CMMC Is Coming: Are You Ready?

Jon Williams and Anna Wright

March 17, 2020

About PilieroMazza

PilieroMazza – a business law firm – serves as a strategic partner to government contractors and commercial businesses from across the United States.

We deliver results for our clients by implementing legal and business solutions that take the client's best interests into consideration. Moreover, PilieroMazza's efficient operational structure and lean approach to staffing matters translates into competitive pricing for our clients, while providing the highest standard of client service and legal acumen.

PilieroMazza is privileged to represent clients in the following areas:

- Audits & Investigations
- Business & Corporate Law
- Cybersecurity & Data Privacy
- False Claims Act
- Government Contracts Law
- Mergers & Acquisitions
- Intellectual Property & Technology Rights
- Labor & Employment Law
- Litigation & Dispute Resolution
- Native American Law
- Small Business Programs & Advisory Services
- Private Equity & Venture Capital

Sign up for our newsletters and blog at

www.pilieromazza.com

Jon Williams

Jon Williams
Partner
jwilliams@pilieromazza.com
888 17th Street, NW
11th Floor
Washington, DC 20006

Jon Williams has nearly 20 years of experience advising contractors on a wide range of government contracting matters and Federal Acquisition Regulation compliance, including the federal procurement programs for small businesses (i.e., the 8(a), HUBZone, WOSB, and SDVOSB programs).

Mr. Williams represents contractors in bid protests, size protests and appeals, and related administrative and court proceedings. He assists large and small contractors in navigating SBA audits and investigations, including subcontracting plan compliance reviews, IG investigations, and suspension and debarment proceedings. He regularly helps contractors to establish teaming, subcontract, joint venture, and mentor-protégé relationships. Additionally, he counsels contractors on cure notice responses, requests for equitable adjustment, claims, and disputes on government contracts.

Anna Wright

Anna Wright
Associate
awright@pilieromazza.com
888 17th Street, NW
11th Floor
Washington, DC 20006

Anna Wright serves as an associate in PilieroMazza's Government Contracts Group.

Assisting clients in a variety of government contracting matters, Ms. Wright guides commercial businesses through bid protests at all levels, size and status protests, requests for equitable adjustment, claims, and appeals. Her work encompasses small business procurement matters, particularly on issues related to eligibility, participation in the federal small business set-aside programs, and maintaining regulatory compliance. Ms. Wright also works closely with PilieroMazza's False Claims Act (FCA) Group and addresses other issues arising under the Federal Acquisition Regulation (FAR) and the Contract Disputes Act (CDA).

While earning her law degree, Ms. Wright served as a law clerk for the U.S. Attorney's Office for the District of Columbia and received the President's Volunteer Service Award.

Overview

- The current cybersecurity landscape
- DoD’s upcoming Cybersecurity Maturity Model Certification, aka CMMC
- What contractors should do to prepare

Increasing Importance of Cybersecurity

- Roughly $600 billion lost *annually* due to bad actors exploiting inadequate cybersecurity protections
- DoD has been leading the way over the last several years in placing more emphasis on cybersecurity
  - Cybersecurity is now the "fourth pillar" of DoD acquisition
  - DoD and other agencies are beginning to place more focus on cybersecurity in evaluation and award decisions
- FAR and DFARS provisions to address cybersecurity are now included in most civilian and DoD contracts
  - FAR 52.204-21: Basic cyber safeguards
  - DFARS 252.204-7012: More extensive cybersecurity requirements, including compliance with NIST SP 800-171

What’s Happening Now

- The current FAR and DFARS cybersecurity provisions only require self-certification; enforcement has been limited
- Enter CMMC
  - Guidance has been in development for over a year
  - Final version of CMMC framework released on January 31, 2020
- CMMC is a third-party certification
  - No more self-certification—no “close enough” determinations
  - Certification will assess contractors’ “cybersecurity hygiene”
  - Goal is to provide an objective, third-party verification to assess and enhance the cybersecurity posture of the defense industrial base

