RISK, FORENSICS AND COMPLIANCE

OPTIMIZING DFARS COMPLIANCE & CMMC READINESS THROUGHOUT THE SUPPLY CHAIN

ankura.com

ankura

HARD FACTS...HARD DATES

Between 2020 and 2025 every new contract procurement from the U.S. Department of Defense (DoD) will require prime contractors and the subcontractors throughout their supply chains to be independently certified at one of five Cybersecurity Maturity Model Certification (CMMC) levels as a condition of bidding.

The CMMC requirement is intended to address the national security risk from what the DoD considers inadequate security of Controlled Unclassified Information (CUI) that is in place – especially at smaller companies - throughout the defense industrial base (DIB), whether domestic or non-U.S. based. Currently available tools and processes have not served the industry well enough.

> "Every company within the DoD supply chain — not just the defense industrial base, but the 300,000 contractors — are going to have to get certified to do work with the Department of Defense...., and then we can really start looking at our supply chain, where our most and greatest vulnerabilities lie.....It's going to take time, it's going to be painful, and it's going to cost money."
>
> *Katie Arrington, CISO, Office of the Undersecretary of Defense for Acquisition, at the October 2019 Intelligence & National Security Summit.*

ANKURA'S EXPERTS

Ankura's CMMC team includes former chief information security, privacy and compliance officers at prime defense contractors, risk management experts, and former law enforcement, intelligence, and national security leaders, who have addressed threats to critical DoD assets, helped develop federal cybersecurity requirements, and understand the security priorities of the U.S. government.

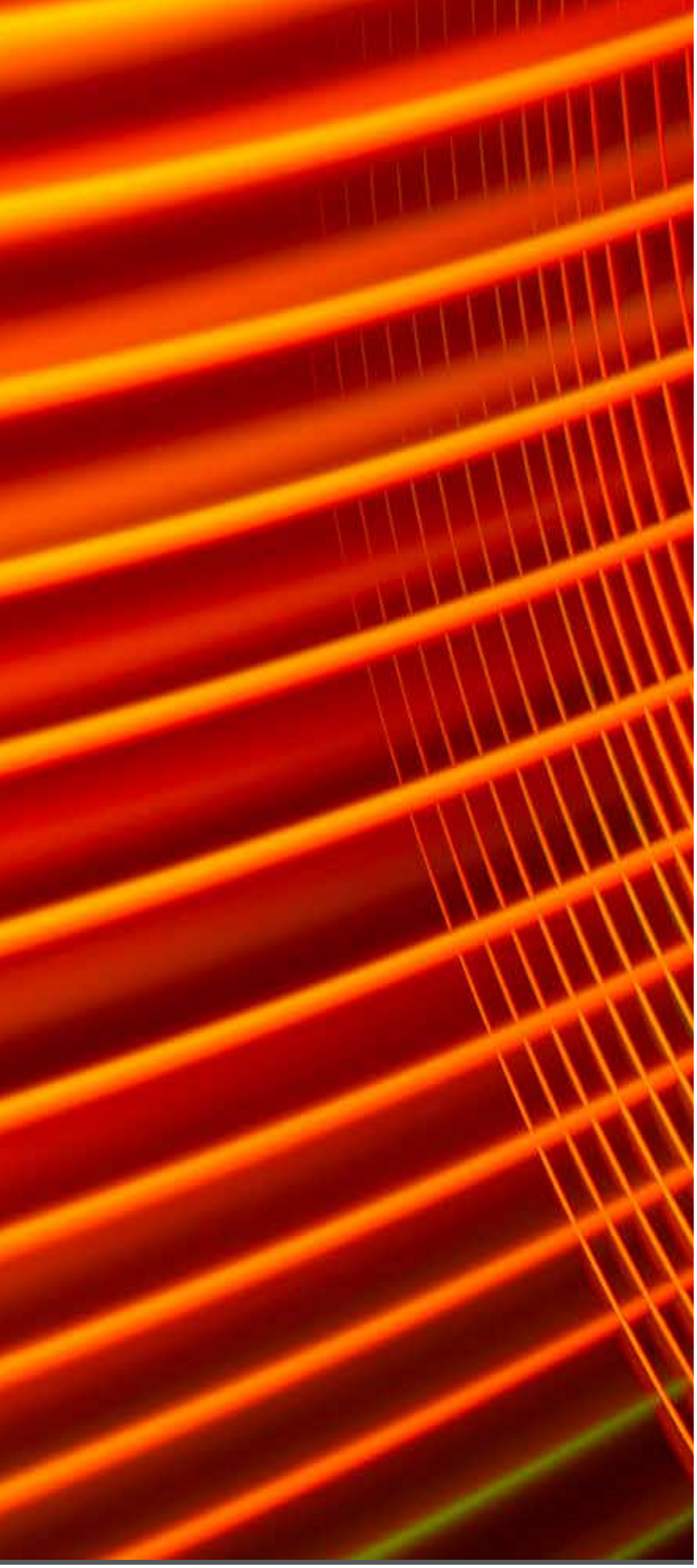
RANDALL H. COOK
Senior Managing Director

