MAYER | BROWN

CMMC: Legal and Regulatory Update

Cybersecurity and Regulation of Contractors

Marcia G. Madsen
Partner
(202) 263 3274
mgmadsen@mayerbrown.com

David A. Simon
Partner
(202) 263 3388
dsimon@mayerbrown.com

February 2020

Agenda

- Introduction
- Proliferation of Cyber Threats
- Background: Cyber Regulatory Challenges – How Did We Get Here?
- Cybersecurity Maturity Model Certification (CMMC)
- Section 889 – Supply Chain Impact

Introduction

MAYER | BROWN

Presenter: Marcia G. Madsen

Marcia G. Madsen is a partner in Mayer Brown's Washington DC office and Chair of the Government Contracts practice and Co-Chair of the National Security practice. She represents contractors in regulatory, policy, transactional, compliance, investigative, and litigation matters involving virtually every federal department and agency. Her clients include defense contractors, information technology contractors, systems integrators, telecommunications companies, engineering firms, insurers, and manufacturing companies.

Marcia's practice includes defense of False Claims Act matters, internal investigations, audits, compliance reviews, bid protests, claims and disputes before administrative forums, and in the federal courts), as well as ADR and mediation proceedings. Areas of concentration include: aerospace and defense, systems integration, information systems and telecommunications and related cybersecurity issues, healthcare and bio-technology, homeland security, environmental remediation, and research and development.

She has chaired the ABA Section of Public Contract Law and multiple section committees including committees on Procurement Fraud, Bid Protests, and Emerging Issues. She chaired the Services Acquisition Reform Act Panel. She is a member of the Federalist Society Administrative Law and Regulation Executive Committee, the Law 360 Government Contracts Editorial Advisory Board, and the GW Law School Government Contracts Advisory Board.

Presenter: David Simon

David A. Simon is a partner in Mayer Brown's Washington DC office and a member of the global Cybersecurity & Data Privacy Practice and the Firm's National Security Practice. A former special counsel at the U.S. Department of Defense (DoD), David has deep experience advising victims of state-sponsored cyber activity, ransomware attacks, and other forms of cyber extortion attacks. He has directed and advised on dozens of complex cybersecurity incident and data breach investigations in the last few years alone. David has counseled companies on major cybersecurity incidents and incident preparedness across virtually every sector of the economy. He advises companies as they address cyber vulnerabilities and breaches, as well as associated legal, regulatory, and reputational consequences. In addition, David helps companies structure, negotiate and protect their commercial and compliance relationships with key national security government agencies.

David is an Adjunct Fellow in Cybersecurity and International Law at the Center for Strategic and International Studies, and a Visiting Research Fellow at the cyber war college at the U.S. National Defense University. In addition, he serves as an independent expert on cybersecurity, data privacy, and counterterrorism law to the United Nations. Previously, he served at the invitation of the NATO Cooperative Cyber Defense Center of Excellence as a peer reviewer of the second edition of the "Tallinn Manual on the International Law Applicable to Cyber Warfare."

Proliferation of Cyber Threats

MAYER | BROWN

Series of High Profile Attacks Prompted Action

- **Army National Guard Data Breach** (2015) exposed personal details of 850,000 current and former soldiers
- **OPM Data Breaches:** (2015) Two breaches in the same year exposed confidential personal information of over 25.7 million people. Attack tied to Chinese government officials
- **Navy Submarine Warfare Data Breach** (Jan./Feb. 2018): Press reports stated that the Chinese Ministry of State Security extracted over 614 gigabytes of data from an unclassified contractor network regarding the development of supersonic anti-ship missiles for use by US submarines in connection with a Naval project known as Sea Dragon
- **DISA Data Breach** (May-July 2019) reported in the press February 20, 2019 – exposed confidential personal information of 200,000 individuals

