DOD'S CYBERSECURITY ASSESSMENT REGIME: *Key Compliance Considerations for Contractors*

APRIL 21, 2021 | PRESENTED BY:

ALEXANDER CANIZARES | SENIOR COUNSEL
PERKINS COIE LLP

Presenter

ALEXANDER CANIZARES

SENIOR COUNSEL, PERKINS COIE LLP

Alexander Canizares represents government contractors and other companies in litigation, investigations, and regulatory matters involving federal departments and agencies. As a former trial attorney with the U.S. Department of Justice's (DOJ) Civil Division, Alex draws on his experience serving as lead counsel in complex cases involving the federal government to advise companies in the aerospace and defense, technology, healthcare, professional services, and other industries, in legal matters related to all phases of federal government procurement. He represents clients ranging from early-stage technology companies to publicly traded *Fortune 100* corporations in bid protest and claims litigation, internal and government investigations, FAR/DFARS compliance, disclosures, cybersecurity, prime-subcontractor disputes, data rights, and diligence related to government contracts in M&A transactions.

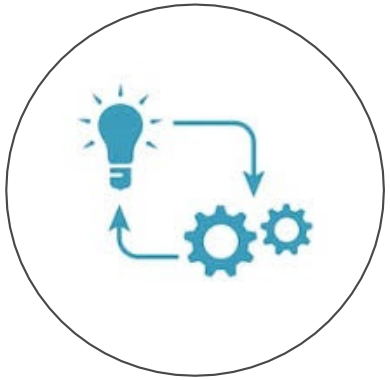
Alex speaks and writes frequently on emerging issues in government contracts and is an adjunct professor of Performance of Government Contracts at GW Law School and a co-chair of the ABA Public Contract Law Section's Contract Claims and Disputes Resolution Committee.

acanizares@perkinscoie.com (202) 654-1769
Full Bio Available at http://www.perkinscoie.com/ACanizares/