SCOTT CORZINE
Senior Managing Director

STEPHEN P. GILMER
Senior Director

ALAN LEVESQUE
Senior Managing Director

WAQAS SHAHID
Senior Managing Director



When CMMC is fully implemented in 2025 the approximately 300,000 companies that comprise the DIB will continue to be obligated to meet the DFARS 7012 requirement to self-attest to the NIST 800 -171 standard for protection of CUI. Even those DIB suppliers of commercial off-the-shelf (COTS) products, which will be exempted from CMMC requirements, must continue to follow the DFARS 7012 clause relative to their cybersecurity posture.

Ankura offers DIB prime contractors and subcontractors effective solutions to get a head start on meeting CMMC requirements. We help entities understand their business intersection with CMMC requirements and provide insight, tools, and assistance to prepare for successful certification. We assess the alignment of contractors and their priority supply chain partners with both NIST 800 -171 and CMMC through a combination of self-assessment tools and control evaluations. We leverage our findings to support client benchmarking, gap identification and remediation, budgeting, project planning, implementation, reporting, and sustainment.

We have assembled a seasoned team of defense, security, compliance, legal, and risk experts – supported by a powerful assessment and compliance engine that is purpose-built for NIST 800 -171 and CMMC requirements. We help DIB contractors understand their compliance risk, accountably manage the compliance process, and gain a clear picture of the security of their critical subcontractors.

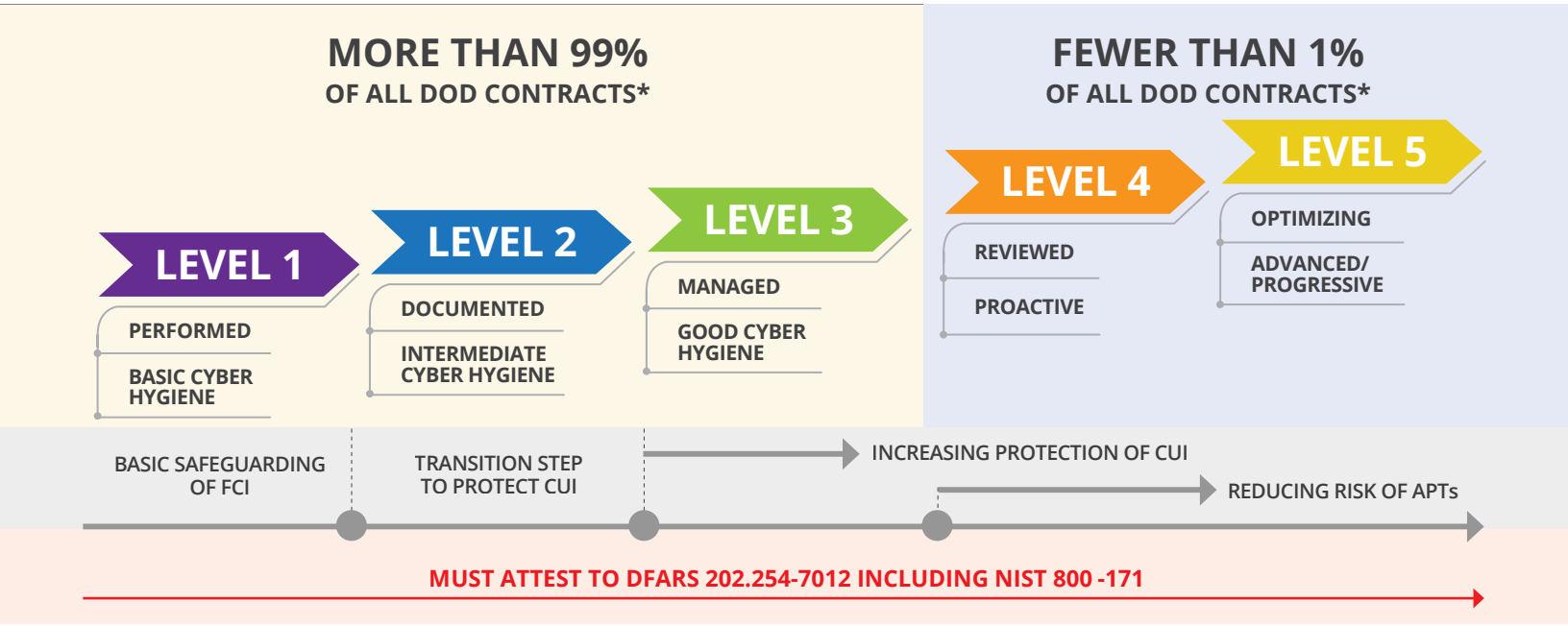
Ankura's interdisciplinary approach is integrated through our assessment and planning platform to enable a comprehensive Common Operational Picture that addresses the needs of key stakeholders: technical visibility into controls and gaps for IT and security officers; compliance, risk, and budgetary visibility for legal, program and compliance officers; and business risk, decision, and progress dashboards for executive leadership and boards.

