, limited time
 - Enforced by contract vehicle

CMMC 2.0: What you should do now


- Get CMMC 2.0 Compliant
 - Assessment objectives: NIST 800-171A
- Don't forget about NIST 800-171 Non-Federal Organizations Controls
 - NIST SP 800-171 Appendix E
 - Controls expected to be routinely satisfied without specification
- Certify – Even if your CUI is not CNSI
 - Business decision / competitive advantage
 - May be required by your prime
 - Inoculates your company and the boss from FCA charges

Timeline & Important Tasks for CMMC 2.0

CMMC 2.0 - Basics

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

CMMC Model 2.0


Model	Assessment
LEVEL 3 Expert 	110+ practices based on NIST SP 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; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices Annual self-assessment

CMMC 2.0 - Basics

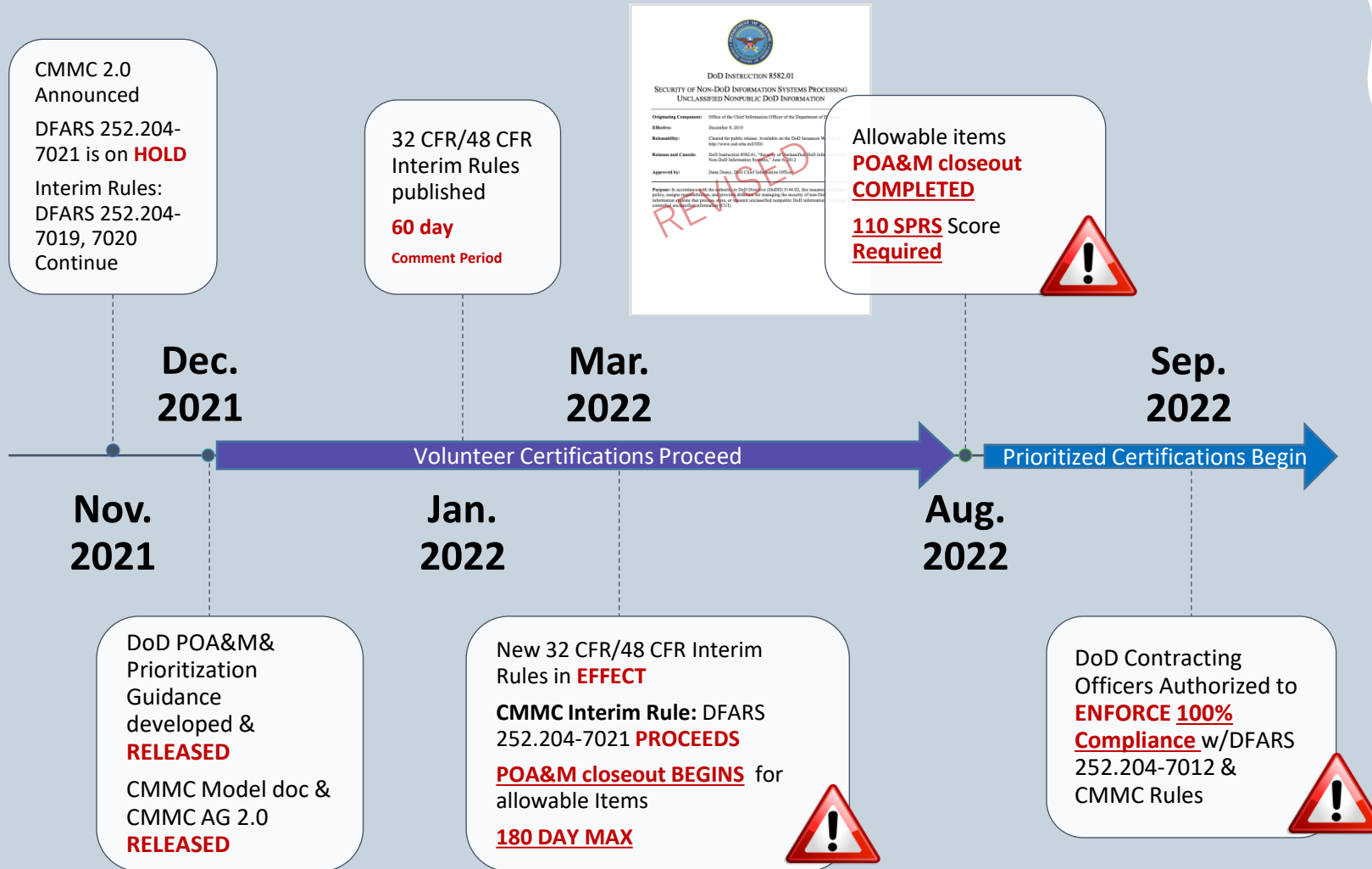
Major Impacts

- Identify “**prioritized acquisitions**” for certification
- ⚠️ “**Non-prioritized acquisitions**” for self-assessment (annual self-attestation)
- CMMC Level 5 under development (1-5%)
- ⚠️ PO&AM’s **allowed**, time-bound to 6 months and enforceable (approx. August 21)
- Waivers & Exceptions - Development of a selective, time-bound waiver process, if needed and approve
- ⚠️ “Removing CMMC-unique practices and all maturity processes from the CMMC Model”
- Rules changes to 32 CFR and 48 CFR

CMMC Model 2.0

	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 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; Annual self-assess- ment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

CMMC 2.0 Program Milestones & Potential Impacts



Level 2
DTC GLOBAL, LLC



Level 2

CMMC 2.0 Important Tasks

Plan and budget POA&Ms to be completed by August/Sept 22.