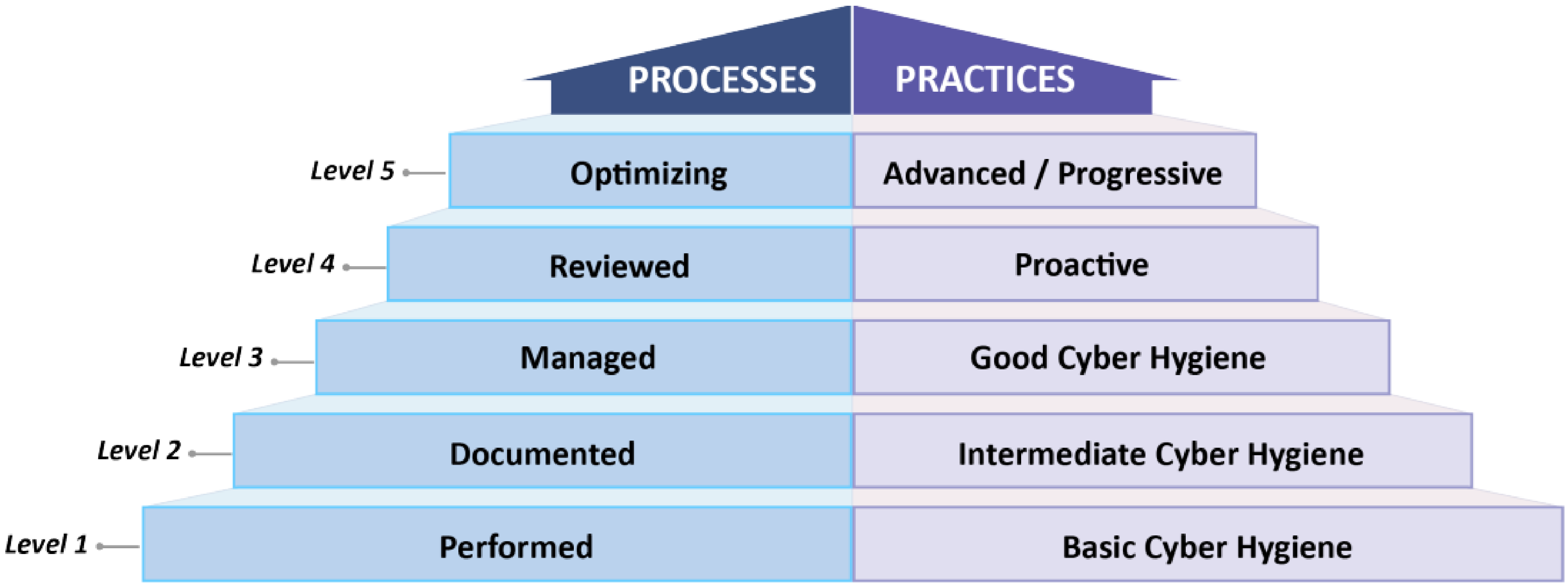
CMMC Overview

- Business system certification, comparable to CMMI
- Five levels of certification, from 1 (lowest) to 5 (highest)
- **Gatekeeper:** CMMC will be required for **all** DoD contractors, both large and small, at the time of award of new DoD contracts
- Must be flowed down to subcontractors
- Required even if you do not have CUI in your IT system
- **Bottom line:** if you work with DoD or in the DoD supply chain, the question is not if you need CMMC, but what level you will need and when

What Is “DoD Sensitive Information”?

- The level of CMMC you will need depends on the type of information in your IT system
- DoD sensitive (unclassified) information encompasses two major “buckets”:
  - **Federal Contract Information (“FCI”):** “information provided by or generated for the Government under contract not intended for public release”
  - **Controlled Unclassified Information (“CUI”):** “information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies,” but is not classified

