June 29, 2026

Big Changes Coming for Government Contractors: Proposed FAR CUI and DoW FOCI Rules, New Quantum Cryptography Order and Ongoing CMMC Rollout

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Tatiana O. Sullivan
Partner / Washington, D.C.
202.371.7063
tatiana.sullivan@skadden.com

Lisa Marie Rechden
Associate / Washington, D.C.
202.371.7505
lisa.rechden@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., NW
Washington, DC 20005
202.371.7000

Executive Summary

- **What's new:** Four significant federal contracting developments are converging to fundamentally reshape cybersecurity and foreign ownership compliance obligations for government contractors across the federal supply chain.
- **Why it matters:** Noncompliance carries substantial consequences, including loss of contract eligibility, False Claims Act liability and operational disruptions.
- **What to do next:** Contractors should consider assessing their cybersecurity posture against NIST SP 800-171 Rev. 3; inventory Department of War contracts for foreign ownership, control or influence applicability; and confirm Cybersecurity Maturity Model Certification assessment readiness.

Government contractors are facing significant changes to their compliance obligations this year; taken together, these developments signal a whole-of-government effort to strengthen cybersecurity and supply chain security as well as foreign influence protections across the federal procurement system:

- **The Federal Acquisition Regulatory (FAR) Council** has published a proposed rule that would extend National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Rev. 3 safeguarding requirements to all federal contractors handling Controlled Unclassified Information (CUI), not only those holding contracts with the Department of War (DoW).
- **A proposed Defense Federal Acquisition Regulation Supplement (DFARS) rule** would require contractors on unclassified DoW[1] contracts valued above $5 million to disclose and potentially mitigate foreign ownership, control or influence (FOCI).
- **A new cryptographic executive order (EO)** accelerates the U.S. government's adoption of post-quantum cryptography (PQC).

[1] Congress has not yet acted on the administration's renaming of the Department of Defense.

– **The DoW Cybersecurity Maturity Model Certification (CMMC) program** is in its initial implementation phase and moving to the second phase in November 2026, which imposes requirements for certain government contractors' systems to undergo third-party assessments in order to be eligible for contract awards.

Noncompliance with these developments carries substantial consequences, including loss of contract eligibility, exposure to False Claims Act liability and operational disruptions from FOCI mitigation measures. The breadth of these requirements, often extending to subcontractors at all tiers and to commercial item contracts, means that virtually every company in the federal supply chain must evaluate its readiness.

Contractors are encouraged to:

– Assess their current cybersecurity posture against NIST SP 800-171 Rev. 3 standards.
– Inventory their DoW contracts for potential FOCI applicability.
– Identify any cryptographic vulnerabilities within their systems.
– Confirm their CMMC assessment readiness against the phased timeline.
– Review flowdown obligations to ensure subcontractors are prepared.

Proposed FAR CUI Rule

On June 23, 2026, the FAR Council issued a proposed rule that would overhaul how government contractors handle CUI[2] across the federal government. Comments on the proposed rule are accepted until July 23, 2026.

If implemented as drafted, the proposed FAR CUI rule would:

– Extend the requirement to implement NIST SP 800-171 Rev. 3 standards from only defense contractors to all federal contractors accessing CUI on their systems.
– Require contractors to flow down all CUI safeguarding requirements to subcontractors at all tiers that access covered CUI.
– Require cloud service providers used by contractors to comply with no less than the FedRAMP Moderate baseline.
– Require offerors that are not compliant with all applicable CUI safeguarding requirements to disclose all areas of noncompliance at proposal submission and submit a formal Plan of Action and Milestones identifying how and when deficiencies will be remediated.
– Provide greater flexibility for contractors to ensure employees are trained on proper CUI protections.
– Require contractors to notify the government within 72 hours of:
  • cybersecurity incidents involving CUI; and
  • discovery of unmarked or improperly marked information they believe constitutes CUI.
– Require federal agencies to provide contractors a standardized form identifying when CUI is part of a contract and the applicable organization-defined parameters for NIST SP 800-171 Rev. 3.

Proposed FOCI Requirements for Nonclassified Contracts

On May 7, 2026, the DoW issued a proposed rule that would amend DFARS to require certain contractors and subcontractors, at any tier, working under unclassified contracts to disclose beneficial ownership and FOCI information to the Defense Counterintelligence and Security Agency (DCSA). The proposed rule represents a significant expansion of DoW's FOCI oversight beyond the traditional classified contracting environment. Comments on the proposed rule are accepted until July 6, 2026.

Key Provisions

If implemented as drafted, the proposed FOCI rule would represent a significant expansion of DoW's FOCI oversight beyond the traditional classified contracting environment.

– **Covered contracts:** The rule applies to DoW contracts valued above $5 million and all prime contractors and subcontractors performing on such contracts, with exceptions for Commercial Off-the-Shelf contracts (unless a senior DoW official determines that a procurement presents a national security risk).
– **Disclosure obligations:** Offerors and contractors on covered contracts must submit a Standard Form 328 in DCSA's National Industrial Security System (NISS), disclosing FOCI information including foreign beneficial owners, foreign touchpoints, material contracts and financial arrangements, and foreign directors and officers.

[2] "Controlled unclassified information" is sensitive but unclassified information created or possessed by the U.S. government and government contractors that must be safeguarded and protected against unauthorized disclosure.