CMMC & NIST 800 -171

The CMMC program is a consolidated framework of information security controls and practices that will apply to all DoD prime and sub-contractors whose information systems touch Federal Contract Information (FCI) or CUI. CMMC requires a formal independent certification in addition to cybersecurity self-attestation to DFARS Clause 252.204-7012 (which applies NIST 800 -171 to all DIB contractors, regardless of anticipated CMMC level).

CMMC consists of 17 core security domains and integrates various existing cybersecurity control standards into one unified standard for DoD contractors to verify the maturity of their cybersecurity programs and practices. Each CMMC domain "crosswalks" to other common cybersecurity frameworks. Contractors that have been developing and managing their security program to such frameworks and standards likely have been making meaningful progress against CMMC requirements as a result.

Because CMMC is prescriptive and requires independent certification, it will significantly impact DIB contractors. CMMC will require demonstration of objective evidence to validate how well DIB contractors have implemented and operationalized their cybersecurity practices and processes against a five-level maturity standard:



**Per Katie Arrington, CISO, Office of the Undersecretary of Defense for Acquisition*

ankura

REGARDLESS OF CMMC MATURITY LEVEL, THE FOLLOWING WILL APPLY IN THE CASE OF EVERY DOD CONTRACT:

- **NIST 800 -171 remains the backbone to:**
  - All CMMC maturity levels
  - Good cyber hygiene for ALL data, not just CUI
  - Improving trust with your prime contractors and your supply chain

- **Vendors across all CMMC maturity levels must continue to self-attest to DFARS cyber requirements embodied in NIST 800 -171.**

- **Failure could:**
  - Make it more difficult for a DoD contract officer to accept self-attestation
  - Potentially trigger a DCMA DIBCAC assessment of your NIST 800 -171 compliance

- **CMMC is intended to improve, not reduce, cyber hygiene and will require deliberate effort for success.**

- **Failing to achieve the requisite CMMC certification will be disqualifying from contract participation; it may take as long as three years to recertify.**

For organizations that can meet NIST 800 -171, then CMMC Levels 1 and 2 are likely secure. CMMC Level 3 requirements consist of 20 additional cybersecurity controls. Organizations that achieve this level of maturity will be positioned to continue to pursue all but the most sensitive DoD contracts that will be rated at CMMC Level 4 or 5. By implementing a smart, phased approach to CMMC readiness now, DIB contractors have the opportunity to deliberately manage cybersecurity program enhancement, reduce compliance risk, and enable continued ability to compete for and win DoD business. Contractors that forego a disciplined approach may increase their risk, shorten their compliance window, and be excluded from DoD contract opportunities.