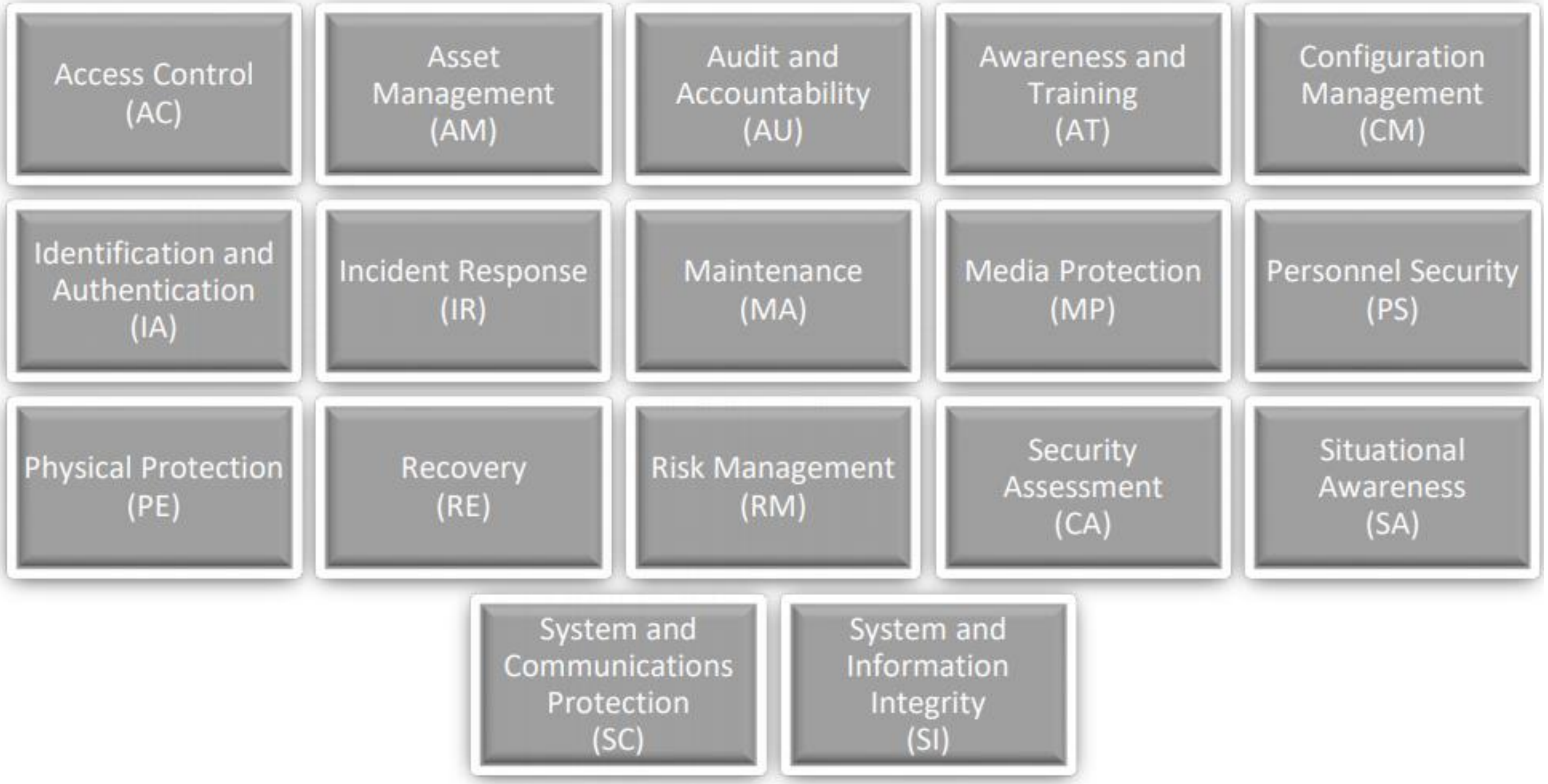
CMMC Levels



	PROCESSES	PRACTICES
Level 5	Optimizing	Advanced / Progressive
Level 4	Reviewed	Proactive
Level 3	Managed	Good Cyber Hygiene
Level 2	Documented	Intermediate Cyber Hygiene
Level 1	Performed	Basic Cyber Hygiene

Figure 2. CMMC Levels and Descriptions

CMMC Domains



- Access Control (AC)
- Asset Management (AM)
- Audit and Accountability (AU)
- Awareness and Training (AT)
- Configuration Management (CM)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Recovery (RE)
- Risk Management (RM)
- Security Assessment (CA)
- Situational Awareness (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

