CONTRACTORS ENTER NEW ERA OF INFORMATION SECURITY COMPLIANCE

by Christoper Bouquet and Mark Martins[1]

Recent changes to the regulations and procedures governing the security of certain unclassified contractor information systems have ushered in a new era for U.S. federal government contractors. In particular, a new version of a Defense Federal Acquisition Regulation Supplement ("DFARS") clause, effective November 10, 2025, began the implementation of a phased roll-out of the most fully developed cyber- and information security regulations protective of controlled unclassified information ever imposed on contractors. In addition, on January 5th, 2026, the General Services Administration ("GSA") issued a new "IT Security Procedural Guide" that will govern information security on certain GSA contracts that require processing, storage or transmission of such information or security protection for such transactions.

"[T]he new requirements, when fully implemented, will focus on contractor submissions of third-party certifications of their compliance and involve extensive government oversight."

The impacts are being felt not only by virtually all defense contractors, but also by any company desiring to do business with the Department of Defense ("DoD") or with its prime contractors, as well as with other agencies or primes whose information systems can be expected, as a result of such business, to traffic in some amount of official U.S. government information. Correspondingly, the changes brought by this new era have posed novel challenges for legal, contract management, and information technology professionals supporting contractor compliance programs.

While previous requirements focused on contractor attestations of compliance and involved modest government oversight, the new requirements, when fully implemented, will focus on contractor submissions of third-party certifications of their compliance and involve extensive government oversight. Third party certifications of compliance will also increasingly be a condition for award of government contracts. Further, these changes are occurring in the midst of the Trump Administration's "revolutionary" overhaul to the Federal Acquisition Regulation ("FAR"), which has to some extent "shuffled the deck" of the government-wide provisions and clauses applicable to information security. As a result, contractors and compliance professionals are now engaged in extensive learning processes concerning the new era and encountering a host of small and large practical challenges. To support these processes and assist with these challenges, this article provides the context and contours of the new era and a few "takeaways."

[1] This article was jointly authored by Christopher C. Bouquet, Esq., of the Law Office of Christopher C. Bouquet, PLLC, and Mark Martins, Esq., of the Mark Martins Law Office, PLLC, whose law practices include advising government contract clients on information security and other compliance matters.

Context

The recent regulatory changes are part of the government's ongoing response to a series of infamous and lesser known but harmful cyber-attacks on contractor information systems.[2] For example, in February 2020, the Russian Foreign Intelligence Service ("Russian FIS") targeted SolarWinds Corporation ("SolarWinds"), a major US network management software company and a contractor to numerous U.S. government agencies.[3]

The well-publicized SolarWinds intrusion is referred to as a "supply chain" attack because the Russian FIS did not target the agency networks directly.[4] Rather, the Russian FIS injected trojanized (hidden) code into a file that was later included in SolarWinds' Orion software updates. SolarWinds then unwittingly released the compromised updates to its federal customers. The trojanized code provided the Russian FIS with a "backdoor"— i.e., a program that can give an intruder remote access to an infected computer. Using a sophisticated computing infrastructure, the Russian FIS was then able to remotely exploit the networks and systems of SolarWinds' customers who had downloaded the compromised updates.[5]

"While the SolarWinds case is a notable example of a supply chain related attack, contractor information systems are vulnerable to numerous other types of attacks, including phishing, malware, malvertising, and 'man-in-the-middle' attacks."

While the SolarWinds case is a notable example of a supply chain related attack, contractor information systems are vulnerable to numerous other types of attacks, including phishing, malware, malvertising, and "man-in-the-middle" attacks.[6] Since all of these attacks can lead to the theft of

[2] An oft-cited data point regarding the financial costs of cyberattacks is an estimate by the U.S. Council of Economic advisors that malicious cyberattacks cost the U.S. economy between $57 billion and $109 billion in 2016 alone, projecting a decade-long burden of between $570 billion to $1.09 trillion. Dep't of Defense, *Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements* at FR 61505, Sept 29, 2020 [DFARS Case 2019-D041]. Of course, the threat is not merely financial, but also increasingly physical. *See also* National Sanitation Foundation (NSF), *Identifying and Protecting Controlled Unclassified Information (CUI)* (Nov. 8, 2021), *available at* https://www.nsf.org/in/en/knowledge-library/protect-controlled-unclassified-information (accessed Mar. 4, 2026) (providing a still-pertinent historical overview of the trend of cyberattacks between 2009 and 2021 and related factors that shaped the U.S. government's efforts to improve and standardize information security).

[3] *Id.* (citing also serious cybersecurity attacks between 2008 and 2021 at the National Archives and Record Administration, Tricare Health Systems, the U.S. Office of Personnel Management, Uber, the Democratic National Committee, Equifax, Marriott, U.S. Customs and Border Protection, and Colonial Pipeline as the largest and most publicized data breaches and estimating that thousands of other cyberattacks went unreported).

[4] Unless otherwise cited, details from this paragraph are from Fortinet, Inc., *SolarWinds Cyber Attack: An Overvie*w (2025), *available at* https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack (accessed Mar. 4, 2026).

[5] U.S. Government Accountability Office, *SolarWinds Cyberattack Demands Significant Federal and Private Sector Response* (Apr. 22, 2021) *available at* https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic (accessed Mar. 4, 2026).

[6] U.S. Congressional Research Service, CRS Product No. R46974, *Cybersecurity: Selected Cyberattacks 2012-2024* (Jan. 8, 2025), *available at* https://www.congress.gov/crs-product/R46974 (accessed Mar. 4, 2026) (tabulating 45 major cyberattacks by type and indicating state sponsor, if known).

sensitive government information, the government is urgently concerned about and has promulgated extensive regulations and other guidance governing contractor information security.

For purposes of this article, the regulations fall into the following categories: (i) general requirements; (ii) requirements applicable to systems that process classified information; and (iii) requirements applicable to systems that process unclassified information. The general requirements of category (i) are set forth in the Federal Acquisition Regulation ("FAR") and consist of certain basic information security requirements and various prohibitions on the use in contractor systems of equipment manufactured by entities affiliated with foreign adversaries of the United States.[7]

"The . . . regulations at 32 CFR Part 2002, Controlled Unclassified Information ("CUI"), set forth executive branch requirements concerning control of CUI—i.e., unclassified information that "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."

