ISSUE THEME
SUBCONTRACT MANAGEMENT

CONTRACT MANAGEMENT

www.ncmahq.org
MAY 2024

Forget the drama, but remember that subcontracting is key to successful industry relationships – and to supporting the U.S. government's mission.

A STUDY IN CONTRAS(C)TS

NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION®
CONNECTING TO CREATE WHAT'S NEXT

COMPETENCIES A.1 B.5 B.6 1.4

THE MATURITY OF SUPPLY CHAIN SECURITY

The Impact of the Cybersecurity Maturity Model Certification on the Defense Industrial Base.

By Michael G. Gruden, Evan D. Wolff, Jennie Wang VonCannon, Maida Lerner, Jake Harrison, and Alexis Ward

The Department of Defense (DoD) faces a formidable challenge in safeguarding its supply chain against foreign threat actors that have effectively exploited vulnerabilities in Defense Industrial Base (DIB) information systems.

In the wake of the 2020 SolarWinds cyberattack and similar incidents, the DoD has intensified its focus on the security of contractors throughout its supply chain.

This article delves into the evolving landscape of the DoD's supply chain cybersecurity. It focuses particularly on the December 2023 Cybersecurity Maturity Model Certification (CMMC) Proposed Rule[1] (Proposed Rule) and the cascading impact it could have on subcontractors, cloud service providers, and other entities embedded in the DoD supply chain if finalized as proposed.

CMMC Background

CMMC is not the DoD's first foray into imposing requirements on contractors and subcontractors to safeguard its supply chain. Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012[2] (DFARS 7012), first introduced in 2013, requires contractors handling Controlled Unclassified Information (CUI) to implement the requirements of National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-171[3] and to flowdown DFARS 7012 requirements to subcontractors.

Over time, the DoD found that contractors and subcontractors were not consistently implementing the DFARS 7012 requirements, and that the risk of sensitive data loss remained.[4]

DFARS 7012 does not require the DoD to verify contractors' implementation of NIST SP 800-171 prior to contract award, so some contractors simply did not implement them. The DoD concluded that still more did not implement them in a manner sufficient to safeguard its supply chain.

In an effort to bolster compliance, the DoD announced the CMMC Program in 2019 and introduced both its initial version of CMMC (CMMC 1.0) and corresponding DFARS Clause 252.204-7021 (DFARS 7021) under an Interim Rule in September 2020.[5] CMMC 1.0 included five levels of CMMC certification based on maturity processes and cybersecurity controls.

The Interim Rule also included two clauses aimed at assessing contractor implementation of cybersecurity requirements, DFARS 252.204-7019 (DFARS 7019) and DFARS 252.204-2020 (DFARS 7020). Through DFARS 7019 and 7020, the DoD attempted to increase DFARS 7012 cybersecurity compliance through a combination of self-assessments and government-led assessments. Unlike DFARS 7021 (which remains dormant pending finalization of the CMMC requirements), DFARS 7019 and 7020 became effective shortly after the Interim Rule was published.

These two clauses represent a midpoint in the DoD's transition from requiring its supply chain to indicate compliance through clause acceptance (i.e. the DFARS 7012 model) to confirming compliance via documented assessments before contract award (i.e. the CMMC model).

In November 2021, the DoD announced "CMMC 2.0," which established a notional updated program structure with three key features: a three-tiered security model, pre-award assessment requirements, and implementation through contracts.[7] The December 2023 Proposed Rule contemplates a revamped CMMC 2.0 Program and defines requirements for the program and for each CMMC level.

FIGURE 1. Five-Level Model of CMMC

This is the previous five-level model of CMMC that has been updated by the Interim Rule.

Source: Department of Defense Chief Information Officer Website[6]

Recent Supply Chain Attacks

The DoD's concern over supply chain cybersecurity is well-warranted. In the past decade, threat actors have consistently targeted entities within the DoD supply chain. Many of the most damaging cyberattacks impacting the federal government, including the infamous 2020 Solar Winds attack, used the federal supply chain as a vector to penetrate federal government information systems.

A short summary of notable supply chain cyberattacks impacting the federal government follows.

