CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) 2.0 FOR DEFENSE CONTRACTORS

Petronella Technology Group, Inc.

Who is Petronella Technology Group (PTG)?

- HQ: Located in Raleigh North Carolina
- Founded in 2002; a small business
- Certified as a Registered Practitioner Organization (RPO) by the CMMC Accreditation Board (CMMC AB)

Who is Craig Petronella?

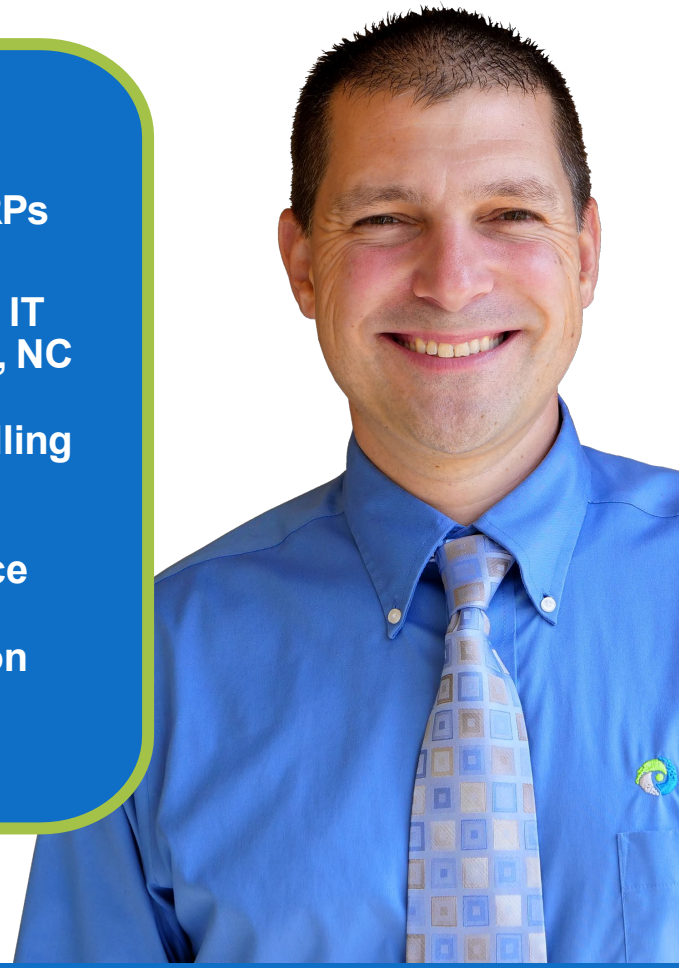
CEO of Petronella Technology Group, Inc. (PTG), a well-known and trusted IT cybersecurity group that specializes in helping DoD contractors and other businesses with DFARS, CMMC, NIST SP 800-53 and NIST SP 800-171/172 security and compliance.

Why is it important to be a CMMC-AB certified Registered Practitioner Organization (RPO) with CMMC-AB certified Registered Practitioners (RPs)?

- **Only RPs are trained in the CMMC assessment process**

KEY TAKEAWAY:
Organizations Seeking Certifications (OSCs) want to pass the audit process on the first try; RPOs can help make that happen.

- **PTG is a CMMC-AB certified RPO with certified CMMC 2.0 RPs**
- **Top cybersecurity & IT authority in Raleigh, NC**
- **#1 Amazon Best-Selling Author**
- **30+ years experience**
- **Frequently quoted on ABC, CBS, NBC, & others**



CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Simplifying Federal Regulations

©Petronella Technology Group, Inc. All rights reserved. | 877.468.2721 | https://petronellatech.com

What is CMMC?

DEPARTMENT OF DEFENSE CERTIFICATION PROCESS THAT

COMBINES VARIOUS CYBERSECURITY STANDARDS INTO ONE UNIFIED STANDARD FOR CYBERSECURITY

Federal Contract Information (FCI)

Controlled Unclassified Information (CUI)

What does CMMC mean for your business?

- Comply today; the requirement to comply is four years old.
- The CMMC 2.0 combines various cybersecurity standards and best practices and maps these controls across 3 Maturity Levels (MLs).
- The MLs build on each other, ranging from *Foundational* cyber hygiene to *Expert.*
- For a given CMMC level, the associated controls (when implemented) **will** reduce risks against a specific set of cyberthreats.
- It is IMPERATIVE for you to be compliant, making a FALSE CLAIM is a serious offense.

