Press Coverage | October 9, 2025

# Preparing For What DOD Cybersecurity Audits May Uncover

**WRITTEN BY**

Michael E. Barnicle | Peter E. Jeydel | Bryan R. Williamson | Hilary S. Cairnie | Bonnie Gill

*This article was originally published on* Law360 *and is republished here with permission as it originally appeared on October 9, 2025.*

The U.S. Department of Defense **released** the final rule implementing the Cybersecurity Maturity Model Certification on Sept. 9.[1] Through the program, the DOD seeks to enhance protections for sensitive information.

Defense contractors' efforts to ramp up their CMMC compliance may reveal prior unknown instances of cybersecurity noncompliance. Similarly, CMMC assessments may highlight unanticipated export control violations.

Ahead of the CMMC program's phased implementation, beginning on Nov. 10, defense contractors and subcontractors should consider how they can assess and address these issues before they come to the attention of enforcement authorities.

**The CMMC Program**

Before the CMMC program was created, the DOD required defense contractors to implement cybersecurity requirements from the National Institute of Standards and Technology's Special Publication 800-171.[2] This previous rule relied on contractors to self-validate and report compliance without outside certification.

This will no longer be the case under the CMMC program. Through the new rule, the DOD requires an assessment and certification, and contractors may be required to allow outside auditors to inspect their information systems.

To compete for defense contracts going forward, contractors' information systems must pass an assessment and achieve a certification level to handle sensitive information.[3] Contractors requiring a CMMC Level 1 to handle federal contract information must complete a self-assessment of their information systems and report the results on the Supplier Performance Risk System.

In some instances, a CMMC Level 2, which is required for certain types of controlled unclassified information, or CUI, can also be obtained through self-assessment.

Companies handling more sensitive CUI must have their information systems externally validated by an outside

organization. For instance, most contractors requiring a CMMC Level 2 certification will need an outside assessment from a certified third-party assessment organization.

To achieve the program's highest certification, CMMC Level 3, the contractor's information system must successfully complete a CMMC Level 2 third-party assessment and a separate assessment from the Defense Industrial Base Cybersecurity Assessment Center.

Both of these outside assessments must be completed once every three years.

While the CMMC assessment process improves transparency in cybersecurity compliance, it also increases the possibility of discovering prior instances of noncompliance. Prior noncompliance, whether intentional or not, may result in adverse government action against the contractor.

**Unintended Compliance Issues: False Claims Act Liability and Export Control Violations**

***False Claims Act***

As the CMMC program increases cybersecurity transparency through its assessment requirements, companies are exposed to increased risk of past violations. Litigation involving contractor cybersecurity fraud is not new.

In 2021, the U.S. Department of Justice **began** its Civil Cyber-Fraud Initiative to target contractors for cybersecurity-related fraud.[4] Relying on the FCA, the DOJ can hold companies accountable for past violations if they knowingly, or even recklessly, misled the government about their cybersecurity compliance.

Under the CMMC program, past cybersecurity violations are more likely to be exposed during the assessment process. For instance, companies who may have misrepresented their compliance with NIST SP 800-171 in past contracts may be at risk of FCA litigation after reexamining their current cybersecurity compliance.

Similarly, companies that attested to compliance without verification are also at risk.

***Export Control Violations***

Sensitive government information like CUI and federal contract information can be subject to the Export Administration Regulations or even the International Traffic in Arms Regulations. The EAR controls many commercial items, including dual-use items that have both commercial and military applications, as well as certain purely military items and spacecraft-related items that were previously ITAR-controlled.

The EAR is administered by the Bureau of Industry and Security within the U.S. Department of Commerce. The ITAR is administered by the Directorate of Defense Trade Controls at the U.S. Department of State. The ITAR controls defense articles and services, as described on the United States Munitions List.

Contractors and subcontractors should be aware that their government contracts may involve ITAR- or EAR-controlled products or technical data, and the DOD is not the only agency that regulates such sensitive information. The State and Commerce Departments may also pursue enforcement actions for export control

violations.

Even companies that do not export their products can face export control violations. For example, so-called deemed exports can occur when controlled technical data is released to foreign nationals in the U.S., e.g., employees or contractors.

In addition, if export-controlled technical data is improperly stored, shared or accessed, e.g., in commercial cloud platforms that are not configured for compliant use with controlled technical data, ITAR or EAR violations can occur.

***Potential Impacts***

All defense contractors should be more cautious and deliberate with their compliance going forward. Contractors with prior violations may be able to mitigate enforcement risk by addressing their cybersecurity and export control compliance gaps as soon as possible, and incorporating new procedures for future compliance.

Those that design or build parts, systems or subcomponents for defense applications, particularly — but not only — when they have overseas suppliers, research and development, manufacturing, etc. may face particularly high risks under the ITAR and EAR.

**Recommendations Moving Forward**

- Develop an understanding of the new CMMC program requirements and train employees to recognize and properly handle federal contract information and CUI.
- Improve internal cybersecurity policies and incident reporting procedures to help prevent future violations.
- Audit data, as well as supply chains, especially if working with third parties.

With the CMMC's incorporation of new assessment procedures and outside compliance audits, the risk of discovering unintended violations in some cases may be high.

Contractors that suspect prior cybersecurity or export control violations should act promptly to limit their potential exposure.

---

[1] https://www.federalregister.gov/documents/2025/09/10/2025-17359/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of.

[2] See Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

[3] For more information about CMMC Levels and assessment requirements, see our prior advisory on the topic at What to Expect When the New CMMC Final Rule Hits Defense Acquisitions on November 10 – Troutman Pepper Locke.

[4] See Press Release, U.S. Dep't of Justice, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (last updated Feb.6, 2025), https://www.justice.gov/archives/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.



**RELATED INDUSTRIES + PRACTICES**

- Privacy + Cyber
- Regulatory Investigations, Strategy + Enforcement
- White Collar Litigation + Investigations