GETTING CMMC RIGHT IS CRUCIAL

The CMMC program materially raises the bar for the cybersecurity posture of suppliers, imposes a requirement for formal certification of cybersecurity program maturity by independent third-party assessors (C3PAOs) licensed by the CMMC Accreditation Body, and may lock companies into their initial certification level for an extended period disqualifying them from participating in Pentagon procurements where the contract requirements call for a higher program maturity level.

The regulation adds a significant additional burden on prime defense contractors that will be required to verify that their subcontractors are also compliant and certified at a CMMC level commensurate with the risk assigned to their possession of CUI. A corresponding burden will fall on subcontractors to achieve the CMMC level necessary for eligibility to participate in DoD contracts.

CMMC is a binary "pass/fail" process: pass 100% of practice and process requirements at the requisite maturity levels or be eliminated from DoD contract participation at that level for an extended period. Contractors simply must get CMMC right the first time.

ANKURA'S COMPLETE CMMC SOLUTION

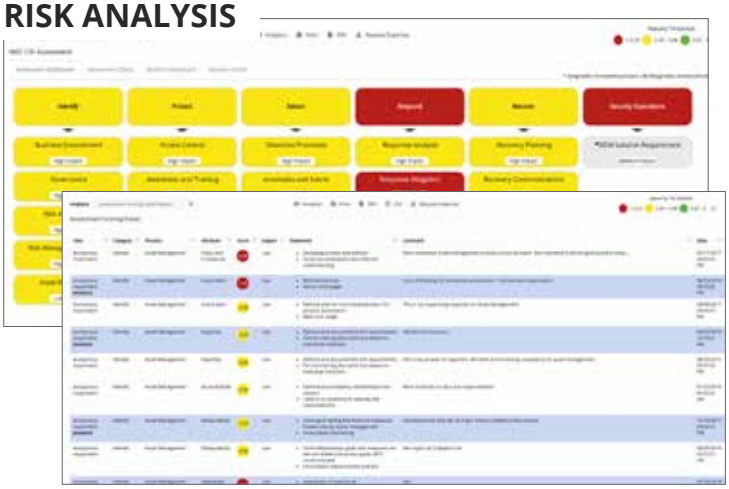
We offer DIB prime and subcontractors a unique, purpose-built solution to assess and improve the status of core compliance obligations with NIST 800 -171 and to the impending CMMC requirements. Our experienced team leverages this assessment platform to:

- Manage and integrate the workflow of NIST 800 -171 and CMMC gap assessments
- Collect artifacts that validate findings and observations
- Design actionable remediation programs with dependable budgetary guidance
- Benchmark cybersecurity posture against 70+ company assessments
- Develop remediation options, recommendations, and project plans
- Create technical, compliance, and risk management oversight reports
- Provide clear visibility to prime contractors into the security of their supply chains

Our cybersecurity defense experts specifically address contractors' current posture against NIST 800 -171 under DFARS requirements; help them understand, create, and accelerate their plan of actions and milestones (POAM) to close remaining compliance gaps; and assess and manage their compliance with the CMMC regulatory regime.