Who must comply with CMMC guidelines?

ALL FEDERAL CONTRACTORS foreign and domestic delivering DoD products and services.

Primes and subcontractors.

Petronella
CYBERSECURITY AND DIGITAL FORENSICS

DFARS Interim Rule:

WHY NOW?

With CMMC, rolling out in **expedited fashion**- Why the Interim Rule and why NOW?

- Hackers are not going to wait for contractors, subcontractors or vendors to get their cybersecurity whipped into shape to start a cyberattack. **HACKERS do not wait on rule-making**!
- Exfiltration of sensitive data by malicious actors around the globe is a threat to both national and economic security.
- The DoD is working with the Defense Industrial Base (DIB) to enhance protection of Controlled Unclassified Information (CUI) along the supply chain.

Petronella
CYBERSECURITY AND DIGITAL FORENSICS

DFARS Interim Rule:

OVERVIEW

Overview of New Rule

"CMMC certification is your Driver's License on the Information Superhighway."

Coming lay-in of CMMC 2.0 has added new contracting requirements:

THREE NEW PROVISIONS:

1. **-7019:** Advises contractors that they must maintain and report their **NIST 800-171** compliance in the **Supplier Performance Risk System (SPRS)**; also explains the three types of assessments/audits (Basic, Medium, High); **already IN FORCE.**

2. **-7020:** Outlines the requirement of contractors to provide the Government access to its facilities if the DoD is renewing a contract or conducting a Medium or High assessment; **already IN FORCE.**

3. **-7021:** Discusses integration of CMMC Maturity Levels 1-3

Petronella
CYBERSECURITY AND DIGITAL FORENSICS

DFARS Interim Rule:

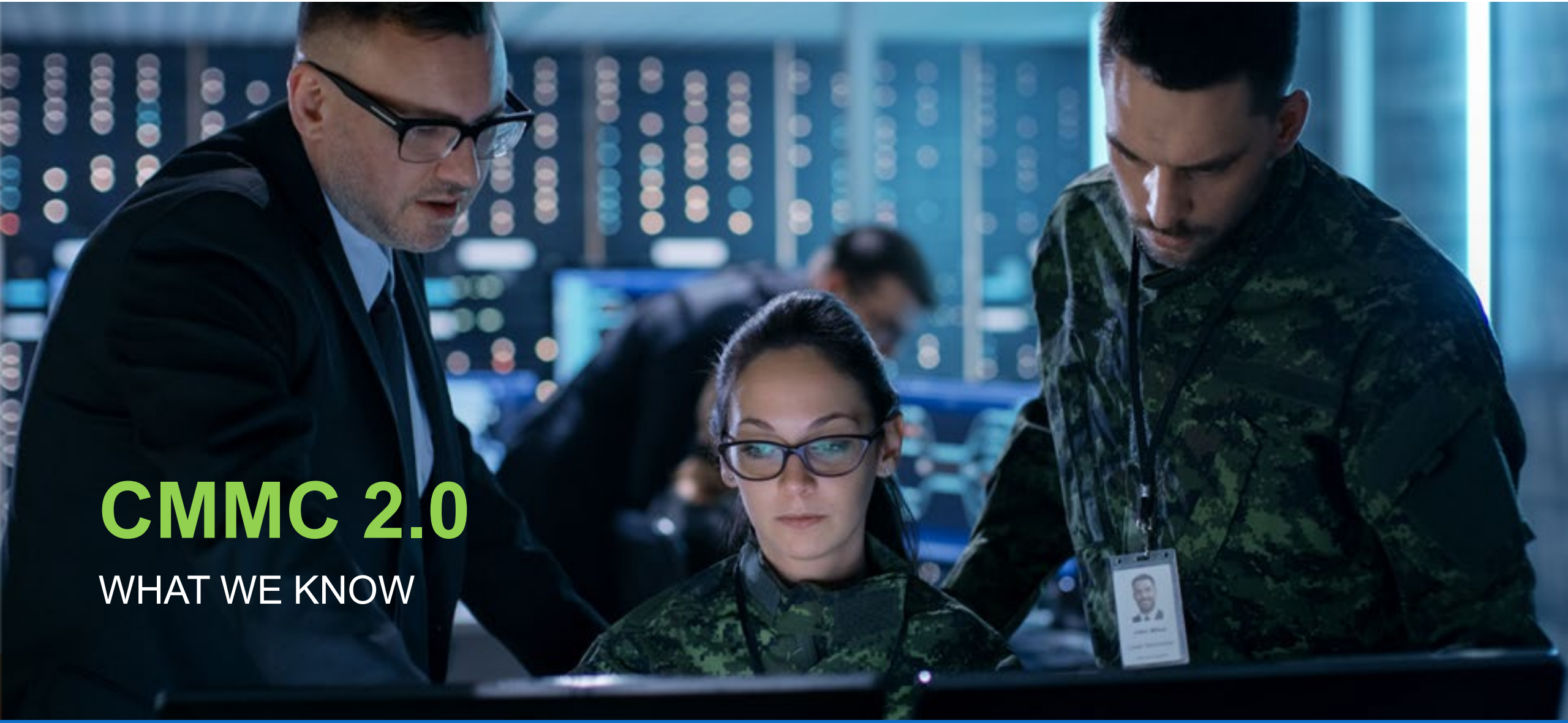
SUPPLIER PERFORMANCE RISK SYSTEMS (SPRS) &

DoD ASSESSMENT METHODOLOGY (DoDAM) SCORE

SPRS Overview

- The SPRS Self-Assessment effectively reinforces Self-Attestation of **NIST SP 800-171.**
- Have you completed your SPRS Self-Assessment? **It was due December 31, 2017.**
- Currently included in **MOST RFPs.**
- Not recommended that contractors wait; DoD wants ALL subs and primes to self-attest **asap.**
- CMMC will roll out after rule-making, but until then, **you MUST complete the SPRS self-assessment.**
- Location: https://www.sprs.csd.disa.mil/

KEY TAKEAWAY:
Have you entered your SPRS score yet?