- **Contract eligibility:** Contracting officers would be prohibited from awarding, modifying or exercising options on covered contracts unless the contractor maintains "eligible" status in NISS, making continued NISS eligibility a prerequisite for contract performance.
- **Mitigation:** Where DoW determines that FOCI or beneficial ownership presents a national security risk, covered contractors must implement mitigation measures within 90 days. DCSA will return a FOCI risk assessment within 25 working days. Mitigation measures may include governance restrictions, board controls, security agreements and other mechanisms consistent with existing FOCI concepts used in the facility security clearance context.
- **Subcontractor flowdowns:** The rule applies to subcontractors at any tier where the applicable subcontract exceeds $5 million. Prime contractors must ensure covered subcontractors maintain an eligible status in NISS throughout performance.

Historically, FOCI review and mitigation requirements arose only in the context of classified contracts and facility security clearances. This rule would establish unilateral authorities for DoW to impose mitigation requirements even where the Committee on Foreign Investment in the United States (CFIUS) clears a transaction. The ongoing reporting rules will also add additional notice and approval requirements in M&A transactions involving covered contractors.

New Cryptographic EO

On June 22, 2026, President Donald Trump issued EO 14412, "Securing the Nation Against Advanced Cryptographic Attacks" (the Cryptographic EO). The Cryptographic EO accelerates the U.S. government's PQC[3] transition by moving up key compliance expectations from 2035 to 2030 in an effort to reduce the risk that adversaries may collect encrypted sensitive data now and decrypt it later once quantum computing matures.

For government contractors, the most immediate impact will come through procurement: The FAR Council is directed to propose rules requiring covered contractors to comply with NIST Federal Information Processing Standards (FIPS) standards, including PQC-compliant algorithms, by December 31, 2030, and to implement vulnerability disclosure policies covering cryptography.

[3] "Post-quantum cryptography" is the latest generation of cryptographic algorithm, relying on complex mathematical problems that are difficult for quantum computers to solve, thereby protecting digital data against attacks from powerful quantum computers.

These requirements are likely to flow down through federal supply chains, making PQC readiness a broader commercial expectation beyond just prime contractors. The DoW's PQC Strategy, released on June 23, 2026, illustrates how significant the operational impact may be, particularly for defense contractors. It requires DoW systems to support PQC by the end of 2030 and use PQC by the end of 2031, affecting:

- Networks
- Weapons systems
- Satellites
- Tactical communications
- Edge devices
- Software
- Firmware
- Public key infrastructure
- Certificates
- Related infrastructure

Government contractors should expect PQC requirements to be built into solicitations, product design, certification pathways, cybersecurity programs and potentially even CMMC obligations. Thus, government contractors should consider:

- Inventorying their cryptographic assets.
- Assessing product and system dependencies.
- Planning for algorithm and certificate migration.
- Updating vulnerability disclosure processes.
- Preparing for PQC compliance.

CMMC Implementation

The DoW is rolling out CMMC requirements in a phased approach over three years, with full enforcement slated for all relevant contracts by November 2028.

Phase 2, which begins on November 10, 2026, incorporates CMMC Level 2 (Third-Party Assessor Organization (C3PAO) certifications) requirements into all applicable new contracts.

Phase 1, which began on November 10, 2025, previously introduced CMMC Level 1 and CMMC Level 2 (self-assessments) requirements into all applicable new contracts.

Failure to comply limits a contractor's eligibility to bid on or win DoW contracts. Submitting false or unvalidated compliance scores carries severe legal and financial liabilities under the False Claims Act.

Big Changes Coming for Government Contractors: Proposed FAR CUI and DoW FOCI Rules, New Quantum Cryptography Order and Ongoing CMMC Rollout

Certification Levels

The CMMC level required of contractors will depend on the sensitivity of data that the contractor will "process, share, or transmit" under a DoW solicitation.

- **Level 1 (basic safeguarding of Federal Contract Information, or FCI):** Contractors must submit annual self-assessment and affirmations of compliance with the 15 security requirements in FAR clause 52.204-21.
  - Required if the contract, task order or delivery order may require the contractor (or subcontractors at any tier) to process, store or transmit only FCI in its information system.
- **Level 2 (broad protection of CUI):** Contractors must submit either a self-assessment or an independent assessment by an authorized C3PAO every three years (as specified in the solicitation), plus annual affirmation verifying compliance with the 110 security requirements in NIST SP 800-171.
  - **Self-assessment:** Required when a contractor handles CUI that is completely outside of the National Archives' CUI Registry Defense Organizational Index Grouping.
  - **C3PAO assessment:** Required when a contractor handles CUI that is within the National Archives' CUI Registry Defense Organizational Index Grouping.
- **Level 3 (higher-level protection of CUI against advanced persistent threats):** Contractors must submit both a C3PAO and a government-led Defense Industrial Base Cybersecurity Assessment Center assessment and verify compliance with NIST SP 800-172.

Key Takeaways and Recommendations

- The proposed FAR CUI Rule would extend NIST SP 800-171 Rev. 3 requirements across all federal agencies, creating a uniform baseline for CUI protection governmentwide.
- The proposed FOCI rule would, for the first time, extend FOCI disclosure and mitigation requirements to unclassified DoW contracts above $5 million, affecting a broad swath of the defense industrial base.
- Contractors with foreign ownership or governance structures and/or access to CUI should consider evaluating their exposure under the proposed FOCI and CUI rules and determining whether to submit comments during the rulemaking process.
- Flowdown requirements in both the FAR CUI Rule and the FOCI rule mean that prime contractors should consider evaluating and managing compliance not only internally but across their entire subcontractor supply chain.
- Government contractors will be faced with PCQ requirements far sooner than previously expected, prompting a rapid understanding of any vulnerabilities in the contractors' systems and their ability to comply with any FIPS issued by NIST.
- CMMC is no longer prospective; Phase 1 is active, and impacted contractors should be prepared for C3PAO assessment requirements beginning in November 2026.