PERKINSCOIE

Agenda

DoD Contractor Cybersecurity: Big Picture



DFARS Interim Rule: Key Considerations

Risk Mitigation Strategies

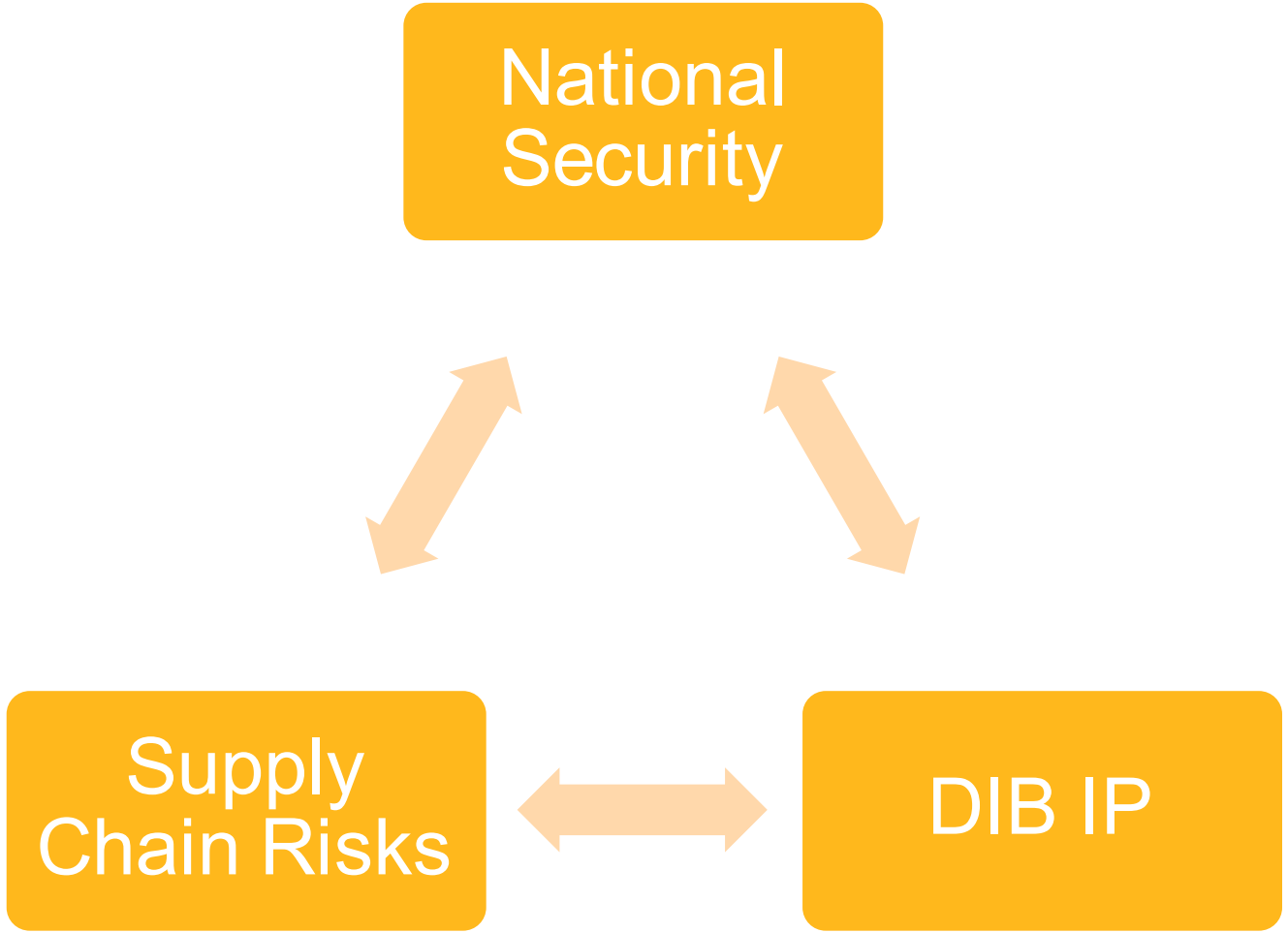
Questions

DOD CONTRACTOR CYBERSECURITY: BIG PICTURE

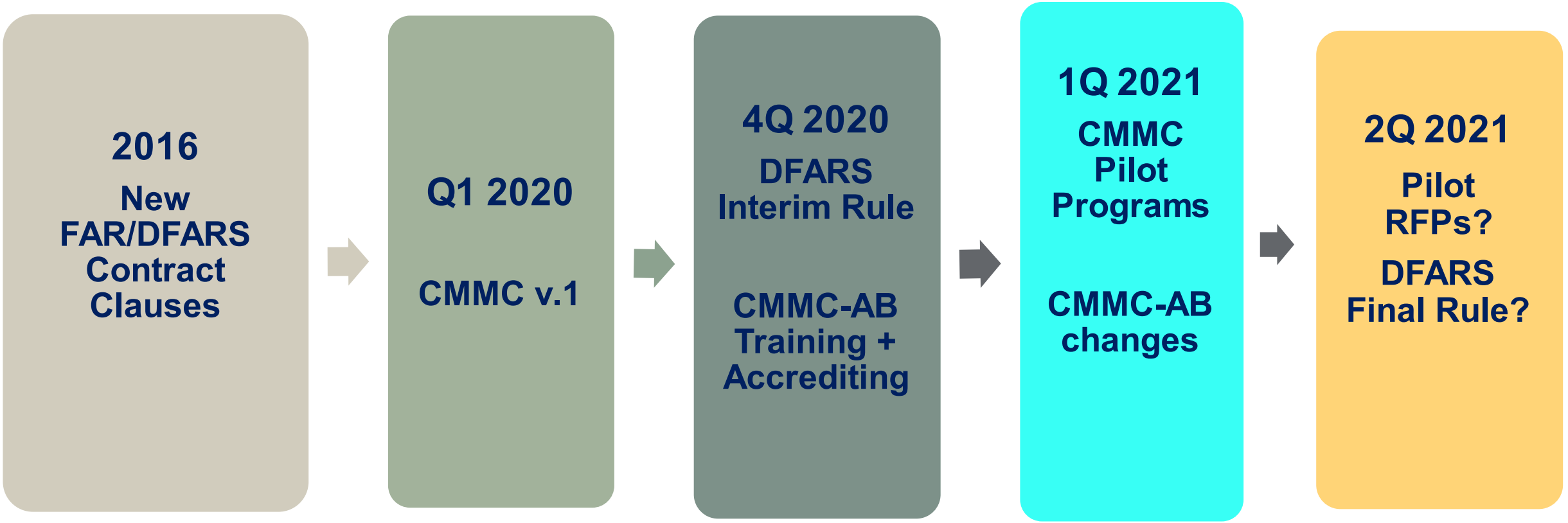
Cybersecurity and the Biden Administration