The category (ii) regulations at 32 CFR Part 117, the National Industrial Security Program Operating Manual ("NISPOM"), govern the security of contractor systems that process "classified national security information," or just "classified information" for short—i.e., information that requires protection against unauthorized disclosure in the interest of national security and which has been so designated in accordance with applicable law and regulation.[8] A FAR clause implements these regulations in contracts requiring handling of such information,[9] which is protected by longstanding procedures, institutions, investigative mechanisms, marking protocols, physical security and facilities safeguards, dedicated official positions, and regulations. Although not strictly part of the new

[7] *See, e.g.,* 48 C.F.R. § 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems), § 52.204-23 (Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities, § 52.204-25 (Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment), § 52.204-27 (Prohibition on a ByteDance Covered Application), § 52.204-30 (Federal Acquisition Supply Chain Security Act Orders—Prohibition). Note that under the FAR Overhaul, the foregoing supply chain security clauses have been moved via issuance of deviation by the Defense Department and other agencies. FAR clause 52.204-21 is renumbered to 52.240-93, and the prescriptive provision directing use of the clause moved from Part 4 (Administrative Matters) to Part 40 (Information Security and Supply Chain Security), in section 40.303-2. FAR clauses 52.204-25, 25, -27, and -30 have been consolidated within a new clause 52.240-91 (Security Prohibitions and Exclusions), with the prescriptive provision also consolidated and moved to Part 40, in section 40.205(b). *See* FAR Part Deviation Guidance for Parts 52 and 40 at https://www.acquisition.gov/far-overhaul/far-part-deviation-guide/far-overhaul-part-52 and https://www.acquisition.gov/far-overhaul/far-part-deviation-guide/far-overhaul-part-40.

[8] 32 C.F.R. § 117.3. The NISPOM implements within private industry Executive Order 13526, *Classified National Security Information* (Dec. 29, 2009), as well as 32 C.F.R. Part 2004—National Industrial Security Program (NISP).

[9] *See* 48 C.F.R. § 52.204-2 (Security Requirements). Under the FAR Overhaul, this clause is renumbered to 52.240-92, and the prescriptive provision directing use of the clause moved from Part 4 (Administrative Matters) to Part 40 (Information Security and Supply Chain Security), in section 40.302-3. *See supra* note 7.

era focused upon in this article, the protection of classified information and the NISPOM do, on occasion, provide a model that may be relied upon by government officials seeking to protect other types of information.

The category (iii) regulations at 32 CFR Part 2002, Controlled Unclassified Information ("CUI"), set forth executive branch requirements concerning control of CUI—i.e., unclassified information that "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."[10] A large and growing body of U.S. National Archives and Records Administration (NARA),[11] National Institute of Standards and Technology (NIST),[12] GSA,[13] and DoD issuances implement these CUI safeguarding and dissemination controls.[14]

"A new version of a DFARS clause . . . implements a phased roll-out of the most fully developed cyber- and information security regulations protective of CUI . . . , thus marking the dawn of the new era . . . ."

Among the most important of these within the DoD are now the further category (iii) regulations at 32 CFR Part 170, Cybersecurity Maturity Model Certification ("CMMC") Program, which require that in certain circumstances contractors obtain

[10] 32 C.F.R. § 2002.4(h).

[11] NARA is the CUI Executive Agent across the U.S. federal government, having been directed by the President to implement Executive Order 13556, Controlled Unclassified Information (Nov. 4, 2010) and to oversee efforts to comply with EO 13556 in the different departments and agencies. Among other things, NARA convenes and chairs a CUI Advisory Council to address matters pertaining to the CUI Program and also approves categories and subcategories of CUI as needed and publishes them in a CUI Registry. 32 C.F.R. § 2002.8(a).

[12] Under EO 13556, NIST was assigned responsibility for issuing government-wide standards for implementing the Order and thus protecting CUI. Consistent with their missions and statutory authorities, neither NARA nor NIST has inherent regulatory authority over separate agencies, and both EO 13556 and 32 C.F.R. Part 2002 preserve most separate agency authority, including the prerogative of each Agency head to approve that Agency's CUI policies for implementing the government CUI program. 32 C.F.R. § 2002.8(b). This is why complete uniformity in protections for non-classified information across the government is likely unattainable, and also would be appropriate, in light of the many different lawful purposes departments and agencies are carrying out. That said, the separate agencies are subject to NARA's actions as the designated Executive Agent and may not develop independent standards that subvert those developed by NIST. Increased standardization and adoption of best practices is indeed underway.

[13] Although there remain differences in the implementation of CUI protections across agencies, increasing commonalities are emerging. These are reflected in U.S. General Services Administration (GSA), Office of the Chief Information Security Officer, CIO-IT Security-21-112, *IT Security Procedural Guide: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Process*, Revision 1 (Jan. 5, 2026) ("GSA IT Guide'), which now governs information technology (IT) system and information security protections in the sprawling, 12,000-person strong GSA, sets requirements for the many contractors that do business with the GSA, and thereby incorporates many best practices across the federal government. One of these best practices is assessment by an outside entity, i.e., a third-party assessor organization.

[14] An established CUI-implementing regulatory mechanism is DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, which requires contractors to provide "adequate security" on all "covered contractor information systems," and specifies a minimum set of information security protections that are necessarily part of any system of adequate security. The apparatus established under this clause forms, within the DoD, the self-assessment paradigm now being supplemented by a third-party assessment paradigm and body of regulations.

third-party assessments and certifications of compliance with specified requirements applicable to both CUI and a broader category of unclassified information referred to as "federal contract information" or "FCI".[15] The regulations define 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."[16]

A new version of a DFARS clause, effective November 10, 2025 and yet another category (iii) regulation, implements a phased roll-out of the most fully developed cyber- and information security regulations protective of CUI and FCI, thus marking the dawn of the new era discussed in this article.[17]

See Appendix A for details concerning the major requirements in each category of information and security regulations, as well as notes concerning changes made in the revolutionary FAR overhaul.

Contours of the New Era

This new era of information security regulation and compliance has markedly different contours from the past, but these contours are implemented using traditional regulatory and procedural means and are intended to carry out understandable government policy goals.

DFARS Changes Implementing the CMMC Program

The CMMC Program (the "Program"), in development for several years[18] and now prescribed in regulations and being implemented, has the following eight stated ***purposes***:[19]

1	Establish requirements for defense contractors and subcontractors to implement prescribed cybersecurity standards for safeguarding FCI and CUI.
2	Establish requirements for conducting assessments of compliance with the applicable prescribed cybersecurity standard for contractor information systems that: ○ process, store, or transmit FCI or CUI; ○ provide security protections for systems which process, store, or transmit CUI; ○ or are not logically or physically isolated from systems which process, store, or transmit CUI.

[15] 32 C.F.R. § 170.9.

[16] 32 C.F.R. § 170.4 (incorporating by reference the definition at 48 C.F.R. § 4.1901).

[17] 48 C.F.R. § 252.204-7021 (Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements).