- Senior Official "affirms" organization meets requirements.
- Expect updates to Terms and Conditions/Enforcement

Shift focus to NIST 800-171/171A, NIST 800-53, and FIPS 200.

Expect NIST 800-171r2, Appendix E Tailoring Criteria/Activities to replace/add tasks/add changes (NFO, NCO, CUI)

Integrate CUI protection requirements into each practice under 32 CFR 2002, NARA/ISOO Guidance, and DoD Policy.
(Appendix E, CUI)



DTC GLOBAL, LLC

TABLE E-8: TAILORING ACTIONS FOR INCIDENT RESPONSE CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
IR-1	Incident Response Policy and Procedures	NFO
IR-2	Incident Response Training	CUI
IR-3	Incident Response Testing	CUI
IR-3(2)	<i>INCIDENT RESPONSE TESTING COORDINATION WITH RELATED PLANS</i>	NCO
IR-4	Incident Handling	CUI
IR-4(1)	<i>INCIDENT HANDLING AUTOMATED INCIDENT HANDLING PROCESSES</i>	NCO
IR-5	Incident Monitoring	CUI
IR-6	Incident Reporting	CUI
IR-6(1)	<i>INCIDENT REPORTING AUTOMATED REPORTING</i>	NCO
IR-7	Incident Response Assistance	CUI
IR-7(1)	<i>INCIDENT RESPONSE ASSISTANCE AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT</i>	NCO
IR-8	Incident Response Plan	NFO

CMMC
2.0



Level 2

CMMC 2.0 Important Tasks

Plan and budget POA&Ms to be completed by August/Sept 22.

- Senior Official “affirms” organization meets requirements.
- Expect updates to Terms and Conditions/Enforcement

Shift focus to NIST 800-171/171A, NIST 800-53, and FIPS 200.



Expect NIST 800-171r2, Appendix E Tailoring Criteria/Activities to replace/add tasks/add changes (NFO, NCO, CUI)

Integrate CUI protection requirements into each practice under 32 CFR 2002, NARA/ISOO Guidance, and DoD Policy.
(Appendix E, CUI)

Update to ePU documentation expected by mid-Dec after release of CMMC 2.0 Model Doc and Assessment Guide

Integrate 2.0 updates into current required policies and procedures (FIPS 200).

Risk Assessments and Security Assessments (RSA) should be updated BEFORE the required annual update of the SSP.

Suppliers & Subs - receive or develop CUI need to be compliant within the same timeline.



DTC GLOBAL, LLC



Level 2

CMMC 2.0 Take Aways

DO NOT WAIT on New Assessment Guide... Standards ALREADY exist in 171A. Get busy.

NIST 800-171/A: Hard to Understand and Hard to Do

Known Fed/DoD CUI Requirements - Protect CUI (and FCI) in every practice/control

Expect to certify for products and services related to warfighting capabilities

VERY LITTLE TIME TO GET THIS DONE

Suppliers & Subs - receive or develop CUI need to be compliant within the same timeline.



Advice for DIB Companies

Advice for DIB Companies

Practical advice – DIB companies can meet the NIST SP 800-171 requirements

- The overall goal is protecting the CUI – POaMs not allowed for major items
- Use existing tools and documentation that fits your business
- Commercial IT clouds are not DFARS compliant – Combine M365/Gworkspace with other solutions to achieve compliance
- Do not sit on the fence – POaMs have short lifespan

Cost-Effective Compliance Options

- Retain your IT investments – Scoping is key
- Achieve data protection – use zero trust principles
- Choose options that fit - DIY - cloud service – in house or outsource/MSP
- Take advantage of vendor compliance documentation (SSP, CRM, Policies)
- Combine technology with documentation and expertise – free or paid

Case Study: DIBCAC High Audit

- Recent 800-171 DIBCAC high assessment (110 controls in scope)
- Mid-sized DIB company – mix of DoD and commercial business
- Environment was M365 Commercial + PreVeil for CUI data sharing and secure messaging
- 5-person DIBCAC team for 9 days
 - Document review, Interviews, evidence collection
- Score: 109/110 near perfect
- Company is ready to pass CMMC 2.0 L2 today

Q&A



→ coalfirefederal.com

→ Stuart.itkin@coalfirefederal.com



→ dtcglobal.us

→ reganedens@dtcglobal.us



→ preveil.com

→ gregg@preveil.com