- High-profile cyber breaches highlight cyber vulnerabilities in the Defense Industrial Base and refocus regulatory and policy agenda
- *Pres. Biden's Interim National Security Strategic Guidance* March 2021
  - "[W]e will make cybersecurity **a top priority**, strengthening our capability, readiness, and resilience in cyberspace. We will **elevate cybersecurity as an imperative across the government**."
- Nominations
  - First National Cyber Director
  - CISA
- FY 2022 Budget
  - $2.1B for CISA—$110M increase from FY 2021
  - $500 for Technology Modernization Fund

CMMC and Cybersecurity Assessment Regime



Evolution of DoD's Regulatory Framework



PERKINSCOIE

DFARS INTERIM RULE: KEY CONSIDERATIONS

Two Tracks of Assessments

CMMC

- **Third-Party Verification**
- 5-year rollout
- Supplement NIST 800-171
- CMMC-AB management

NIST 800-171 Assessments

- **Basic (Self) and DoD Assessments**
- Immediate impact
- Tied to NIST 800-171/DFARS
- DoD oversight

Two Tracks of Assessments

NIST 800-171

- Teeth to DFARS 252.204-7012.
- Verify compliance with NIST 800-171.
- Required for all solicitations and contracts except COTS.
- Basic Assessment score (not more than 3 years old) required for award.
- Plan of Action/Milestones permitted.
- Medium & High Assessments (DoD).

CMMC

- Five-level maturity model supplements NIST 800-171.
- Third party conducts assessments.
- Phased rollout to Oct. 2025.
- Go/No Go criterion.
- Full implementation required.
- OUSD A&S role.
- Civilian agencies (DHS, GSA).

NIST SP 800-171 Assessments

- **Basic Assessments**
  - Self-assessment tied to NIST 800-171.
  - Scores posted to Supplier Performance Risk System as condition for award.
  - Threshold Q: do you have CDI?
  - Weighted (highest: 110; lowest: -200).
  - Must identify CAGE code(s).
- **Medium + High Assessments**
  - DoD (DIBCAC) performed.
  - Estimated 200 Medium and 110 High Assessments annually.
- DFARS -7019 and -7020 clauses.

PERKINSCOIE

CMMC and Third-Party Verification

- Third-party assessments (C3PAOs) via contracts (DFARS 252.204-7021).
- Must be certified at time of award and maintain certification.
- Five levels of maturity
  - *Level 1 – Basic*
  - *Level 2 – Intermediate*
  - *Level 3 – Good*
  - *Level 4 – Proactive*
  - *Level 5 – Advanced/Progressive*
- DoD: at least 200 entities will undergo assessment each year.

