wiley

ALERT

FAR Council Unveils Long-Anticipated Rule for Controlled Unclassified Information

January 28, 2025

WHAT: The FAR Council published a proposed rule to incorporate the Controlled Unclassified Information (CUI) Program into the acquisition process and, in doing so, seeks to more clearly define government and contractor roles and responsibilities for handling CUI wherever it resides.

WHEN: The proposed rule was published on January 15, 2025. Comments are due by March 17, 2025, but this could be affected by President Trump's January 20, 2025 Executive Order, "Regulatory Freeze Pending Review."

WHAT IT MEANS FOR INDUSTRY: Although the Trump Administration could decide to delay or modify the proposed rule, consistent with its Executive Order titled "Regulatory Freeze Pending Review," federal contractors should prepare for the rule to move forward in some form because it continues a focus on contractor cybersecurity and safeguarding CUI that has stretched across presidential administrations, including the first Trump Administration. Since the Government introduced the CUI program 15 years ago, it has struggled with how to apply the rules being developed to information outside the hands of federal employees and federal networks. This proposed rule is the Government's most significant attempt to address questions that have persisted. Unlike the U.S. Department of Defense (DoD) rules that have preceded it, which focused specifically on the security of contractor information systems that handle CUI (and then, later, how to verify each contractor's compliance), this proposal attempts to create a comprehensive framework for the handling of non-public information related to U.S. government contracts:

Authors

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Lori E. Scheetz
Partner
202.719.7419
lscheetz@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Vaibhavi Patria
Associate
202.719.4667
vpatria@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Cybersecurity

Government Contractors & Grantees

Government Contracts

- **All Non-Public, Unclassified Information:** The proposed rule broadly recognizes two tiers of information regulated under this framework: CUI and other "Covered Federal Information" (previously referred to as Federal Contract Information). Although the proposed rule focuses mostly on CUI, contractors should not neglect the safeguarding requirements and limitations on using Covered Federal Information as well. The proposed rule also reminds contractors that there are different types of CUI, including CUI Basic and different subcategories of CUI Specified, which may have heightened dissemination and security controls.
- **Finally, Some Contract-Specific Government Guidance:** In a long-overdue move, the proposed rule assigns key threshold tasks to Government officials: for each contract, the Government must identify on a proposed Standard Form whether the contractor is expected to handle CUI, and if so, what types of CUI, whether the relevant information system should be considered a Federal Information System, and any other security controls or access restrictions. The proposed rule even contemplates that the safeguarding requirements apply only to CUI that the Government identifies on this new Standard Form. Of course, that line may be of little comfort because, as noted below, contractors must separately verify that the Government's guidance is accurate and report inaccuracies or mismarked CUI within 8 hours.
- **IT Security Requirements:** The proposed rule requires contractors to secure all networks that handle CUI. How they do that depends on the relationship between the network and the underlying contract requirements, whether the network is based on cloud infrastructure, the type of CUI, and the contracting agency's desire for additional protections. Continue reading for our table comparing these requirements.
- **Faster-Than-Rapid Reporting:** The proposed rule also contemplates some of the quickest reporting timelines yet through two different reporting triggers (much faster than DoD's 72-hour "rapidly report" timeframe under DFARS 252.204-7012). First, the proposed rule requires contractors to report "suspected or confirmed" CUI incidents within 8 hours. Second, the proposed rule requires contractors to report any unmarked, mismarked, or unidentified CUI by the Government within 8

International Trade
National Security
Privacy and Cybersecurity Litigation and Investigations
Privacy, Cyber & Data Governance
Telecom, Media & Technology

hours.

- **Contractor Training Required:** The proposed rule also seeks to standardize a training requirement for all contractor employees that might handle CUI, although the proposal defers to individual contracting agencies for many key aspects, including who needs the training, how often, who can provide the training, and any additional topics that must be included.
- **Flowdowns and Further Dissemination:** The proposed rule contemplates that virtually all of these requirements will flow down to subcontractors. This means, among other things, that prime contractors will need to prepare a Standard Form providing contract-specific guidance to each of their subcontractors, just as the Government must do for each prime contract.
- **Verification & Enforcement:** The Government chose not to require what it described as a "100 percent inspection requirement" as part of this framework. Instead, however, it reserved broad rights to inspect contractor compliance, added financial consequences when a contractor is "at fault for a CUI incident," and reminded everyone of the Government's many broad enforcement tools.