Figure 4. CMMC Domains

CMMC Framework – Key Terms

- **Domains:** broad categories of cybersecurity controls
- **Capabilities:** sub-categories of technical ability within each domain
- **Practices:** specific activities performed to support your cybersecurity capabilities
  - CMMC measures how well you adhere to the specific practices required to achieve your desired CMMC Level
- **Processes:** documentation, management, review, and optimization of cybersecurity activities you perform
  - Examples: company policies, handbooks, and procedures

CMMC Level 1

- Basic requirements intended to be easily attainable for all small businesses
- Appropriate if you only handle FCI, but not if you handle CUI
- The 17 required security practices track the basic cybersecurity safeguards in FAR 52.204-21, including:
  - Use a spam filter for emails
  - Install and enable antivirus software
  - Require usernames and passwords to log on to company systems
  - Internally limit who has access to information (e.g., allow only the payroll department to view payroll information)
  - Escort visitors to prevent unauthorized access to your systems

CMMC Level 2

- Requires documented cybersecurity practices and policies
- Intended to help small businesses progress from Level 1 to Level 3
  - Like Level 1, not appropriate if you have CUI
  - Unlike Level 1, significant increase in required practices – so why not go to Level 3?
- Examples:
  - Disable unnecessary software/applications
  - Lock accounts after a certain number of unsuccessful logins
  - Perform weekly system backups
  - Create a system security plan (“SSP”) for your company

CMMC Level 3

- Expected to be the requirement for most DoD prime contracts
  - The required practices track NIST SP 800-171, which is already included in most DoD contracts through DFARS 252.204-7012
- Step up from Level 2 to “managed” cybersecurity practices and implementation; necessary if you handle CUI
- Documented vs. managed
  - Documented (Level 2): high-level policy statements, plus basic plans for individuals responsible for compliance
  - Managed (Level 3): documented PLUS mission statement, SMART goals, training objectives, and keeping track of skills, funding, and tools—essentially, methodically institutionalizing cybersecurity

CMMC Level 3

- Examples:
  - Use FIPS-validated encryption modules to store sensitive information
  - Block company computers from accessing known malicious websites
  - Separate individual duties to avoid conflicts of interest (e.g., one person is responsible for creating a program or policy, and another is responsible for testing it)
  - Keep abreast of cyber threat intelligence information and update your threat profiles, vulnerability scans, and risk assessments
- Employee training is critical
  - Must be able to show that you are actively keeping your employees apprised of overarching policies, as well as their individual responsibilities

CMMC Levels 4-5

- Level 4 requires companies to “review and measure practices for effectiveness[, …] take corrective action when necessary[,] and inform higher level management of status or issues on a recurring basis”
- Level 5 requires companies to “standardize and optimize process implementation” across their organizations
- Levels 4-5 are only required when there is a high likelihood of “advanced persistent threats”
    - Likely not applicable to the majority of defense industrial base contractors

When Will You Need CMMC?

- DoD is taking a "crawl, walk, run" approach
  - DoD will start with approx. 10 "pathfinder programs" this year
  - Priority programs like nuclear modernization and missile defense
- FY21-FY25: "Phased Rollout"
  - DoD estimate of the total number of contracts requiring CMMC:

FY21:	15
FY22:	75
FY23:	250
FY24:	479
FY25:	479

- FY26: CMMC required for <u>all</u> DoD contracts

When Will You Need CMMC?

- DoD estimate of the total number of contractors and subcontractors that will need CMMC:
  - FY21: 1,500
  - FY22: 7,500
  - FY23: 25,000
  - FY24: 47,905
  - FY25: 47,905
- DoD estimates > 50% of certified firms will be at Level 1
- New DFARS clause must be issued and added to contracts
  - DoD will use the new DFARS clause to add CMMC to new contracts and re-competes
  - No plan to add the DFARS clause to existing contracts

How to Obtain CMMC

- TBD!
- The “Accreditation Body” was formed in January and will oversee third-party assessment organizations (“C-3PAOs”)
- No C-3PAOs have been accredited yet; perhaps by summer 2020
- Contractors will apply for a specific level of certification and certifiers will evaluate only up to the requested level
  - If you request Level 3, that is the highest level you will receive – but the certifier can also decide you are only eligible for Level 1 or Level 2
- Certification is expected to be good for 3 years
- Costs of certification are currently unknown

What Should You Do to Prepare?