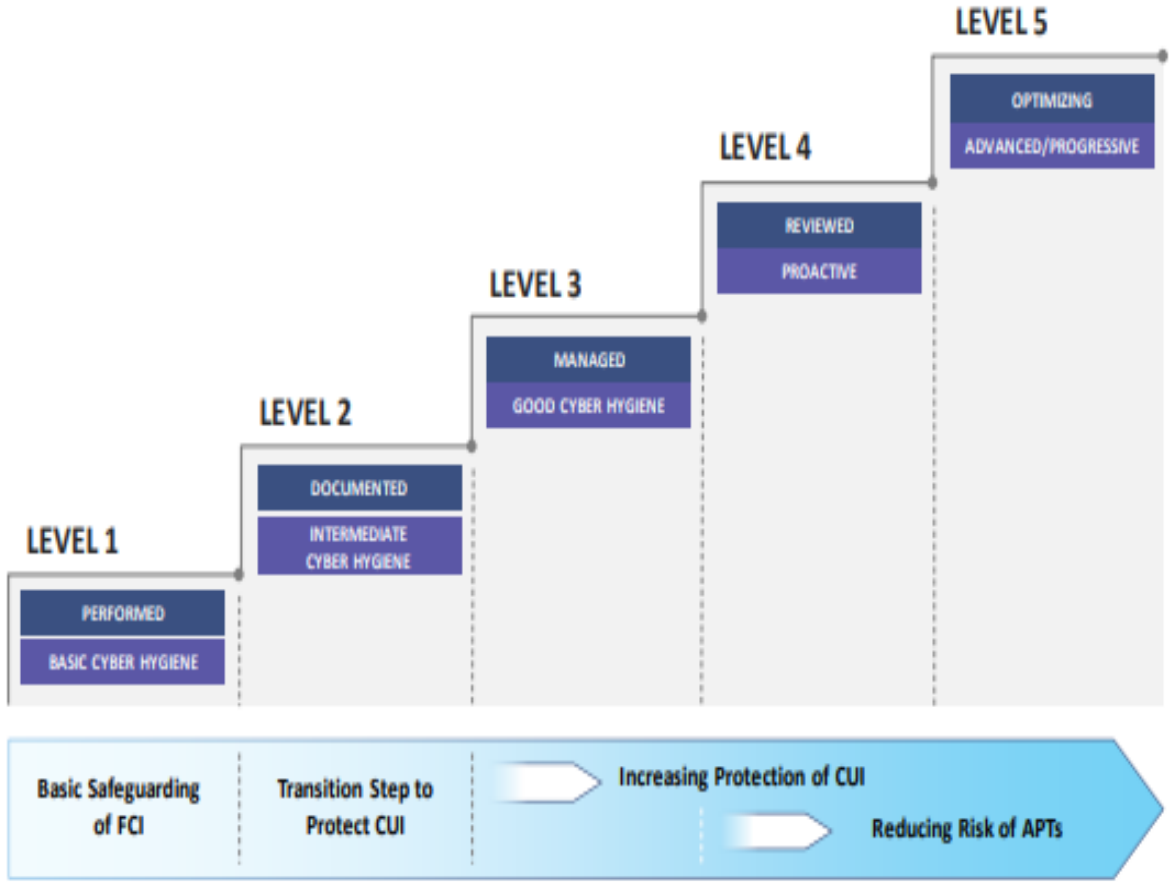


Figure 3. CMMC Levels and Associated Focus

Source: DoD CMMC v.1.02

PERKINSCOIE

CMMC—Update and Next Steps

DOD DEVELOPMENTS

- DoD in process of reviewing the CMMC program.
- Leadership changes in UOSD/A&S.
- To watch for:
  - Final rule
  - CMMC model revisions
  - CMMC Assessment Guide
  - Guidance re: reciprocity
  - Congress oversight