- 2020 Solar Winds Cyberattack: In February 2020, Russian threat actors inserted malware into a software update that SolarWinds, a Texas-based IT management software company, rolled out to 18,000 customers including federal government entities and significant government contractors. Making matters worse, the malware was not detected for months allowing the threat actors to run amuck within infected networks and systems. This unfettered access may have allowed the threat actors to compromise entities that did not use any SolarWinds products but were connected to SolarWinds' users through the supply chain.
- 2021 Microsoft Exchange Cyber Attack: In March 2021, Microsoft reported that threat actors had

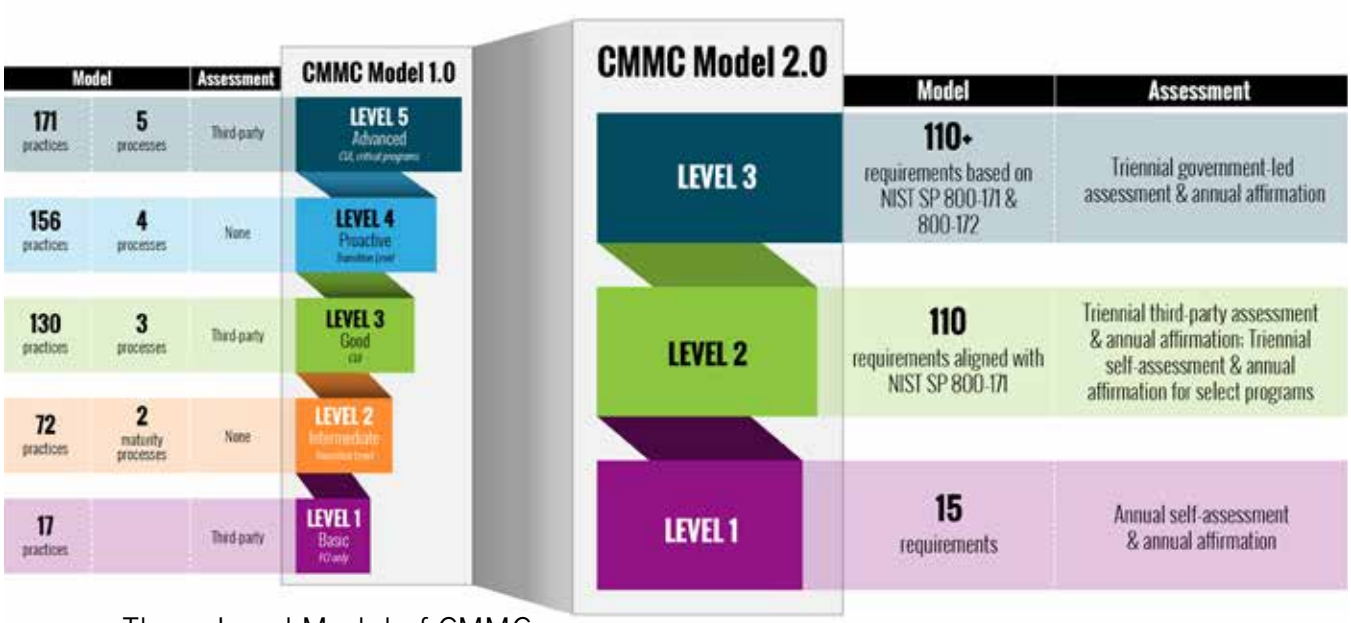

FIGURE 2. Three-Level Model of CMMC

This is a comparison chart between CMMC Models 1.0 and the planned CMMC Model 2.0. Please note that the CMMC Model 2.0 is notional until rulemaking is completed.

Source: Department of Defense Chief Information Officer Website[8]

exploited vulnerabilities to gain access to several versions of Microsoft Exchange Server, including versions used by federal agencies. The vulnerabilities initially allowed threat actors to make authenticated connections to Microsoft Exchange Servers from unauthorized external sources. Once the threat actor made a connection, they were able to take advantage of other vulnerabilities to install web shells that enabled the actors to remotely access a Microsoft Exchange Server, allowing them to continue malicious activities even after the initial vulnerabilities were patched.