- Don’t wait until the last minute – begin preparing now
- Be wary of scams
- Start by answering key questions:
  - Do you work directly with DoD or in the DoD supply chain?
  - Do you have FCI or CUI in your network?
  - Who are the prime contractors you work with, and what are they doing/saying about CMMC?
  - When are the recompetes or new contracts for your key programs?
  - How close are you to Level 1 or Level 3?

Get Level 1 Ready

- Focus on Level 1 **now**
  - Bare minimum for CMMC, and may be all you need
  - Already required for nearly all contractors through the FAR
  - Should be relatively easy to attain for most firms, if not already there
  - Low cost to implement
- PilieroMazza is helping contractors assess Level 1 readiness & implement necessary procedures
  - Understand & implement the Level 1 requirements
  - Have a Level 1 Plan

Review, Update, and Strategize

- Review/update employee policies and training
- Review/update your teaming agreements, subcontracts, NDAs, and other contracts with 3rd parties
  - Flow-down (or resist flow-down) depending on your situation
  - Risk-shifting provisions are critical
- Consider potential for protests
  - Does a solicitation incorrectly include (or not include) CMMC or other cybersecurity requirements?
  - Solicitation protests are due by the proposal due date

Leverage Available Resources

- Potential assistance from prime contractors
  - SBA's All Small Mentor-Protégé Program
  - DoD's Mentor-Protégé Program allows reimbursement of mentor's costs related to assisting protégé
  - Consider keeping sensitive information on the prime's systems only
- Take advantage of free resources
  - DoD intends to release training guides later this month
  - DoD plans to have training available through DAU later this year
  - DoD is also working with PTACs to provide training
- Talk to your insurance broker about cybersecurity insurance

Key Takeaways

- There are still more questions than answers
- But CMMC is coming—it's not a question of if, but of when, and what level, so start preparing now
- Every DoD contractor will need at least Level 1, so focus now on getting Level 1 ready
  - Gain a competitive edge by showing your government customers and contracting partners that you are ahead of the curve and ready for CMMC
- Determine if you need higher than Level 1 based on the type of information you handle, the contracts you perform, and the companies with which you work

How PilieroMazza Is Helping Contractors Prepare

- Determine cybersecurity requirements to which you are already subject, and develop compliance strategies
- CMMC Levels 1 and 3 readiness assessments and preparation of internal plans
- Review/revise employee handbooks, policies, and training
- Review/revise teaming agreements, subcontracts, and NDAs
- Review of solicitation requirements and protest assessments
- Incident response training and execution
- Communication with government officials on applicability and scope of contractual cybersecurity requirements

Helpful Links

- DoD Office of the Under Secretary of Defense for Acquisition & Sustainment
  - Home Page: https://www.acq.osd.mil/
- CMMC
  - Home Page: https://www.acq.osd.mil/cmmc/index.html
  - FAQs: https://www.acq.osd.mil/cmmc/faq.html
  - Final Guidance: https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf
  - Appendices: https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Appendices_20200203.pdf
    - Includes discussions and clarifications for each level
  - Public Briefing: https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf
  - Press Conference: https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2072073/press-briefing-by-under-secretary-of-defense-for-acquisition-sustainment-ellen/
- CUI
  - CUI Registry: https://www.archives.gov/cui
  - CUI Training: https://www.archives.gov/cui/training.html

Questions?

Jon Williams
Partner
PilieroMazza PLLC
jwilliams@pilieromazza.com

Anna Wright
Associate
PilieroMazza PLLC
awright@pilieromazza.com

Disclaimer
This communication does not provide legal advice, nor does it create an attorney-client relationship with you or any other reader. If you require legal guidance in any specific situation, you should engage a qualified lawyer for that purpose. Prior results do not guarantee a similar outcome.

Attorney Advertising
It is possible that under the laws, rules, or regulations of certain jurisdictions, this may be construed as an advertisement or solicitation.