EXCEPTIONAL VISIBILITY INTO THE COMPLIANCE PROCESS

RISK ANALYSIS

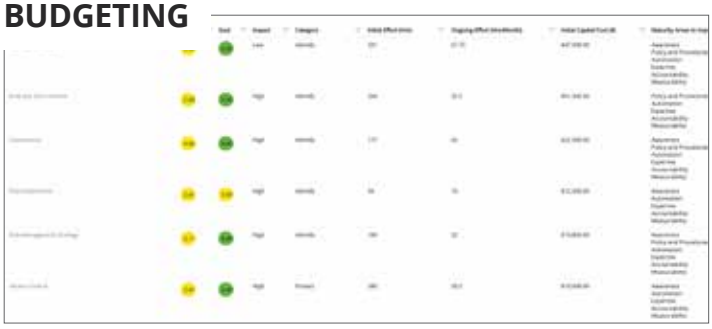


TRACKING COMPLIANCE & POSTURE IMPROVEMENT

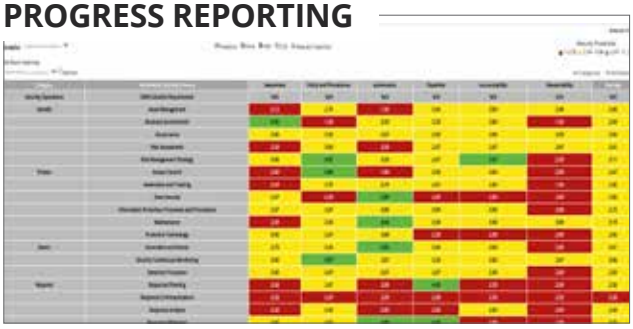
RESOURCE PLANNING

WORKFLOW MANAGEMENT

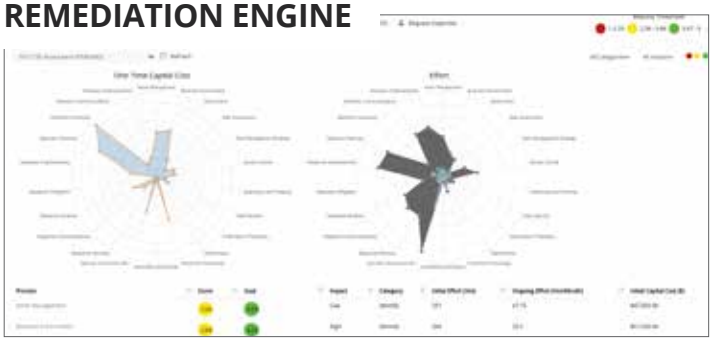
BUDGETING



PROGRESS REPORTING



REMEDIATION ENGINE



BOARD REPORTING

ankura

START NOW

Implementation of the DoD's CMMC program continues aggressively, with only minor COVID-19 related delays. CMMC impact will be definitive for all contractors because compliance determination is binary. Passing 100 percent of the controls required at each of the five CMMC levels permits your organization to participate in DoD procurements at the attained maturity levels.

Even though CMMC enforcement may not officially begin for your organization and your contracts immediately, it can reasonably take several years of security transformation to achieve confidence with your level of cyber maturity, while preparing for your formal maturity certification. Spreading the cost of remediation over several years is financially prudent, because preparation and compliance might entail new hiring, technology investments, advanced training programs, and a shift toward a more effective security culture.

Meanwhile, your organization and all defense suppliers remain obligated under DFARS to continue self-attesting to compliance with NIST 800 -171. Defense acquisitions will continue to consider your DFARS compliance as a material procurement requirement. If a certification board fails your organization on controls you claim to meet, it may imperil your access to new DoD contracts and expose your organization to heightened scrutiny and audit risk.

All DIB contractors and their supply chain partners should take immediate steps to understand their cybersecurity posture, identify and close their compliance gaps, and validate that they will be ready to successfully undergo third-party CMMC certification when their DoD contracts require CMMC compliance. Prime contractors should insist on tools that provide credible visibility into the compliance preparedness of their critical supply chain partners.

The most effective security compliance alternative available to the defense industrial base is our process management solution that provides exceptional insight into the compliance state and maturity roadmap of contractors and their critical supply chain partners.

RANDALL H. COOK
randy.cook@ankura.com
+1.203.521.1856 Mobile

SCOTT CORZINE
scott.corzine@ankura.com
+1.917.930.5300 Mobile

STEPHEN P. GILMER
steve.gilmer@ankura.com
+1.248.832.3808 Mobile

ALAN LEVESQUE
alan.levesque@ankura.com
+1.203.745.9057 Mobile

WAQAS SHAHID
waqas.shahid@ankura.com
+1.571.338.1870 Mobile

ABOUT US

Ankura is a business advisory and expert services firm defined by *HOW* we solve challenges. Whether a client is facing an immediate business challenge, trying to increase the value of their company or protect against future risks, Ankura designs, develops, and executes tailored solutions by assembling the right combination of expertise. We build on this experience with every case, client, and situation, collaborating to create innovative, customized solutions, and strategies designed for today's ever-changing business environment. This gives our clients unparalleled insight and experience across a wide range of economic, governance, and regulatory challenges. At Ankura, we know that **collaboration drives results.**