Cybersecurity Threats to Government Contractors

- Cybersecurity threat actors have targeted companies across almost all major sectors, but the defense industrial sector is a prime target for cyber attacks
  - June 2018 Navy submarine warfare breach
  - Documents released in January 2015 indicated that Chinese actors had stolen a large amount of military data, including data related to the F-35 Joint Strike Fighter
  - In August 2015, Dell exposed a Chinese group codenamed Emissary Panda that was engaged in widespread espionage activities against US and UK defense contractors
- Because of their role in national defense and access to sensitive national security information, contractors, especially those dealing with DoD (and their subcontractors and suppliers) face unique and increasing cybersecurity requirements

War Story: Small-Defense Contractor

- **Scenario**
  - A small defense contractor of fewer than 100 employees that supports the USG discovered persistent access over multiple years. The contractor's systems were eliminated, the company was forced to move to off-band communications, and subsequently replaced its IT systems
  - Per DFARS the company notified the DC3, despite not being an active member of the DIB
  - Through a subsequent investigation by CrowdStrike, it was determined that the threat actor was the Chinese PLA, with a view to obtaining stolen intellectual property
  - Cyber attacks can target and take control of companies barely large enough to have a facility clearance, but can still have access to CUI and sensitive information

Background: Cyber Regulatory Challenges – How Did We Get Here?

MAYER | BROWN

Civilian Agency Cyber Regs - Overview

- NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, released June 2019 and finalized 2/21/2020 (Initially released in 2015; Rev. 1 released in December 2016). 110 security controls to be implemented by contractors that process, store, or transmit CUI
  - At the same time NIST released a draft SP 800-171B intended to address controls for high value assets at risk of advanced persistent threats (APT). Second draft for comment is expected
- May 2016: new FAR subpart and contract clause governing basic protection of contractor information systems that process, store, or transmit Federal Contract Information (FCI). Codified in FAR Subpart 4.19, contract clause at FAR 52.204-21.
  - Does not require compliance with SP 800-171
- June 2016: National Archives and Records Administration issues final rule for managing controlled CUI

FAR Cyber Rule Protecting FCI

Contracting officers **must include the FAR cyber contract clause** in all contracts or solicitations where the contractor or subcontractor "may" have "Federal contract information" on its systems

- Federal contract information = Information, not intended for public release, provided by or generated for Government under a contract to provide a product or service

This requirement does not apply to contracts for solely commercially available off-the-shelf items ("COTS") or acquisitions below the SAT

While the FAR cyber rule mandates certain specific security controls, unlike the DFARS cyber rule, it does not require compliance with SP 800-171 and does not include an incident reporting requirement

Federal Acquisition Regulation – Security Controls

The rule sets out fifteen "basic safeguarding . . . security controls" that contractors must employ "to protect covered contractor information systems"

These include:

– Limit system access to authorized users	– Limit system access to transactions and functions that authorized users are permitted to execute	– Verify and control/limit connections to and use of external systems
– Control information posted or processed on publicly accessible systems	– Provide protection from malicious code at appropriate locations within organizational information systems	– Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.
– Sanitize or destroy media containing government information before disposal or release for reuse	– Limit physical access to systems, equipment, and the respective operating environments to authorized individuals	– Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices

DFARs Cyber Regs – Overview

- Oct. 2016: DFARS rule requiring covered contractors to "provide adequate security on all covered contractor information systems" ("at a minimum" includes implementation of NIST SP 800-171) and to report any "cyber incident" within 72 hours. Codified mostly at **DFARS 252.204-7012.** Contractors must certify compliance per DFARS 252.204-7008(c)
  - Requires defense contractors to provide DoD personnel with access to equipment and information to assess the impact of such penetrations. Also imposes substantial security requirements applicable to cloud computing services procured by components of DoD
- Applies to contractors that operate "**covered contractor information systems**"; i.e., "an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits **covered defense information**" (CDI). DFARS 252.204-7012
  - Must be flowed down to subcontracts (including those for commercial items) for operationally critical support or that involve covered defense information
  - Prime has the responsibility to determine if information required for the subcontract performance is CDI

