GEORGE MASON UNIVERSITY | Continuing and Professional Education

https://cpe.gmu.edu/
703-993-4800

Cybersecurity

PUBLIC CONTRACTING INSTITUTE

publiccontractinginstitute.com
202-775-7240

David Shafer

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

Dave leads 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.

Dave also counsels clients on a broad range of business and finance matters, such as mergers and acquisitions, purchase and sale of private businesses, commercial financing, private offerings of debt and equity securities, venture capital and private equity transactions, and general governance issues.

Anna Wright

Anna Wright
Associate
PilieroMazza PLLC
Government Contracts
202.857.1000
awright@pilieromazza.com

Assisting clients in a variety of government contracting matters, Anna 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. Anna 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).

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 to receive our communications at
www.pilieromazza.com

Overview

- Current landscape for cybersecurity
- DFARS 252.204-7012 and NIST SP 800-171
- What is CUI?
- Overview of the Cybersecurity Maturity Model Certification ("CMMC")
- Recommendations to prepare and ensure compliance

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
  - DFARS proposed rule: self-assessment requirements

Key FAR Definitions

- **Covered contractor information system**: "an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information"
- **Federal contract information ("FCI")**: "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments"
- **Information system**: "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information"

What Does the FAR Cover?

- FAR 52.204-21: requires contractors to apply fifteen "basic safeguarding requirements and procedures"
- Intended to establish lowest baseline for protecting FCI
- Requirements and procedures include both physical protections, e.g., ensuring only authorized individuals may physically access servers, and cyber protections, e.g., installing antimalware software
- 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
  - Because definition of FCI is so broad, this means FAR 52.204-21 applies to virtually every Federal contract—even the contract itself can be considered "FCI" to the extent it is not publicly available

DFARS Cybersecurity Landscape

- Currently applicable: **DFARS 252.204-7012**
  - Tracks to NIST 800-171 requirements
- Soon applicable: **DFARS 252.204-7019, -7020, and -7021**
  - 7019: notice of NIST SP 800-171 assessment requirements
  - 7020: implements assessment
  - 7021: will eventually implement CMMC

What Is NIST SP 800-171?

- Key cybersecurity guidelines for DOD contractors (implemented through DFARS 252.204-7012 and new self-assessment)
- Provides performance-based, standardized security requirements for nonfederal IT systems
- Goal: protect controlled unclassified information ("CUI")
- Organized into 14 security "families"

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

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

Drill Down on CUI

- Two key points:
  - The government should mark CUI when it is provided to you in your performance of a contract; if not marked by the government, likely not CUI unless…
  - The contractor (or another party on its behalf) otherwise collects, develops, receives, transmits, uses, or stores CUI in support of contract performance
- Industry categories and examples of CUI (from the CUI Registry):
  - "Controlled Technical Information" includes research and engineering data, drawings, specifications, manuals, and computer software
  - "Law Enforcement" includes procedures for law enforcement operations, investigations, prosecutions, or enforcement actions
  - "Privacy" is divided into subcategories such as health records, genetic information, death records, military

Who Currently Has to Comply with the NIST Standards?

1. Contractors with DoD contracts containing **DFARS 252.204-7012**
   - This DFARS clause should be in all DoD contracts, including commercial item procurements, except for contracts solely for the acquisition of Commercial Off the Shelf ("COTS") items
2. That own or operate a **nonfederal** contractor information system
   - Different security requirements apply to contractor information systems part of an IT service or system operated on behalf of the Government (i.e., a federal system)
3. And have **CUI** in their nonfederal contractor information system

Who Will Have to Comply with the NIST Standards?

- DFARS 252.204-7020: effective November 30, 2020, DoD contractors and subcontractors will need to perform the NIST SP 800-171 assessment and post to the Supplier Performance Risk System ("SPRS")
  - Three "levels" of assessment:
    - Basic is a self-assessment using the scoring rubric
    - Medium and High are DoD-conducted assessments; difference between two depends on the sensitivity of information and strenuousness of DoD audit
  - Before subcontracting, prime contractors will need to ensure subcontractors have at least a Basic assessment posted in SPRS
- Exception: contracts and subcontracts solely for acquisition of COTS items

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
  - Exact subtraction is listed next to each control in assessment sheet
  - No minimum score requirement; score may be negative
- To post assessment to SPRS, contractors must have a system security plan ("SSP")
  - Contractors must also provide a plan of action and milestones ("POAM") addressing any areas in which they do not currently comply with the NIST standards

