PILIERO MAZZA

Cyber Security Compliance for Small Businesses

David Shafer, Attorney, Cybersecurity & Data Privacy, PilieroMazza PLLC
Anna Wright, Attorney, Cybersecurity & Data Privacy, PilieroMazza PLLC

December 3, 2020

David Shafer

David Shafer
Attorney
PilieroMazza PLLC
Cybersecurity & Data Privacy
410.500.5551
dshafer@pilieromazza.com

Dave leads the PilieroMazza's Cybersecurity & Data Privacy team, where he and his colleagues counsel clients on matters related to cybersecurity and information privacy, including compliance with federal and state statutes and regulations, as well as industry standards and emerging regulatory requirements. He is experienced in interpreting statutes, regulations, and agency guidance to aid clients in the development of internal policies and procedures, and guiding companies through incident response and notifications following a data breach.

PILIERO MAZZA

Anna Wright

Anna Wright
Attorney
PilieroMazza PLLC
Cybersecurity & Data Privacy
202.857.1000
awright@pilieromazza.com

A member of the Firm's Cybersecurity & Data Privacy team, Anna works actively to help clients come into compliance with cybersecurity and data privacy laws. In particular, she assists government contracts working with the Department of Defense (DOD) to assess and meet their compliance obligations for the Cybersecurity Maturity Model Certification (CMMC), which impacts a contractor's ability to bid for and maintain a contract with the DOD.

PILIERO MAZZA

About PilieroMazza

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

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 translate 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
- Business Succession Planning
- Corporate and Organizational Governance
- Cybersecurity & Data Privacy
- Debt Financing
- Employee Incentive and Bonus Plans
- False Claims Act
- Government Contracts
- Government Contract Claims & Appeals
- Intellectual Property & Technology Rights
- Labor & Employment
- Labor & Employment for Government Contractors
- Litigation & Dispute Resolution
- Mergers & Acquisitions
- Native American Law & Tribal Advocacy
- Private Equity & Venture Capital

Subscribe to our mailing lists at www.pilieromazza.com

PILIERO MAZZA

Roadmap

- Cybersecurity and CMMC Introduction
- Review of CMMC Certification Levels
- Actions to Take Now
- Cybersecurity's Impact on Awards and Protests
- Leveraging Mentor-Protégé Relationships

PILIERO MAZZA

Introduction and Overview

PILIERO MAZZA

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
- FAR and DFARS provisions to address cybersecurity are now included in most government and DoD contracts

PILIERO MAZZA

What Does the FAR Cover?

- FAR 52.204-21: requires contractors to apply fifteen "basic safeguarding requirements and procedures"
- Applies to all procurements in which "the contractor or subcontractor at any tier may have federal contract information residing in or transiting through its information system," per FAR 4.1903

What Is "DoD Sensitive Information"?

- 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

PILIERO MAZZA

Ongoing Shift to CMMC

- The current FAR and DFARS cybersecurity provisions only require self-certification; enforcement has been limited
  - But, potential of breach of contract, adverse past performance, protest risk, and False Claims Act liability if certification of compliance is incorrect
- New NIST assessment attempts to bridge the gap
  - Attaches a numeric score to compliance and allows clearer picture of actual cyber risk
- 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

