Insights: Alerts

After a Short 15-Year Wait, the Government Finally Tries to Define What the Heck Controlled Unclassified Information (CUI) Actually Is, but Questions Still Remain

January 16, 2025

Written by **Gunjan R. Talati, Katherine S. Klein**

Over the last two decades, federal contractors have been frustrated by the Government's hodgepodge approach to regulating Controlled Unclassified Information (CUI). Various agencies have implemented differing definitions, rules, and protections related to CUI and its safeguarding in contractor systems.

In 2010, the Obama Administration issued Executive Order 13556 acknowledging the "inefficient, confusing patchwork" of CUI – and commanding agency heads to create standard categories of CUI categories, safeguarding, and dissemination controls. Finally, on January 14, 2025, almost fifteen years after President Obama's Executive Order, the Federal Acquisition Regulatory (FAR) Council issued a pair of long-awaited proposed regulations, seeking to standardize the protection of CUI and modernize conflicts of interest rules.

The New Proposed Rule

The proposed rule introduces a new standard form (called "SF XXX" in the regulations) to "support uniformity in Governmentwide implementation of [CUI] policies." The proposed rule also adds two new clauses and a provision to enable contractor reporting and compliance responsibilities in Federal solicitations and contracts.

The New Standard Form "SF XXX"

According to the proposed regulations, SF XXX will be included in solicitations and contracts that may result in the handling of CUI that will ultimately become performance requirements during contract performance. Specifically, SF XXX is meant to identify roles and responsibilities for agencies and contractors when:

1. CUI is located on Federal information systems within a Federal facility; or
2. CUI resides on or transits through contractor information systems or within contractor facilities.

Based on the regulations, the contractor shall permit access to CUI only as described in the SF XXX. Moreover, each contractor will need to review SF XXX prior to contract performance to determine what information under the contract is considered CUI and how to properly safeguard the CUI.

If the contractor needs to flow CUI down to a subcontractor, then the contractor will also be required to prepare an SF XXX and distribute it to the subcontractor to ensure the subcontractor properly safeguards CUI. Any

contractor or subcontractor employee that handles CUI will be required to complete training on safeguarding CUI, as specified on the SF XXX.

Proposed FAR Clause - FAR 52.204-XX

Identification of CUI on the SF XXX triggers compliance requirements specified in the new contract clause at FAR 52.204-XX entitled Controlled Unclassified Information.

In what will be familiar to Department of Defense (DoD) contractors, FAR 52.204-XX seems to be modeled after the existing Defense Federal Acquisition Regulation Supplement (DFARS) rules concerning CUI (specifically DFARS 252.204-7012). DFARS 252.204-7012 requires (among other things) contractors to provide adequate security to safeguard CUI when residing on, or transiting through, the contractor's internal information system or network. This clause further requires that all contractors bring their security systems into compliance with all 110 cybersecurity controls established in the National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171 protocols or submit a request to vary from NIST SP 800-171 in writing to the Contracting Officer. For a successful variance request, the contractor must have an alternative, but equally effective, security measure to the NIST SP 800-171 that may be implemented in its place.

As many federal contractors know, the NIST SP 800-171 requirements are extensive, covering 110 security controls, including access control, configuration management, and system and information integrity. If contractors have yet to encounter NIST SP 800-171 standards in federal contracting, one can get a sense of what the system requirements look like by viewing Revision 2 (Revision 3 was published in May 2024 but is not required by the proposed rule). A limited number of contractors may also be required to comply with NIST SP 800-*172* if the CUI stored on or transiting through their system is associated with a critical program or high-value assets. The proposed rule states that contractors subject to these enhanced security requirements "may incur additional process/information technology configuration, network isolation, and security operations center/threat-related costs."

Prime contractors that flow down CUI to subcontractors will also be required to flow down the compliance requirements of the clause at FAR 52.204-XX; a requirement that applies at all subcontract tiers.

Proposed FAR Clause - FAR 52.204-YY

The proposed regulations state that when the contract does not identify CUI, the new contract clause at FAR 52.204-YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information, is used in lieu of the CUI clause.

FAR 52.204-YY requires the contractor to notify the Contracting Officer if there appears to be unmarked or mismarked CUI or a suspected CUI incident related to information handled by the contractor in performance of the contract. This clause also requires the contractor to properly mark proprietary business information to ensure adequate protection. Similar to FAR 52.204-XX, FAR 52.204-YY must be flowed down through all subcontract tiers.

Compliance Considerations

With this new rule comes a new set of compliance concerns for federal contractors. As many federal contractors are aware, prosecutions related to noncompliance with cybersecurity regulations have skyrocketed in recent years, following the launch of the Department of Justice's (DOJ) Civil Cyber-Fraud Initiative in 2021. In a recent enforcement action, Penn State was accused of disregarding federal contracting requirements for protecting

CUI and submitting false claims to the Government. Penn State had several contracts with the DoD, among other government agencies. According to the DOJ, Penn State failed to abide by numerous DFARS clauses related to cybersecurity, including DFARS 252.204-7012 and additionally did not institute NIST SP 800-171 protocols. Allegedly, Penn State submitted false security compliance reports attesting that the school had adopted adequate measures to protect CUI when in fact they had not. According to the Government, Penn State knowingly submitted these false certifications to remain eligible for DOD contracts. In October 2024, Penn State agreed to pay $1.25 million to resolve the allegations.

If the Federal Acquisition Regulatory Council's proposed rule is finalized, the cybersecurity mandates at issue in the Penn State lawsuit and other DOJ actions will become required for all federal contracts. This is likely to lead to an even greater number of DOJ prosecutions.

Currently, contractors are able to comment on this new rule on or before March 17, 2025, via the Federal eRulemaking portal.

Related People

Gunjan R. Talati

t 404.815.6503

gtalati@ktslaw.com

Katherine S. Klein

t 404.745.2447

kklein@ktslaw.com