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

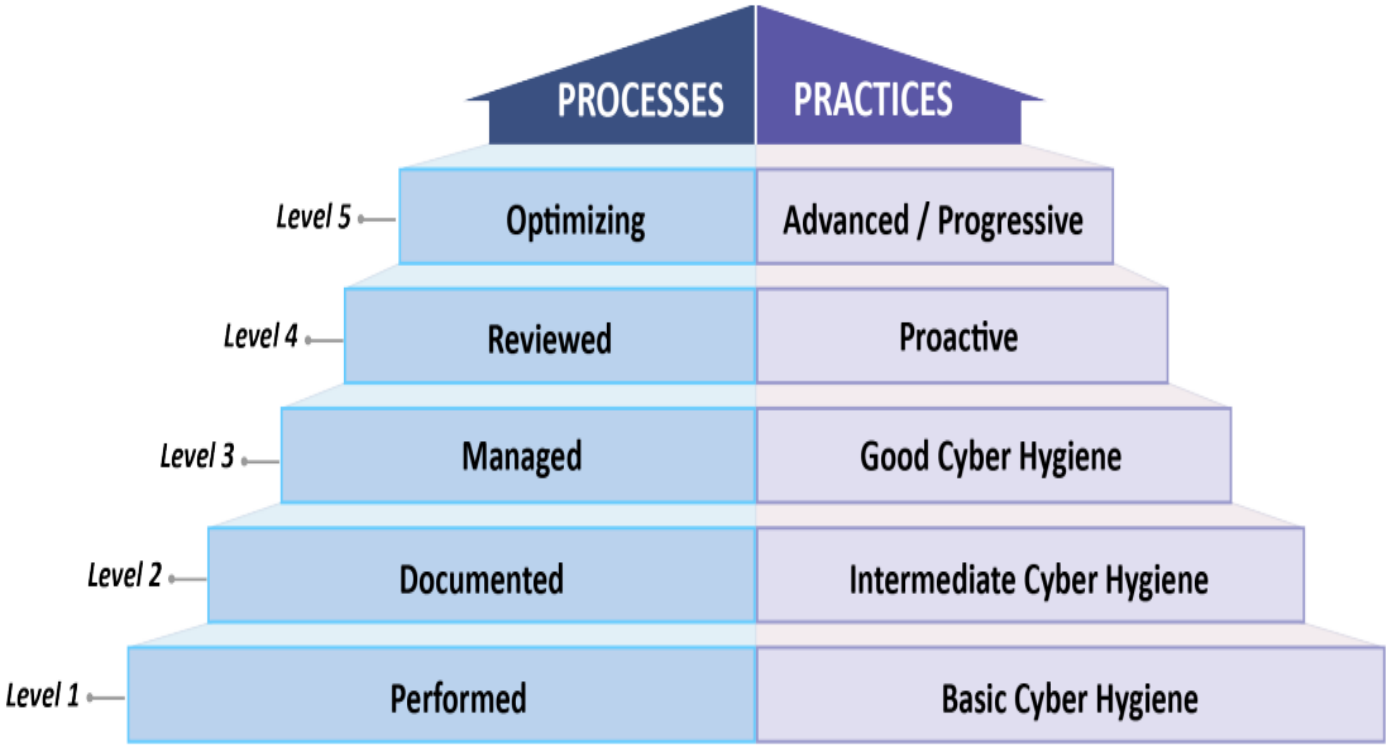
Ongoing Shift to CMMC

- 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

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

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

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 largely track NIST SP 800-171
- 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

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

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 issued and added to contracts
  - DoD will use the new DFARS clause to add CMMC to new contracts and re-competes, expected by this fall
  - 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; 25 individual assessors have completed the provisional trainings to date, but no companies
- 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

CMMC 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

Exception for COTS

- DFARS 252.204-7012 does not apply to contractors that **only** perform contracts that are **solely** for COTS, which are:
  - A commercial item;
  - Sold in substantial quantities in the commercial marketplace; and
  - Offered to the federal government, under a contract or subcontract at any tier, without modification, in the same form as it is sold in the commercial marketplace
- If you have some contracts that are not for COTS, or not solely for COTS, the blanket exception does not apply
- Likewise, for CMMC and the NIST assessment, contractors (both prime and sub) who solely produce COTS items will not require certification

Exception for Commercial Item Contracts?

- Unlike for COTS, there is no blanket exception for commercial items
  - All COTS are commercial items, but all commercial items are not necessarily COTS
- DFARS 252.204-7012 recognizes that, on many commercial item procurements, DoD does not provide covered defense information to the contractor as a necessary component of performing the work
  - In this scenario, DFARS 252.204-7012 does not apply
  - BUT, must still post NIST assessment to SPRS
- Similarly, no non-COTS commercial item exception to CMMC or the NIST assessment

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
  - Operationally critical support is essential to mobilization, deployment, or sustainment of the Armed Forces in a contingency operation
- 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
  - So, the fact that a prime contract requires Level 4 certification does not necessarily mean the subcontract will also require that Level

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
- 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?

Get Level 1 Ready

- Perform the NIST self-assessment now
  - Unless you only sell COTS items or do no business at all with DoD, you will need to post your assessment to SPRS
  - Assessment requires an SSP and POAM
- Then, focus on CMMC Level 1
  - 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
- Assess Level 1 readiness and 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 agreements, particularly for flow-down provisions
- Consider potential for protests of solicitation terms
- Potential assistance from prime contractors through SBA or DoD mentor-protégé programs
- Talk to your insurance broker about cybersecurity insurance

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/

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

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

Questions?

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

Anna Wright
Associate
PilieroMazza PLLC
Government Contracts
202.857.1000
awright@pilieromazza.com