CMMC Supply Chain Broad Applicability

As a result of the endless supply chain cyber threats, it is no surprise that CMMC is expected to be the most far-reaching cybersecurity regulation released by the DoD. It estimates more than 200,000 companies within its scope, virtually all contractors and subcontractors that handle Federal Contract Information (FCI) and/or Controlled Unclassified Information (CUI) under a DoD contract.[9]

The Proposed Rule states that CMMC requirements will be included in all DoD solicitations valued above the micro-purchase threshold, except for procurements that are exclusively for commercially available off-the-shelf (COTS) items. CMMC requirements, however, are not applicable under the Proposed Rule to government information systems operated by contractors or subcontractors "on behalf of" the government (i.e. "Federal Information Systems").

The Proposed Rule defines FCI as "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 that on public web sites) or simple transactional information, such as that necessary to process payments."

Examples of FCI include information generated or produced as part of contract performance, such as company and government communication or contract deliverables.

The Proposed Rule defines CUI in accordance with 32 CFR § 2002.4(h) as "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls."

CUI covers many categories of unclassified regulated data handled during contract performance, including Controlled Technical Information (CTI), Export Controlled Information, Protected Critical Infrastructure Information (PCII), and

Elevating the Federal Procurement Experience:

The Journey to Smart Business Buying

Sponsored by Amazon Business

In the digital age, especially for federal procurement leaders, the expectation of Amazon-level customer experience isn't just a lavish ideal; it's becoming the benchmark against which all B2B solutions are measured. This shifts the paradigm drastically, forcing procurement leaders to consider not just cost, but nuanced elements that directly affect the efficiency and satisfaction of the end user's smart business buying journey.

Redefining Customer Experience in Federal Procurement

The term 'customer experience' often conjures images of smiling retail consumers swiping through mobile apps or strolling through flagship stores. However, the essence of customer experience transcends B2C sectors—it's a universal concept. This is particularly true in the realm of federal procurement, where the 'customer' can range from a soldier on a base to a doctor in a military hospital, each expecting the reliability and seamlessness commonly associated with e-commerce giants.

Customer experience within federal procurement now integrates entire operational cycles, from the intuitive browsing of an expansive product catalog to the precise fulfillment and delivery of each item. With Amazon Business, the promise is not just cutting costs and saving time; it's about transforming service quality and operational effectiveness.

Government bodies operate on a large-scale and require efficient, robust systems that can handle complex purchasing dynamics while ensuring compliance and security. Amazon Business understands that these institutions don't just need a vendor; they need a strategic partner.

The Pivotal Role of E-Procurement in Government Bodies

The landscape of federal procurement is evolving at an unprecedented pace. The shift to e-procurement is not merely a trend; it's a seismic transformation. E-procurement systems have the power to streamline processes, enforce compliance, and offer a level of visibility and data analysis that far surpasses what traditional methods can provide.

However, adopting an e-procurement model is only the first step. The selection of a partner in this arena is what elevates this process and turns it into a mission-critical asset. Amazon Business stands as a beacon here, with capabilities that stretch beyond the transac

tional realm, woven into the very fabric of the government's buying strategy.

Managing Spend, Not Just Tail Spend

In the past, the focus of procurement reforms often centered on reducing 'tail spend'—those small, fragmented purchases that can elude visibility and control. However, Amazon Business expands this scope, aiming to manage the entirety of the government's spend. By consolidating purchasing under one system, the management of spend becomes comprehensive, enabling greater leverage in negotiating contracts and reducing overall costs.

Modernizing Legacy Processes

Legacy processes in federal procurement can be encumbered by paperwork, chain-of-command delays, and outdated cataloging systems. Amazon Business steps in with a suite of tools designed to modernize these processes, from detailed Spend Analysis, custom Approval Workflows, reconciliation, and more. This modernization isn't just about technology; it's an enabler that liberates resources to focus on strategic decision-making.

The Power of Built-In Tools

The true value of Amazon Business as a partner to the federal government lies in its arsenal of built-in tools. These tools enable teams to define guardrails and adhere to strict budget restrictions, all while providing dashboards and analytics that forecast trends and highlight opportunities for greater efficiency.