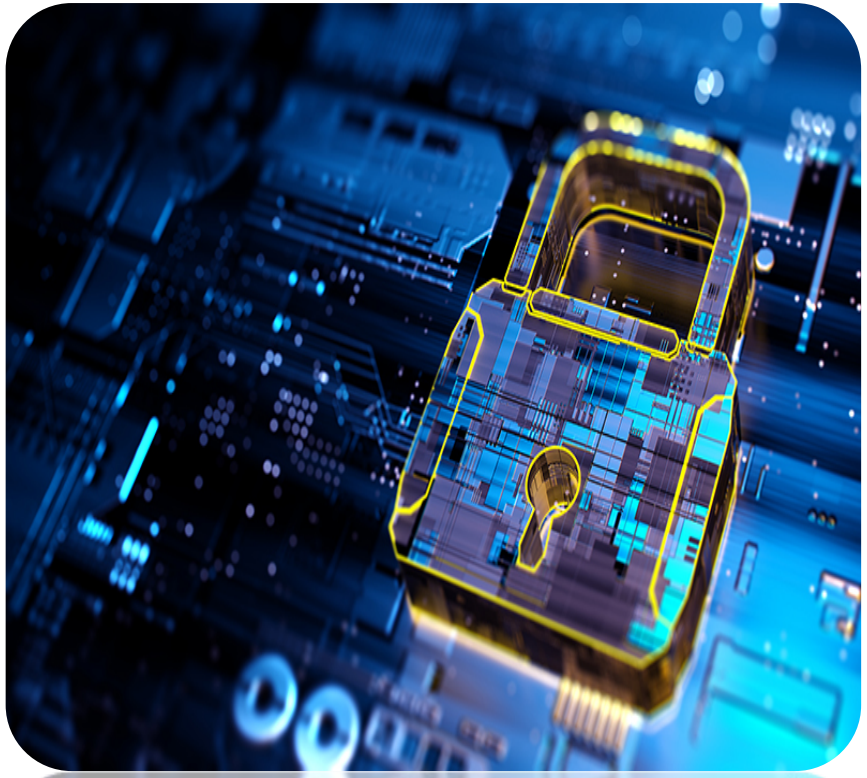
PILOT PROGRAMS

- DoD plans for up to 15 in 2021.
- New RFPs in acquisitions.
- USD A&S approval.
- CMMC assessments and certifications.
- Default is CMMC Level 3.
- Up to 475 prime contracts through Oct. 2025.

Cost Recovery and Impact on DIB

- Significant uncertainty remains regarding the ability to recover CMMC compliance costs.
- Impact on small businesses and DIB overall.
- NIST 800-171 Costs.
  - Contractors subject to DFARS 252.204-7012 "***should have already implemented*** these cybersecurity requirements and incurred the associated costs; therefore, those costs are not attributed to this rule."
- Tracking of CMMC implementation costs.
- FAR Part 31 cost principles and REAs.

CUI and CDI: Uncertainty Regarding Definitions



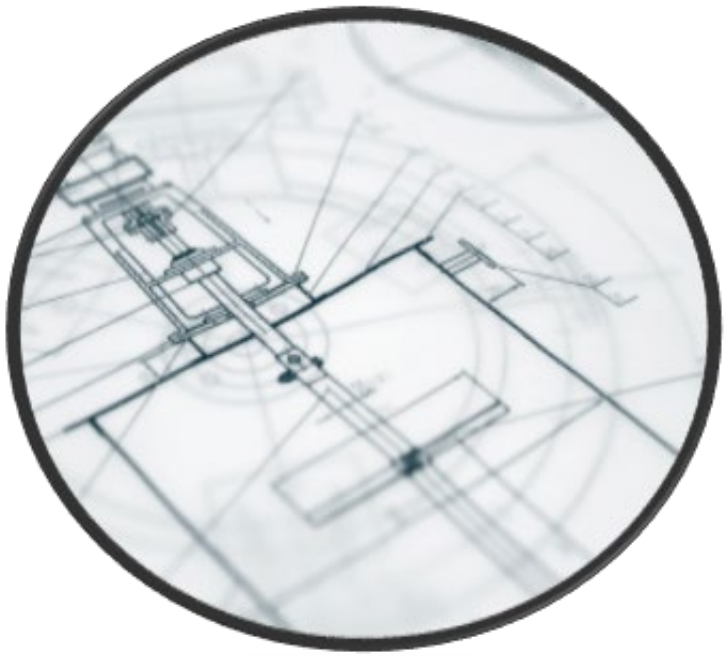
- Identifying what is CUI or CDI and how it should be marked or treated remains a **significant challenge for industry**.
- **Controlled Unclassified Information (CUI)**
  - Government created or owned
  - Requires safeguarding or dissemination controls consistent with applicable laws, regulations and Gov-wide policies.
- Guidance from USG.
  - DoD Instruction No. 5200.48 (Mar. 6, 2020) – terms and marking.