Covered Defense Information (CDI)

Covered Defense Information encompasses "Controlled Unclassified Information" (CUI) (as set forth in the CUI Registry) that is either:

1. Marked or otherwise identified by DoD as such; or is
2. Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract

DFARS 252.204-7012

The CUI Registry is maintained by the National Archives, and includes **dozens of categories** of CUI based on requirements of existing law. See https://www.archives.gov/cui

Controlled Unclassified Information (CUI)

- Several categories of CUI (and potentially CDI) include:
  - **Export Controlled Information**: including, "Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives"
  - **Protected Critical Infrastructure Information**: "As defined by 6 USC 131-134, and 6 CFR 29, PCII relates to threats, vulnerabilities, or operational experience related to the national infrastructure"
  - **DoD Critical Infrastructure Security Information**: "Information that, if disclosed, would reveal vulnerabilities in the DoD critical infrastructure and, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities"
  - **Source Selection Information**: Certain "information that is prepared for use by an agency for the purpose of evaluating a bid or proposal to enter into an agency procurement contract, if that information has not been previously made available to the public or disclosed publicly"
  - **General Proprietary Business Information**: "Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications"

Challenges Raised by DFARS Approach to CDI

- ***DoD has stated that responsibility for identifying CDI falls on the Agency***
- Specifically, the Contracting Agency has obligations to:
  - Notify the contracting officer when a contract could lead to a contractor receiving or creating CDI;
  - "Mark or otherwise identify information that will be provided to the contractor in support of the performance of the contract"; and
  - "Determine if CDI is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor"
- **Contracting officers are required to mark CDI or identify it in the contract or order.**

However, informal guidance from the DoD Office of the General Counsel suggests that government contracting officers either do not engage in the proper marking and identification or do not do so consistently. *This implementation failure would not shield a contractor from potential liability, administrative sanction, or reputation harm arising out of the compromised CDI. If the contractor "becomes aware that CDI or operationally critical support" information is involved in performance of the contract, it should contact the responsible contracting officer*

DFARS Cyber Rule – "Adequate Security"

- Contractors and subcontractors must provide "adequate security" for covered systems. 48 C.F.R. § 204.7302. Elements of adequate security include:
  - Implementing administrative, technical, and physical safeguards if using cloud computing (FEDRAMP applies if external cloud provider)
  - Implementing security requirements specified in NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" that are in effect at the RFP date
- Contractors were required to implement the then existing NIST SP 800-171 no later than December 31, 2017
- These safeguarding requirements apply to *all* covered contractor information systems, not only those that are used to perform a particular contract

DFARS Final Rule – Incident Reporting

- Upon identifying a cyber incident, the contractor must:
  - "Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts"
  - Report the incident to DoD at http://dibnet.dod.mil **within 72 hours**
  - "[P]reserve and protect images of all known affected information systems . . . and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report"
  - Allow DoD to access "additional information of equipment that is necessary to conduct a forensic analysis"
  - *If malicious software is identified*, then the contractor must submit the software to DoD Cyber Crime Center (DC3)

Contractors Face Expanding Cyber Requirements

- In September 2018 as a result of the MSS breach, the Navy issued a memorandum on "Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks" that immediately established additional requirements for contractors built on DFARs requirements. Navy requirements were updated in 2019 (Annex 16) to include specific controls and reporting requirements. The requirements include:
  - Delivery and approval of a contractor's SSP
  - Specific controls such as multi-factor authentication, and annual audit of user privileges
  - Sharing information on cyber incidents with DoD within 15 days
  - Allowing NCIS "to install network sensors" on contractor information systems if intelligence indicates actual or potential vulnerability
  - Suspending or reducing payments for non-compliance