[18] *See, e.g.,* DFARS Case 2019-D041, *supra* note 2, at FR 61505-61506 (providing the background for why DoD developed the CMMC Program and noting that the framework was intended to build upon the CUI protection standards being implemented across the federal government generally but also to "*add*[] *a comprehensive and scalable certification element to verify* the implementation of processes and practices associated with the *achievement of a cybersecurity maturity level*." *Id.* at FR 61505 (emphasis added).

[19] The numbered items in this paragraph digest the purpose statement at 32 C.F.R. § 170.1.

3	Provide DoD with a viable means of conducting the volume of assessments necessary to verify contractor and subcontractor implementation of required cybersecurity requirements.
4	Ensure defense contractors are properly safeguarding FCI and CUI that is processed, stored, or transmitted on defense contractor information systems, mindful that FCI and CUI must be protected to meet evolving threats and to safeguard nonpublic, unclassified information that supports and enables the warfighter.
5	Provide a consistent methodology to assess a defense contractor's implementation of required cybersecurity requirements.
6	Utilize (rather than replace) the already existing security standards set forth in: ○ 48 C.F.R. § 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems* (the 15 basic contractor information systems safeguarding requirements in a standard FAR clause that has been substantially unchanged for the past 10 years);[20] ○ NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Revision 2, February 2020 (includes updates as of January 28, 2021); ○ selected requirements from NIST SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*, February 2021.
7	Balance the need to safeguard FCI and CUI and the requirement to share information appropriately with defense contractors in order to develop capabilities for the DoD.
8	Provide DoD with increased assurance that FCI and CUI will be adequately safeguarded when residing on or transiting contractor information systems.

Whereas all but one of the foregoing stated purposes look attainable with determined and persistent government and contractor implementation and with incorporation of lessons learned over time, achievement of the seventh would seem to require an eventual reduction of the costs and challenges that government contractors and subcontractors are experiencing at the start of this new era. Like other commendable statements of purpose in procurement-related regulations,[21] achieving a balance of government and industry interests is much easier said than done.

[20] *See supra* note 7 (noting that as a result of the FAR Overhaul, and DoD's issuance of a deviation consistent with that process, this clause is renumbered as 52.240-93).

[21] *See, e.g.*, Dep't of Defense, Instruction (DoDI) 5010.44, *Intellectual Property (IP) Acquisition and Licensing* at ¶ 1.2b(3) (Oct. 16, 2019) (including as a "core principle govern[ing] the DoD acquisition, licensing, and management of IP" the negotiation of "specialized provisions for IP deliverables and associated license rights whenever doing so will more effectively balance DoD and industry interests than the standard or customary license rights").

On October 15, 2024, DoD issued the final rule[22] establishing the CMMC Program (the "Program Rule") within the Department and directing DoD components and officials, and particularly program managers, to implement the Program.[23] On December 16, 2024, this final rule became effective. The 24 sections and Appendix A of the rule outline the Program's purpose, define terms, state essential Program policy, assign government roles and responsibilities, describe the CMMC Assessment and Certification Ecosystem, and set forth the key elements of the Program. In short, ***CMMC is a three-level framework for assessing a DoD contractor's or subcontractor's information security protections***, one designed to comprehensively address DoD's contractor situation and to be scalable to a progression of government requirements for and contractors' maturity levels in providing such protections. The following table summarizes the requirements applicable at each level:

Level	***Requirements***
1	15 "basic" information security requirements set forth in FAR 52.204-21/52.240-93
2	110 requirements of NIST SP 800-171 Revision 2
3	Level 2 requirements + 24 of 35 requirements of NIST SP 800-172 Revision 2

Under the Program Rule, DoD program officers or requiring activities must determine, for each acquisition, which level will apply and, for each level, a particular CMMC compliance "status" that the contractor must meet prior to award and throughout the performance of the resulting contract.

A CMMC status is an assessment that measures the state of a contractor's compliance with the requirements applicable to a level.[24] The statuses are either final or conditional. If the agency assigns a final CMMC status requirement to an acquisition, the contractor must comply with all the requirements of the level.[25] If the agency allows a conditional status, then the contractor has to meet certain critical requirements, achieve a score of 80% of the total possible points prescribed by the scoring methodology, prepare a plan of action and milestones ("POA+M") for

[22] Most U.S. federal rulemaking follows procedures under 5 U.S.C. § 553, part of the Administrative Procedures Act (APA). That statute requires an agency to publish notice of proposed rulemaking in the Federal Register and to give interested persons an opportunity to participate in the rulemaking through submission of written data, views, or arguments. Publication of the final rule in the Federal Register then constitutes the culminating event in the rulemaking process. *Natural Resources Defense Council v. National Highway Traffic Safety Administration*, 894 F.3d 95 (2018). For procurement policies, 41 U.S.C. § 1707 establishes additional requirements beyond the APA . Under § 1707, a procurement policy, regulation, procedure, or form may not take effect until 60 days after it is published for public comment in the Federal Register if it relates to the expenditure of appropriated funds and has a significant effect beyond the internal operating procedures of the agency or has a significant cost or administrative impact on contractors or offerors. Within DoD, the DFARS is issued subject to the authority, direction, and control of the Secretary of Defense and contains requirements of law and DoD-wide policies. The making or amending of DFARS rules is thus subject to an overlay of further rulemaking policy and procedure governed by regulations such as 48 C.F.R. 1.301 and 48 C.F.R. 201.301.

[23] Dep't of Defense, Final Rule Regarding Cybersecurity Maturity Model Certification Program (CMMC), 89 FR 83092 (Oct. 15, 2024), available at https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program#h-56 (accessed Mar. 5, 2026).

[24] 32 C.F.R. § 170.4.

[25] 32 C.F.R. § § 170.15, 170.17, and 170.18.

correction of the non-compliances, execute the POA+M within 180 days of contract award, and then undergo another assessment to determine whether it complies with all the requirements.

Failure to comply with all requirements at that point would be a breach of the contract. For level 1, the assessment is binary—either contractors meet all of the requirements or they are non-compliant. Therefore, a conditional status is not allowed for level 1. However, a conditional status is allowed for both levels 2 and 3.[26]

The CMMC status types vary depending on the type of assessment that the agency requires. There are three types of assessments:

- Self-assessments, which are submitted by the contractor to the Supplier Performance Risk System ("SPRS") portal;
- Assessments conducted by certified third-party assessment organization ("C3PAO") and accompanying certificates of compliance, which are submitted by the C3PAO to a DoD enterprise system and then transmitted to SPRS; or
- Assessments conducted by DoD's Defense Industrial Base Cybersecurity Assessment Center ("DIBCAC"), which are submitted by DIBCAC to the enterprise system and then transmitted to SPRS.