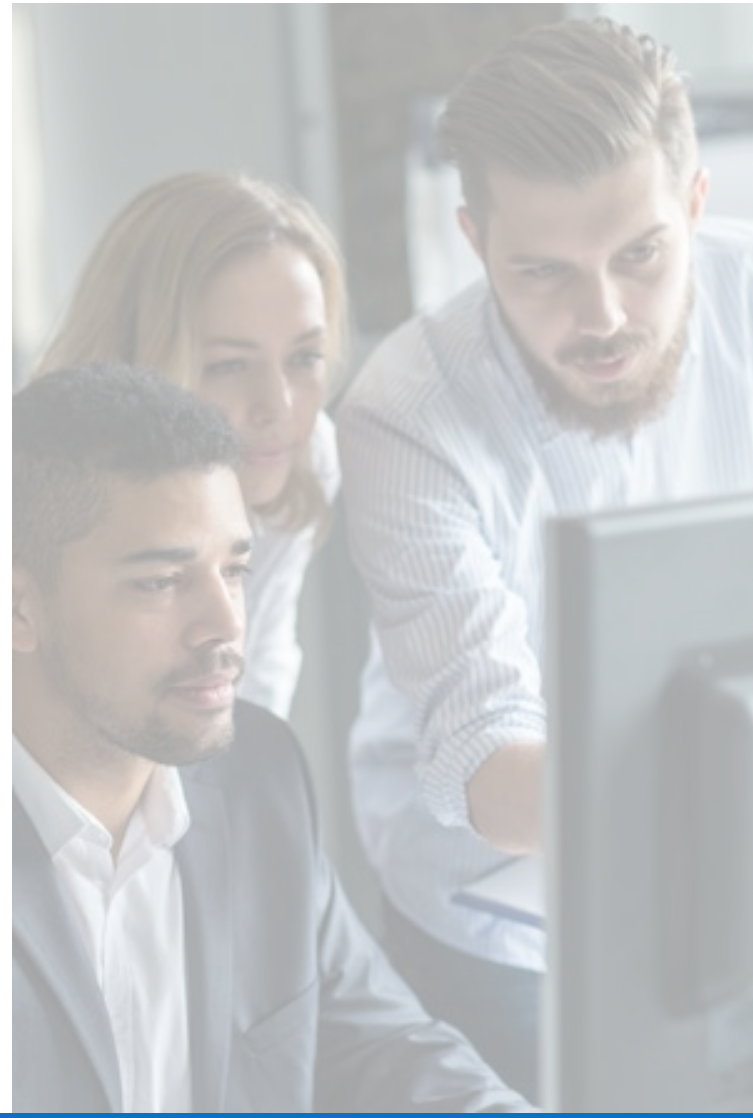


CMMC 2.0

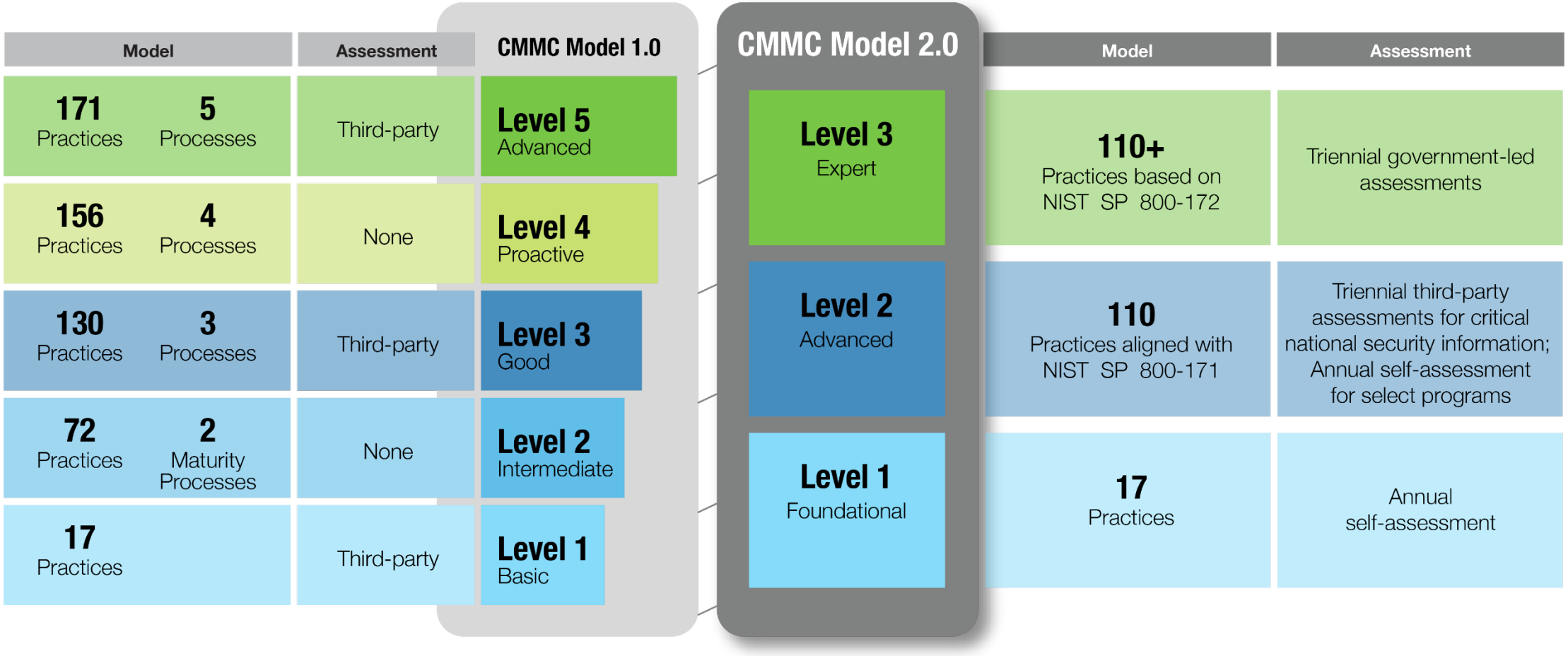
WHAT WE KNOW

Cybersecurity Maturity Model Certification 2.0

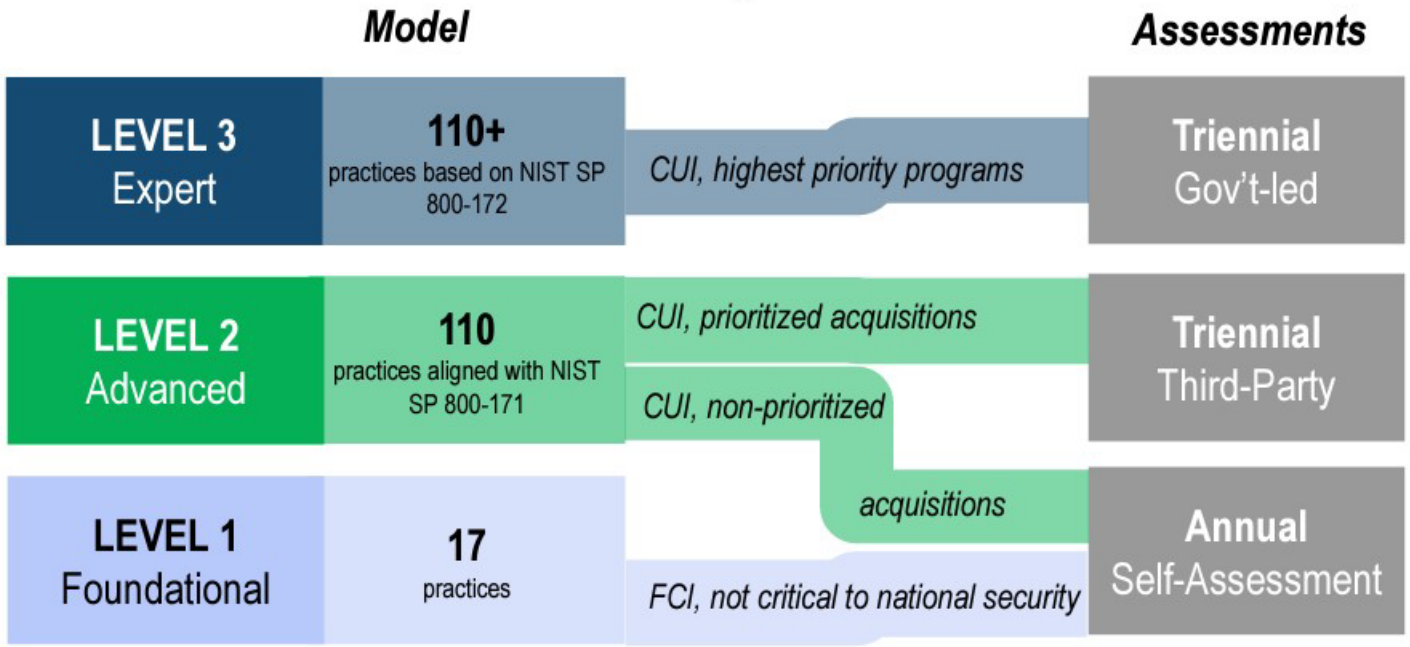
- **CMMC has been simplified, but it's not going away**
  - From five to three Maturity Levels (MLs)
  - ML 1 is now self-certifying; only if FCI is handled, vice CUI
- **DFARS 252.204-7012 & NIST 800-171 are still required today**
  - No changes to clauses 7019 / 7020
  - SPRS self-attestation still mandatory; ML 2 & ML3
- **DoD enforcement to be more aggressive from DoD**
  - Civil Cyber-Fraud Initiative will create more False Claim Act Participants
  - Expect more demanding flow-down requirements from primes
  - **Whistleblowers can report any contractor non-compliance!**



Cybersecurity Maturity Model Certification 2.0



Cybersecurity Maturity Model Certification 2.0



Note: The information in this presentation reflects the Department's strategic intent with respect to the CMMC program. The Department will be engaging in rulemaking and internal resourcing as part of implementation, and program details are subject to change during these processes.

Cybersecurity Maturity Model Certification 2.0

Petronella™
CYBERSECURITY AND DIGITAL FORENSICS

KEY TAKEAWAY:
Waivers and POAMS will be extremely difficult to attain, so pretend like they don't exist.