The Journey to Smart Business Buying

The evolution of smart business buying requires federal procurement leaders to embrace a strategic approach that transcends mere transactions, aiming for an intelligent, responsive purchasing environment in-sync with fiscal and operational objectives. Aligning with e-procurement partners capable of supporting diverse goals such as responsible purchasing and economic growth, these partnerships are vital in adapting procurement processes to the fast-paced global market. Such collaborations ensure procurement is not only agile but also ethical, aligning with Corporate Social Responsibility principles. By engaging with leading-edge partners, federal procurement departments can achieve excellence in customer experience and strategic innovation, marking a significant step towards future-proofing procurement practices and enhancing national welfare.

Leveraging Amazon Business for Federal Acquisition

The call-to-action for federal procurement leaders is clear—It's time to take a strategic approach to procurement, and Amazon Business stands ready to assist agencies of all sizes at every step of the way. The future of federal acquisition rests in the hands of those willing to innovate, and the tools and features provided by Amazon Business pave the way for a new era of efficiency and foresight.

amazon business

Visit business.amazon.com/government to learn more about smart business buying solutions.

Personally Identifiable Information (PII). The DoD maintains a full list of CUI categories at the DoD CUI Registry.[10]

CMMC Levels and Assessment Types

The Proposed Rule sets forth a three-tiered CMMC model. The DoD will determine the applicable CMMC Level for each procurement in the solicitation documents. The Proposed Rule and the corresponding guidance documents confirm that CMMC will incorporate three assessment types first proposed in the November 2021 CMMC 2.0 draft: Self-Assessments, Certified Third-Party Assessment Organization (C3PAO) Assessments, and Government-Led Assessments.

Contractors and subcontractors must have the requisite CMMC assessment score entered into the DoD's Supplier Performance Risk System (SPRS) portal before they are eligible for contract award under solicitations requiring CMMC.

Uploading a passing CMMC Level 1 or Level 2 Self-Assessment to SPRS confers CMMC "compliance" status. Submission of a passing C3PAO or Government-Led Assessment to SPRS also confers CMMC "certification." For this reason, the Proposed Rule frequently refers to C3PAO and Government-Led Assessments as "certification assessments."

- CMMC Level 1 includes 15 requirements listed in Federal Acquisition Regulation (FAR) clause 52.204-21(b)(1) and is expected to apply to contractors and subcontractors that store, process, or transmit FCI. All entities subject to CMMC Level 1 will be required to submit an annual Self-Assessment confirming their compliance.
- CMMC Level 2 includes 110 requirements from the NIST SP 800-171, Rev. 2 and is expected to apply broadly to contractors and subcontractors that store, process, or transmit Controlled Unclassified Information (CUI). While a small number of entities subject to Level 2 will be permitted to self-assess, the vast majority will need to engage a C3PAO to conduct an outside assessment evaluating their compliance with NIST SP 800-171. Regardless of whether a Self-Assessment or a C3PAO Assessment is required, Level 2 assessments must be performed every three years.
- CMMC Level 3 is derived from 24 select requirements from NIST SP 800-172 and is expected to apply to a small group of DoD contractors and subcontractors that store, process, or transmit high-value CUI. At Level 3, only Government-Led Assessments performed by the DoD's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) will be permitted. CMMC Level 2 certification (and, accordingly, a C3PAO assessment confirming compliance with NIST SP 800-171) is required before contractors or subcontractors can seek Level 3 certification. Like Level 2 assessments, Level 3 assessments must be re-performed every three years following the initial assessment.

Plan of Action and Milestone Approvals

CMMC requires that any security control not met is recorded by a Plan of Action and Milestone (POA&M) document detailing how, and by when, the contractor will fully implement any pending controls. However, how many and what kind of POA&Ms are allowed depends on the applicable CMMC Level. For example, CMMC Level 1 does not allow for any POA&Ms, but Level 2 and Level 3 permit POA&Ms for some controls under certain conditions.

Contractors with any open POA&Ms can receive only a conditional certification or compliance status.[11] POA&Ms must be closed out within 180 days, confirmed by a closeout assessment, or the contractor will lose its conditional status or certification.

These POA&M nuances are important for contractors to consider regarding their supply chain risk management because a subcontractor could attest compliance with CMMC while possessing only conditional certification that could expire if POA&Ms are not remediated and closed within the required time frame.