While lower-level statuses require contractors to submit self-assessments of compliance to DoD, the higher-level statuses require assessment and certification by either a C3PAO or DIBCAC.[27] The following table summarizes the different CMMC statuses the agencies may specify, the assessment requirement, and the criteria required to qualify for the status:

Level	***CMMC Status***	***Assessment Requirements***	***Criteria to Qualify for Status***
1	Final Level 1 (Self)	Self-assessment	Meet all criteria
2	Conditional Level 2 (Self)	Self-assessment	Meet all critical criteria + 80% score + POA&M
	Final Level 2 (Self)	Self-assessment	100% score
	Conditional Level 2 (C3PAO)	C3PAO assessment	Meet all critical criteria + 80% score + POA&M
	Final Level 2 (C3PAO)	C3PAO assessment	100% score
3	Conditional Level 3 (DIBCAC)	DIBCAC assessment	Meet all critical criteria + 80% score + POA&M
	Final Level 3 (DIBCAC)	DIBCAC assessment	100% score

The Program Rule requires agency officials to select the applicable status based on factors such as (i) criticality of the associated mission capability; (ii) type of acquisition program or

[26] 32 C.F.R. § 170.21.

[27] 32 C.F.R. § § 170.4, 170.7, and 170.9.

technology; (iii) the threat of loss of the FCI or CUI to be shared or generated in relation to the effort; (iv) impacts from exploitation of information security deficiencies; and (v) other relevant policies and factors, including Milestone Decision Authority guidance. [28]

The Program Rule also requires roll out of CMMC in a planned sequence, culminating in a 4-phase implementation over what is envisioned to be a three-year period lasting until November 10, 2028. Here are the highlights of the sequence and phasing:

- ***Phase 1.*** Began on the effective date of the final rule amending the DFARS (thus November 10, 2025) and continues through November 9, 2026. In this phase, DoD has stated an intent to include the requirement for CMMC statuses of ***Level 1 (Self) or Level 2 (Self) for all applicable DoD solicitations and contracts as a condition of contract award***. DoD may, at its discretion, include the requirement for CMMC Status of Level 1 (Self) or Level 2 (Self) for applicable DoD solicitations and contracts as a condition to exercise an option period on a contract awarded prior to the effective date. DoD may also, at its discretion, include the requirement for CMMC Status of Level 2 (C3PAO) in place of the Level 2 (Self) CMMC Status for applicable DoD solicitations and contracts.
- ***Phase 2.*** Slated to begin one calendar year following the start date of Phase 1 (and thus November 10, 2026) and continues through November 9, 2027. In addition to Phase 1 requirements, DoD intends to include the requirement for CMMC Status of ***Level 2 (C3PAO) for applicable DoD solicitations and contracts as a condition of contract award***. DoD may, at its discretion, delay the inclusion of a requirement for CMMC Status of Level 2 (C3PAO) to an option period instead of as a condition of contract award. DoD may also, at its discretion, include the requirement for CMMC Status of Level 3 (DIBCAC) for applicable DoD solicitations and contracts.

> ***"On November 10, 2025, the final rule amending the DFARS became effective, . . . thus commenc[ing] the four phases of CMMC Program implementation."***

- ***Phase 3.*** Begins one calendar year following the start date of Phase 2 (and thus November 10, 2027) and continues through November 9, 2028. In addition to Phase 1 and 2 requirements, DoD intends to include the requirement for CMMC Status of Level 2 (C3PAO) for all applicable DoD solicitations and contracts as a condition of contract award and as a condition to exercise an option period on a contract awarded after the effective date. DoD also intends to include the requirement for ***CMMC Status of Level 3 (DIBCAC) for all applicable DoD solicitations and contracts as a condition of contract award***. DoD may, at its discretion, delay the inclusion of requirement for CMMC Status of Level 3 (DIBCAC) to an option period instead of as a condition of contract award.
- ***Phase 4, full implementation.*** Begins one calendar year following the start date of Phase 3 (and thus November 10, 2028). DoD will include CMMC Program requirements in all applicable DoD solicitations and contracts including option periods on contracts awarded prior to the beginning of Phase 4.[29]

[28] 32 C.F.R. § 170.5

[29] The bullets in this paragraph digest the applicability statement at 32 C.F.R. § 170.3.

On September 10, 2025, DoD issued the final rule amending the DFARS—consistent with and complementary to the prior year's establishment of the CMMC Program Rule —to incorporate CMMC-related contractual requirements binding upon contractors and subcontractors handling FCI and CUI.

On November 10, 2025, the final rule amending the DFARS became effective, changing DFARS Part 204, as well as corresponding contractual clauses at DFARS Part 252. These CMMC-related changes to DoD procurement regulations thereupon became codified at 48 C.F.R. Parts 204 and 252.[30] November 10, 2025 thus commenced the four phases of CMMC Program implementation.

The new November 2025 version of DFARS clause 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements, (the "DFARS Clause") is at the heart of CMMC implementation for defense contractors and subcontractors. Though relatively brief by procurement regulation standards, the new clause is deceptively dense, incorporating by reference hundreds of pages of information technology and security controls, requirements, standards, and procedures, any single one of which could now become the difference between gaining or losing a contract, as well as scores of definitions and acronyms and several important new players and roles.

Boiled down to its essence, the DFARS Clause creates four requirements of DoD contractors, each of which is tied to the three-levels-three-assessors CMMC framework introduced above and depicted in Figure 1 below and an associated CMMC status. Here are the four requirements:

1 ***Current CMMC Status at Specified Level:*** Contractors must have and maintain for the duration of the contract a current CMMC status at the specified CMMC status or higher: for all information systems used in performance of the contract, task order, or delivery order that process, store, or transmit FCI or CUI.[31] "Current," with regard to CMMC status for purposes of the clause, is intricately defined under the clause, with—

- conditional statuses generally having a 180-day duration before a new assessment is necessary,
- final statuses for Level 1 generally having a 1-year duration before a new assessment is necessary,
- and final statuses for Levels 2 and 3 generally having a 3-year duration before a new assessment is necessary

—assuming no changes in compliance with requirements and a corresponding affirmation of continuous compliancy not older than 1 year by the affirming official.[32]

[30] As a result of the FAR Overhaul, DoD issued class deviations to Parts 204 and 240, resulting in the movement, effective February 1, 2026, of the CMMC content to section 240.371, though the CMMC-related contract clauses are to remain in the 252.204 series for the time-being. *See, e.g.,* Office of the Assistant Secretary of War, Principal Director for Defense Pricing, Contracting, and Acquisition Policy, Memorandum for DoD Component Acquisition Executives and Procurement Officials, subj: Class Deviation—Revolutionary Federal Acquisition Regulation (FAR) Overhaul Part 40, Defense FAR Supplement (DFARS) Part 240 (Dec. 18, 2025), *available at* https://www.acquisition.gov/sites/default/files/page_file_uploads/DoD_RFO_Deviation_Part-40.pdf (accessed Mar. 5, 2026).