Expanding Implementation Enforcement

- DoD exhibiting frustration with pace of cyber security implementation
  - January 2019: Under Secretary (A&S) Memo regarding "Addressing Cybersecurity Oversight as part of a Contractor's Purchasing System Review" directs DCMA to audit prime contractor review of first tier subcontractor compliance with DFARs where requirements to protect DoD CUI have flowed down
  - February 2019: Undersecretary (A&S) Memo regarding "Strategically Implementing Cyber Security Contract Clauses" expresses frustration that the contract-by-contract approach to DFARs implementation is "inefficient" and "impedes effective implementation" of requirements to protect DoD's CUI. Directs DCMA to develop a strategy for no-cost bilateral block changes to: (i) require delivery of contractor's SSP; (ii) document industry cyber readiness at a strategic level; and (iii) apply a standard methodology to recognize cyber readiness at a strategic level

Expanding Implementation Enforcement, cont.

- November 2019: Under Secretary (A&S) Memo regarding "Assessing Contractor Implementation of Cybersecurity Requirements" references Feb. 5 assessment memo and describes 3 assessment levels. Memo states that DCMA and DCSA conducted a pilot in June 2019 and completed "High" assessments for DoD's largest contractors
- "The standard DoD-wide methodology for assessing DoD contractor implementation of the security requirements of NIST SP 800-171 will be implemented in the DFARS." Expected to use the three levels

Expanding Implementation Enforcement, cont.

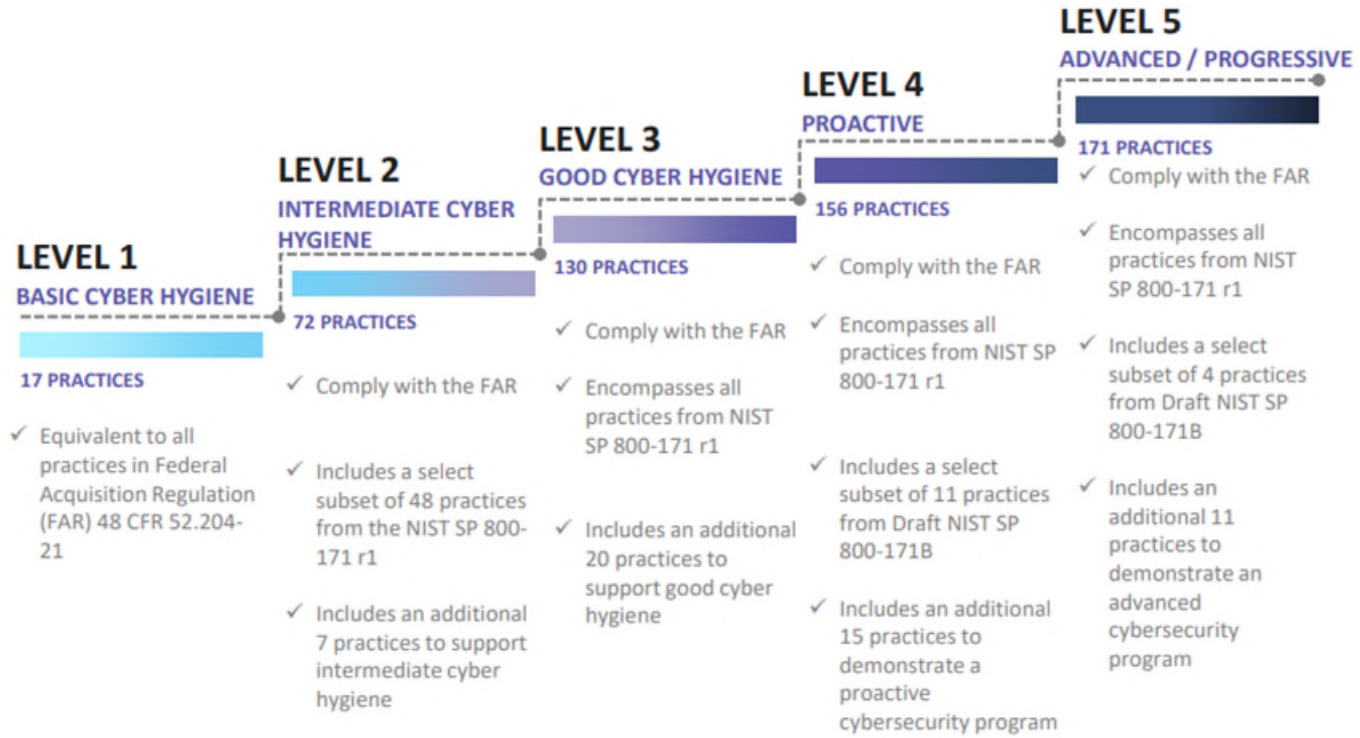
- Description of the three levels as follows:
  - Basic Assessment: Contractor self-assessment of SSP created according to NIST SP 800-171 – "low" confidence level in the score
  - Medium Assessment: DoD review of the SSP plus interviews, discussion and clarification with the contractor – "medium" confidence level in the score
  - High Assessment: DoD review of the SSP along with interviews, discussion, and contractor clarification, as well as an on-site validation of contractor implementation pursuant to SP 800-171A "Assessment Procedures for CUI" – "high" level of confidence in the score