Impact on Source Selection and Competition

- **What will become of Basic Assessment?**
  - Any weight given to self-scores?
  - Responsibility (FAR Subpart 9.1)?
- **CMMC and Bid Protest Litigation**
  - Pre-award protests of CMMC Level.
    - ***Oracle v. United States*** (Fed. Cir. 19-2326) (Sept. 2020): "Hesitant" to "override the agency's judgment as to its needs" for security.
  - Organizational Conflicts of Interest (OCIs).

PERKINSCOIE

Determining CMMC Levels

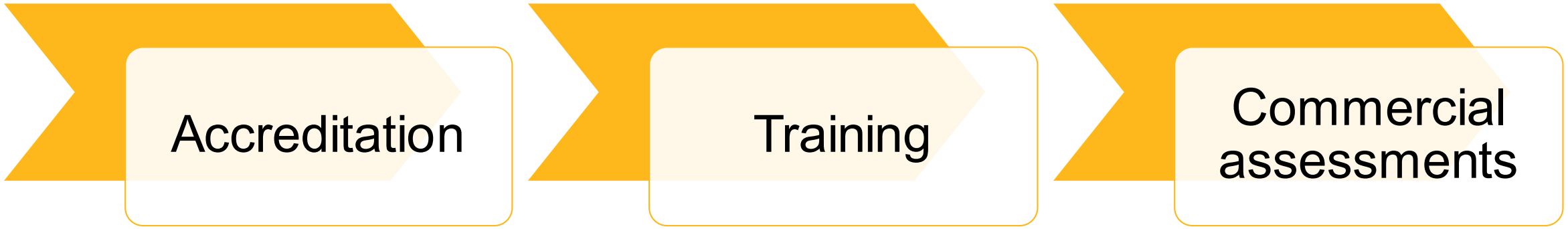


- DoD estimates that nearly 70% of companies in DIB will not need CMMC Level 3 or higher.
- Process for determining CMMC Levels at prime and lower tiers remains uncertain.
  - Interim rule requires mandatory flow-down (except COTS).
  - Primes must ensure that subs are certified at "appropriate" level prior to subcontract award.
- DoD guidance to Program Managers
  - DoDI 5000.90 - Guidance for crafting RFPs

Cloud and Reciprocity

- Ongoing questions about extent to which reciprocity will be available between CMMC and other certification programs, e.g., FedRAMP.
- Key issue: Plans of Action & Milestones.
- DFARS requires contractors using CSPs to “ensure” that CSP meets FedRAMP Moderate baseline.

CMMC Accreditation Ecosystem



RISK MITIGATION STRATEGIES

CMMC and Risk Management

- Compliance as ongoing responsibility
- Cross-functional team approach
- Documentation of compliance and decision-making (not just SSP)
- Nature of data will drive strategy: do you have CUI?
- Gap analysis/preparation
- Enclaves + multi-CMMC levels
- Tracking implementation costs
- Managing subcontractors

CMMC Assessment Disputes

Contractors may dispute the "**outcome of a C3PAO assessment**"

CMMC-AB review disputes re: "claimed errors, malfeasance, or ethical lapses" by a C3PAO.

May appeal to CMMC-AB.

Numerous open questions as to how process will work, scope of review, legal remedies available.

False Claims Act Risks

- **The FCA and Cybersecurity Non-Compliance**
  - Knowing submission of false or fraudulent claims.
  - Implied false certification liability based upon cybersecurity non-compliance.
  - Issues re: good faith and reasonable interpretations of ambiguity.
- ***Markus v. Aerojet Rocketdyne*** **(E.D. Cal. 2019)**
  - *Qui tam* relator alleged contractor fraudulently entered into DoD and NASA contracts despite knowing non-compliance with cyber controls.
  - Court declined to dismiss: relator sufficiently pled "materiality."
- **Risk Mitigation**:
  - Documentation of decisions + communication with USG.
  - Ethics and internal controls, training, incorporating agency guidance.
  - Mandatory disclosures (FAR 52.203-13).

QUESTIONS?

ACANIZARES@PERKINSCOIE.COM
(202) 654-1769
HTTP://WWW.PERKINSCOIE.COM/ACANIZARES/