[31] DFARS 252.204-7021(d)(1)(i).

[32] DFARS 252.204-7021(a).

2	***Correct CMMC Level Flowed Down to Subcontractors:*** Contractors must consult 32 CFR 170.23 related to the flow down of the CMMC requirements, and flow down the correct CMMC level/status requirement to subcontracts involving processing, storing, or transmission of FCI or CUI.[33]
3	***FCI/CUI Handled According to Specified CMMC Level:*** Contractors and subcontractors may only process, store, or transmit FCI or CUI on information systems that have a CMMC status at the specified CMMC level required, or higher.[34]
4	***Continuous Compliance With the Specified CMMC Level Requirements Affirmed in SPRS for Self and All Subcontractors:*** Contractors and subcontractors must ***c***omplete on an annual basis, and maintain as current, an affirmation, by the affirming official (see 32 CFR 170.4), of continuous compliance with the requirements associated with the CMMC level required . . . in the Supplier Performance Risk System (SPRS) (https://piee.eb.mil) for each CMMC Unique Identifier (UID) applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract,[35] and ensure all subcontractors and suppliers do similarly.[36]

It bears emphasis that the new era is upon us. Until November 9, 2028, which coincides with the end of Phase 3 of the implementation program discussed above, contracting officers only have to include the DFARS Clause "if the program office or requiring activity determines that the contractor is required to have a specific CMMC level."[37]

On November 10, 2028, however, contracting officers will be required to include the clause in all contracts involving FCI or CUI so long as the program office or requiring activity has determined that contractors will be required to use contractor information systems to process, store, or transmit FCI or CUI in the performance of a contract.[38] This will even extend to contracts using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for those solely for the acquisition of commercially available off the shelf items.

---

[33] DFARS 252.204-7021(d)(1)(ii).

[34] DFARS 252.204-7021(d)(2).

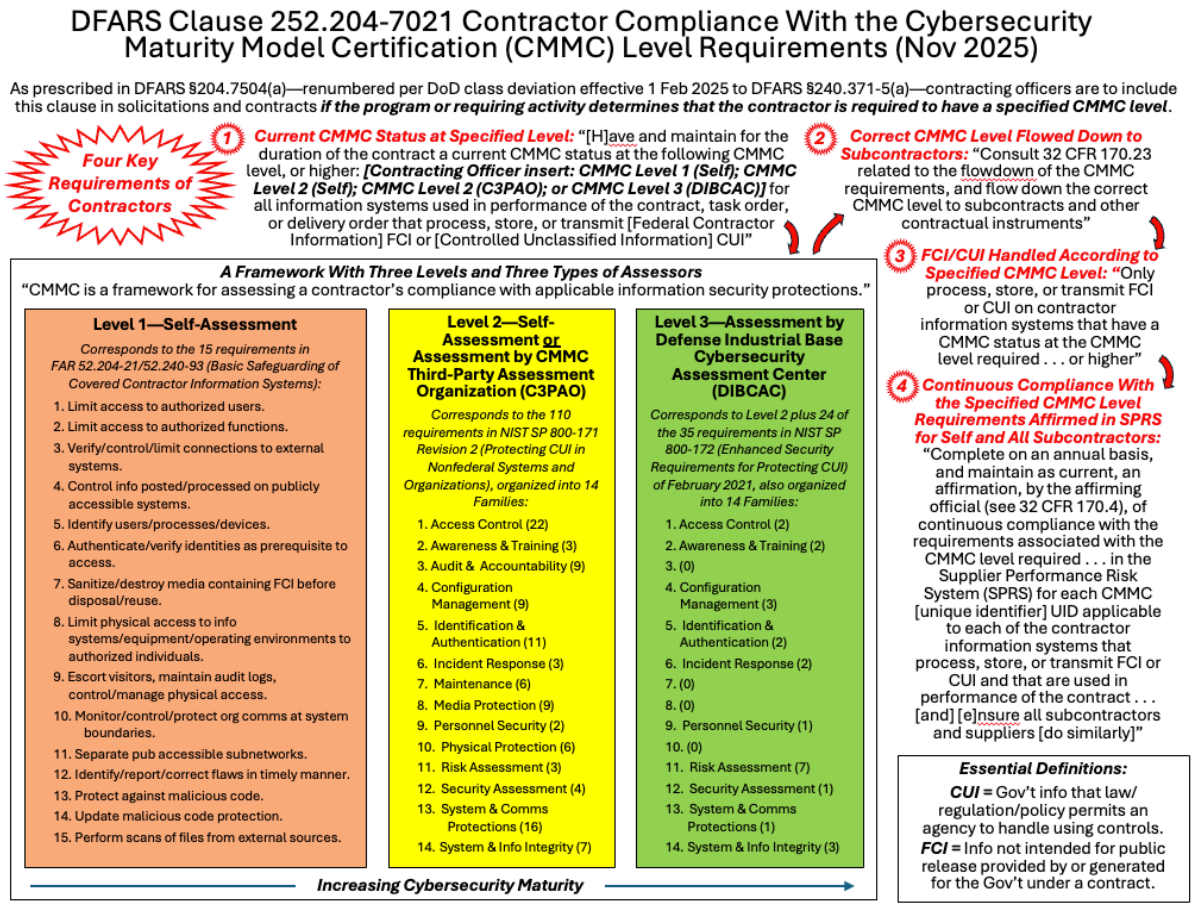
[35] DFARS 252.204-7021(d)(3). Separately, a contractor is required to report to the contracting officer the CMMC Unique Identifiers (UIDs) issued by SPRS for contractor information systems that will process, store, or transmit FCI or CUI during performance of the contract, as well as any changes in the CMMC UIDs generated in SPRS throughout the life of the contract, task order, or delivery order, if applicable. DFARS 252.204-7021(e)(1). The Unique Identifier mechanism within SPRS recognizes that clearly specifying the information system or systems being assessed in connection with a particular contractor is critical to evaluating compliance, and thus having confidence in a contractor's ability to safeguard information worthy of protection.

[36] DFARS 252.204-7021(d)(4).

[37] DFARS 204-7504(a)(1) (renumbered per DoD class deviation effective 1 Feb 2025 to DFARS §240.371-5(a)(1)).