Cybersecurity Maturity Model Certification (CMMC)

Overview of CMMC 1.0

- Jan. 30, 2020: DoD issued CMMC 1.0 to provide a unified cybersecurity standard for DoD contractors & suppliers across the entire DIB (300,000+ companies)
- Builds upon the FAR rule (protecting FCI) and DFARS rule (requiring contractors to maintain "adequate security" on all covered contractor info systems)
  - Incorporates a variety of standards, including NIST SP 800-171, NIST SP 800-171B, NIST SP 800-53, ISO 27001, ISO 27032, AIA NAS 993, CIS Critical Security Controls 7.1, and CERT Resilience Management Model®
- Establishes a scaled benchmark against which an organization's level of cyber preparedness can be assessed and certified across five levels of cyber "maturity," ranging from Level 1 ("Basic Cyber Hygiene" required to protect FCI) to Level 3 (the minimum level for companies that access or generate CUI) to Level 5 ("Advanced / Progressive")
- Certification to be performed not by the gov't but by CMMC Third-Party Assessment Organizations (C3PAOs), which first will be accredited and vetted by a C3PAO Accreditation Board (AB)

The Maturity Scale



Certification to be performed by C3PAOs

- An Accreditation Body (AB) – an independent, non-profit, industry-funded board composed of members of the DIB and cybersecurity community – apparently was created in mid-January 2020, and will be responsible for training and certifying candidate C3PAOs
  - The AB recently launched its website, available at cmmcab.org.
  - Board members include Ty Schieber (chairman), Akin Akinbosoye, Mark Berman, Wayne Boline, Jeff Dalton, Nicole Dean, Regan Edens, James Goepel, Chris Golden, Karlton D. Johnson, Richard H. Klodnicki, Tim Rudolph, Ben Tchoubineh, and John Weiler
- No details have been revealed about which companies will perform the certification, what the certification process will look like, how long it will take and at what cost, and whether contractors will be able to appeal in the event of a failed audit

Guidance from DoD Press Event re CMMC 1.0

- Certification requirement will apply to both procurement contracts as well as Other Transaction Agreements (OTAs), including suppliers and SBs across the DoD supply chain
- Certification, once obtained, will be for a three-year period, and the deadline for certification will be upon notice of awarding a contract. Failure to certify will bar a company from receiving the contract
- Expected that prime contractors will help suppliers and lower-tier contractors comply with the certification requirements, but left unaddressed any additional costs incurred by prime contractors for these accommodations
- The level of certification required (Levels 1-5) will depend on whether contract performance requires the contractor to use or generate sensitive information
- CMMC will ***not apply retroactively*** but will only apply to new contracts, and will be phased in over the next five years. Initially will be limited to roughly 10 "Pathfinder" programs, which will each affect approximately 150 contractors and subcontractors
  - RFIs for Pathfinders to be released c. June 2020; RFPs to be released c. Sept. 2020