PILIERO MAZZA

CMMC Overview

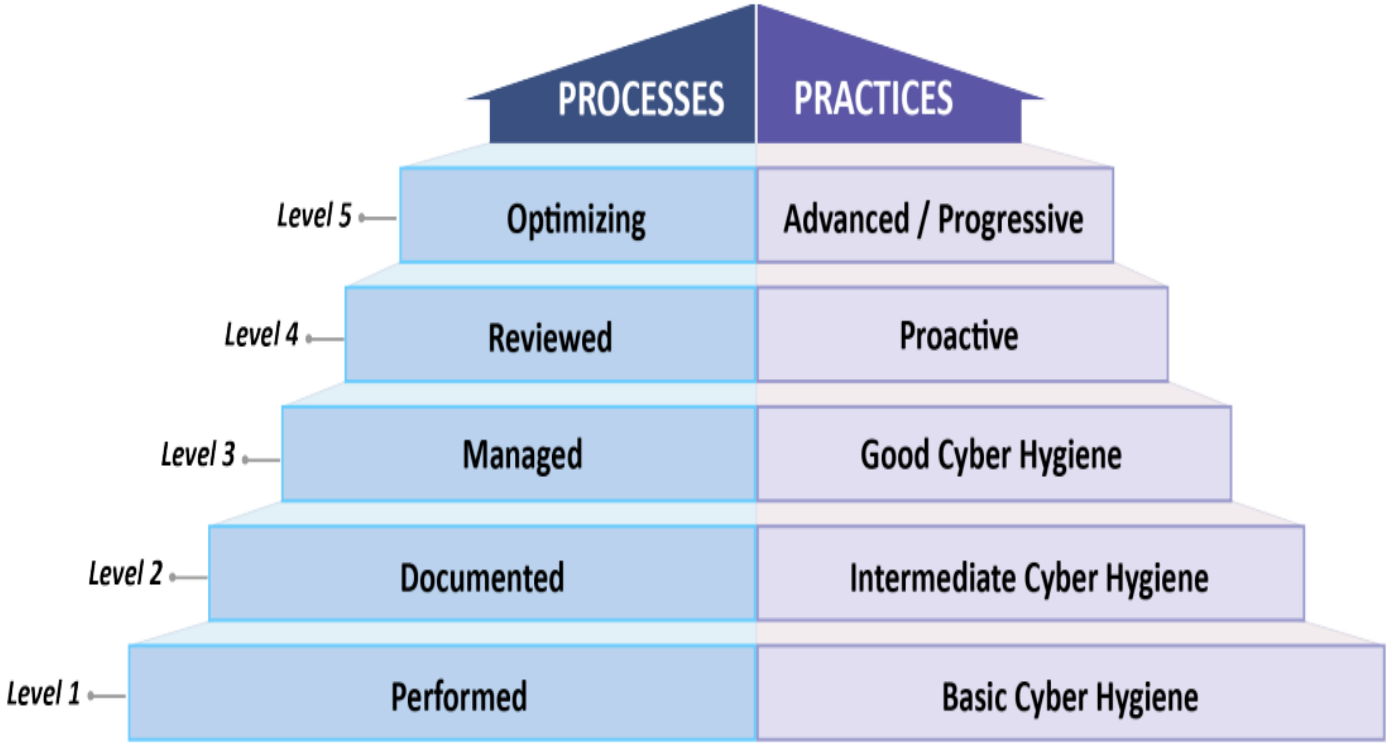
- Business system certification, comparable to CMMI
- Five levels of certification, from 1 (lowest) to 5 (highest)
- **Gatekeeper:** CMMC will be required for **all** DoD contractors, both large and small, at the time of award of new DoD contracts
- Must be flowed down to subcontractors
- Required even 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

PILIERO MAZZA

CMMC Levels and Assessment

PILIERO MAZZA

CMMC Levels



PILIERO MAZZA

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

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?

CMMC Level 3

- Expected to be the requirement for most DoD prime contracts; largely tracks to NIST SP 800-171
- Step up from Level 2 to “managed” cybersecurity practices and implementation; necessary if you handle CUI

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”

PILIERO MAZZA

What Will You Need for 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 all DoD contracts

PILIERO MAZZA

What to Do Now

PILIERO MAZZA

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 only need Level 1
- New DFARS clause must be added to contracts

PILIERO MAZZA

How to Obtain CMMC?

- The “Accreditation Body” was formed in January and will oversee third-party assessment organizations (“C-3PAOs”)
- **No C-3PAOs have been accredited yet**
- Certain Practitioners and Assessors have been certified
- Contractors will apply for a specific level of certification and certifiers will evaluate only up to the requested level
- Certification is expected to be good for 3 years

PILIERO MAZZA

CMMC Estimated / Projected Costs

CMMC Cert	Avg non-recurring eng'g costs	Recurring eng'g costs	Avg assessment costs	Total annual assessment costs
Level 1	$0	$0	$1,000	$1,000
Level 2	$407	$20,154	$7,489	$28,050
Level 3	$1,311	$41,666	$17,032	$60,009
Level 4	$46,917	$301,514	$23,355	$371,786
Level 5	$61,511	$384,666	$36,697	$482,874

PILIERO MAZZA

What Should You Do to Prepare for the Current Requirements and the Upcoming CMMC?

- Don’t wait until the last minute – begin preparing now
- Be wary of scams (Only a C3PAO can issue the certification)
- 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?
  - Do your current contracts require compliance with NIST 800-171?
  - 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?