[38] DFARS 204-7504(a)(2) (renumbered per DoD class deviation effective 1 Feb 2025 to DFARS §240.371-5(a)(2)).

The following diagram summarizes the requirements of the DFARS Clause:



GSA Procedural Changes Requiring Third-party Assessments of Compliance

A recent promulgation by the GSA is another marker of the dawn of the new era of information security compliance. In particular, on January 5th, 2026, the GSA issued a new "IT Security Procedural Guide" that will govern information security on certain GSA contracts that require processing, storage or transmission of CUI or security protection for such transactions ("GSA IT Guide").[39] In its expanding role as a central hub for federal government procurements, the GSA manages a wide array of contract programs used by agencies across the federal government, including the DoD.

For example, GSA manages the government wide Multiple Award Schedule or "GSA Schedule" program for numerous categories of products and services. GSA also manages various specialized multiple award government-wide acquisition programs for advanced technology and professional services such as Polaris, OASIS+, and Alliant Phase 2 and 3. Under these programs, GSA enters into indefinite delivery, indefinite quantity type contracts with multiple providers and then makes the contracts available to agencies across the government for

[39] GSA IT Guide, *supra* note 13, *available at* https://www.gsa.gov/system/files/Protecting-Controlled-Unclassified-Information-%28CUI%29-in-Nonfederal-Systems-and-Organizations-Process-%5BCIO-IT-Security-21-112-Rev-1%5D.pdf.

their use. With relative ease and efficiency, agency procurement officials can then conduct competitions for and issue task or delivery orders under these contracts. In total, GSA facilitates agency procurements valued at over $84 billion per year.[40] Therefore, the issuance of the GSA IT Guide was a significant development.

GSA elected to issue the GSA IT Guide as a procedural document as opposed to a FAR rule. However, as one commentator noted "treating it as internal or optional would be a mistake. In practice, [the GSA IT Guide] is shaping who competes for future GSA work involving CUI."[41] Indeed, the introduction to the GSA IT Guide makes clear that, as a matter of policy, GSA has decided to incorporate it into new or amended solicitations for acquisitions that involve CUI.[42] While the introduction also states that the GSA Chief Information Security Officer ("CISO") must approve its incorporation into solicitations and contracts[43], given the current emphasis on contractor information security, we expect the CISO to issue broad authorizations for its use.

Like the CMMC rules, the GSA IT Guide applies only to those systems or "components" of contractor systems that "process, store, or transmit CUI, or provide security protection for components."[44] In addition, like the CMMC rules, the GSA IT Guide requires compliance with NIST 800-171 and 800-172. However, ***while the CMMC rule requires compliance with NIST 800-171 rev. 2 at Level 2 and certain requirements of NIST 800-172 rev 2 at Level 3, the GSA IT Guide requires compliance with NIST 800-171 rev 3 and specified requirements of NIST 800-172 rev 3 (draft).***[45] ***In addition, the processes involved under the CMMC rules and the GSA IT Guide are very different.*** Under the CMMC rule, the DoD requires submission of either self or third-party assessments/certifications of compliance as a condition for eligibility for award of a contract but does not approve contractor systems. However, under the five-phased compliance process in the GSA IT Guide, GSA must specifically approve contractor systems for use on contracts involving CUI. The following table summarizes these processes:

Phase	***Major Requirements***
1-Prepare	Contractor completes security categorization template to determine types of information stored, processed, or transmitted, attends kickoff meeting with GSA to review the processes, and presents to GSA solution architecture to meet critical security capabilities. The GSA security team provides feedback concerning potential areas of concern.
2-Document	Contractor submits a number of deliverables to GSA, including a Systems Security and Privacy Plan, Privacy Threshold Assessment, Privacy Impact Assessment, and Supply Chain

[40] U.S. General Services Administration, "Sell to the Government," *available at* https://www.gsa.gov/sell-to-government (accessed on March 23, 2026).

[41] StratoKey Data Security Company, *GSA's CMMC Style-Cybersecurity Guide, CIO-IT Security-21-112* (Feb. 27, 2026), *available at* https://www.stratokey.com/blog/gsas-cybersecurity-requirements-cio-it-security-21-112 (accessed on March 1, 2026).

[42] GSA IT Guide, *supra* note 13, at Sec. 1.

[43] GSA IT Guide at Sec. 1.2.

[44] GSA IT Guide at Sec. 1.2.

[45] GSA IT Guide at Secs. 1 and 2.3.2.

Phase	*Major Requirements*
	Risk Management Plan. The GSA IT Guide sets forth detailed requirements for each of these deliverables.
3-Assess	An accredited third-party assessment organization or GSA approved assessor plans and conducts an assessment the covered contractor systems and produced a Security Assessment Report and Plan of Action and Milestones ("POA&M") for correction of any non-compliances. The GSA IT Guide sets forth detailed requirements for the deliverables required in this phase.
4-Authorize	During this phase, the contractor assembles and submits to GSA a detailed approval package that requests approval by the GSA Chief Information Systems Officer ("CISO") of the covered systems. The contractor then engages in a dialogue with GSA concerning any questions and non-compliances, culminating in approval or rejection of the systems by the CISO via a Memorandum for Record ("MFR").
5-Monitor	During this phase, the contractor engages in ongoing continuous monitoring of compliance, including structured quarterly, annual, and triennial deliverable obligations.[46]

Following are other significant differences between the CMMC rule and the GSA IT Guide. In particular:

- While the CMMC rules cover systems involving both CUI and the broader category of FCI, the GSA IT Guide only covers systems involving CUI.[47]
- The CMMC rules do not directly refer to NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, September 2020, the NIST IT security and privacy standard applicable to federal agencies.[48] By contrast, the GSA IT

[46] GSA IT Guide at Sec. 2.

[47] GSA IT Guide at Sec. 1.2.

[48] Developed by NIST to meet its statutory responsibilities under the Federal Information Security Management Act of 2002, Pub. L. 107-347 (FISMA, originally codified at 44 U.S.C. § 3541, et seq.) and later revised to incorporate new Congressional mandates in the Federal Information Security Modernization Act of 2014, Pub. L. 113-283 (newly adopting the FISMA acronym, codified at 44 U.S.C. § 3551 et seq.), NIST SP 800-53 is the grandparent for modern IT security measures, providing:

> a *catalog* of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs.