CMMC Senior Official Affirmations

In addition to detailing the assessment process, the Proposed Rule includes an obligation for contractors and subcontractors to affirm their ongoing compliance with CMMC requirements. Specifically, a senior official from the prime contractor, as well as any subcontractor subject to CMMC, will be required to affirm compliance with their CMMC Self-Assessment or Certification Assessment upon:

- Completion of any CMMC assessment
- Annually after achieving any CMMC Level compliance status or certification
- Following a POA&M closeout

assessment (if applicable)[12]

Like assessment scores, the affirmation must be submitted electronically via Supplier Performance Risk System (SPRS).[13] Contractors will not be eligible for award under a contract requiring CMMC until they have achieved the requisite CMMC compliance status or certification *and* uploaded their affirmation to SPRS.

CMMC Flowdown Requirements

CMMC includes flowdown requirements in an effort to safeguard the DoD supply chain. Flowdown requirements are contract terms that require the prime contractor to include the same or similar requirements that they must comply with in any contract with a subcontractor.

Specifically, CMMC's flowdown provisions require the higher-tier contractor to ensure that all its subcontractors that process, store, or transmit FCI or CUI comply with the applicable CMMC Level. The CMMC Level that the subcontractor will have to adopt will depend on what information – FCI or CUI – the subcontractor handles.

With regard to cloud service providers, the Proposed Rule confirms that contractors subject to CMMC Levels 2 or 3 will be permitted to store, process, or transmit CUI in cloud environments if the contractor has evidence that the cloud environment is FedRAMP Moderate/High-authorized or meets FedRAMP Moderate/High-equivalent security controls.

Supply Chain Risk Management

Because CMMC makes clear that prime contractors will be responsible for the compliance of their subcontractors, prime contractors must have a thorough understanding of both CMMC requirements and their supply chain. If a contractor knows its subcontractors are not complying, or cannot comply, with CMMC requirements but are still handling the contractor's CUI or FCI, the contractor will be at significant risk.

Therefore, contractors will need to analyze their supply chain to assess compliance and implement any necessary safeguards or mitigation techniques to manage compliance gaps. The first step in this supply chain cyber analysis is to determine which portions of their data that will be handled by subcontractors constitute FCI or CUI requirements.

After understanding the categories of regulated data handled, contractors will need to review the contract requirements associated with their subcontractors. Because they are responsible for compliance of the entire supply chain, prime contractors and higher-tiered subcontractors that also have lower-tiered subcontractors handling FCI or CUI should independently determine subcontractor CMMC compliance capability.

If the contractor determines the lower-tiered subcontractor is not complying, or cannot comply, with the CMMC flowdown requirements, the contractor should determine if the potentially non-compliant subcontractor is critical to completion of the contract.

If the non-compliant subcontractor is critical to the contract, the contractor will need to consider workarounds that keep its FCI and CUI safeguarded. These workarounds could include keeping the FCI and CUI out of the subcontractors' networks by not sharing the protected information or requiring the subcontractor to access protected information only from the contractor's networks.

Other mitigation strategies may include requiring the subcontractor to use government-furnished equipment or information systems to handle the protected information or limiting access to physical forms. Each of these workarounds should be documented and, as appropriate, included in contractual agreements between the contractor and subcontractors.

CMMC Supply Chain Compliance (Enforcement) Risks

What can happen if the CMMC 2.0 rules are not followed? The good news is that government contractors are already well-versed in the importance of complying with government contracting rules, regulations, and best practices. CMMC 2.0 creates a few more dimensions to compliance risk that those in the supply chain should be aware of.

The mechanism by which the U.S. government has chosen to enforce the cybersecurity rules that apply to government contractors is the Civil Cyber-Fraud Initiative.

Launched in October 2021, this Department of Justice (DOJ) initiative seeks to combat cyber threats by leveraging the False Claims Act (FCA) to civilly prosecute government contractors who put U.S. information or systems at risk by *knowingly*:

1. Providing deficient cybersecurity products or services.
2. Misrepresenting cybersecurity practices or protocols.
3. Violating obligations to monitor and report cybersecurity incidents and breaches.

Of course, the key word is *knowingly*, which is:

1. Having actual knowledge of the information.
2. Acting in deliberate ignorance of the truth or falsity of the information.
3. Acting with reckless disregard of the truth of the claim.