PILIERO MAZZA

Get Level 1 Ready

- Perform the NIST self-assessment
- Then, focus on CMMC Level 1
- Assess Level 1 readiness and implement necessary procedures

PILIERO MAZZA

Impact on Awards and Agreements

PILIERO MAZZA

Applicability to Subcontractors

- DFARS 252.204-7012 must be flowed down to subcontractors, **but only** when subcontract performance is for "operationally critical support" or CUI is necessary for performance of the subcontract
- Contractor may consult with the CO if uncertain about whether to flow down the clause to subcontractors
- CMMC applies to subcontractors, but primes may flow down a different level requirement to subs

PILIERO MAZZA

Review, Update, and Strategize

- Review/update employee policies and training
- Review/update your agreements, particularly for flow-down provisions
- Consider potential for protests of solicitation terms
- Talk to your insurance broker about cybersecurity insurance

PILIERO MAZZA

Leverage Existing Relationships

PILIERO MAZZA

Mentor-Protégé Relationships

- Potential assistance from prime contractors through SBA or DoD mentor-protégé programs
- DoD mentor-protégé program allows mentors to be reimbursed for certain mentoring costs, and may cover helping protégé obtain CMMC certification

Helpful Links - 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_ModelMain_V1.02_20200318.pdf
- Appendices: https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf
  - Includes discussions and clarifications for each level
  - Available in Excel: https://www.acq.osd.mil/cmmc/docs/CMMCModelExcel_V1.02_20200318.xlsx
- Public Briefing: https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf
- Errata Sheet: https://www.acq.osd.mil/cmmc/docs/CMMC_Errata_20200318.pdf
- Press Conference: https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2072073/press-briefing-by-under-secretary-of-defense-for-acquisition-sustainment-ellen/
- Accreditation Body: https://www.cmmcab.org/

PILIERO MAZZA

Helpful Links - OUSD, CUI, and NIST

- DoD Office of the Under Secretary of Defense for Acquisition & Sustainment
  - Home Page: https://www.acq.osd.mil/
- CUI
  - CUI Registry: https://www.archives.gov/cui
  - CUI Training: https://www.archives.gov/cui/training.html
- NIST
  - Home Page: https://www.nist.gov/
  - 800-171: https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
- SPRS
  - Home Page: https://www.sprs.csd.disa.mil/
  - Scoring Sheet and Instructions: https://www.sprs.csd.disa.mil/pdf/SPRS_DataEvaluationCriteria.pdf

PILIERO MAZZA

Backup Slides

PILIERO MAZZA

DFARS Cybersecurity Landscape

- **DFARS 252.204-7012 :** Tracks to NIST 800-171 requirements
- **DFARS 252.204-7019, -7020, and -7021**: Implement new NIST SP 800-171 self-assessment requirements

PILIERO MAZZA

What Is NIST SP 800-171?

Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Management
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

PILIERO MAZZA

Who Has to Comply with the NIST Standards?

1. Contractors with DoD contracts containing **DFARS 252.204–7012**
2. That own or operate a **nonfederal** contractor information system
3. And have **CUI** in their nonfederal contractor information system

PILIERO MAZZA

NIST SP 800-171 Assessment Scoring

- Intended to be an intermediate step between fully self-certified current landscape, and fully third-party certified CMMC future landscape
- Start assessment with 110 points and subtract between 1 and 5 points for each noncompliance with NIST controls
- To post assessment to SPRS, contractors must have a system security plan (“SSP”)

NIST Assessment Projected Costs

Assessment	Cost/ assessment	Annual cost/ entity	Total unique entities	Annual cost all entities
Basic	$75	$25	26,469	$655,637
Medium	$909	$303	444	$134,467
High	$50,676	$16,892	243	$4,104,756
Total			27,156	$4,894,860

PILIERO MAZZA

2019 NDAA Section 889

- Broadly, bans sale of certain Chinese-manufactured telecom equipment and services to the Government ((a)(1)(A)) and also use of such equipment/services in contractor businesses ((a)(1)(B))
  - Sales ban went into effect last year, but usage ban went into effect August 13, 2020
  - Prime contractors are not permitted to use any banned products or services anywhere in their organizations—subcontractors are not permitted to use any banned products or services in anything they provide to primes
- FAR reps and certs require inquiry into whether you use these banned products or services
  - And if you discover banned use or sale, you must report it within one business day, with a follow-up report 10 business days later
- No limits on application (e.g., type or size of contract)
- DoD has a partial waiver through September 30, 2022

PILIERO MAZZA

Questions?

David Shafer
Attorney
PilieroMazza PLLC
Cybersecurity & Data Privacy
410.500.5551
dshafer@pilieromazza.com

Anna Wright
Attorney
PilieroMazza PLLC
Cybersecurity & Data Privacy
202.857.1000
awright@pilieromazza.com

PILIERO MAZZA