U.S. National Institute of Standards and Technology, *Special Publication 800-53, Revision 4—Security and Privacy Controls for Federal Information Systems and Organizations* at iii (April 2013) (emphasis added) (superseded by Revision 5, but accurately recording the history and security control cataloging intent of NIST SP 800-53). Subsequently, the controls in NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems*

Guide requires compliance with certain parts of that standard if processing, transmission or storage of PII is within the scope of the contract.[49]

- Unlike the CMMC rule, the GSA IT Guide does not prescribe a phase-in period. Rather, it will apply immediately upon issuance of any solicitation that incorporates it.[50]
- While the CMMC rule requires contracting officials to specify different levels of compliance requirements depending on the requirements of the acquisition, the GSA IT Guide adopts a "one size fits all" approach under which all specified requirements apply regardless of the acquisition. However, as noted, certain privacy related requirements only apply if processing of personal identifying information is within the scope of the contract.[51]

"The CMMC rules and the GSA IT Guide take different approaches concerning circumstances in which contractors may receive awards pending completion of POA&M."

- The CMMC rules and the GSA IT Guide take different approaches concerning circumstances in which contractors may receive awards pending completion of POA&M. Under the CMMC rules, depending on the sensitivity level of the CUI, the DoD agency may specify that contractors must have prior to award a final CMMC status demonstrating full compliance with the applicable requirements for the level. In other cases, the agency may permit contractors to receive awards in a "conditional" status pending completion of corrective actions concerning non-critical requirements. On the other hand, the GSA IT Guide allows approval of systems that are not fully compliant in all cases if certain "showstopper" controls are implemented and the contractor documents a POA&M for the correction of non-compliances. The showstopper controls consist of specified NIST 800-171 rev 3 requirements concerning access enforcement. secure remote access, multi-factor authentication, vulnerability monitoring and scanning, boundary protection, transmission and storage confidentiality, cryptographic protection, flaw remediation and replacement of unsupported system components.[52]

---

and Organizations (2015) were selected and adapted by NIST from the catalog in NIST SP 800-53 to address growing concerns about how to safeguard CUI processed, stored, or transmitted on behalf of the federal government but outside information systems that were government owned and operated. *See, e.g.*, NIST SP 800-171, rev. 2, at vi ("The requirements recommended for use in this publication are derived from . . . the moderate security control baseline in [SP 800-53] and are based on the CUI regulation [32 CFR 2002]."). As discussed elsewhere in this article, NIST SP 800-171 revision 2 is the main IT security reference utilized by DoD, while the current revision 3 is being utilized elsewhere in the U.S. government, including at GSA. Whereas NIST SP 800-53 consists of hundreds of specific controls within 20 Security and Privacy Control families, NIST SP 800-171 comprises a subset of the NIST SP 800-53 controls within 14 (NIST SP 800-171, rev. 2) or 17 (NIST SP 800-171, rev. 3) families that are either identical to or closely related to the NIST SP 800-53 family structure.

[49] GSA IT Guide, *supra* note 13, at Sec. 1.

[50] GSA IT Guide at Sec. 1.2.

[51] GSA IT Guide at Secs. 1 and 2.3.2.

[52] GSA IT Guide at App. C.

Takeaways

Based upon our experiences, consultations with concerned contractors, comments submitted in connection with rulemaking, survey data and other information published by the Defense Contract Management Agency, and other sources, here are a few key takeaways for the early days of this new era:

- ***Gain Proper Information Security Credentials if You Wish to Compete for Government Contracts.*** Proper information security credentials will be a precondition to eligibility to compete in acquisitions for contracts involving CUI and FCI. This is true under both CMMC and the GSA IT Guide. Therefore, any companies planning to compete in such acquisitions will need to invest in the compliance infrastructure necessary to obtain these credentials and, if successful, to comply with the applicable requirements in the performance of their contracts.
- ***Assemble the Correct Information Security Infrastructure.*** The compliance infrastructure required to compete in the federal market should consist of (i) trained internal key personnel familiar with the rules of the new era to lead the effort; (ii) policies and procedures documenting internal controls designed to ensure adherence with the rules; (iii) information system architecture and deployed systems that meet all applicable requirements; (iv) external experts, including C3PAO organizations, that help guide compliance and perform compliance assessments; and (v) because "compliance is a team sport", training programs for all employees affected by the new rules.
- ***Adopt a Learning Mindset.*** To effectively support the company's business objectives, legal, contract management, and information technology professionals supporting contractor compliance programs will need to learn a finite but substantial body of rules governing the new era.
- ***Be Mindful that the Hazards of Noncompliance are Great.*** In addition to supporting the company's business objectives, effective compliance will mitigate unique risks that contractors face in the federal market. In particular, the False Claims Act ("FCA") contains both civil and criminal penalties for anyone who knowingly presents a false claim to the government for payment.[53] Contractors can be liable under the civil FCA for submitting information with "reckless disregard" or "deliberate ignorance" of its accuracy. Compliance with these statutes requires scrupulous honesty and a strong commitment to accuracy in information presented in all communications with the government. Under the Department of Justice's ("DOJ's") Civil Cyber-Fraud Initiative, DOJ has been aggressively pursuing civil FCA actions against contractors that falsely certified compliance with applicable information security requirements of the old era. Although compliance is fully attainable with correct preparation, and the rewards of

"Although compliance is fully attainable with correct preparation, and the rewards of successfully competing for government contracts can justify the risks, we expect that active policing of noncompliance will continue into the new era."

[53] 18 U.S.C. § 287; 31 U.S.C. § 3729.

successfully competing for government contracts can justify the risks, we expect that active policing of noncompliance will continue into the new era.

- ***Plan for Stringency.*** The differences between the CMMC rules and the GSA IT Guide highlight the need for contractors to incorporate the constraints of the information security regulatory environment into their strategic and operational business planning processes. For example, a company planning to sell the same products and services to both DoD and GSA will want to consider implementing a compliance infrastructure that ensures compliance with the most stringent standards. In addition, company business plans should reflect the highest level CMMC status necessary to achieve company objectives and include budgets and plans for achieving that status prior to the projected announcement dates of the opportunity.
- ***Prepare for Flowing Down to Subcontractors.*** Contractors should develop and implement plans for its purchasing functions to flow-down information security requirements to subcontracts that involve CUI or FCI. 32 C.F.R. § 170.23 purports to provide some guidance for DoD contractors, but the hardest practical questions will need to be answered by contractor purchasing personnel and their compliance experts, such as anticipating what kind of information, i.e., FCI, CUI, both, or neither, will be processed, stored, or transmitted by a subcontractor in performance of the subcontract. In connection with this, contractors will need to develop information security classification guides modeled on the classified information regulations, that help purchasing personnel make the required determinations.
- ***Communicate as Appropriate with the Government.*** Contractors should expect it will be necessary to submit comments and questions to the agencies in response to requests for information, sources sought notices and solicitations that might encourage the agency to re-think overclassification of an information security requirement based on criteria in the governing guidance. For example, if a contractor with a CMMC status of "Final Level 2 (Self-Assessment)" wants to propose against a solicitation announcing a CMMC status requirement of "Final Level 2 (C3PAO)", the contractor should consider making the case for the lower-level status in a question based on the statement of work of the solicitation and the criteria in the CMMC Program Rule. Such attempts may make good business sense because the difference between Levels 1 and 2 (Self) and Levels 2 (C3PAO) and 3 (DIBCAC) is stark, in terms of compliance and expense for a contractor seeking DoD awards.
- ***Find a Good Third-Party Assessment Organization.*** Contractors will need to determine how to find a good third-party assessment organization. While the rules require use of an organization that has been certified as meeting certain requirements, quality and availability of these organizations should be expected to vary considerably, as with many inspection services. Beyond description of the CMMC Assessment and Certification Ecosystem at 32 C.F.R. §§ 170.8-170.13 and the certification and instruction standards referenced therein, there is as yet little regulatory guidance to aid contractors in finding an outside party whose decisions and actions may deeply impact important business interests.