Self-assessment at Maturity Level 1; this is self-attestation

Self-assessment allowed for SOME ML2 contractors

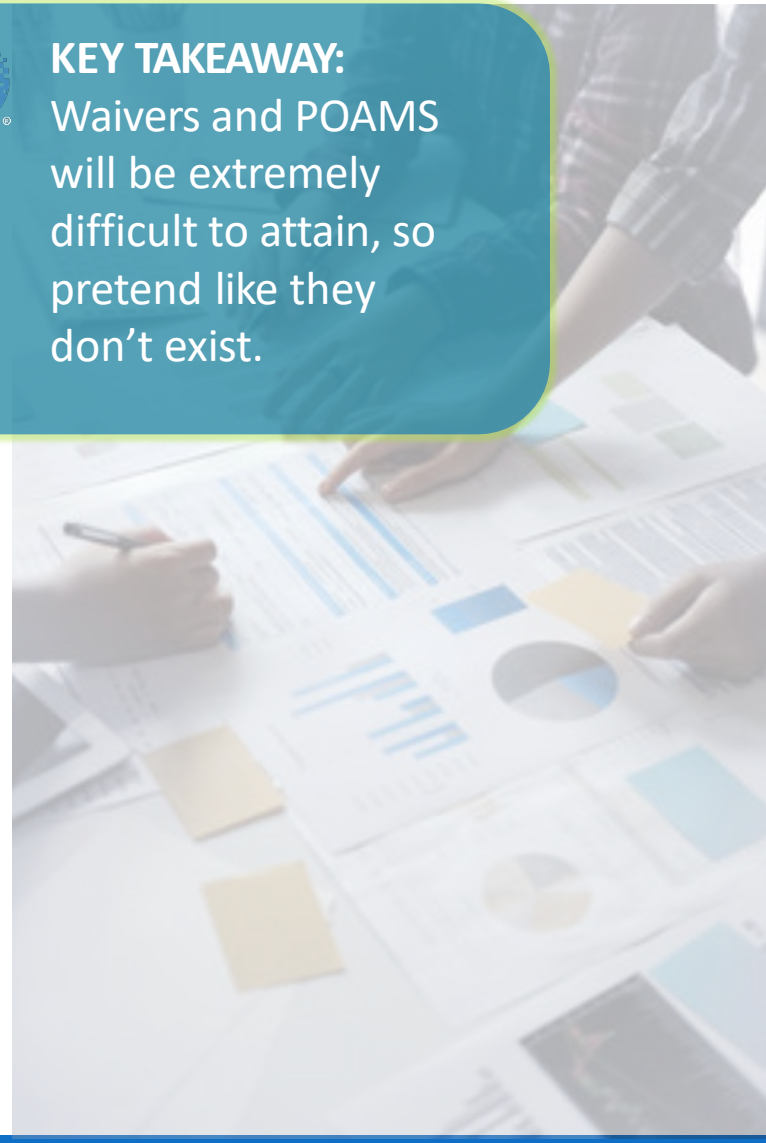
- Allowed if the contractor is not handling "critical national security information."
- The definition of "critical national security information" is to be defined during the Rulemaking stage.

Limited Plan of Action and Milestones (POAMs) and Waivers allowed

- These will only be temporary waivers and will be difficult to attain.
- The parameters for POAMS and waivers will be defined during the Rulemaking stage, but OSCs will not be allowed to POAM the "heavily-weighted" controls.
- POA&Ms allowed under 2.0, for a 180-day period.

DoD certifications at Maturity Level 3 – an increased responsibility/role

Contractors are encouraged to comply with "heavily-weighted" NIST controls as soon as possible to be positioned for deluge of CUI being released under coming procurements



Benefits of NIST and CMMC Compliance

Increased Security

Being NIST 800-171 compliant will significantly reduce the likelihood of a breach, and if you are breached it will decrease the impact of the breach.

Competitive Advantage

Once you have put in the time, energy and money it requires to be NIST 800-171 compliant, you gain a competitive advantage over other businesses who are not.

Peace of Mind

You won't lose sleep wondering if you are going to lose your contract and your reputation because you failed to comply.

CMMC 2.0 Takeaways

- ✓ POA&Ms have changed DRAMATICALLY; now good for **180 days**.
- ✓ Most “heavily- weighted of the 110 controls” **cannot** be part of a POAM. Suggest identify these and commence maturity!
- ✓ Prescription to comply with NIST SP 800-171 is found in **almost 100 %** of DoD Prime & Subcontracts
- ✓ If so when you sign your contract you are **self-attesting compliance** with both FAR 52.204-21 and DFARS 252.204-7012.
- ✓ Controlled Unclassified Information (CUI) will become routine in most procurements; expect **a “flood” of CUI.**
- ✓ To gain access to CUI it will likely require the right **Maturity Level or SPRS Score.**
- ✓ DoD Major Primes will be some of the **strictest enforcers** of NIST 7012/7013 compliance.
- ✓ If you rely on a 3rd Party MSP, that **does not relieve you of compliance** in any manner; suggest early meetings with MSP to discuss responsibilities and roles. **MSPs must be DFARS, CMMC, NIST conversant!**

You Handle CUI - What's Next For Your Business?

1. Review my system security plan (SSP) against NIST SP 800-171.
2. Perform a Gap Analysis to identify short falls in your System Security Plan (SSP).
3. Plan of Action and Milestones (POAMs) will follow your Gap Analysis .
4. Are you ready to input your SPRS score?
5. Is your cloud provider FedRAMP approved?

Petronella™
CYBERSECURITY AND DIGITAL FORENSICS

It’s Complicated, Let’s Talk

Call Craig at 919-601-1601 or visit **petronellatech.com**