CMMC 2.0 leverages a robust certification process to enable the government to establish knowing conduct when it comes to cyber enforcement. In order to find a government contractor liable under the FCA, the government must establish some intent or knowledge of wrongdoing based on the defendant's knowledge and subjective beliefs at the time the claim or statement was made.[14]

Three areas of CMMC cybersecurity that are prime for enforcement are: the failure to meet specific contract terms, misrepresentation of the company's cybersecurity controls and practices, and failure to timely report suspected breaches.

FCA liability may potentially attach to each of the certifications required under CMMC 2.0. Because a senior official must attest continuing compliance for each CMMC level — annually and also after every CMMC assessment for Levels 2 and 3 — the number of potential vectors of liability has grown exponentially. This can come in two forms: express or implied certification.

When a government contractor expressly certifies compliance with a required contract provision, statute, regulation, or governmental program in connection with a claim, they can potentially face FCA penalties where such certification is false or made with reckless disregard of the truth.

Potential predicates for liability include CMMC status revocation, inaccurate Self-Assessments, failure to provide C3PAO or the government with accurate information for Certification Assessments, and failure to close out POA&Ms within 180 days.

Under the implied certification theory, a government contractor's failure to disclose material facts or update the certification to reflect changed circumstances may, depending on the circumstances, also give rise to FCA liability.

The consequences for being found liable under the FCA for false claims can be significant damages awards or settlement amounts. The damages include not only the monetary loss of the benefit the government received under the contract less the amount paid, but also treble or multiplied damages to compensate the government for the costs, delays, and inconveniences caused by the fraudulent claims; per-claim penalties; and attorneys' fees.

An individual or company found liable under the FCA may also face suspension and debarment.

To date, the DOJ has announced four cyber-related FCA settlements that may indicate potential liability in the case of CMMC non-compliance. The first was in March 2022, when a contractor paid $930,000 to resolve allegations that it falsely represented compliance with contract requirements relating to the secure storage of medical records.[15]

In July 2022, a federal contractor settled with the government for $9 million to resolve claims that it failed to comply with *DFARS* and NFARS contract clauses, which included certifying compliance with 110 NIST cybersecurity controls.[16]

In March 2023, a company agreed to a $300,000 settlement after being accused of failing to properly maintain, patch, and update the software systems underlying a federally funded website.[17]

Finally, in September 2023, the DOJ settled with a telecommunications services government contractor for $4 million after it self-disclosed that the services it provided to federal agencies under its GSA contracts did not comply with applicable cybersecurity requirements.[18]

Supply chain contractors should be aware that each affirmation made regarding their cybersecurity protocols under CMMC carries with it not only the requirement that such certifications are true and accurate, but also that they should be updated to reflect any changed circumstances that render them untrue or inaccurate.

The DOJ has made it very clear that it will wield the mighty sword of the FCA to ensure cybersecurity but also that it will look favorably upon contractors that are transparent in a timely manner where there may be deficiencies.

Five Recommendations for DoD Contractors and Subcontractors

While CMMC is not in effect (yet), DoD contractors, subcontractors, and other entities involved in the DoD supply chain should act now to evaluate their potential obligations under CMMC.

Here are five steps firms in the DoD supply chain may consider to prepare for CMMC's implementation.

1. Analyze contracts and identify types of information that you are currently handling (e.g., FCI or CUI).
2. Analyze your position within the

supply chain. Identify types of information that you receive from higher-tier contractors or will need to flowdown to subcontractors under DoD contracts.

3. Review your company's CMMC technical documentation (System Security Plan (SSP)), including conducting a privilege compliance assessment, if needed, and consider developing an enterprise-wide compliance strategy working with technical, compliance and legal team members, and external parties including, as appropriate, C3PAOs, technical consultants, and outside law firms.
4. Complete a supply chain risk management analysis in which your company's critical suppliers are identified, compliance is evaluated, and mitigation strategies are devised depending upon levels of compliance.
5. Enhance and/or develop internal corporate policies relating to supply chain cyber risk management, technical compliance, administrative controls, and data sharing.