Unanswered Questions

- Unclear how certification requirements will flow down to lower-tier suppliers, subcontractors or advisors
  - Will suppliers of COTS items be treated as part of the DIB for certification purposes? Will providers of professional services that regularly work with contractors be covered by the requirements?
- Unclear how certification levels could be disputed, or which levels would be required for a particular procurement
  - Requirements could well be challenged as unreasonable, overly broad or restricting competition
- Will it be possible to accredit 300,000+ companies—including an estimated 12-16,000 that handle CUI—in less than five years?
  - Will extensions be available if an accreditation or certification backlog makes it impossible to be certified on time?
  - Companies involved in the early stages of procurement certification could have competitive advantages over other companies waiting to be certified

CMMC Preparedness

- Conduct your own cyber risk assessment: Assess your maturity ranking and implement any potential remediation measures before the formal certification comes per the CMMC
  - Identify applicable legal and third-party obligations
  - Assess compliance with industry standards (e.g., Auto-ISAC, NIST, ISO, SAE, etc.)
  - Identify potentially material vulnerabilities and cyber-risk factors
  - Coordinate review with Audit, Compliance, IT, Legal, and other relevant departments; report to Board
- Maintain confidentiality and privilege: Ensure engagement by Legal and potentially outside counsel on the development of policy documents and the identification of potential cyber risks
  - Develop and follow internal information controls and communications protocols to protect privilege
  - Share information internally on a "need to know" basis

Section 889 - Supply Chain Impact

MAYER | BROWN

Interim Rules re Chinese Telecom Suppliers

- FY 2019 NDAA Section 889(a)(1)(A) prohibits agencies from procuring "any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system." Covered telecom components include components from Huawei, ZTE and several other companies connected to the Chinese government
  - Interim Rule (Aug. 2019) created a new FAR Subpart 4.21 and two new contract clauses: FAR 52.204-24 and 52.204-25 (both effective Aug. 13, 2019)
  - Additional Interim Rule (Dec. 2019) created FAR 52.204-26 (effective Dec. 13, 2019)
  - All three contract clauses apply to all contracts and TOs, including commercial items, below micro-purchase threshold, and COTS
- Requires prime contractors to take additional steps to certify suppliers (inaccurate certification poses risk of False Claims Act liability)
- Definition covers "any subsidiary or affiliate" but does not name them
  - Pursuant to Dec 2019 interim rule, these will be listed in SAM as "excluded parties"

Interim Rules re Chinese Telecom Suppliers (cont.)

- **FAR 52.204-24** – Contractors must submit a representation with their offer identifying whether the offer will include any "covered telecommunications equipment or services." If a contractor checks that it "will" do so, it must identify all such equipment or services and describe their proposed use under the contract
  - Representation must be made on offer-by-offer basis (but see FAR 52.204-26)
- **FAR 52.204-25** – Prohibits use of covered telecom equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless a waiver or exception applies
  - If contractor discovers such equipment / services, must report basic info *within 1 business day* and send follow up report *within 10 business days*
- **FAR 52.204-26** – offerors will be required to review excluded parties on SAM and certify annually whether each offer includes covered telecom equipment / services
  - If none of contractor's offerors include covered telecom equipment and services, can make ***blanket representation*** instead of separate representation for each offer.

Forthcoming Rule re Chinese Telecom Suppliers

- FY 2019 NDAA Section 889(a)(1)(B) prohibits agencies from "enter[ing] into a contract (or extend[ing] or renew[ing] a contract) with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of ***any*** system"
  - This provision will be effective Aug. 13, 2020.
  - No interim rule yet; a draft rule is still pending OIRA and OMG review. (FAR Case 2019-009)

Questions?

Americas | Asia | Europe | Middle East

mayerbrown.com