However, the Cyber Accreditation Board's Marketplace is one important place to visit early in the search.[54]

- ***Stay Current.*** Contractor compliance professionals will need to keep abreast of continuing developments in the information security regulatory environment.

[54] According to its website, "the Cyber Accreditation Board is the official accreditation body of the Cybersecurity Maturity Model Certification (CMMC) ecosystem and the sole authorized non-governmental partner of DoD in implementing and overseeing the CMMC conformance regime." In connection with that role, the Board authorizes and accredits CMMC Third-Party Assessment Organizations (C3PAOs). The marketplace lists all these organizations. *See* https://cyberab.org/Catalog#!/c/s/Results/Format/list/Page/1/Size/9/Sort/NameAscending (accessed Mar. 26, 2026).

Appendix A
Overview of FAR and DFARS Information Security Requirements[55]

FAR/DFARS Reference	*FAR Overhaul Reference*	*Overview*
General Requirements		
FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems	52.240-93, Basic Safeguarding of Covered Contractor Information Systems	Basic requirements applicable to systems that process, store or transmit FCI
FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities.	52.240-91, Security Prohibitions and Exclusions	Supply chain restriction
FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.	52.240-91, Security Prohibitions and Exclusions	Supply chain restriction
FAR 52.204-27 Prohibition on a ByteDance Covered Application	52.240-91, Security Prohibitions and Exclusions	Supply chain restriction
FAR 52.204-30 Federal Acquisition Supply Chain Security Act Orders—Prohibition	52.240-91, Security Prohibitions and Exclusions	Supply chain restriction
DFARS 252.239-7010 Cloud Computing Services	Same	Applies to DoD contracts when contractor uses cloud computing to provide information technology services; requires compliance with Cloud Computing Security Requirements Guide; contractor must maintain government data within the U.S.

[55] This list only includes contract clauses and omits solicitation notices and representations and certifications pertaining to information security.

Requirements Applicable to Systems that Process Classified Information		
FAR 52.204-2, Security Requirements	52.240-92, Security Requirements	Implements classified information handling regulations on government contracts.
Requirements Applicable to Systems that Process Controlled Unclassified Information		
DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting	Same	Specifies minimum information security requirements for contracts involving covered defense information, including compliance with NIST SP 800-171 and compliance with Moderate FEDRAMP baseline requirements for external cloud services providers used by contractor in performance; also governs cyber incident reporting.
DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements	252.240-7997	Requires contractors to provide government access to facilities and systems to conduct certain assessments; FAR overhaul eliminated pre-award self-assessment requirements, presumably in anticipation of CMMC roll-out.
DFARS 252.204-7021 Cybersecurity Maturity Model Certification (CMMC) Requirements	Same	Comprehensive information security regulations for certain DoD contractors, as described above.

Appendix Notes Regarding the FAR Overhaul:

- The Trump Administration is in the throes of a "revolutionary" overhaul to the Federal Acquisition Regulation ("FAR") system. President Trump launched the project on April 15, 2025, when he issued Executive Order No. 14275, "Restoring Common Sense to Federal Procurement," and since then the Administration has been busy implementing that Order. In short, EO 14275 requires the deregulation of the federal procurement enterprise and the empowering of agencies to act nimbly and effectively in the best interests of the nation. To achieve this, EO 14275 directed the Administrator of the Office of Federal Procurement Policy ("OFPP"), in coordination with the Federal Acquisition Regulatory Council (the "FAR Council") and various agency officials, to take action within 180 days to amend the FAR so that it "contains only provisions that are required by statute or essential to sound procurement."[56]

- The Office of Management and Budget ("OMB") instructed the cognizant officials to implement EO 14275 in two phases.[57] Phase I, which is complete, involved leveraging agency authority in

[56] Executive Order No. 14275 at Sec. 2.

[57] Office of Mgmt & Budget, Exec. Office of the President, OMB Memorandum no. M-25-26, *Overhauling the Federal Acquisition Regulation* (2025), available at https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-26-Overhauling-the-Federal-Acquisition-Regulation-002.pdf (accessed Mar. 26, 2026).

FAR Subpart 1.4 to issue FAR deviations ahead of formal rulemaking.[58] In this phase, the FAR Council issued, on a rolling basis, guidance to the agencies with model deviation text by FAR part. Agencies then had thirty days to adopt the FAR deviations based on the model text.[59]

- As of March 1st, 2026, the FAR Council had issued model deviation text with changes to all of the 53 sections of the FAR and most of the major agencies had adopted the deviations and associated changes to their FAR supplements. In Phase II, leveraging the work done in Phase I, the FAR Council will undertake formal rulemaking to change the FAR and deregulate federal procurement across all agencies.

* * * * *

The foregoing article was prepared for the general information of clients and other friends of the Mark Martins Law Office, PLLC and the Law Office of Christopher C. Bouquet, PLLC. It is not meant as legal advice with respect to any specific matter and should not be acted upon without counsel from an attorney. If you have any questions or require any further information regarding these or other related matters, please contact us. This material is considered Attorney Advertising.

APRIL 2, 2026

[58] *See* the FAR Council's May 2d, 2025 memorandum for detailed guidance concerning the issuance of the FAR deviations at https://www.acquisition.gov/sites/default/files/page_file_uploads/FAR-Council-Deviation-Guidance-on-FAR-Overhaul.pdf (accessed Mar. 26, 2026).

[59] For transparency, the OFPP and FAR Council have been posting the model text and the deviations on the "Revolutionary FAR Overhaul" or "RFO" website.