While the Defense Industrial Base (DIB) supply chain will likely remain a target of nation state threat actors, and, in turn the DoD, contractors that implement sound supply chain cyber risk-management practices now should be better positioned to receive government contracts once the DoD finalizes CMMC in the near future. CM

Michael G. Gruden, a counsel at Crowell & Moring LLP's Washington, D.C. office, is a former Pentagon information technology acquisition branch chief and a leading cybersecurity lawyer who helps government contractors navigate privacy, cybersecurity, and contract compliance requirements. Drawing from his experience at the U.S. Department of Defense and U.S. Department of Homeland Security, Gruden represents some of the nation's largest defense contractors and tech companies as they prepare to meet CMMC requirements and mitigate cyber threats. He can be reached at mgruden@crowell.com.

Evan D. Wolff is a partner in Crowell & Moring›s Washington, D.C. office where he helps lead the Privacy & Cybersecurity practice. With a national reputation for his deep technical background and understanding of complex cybersecurity legal and policy issues, Wolff represents numerous critical infrastructure companies, trade organizations and the nation's largest defense contractors. He can be reached at ewolff@crowell.com.

Jennie Wang VonCannon is a trial lawyer and advisor with a proven track record of success in both the courtroom and the boardroom – with extensive experience and deep understanding of corporate defense in both criminal and civil contexts, cybersecurity, and intellectual property matters. She served for more than 11 years as a federal prosecutor culminating in her selection to serve with distinction as the Deputy Chief of the Cyber and Intellectual Property Crimes Section of the National Security Division of the U.S. Attorney's Office for the Central District of California. She can be reached at jvoncannon@crowell.com.

Maida Lerner is senior counsel in Crowell & Moring's Washington, D.C. office and part of the firm's Cybersecurity & Privacy and Government Contracts Groups. She advises clients across a variety of sectors including government contracts, pipeline, transportation, health care, and manufacturing, in the areas of cybersecurity and privacy compliance. She can be reached at mlerner@crowell.com.

Jake Harrison is an associate in Crowell & Moring's Washington, D.C. office. He counsels government contractors on compliance and regulatory issues, with a focus on cybersecurity and data privacy compliance. He can be reached at jharrison@crowell.com.

Alexis Ward is an associate in Crowell & Moring's Los Angeles office, where she is a member of the privacy and cybersecurity and government contracts groups. She can be reached at award@crowell.com.

ENDNOTES

1 https://www.defense.gov/News/Releases/Release/Article/3626384/cybersecurity-maturity-model-certification-program-proposed-rule-published/
2 https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
3 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
4 https://media.defense.gov/2023/Dec/04/2003351370/-1/-1/1/DODIG-2024-031%20SECURE.PDF
5 https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of
6 https://dodcio.defense.gov/CMMC/About/
7 https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/
8 https://dodcio.defense.gov/CMMC/About/
9 https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program Table 3 - Estimated Number of Entities by Type and Level
10 https://www.dodcui.mil/CUI-Registry-New/
11 Conditional Certification Assessment and Conditional Self-Assessments are awarded when, upon completion of an assessment, there are open POA&Ms but the POA&Ms and remaining security controls meet all CMMC requirements.
12 POA&M closeout assessments are only required if the organization has submitted a POA&M.
13 Supplier Performance Risk System (SPRS) is defined per DoDI 5000.79 as the "authoritative source to retrieve supplier and product PI [performance information] assessments for the DoD [Department of Defense] acquisition community to use in identifying, assessing, and monitoring unclassified performance."
14 *Schutte v. Supervalu*, --- U.S. ---, No. 21-1326 (Jun. 1, 2023) (available at https://www.supremecourt.gov/opinions/22pdf/21-1326_6jfl.pdf; last visited February 22, 2024).
15 https://www.justice.gov/opa/pr/medical-services-contractor-pays-930000-settle-false-claims-act-allegations-relating-medical
16 https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity
17 https://www.justice.gov/opa/pr/jelly-bean-communications-design-and-its-manager-settle-false-claims-act-liability
18 https://www.justice.gov/opa/pr/cooperating-federal-contractor-resolves-liability-alleged-false-claims-caused-failure-fully

This article appeared in the May 2024 issue of Contract Management magazine, published by the National Contract Management Association. Used with permission.