Background

This FAR proposed rule has been many years in the making. Almost 15 years ago, President Obama issued Executive Order 13556, Controlled Unclassified Information. That EO kicked off a program for managing unclassified information that still requires safeguarding or dissemination controls under existing law, regulation, or government-wide policy. To implement the EO, the National Archives and Records Administration (NARA) issued a final rule in 2016 that established policies for agencies on designating, marking, safeguarding, disseminating, and disposing of CUI, which was codified at 32 CFR Part 2002.

NARA's final rule defined CUI; established two principal categories (CUI Basic & CUI Specified); and designated itself as the executive agent responsible for maintaining a comprehensive "Registry" that catalogs the types of information that qualify as CUI, the underlying statutory, regulatory, or policy basis for the restrictions, and any specific markings, dissemination restrictions, or other policies.

NARA intended for agencies to incorporate these requirements into their procurement contracts. 32 CFR 2002.4(c) ("When disseminating or sharing CUI with non-executive branch entities, agencies *should* enter into written agreements or arrangements that include CUI provisions *whenever feasible*."). But the FAR Council has taken its time deciding how to do so. Meanwhile, DoD prescribed a series of its own contract clauses dealing primarily with contractor information systems that handle CUI, and other agencies have taken *ad hoc* approaches to protecting CUI shared with their contractors. This proposal, which has been in process for roughly eight years, reflects the FAR Council's attempt to comprehensively address CUI.

Structure of the Proposed Rule

The proposed rule implements these policies through four principal additions to the FAR:

- **Internal FAR Guidance**: The proposed rule adds FAR 4.403 (Controlled Unclassified Information) and FAR 4.404 (Basic Safeguarding of Covered Contractor Information Systems), which provide guidance to

contracting officers on how to implement the requirements in this proposed rule, including which clauses to include in future solicitations and contracts. The proposed rule also makes complementary changes to several other sections of the FAR that provide guidance to contracting officers on such topics as acquisition planning and describing agency needs.

- **Expected CUI Contract Clause and Form:** The proposed rule adds FAR 52.204-XX (Controlled Unclassified Information) and an accompanying Standard Form XXX. These items will be included in all contracts for which the requiring activity within the Government has determined that the contractor "is expected to collect, develop, receive, transmit, use, handle, or store CUI under this contract." This clause implements the requirements discussed throughout this summary.
- **Unexpected CUI Contract Clause:** The proposed rule adds FAR 52.204–YY (Identifying and Reporting Information That Is Potentially Controlled Unclassified Information) for all other contracts for which the requiring activity does not expect the contractor to handle CUI. This clause is more limited, but it still has several significant requirements. Most significantly, this clause requires contractors to notify the contracting officer within 8 hours of discovery if the contractor identifies any information that the contractor "believes, or has reason to know, is CUI." It also includes a broad nondisclosure obligation, which prohibits the contractor from using any non-public "Government-provided information for its own purposes" regardless of whether that information is CUI.
- **General CUI Solicitation Provision:** The proposed rule adds FAR 52.204–WW (Notice of Controlled Unclassified Information Requirements) for all solicitations. This provision contemplates that agencies may need to share CUI with contractors before awarding a contract. Among other things, it also provides that offerors "should" notify the contracting officer within 8 hours of discovering any CUI that was not marked, nor marked properly, or not identified in the Standard Form XXX associated with the future contract. It also includes the same broad non-disclosure obligation noted above.

The proposed rule also includes conforming edits to the terms and conditions for contracts for commercial products or commercial services because this rule applies to all contracts except those exclusively for commercially available off-the-shelf (COTS) items. The following sections provide more detail on the substance of the requirements implemented through these new additions to the FAR.

Defining CUI, Including Basic and Specified

As noted above, NARA previously defined CUI and the two subcategories of CUI Basic and CUI Specified. This proposed rule elaborates on the CUI definition by introducing two exceptions beyond those specifically articulated by NARA, although neither meaningfully changes its scope. The proposed rule also adopts NARA's definitions for the two categories of CUI – CUI Basic and CUI Specified. This distinction informs the relevant security controls applicable under the proposed rule.

Controlled Unclassified Information. NARA's regulations define CUI as unclassified "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." 32 CFR 2002.4(h). This proposed rule clarifies two additional

exceptions not expressly stated in NARA's rules.

First, it excludes from the CUI definition "Covered Federal information," which was previously known as "Federal Contract Information." This exclusion in the CUI definition, however, is redundant, because the proposed rule defines Covered Federal Information as essentially all non-public "information provided by or created for the Government" that does not qualify as CUI. The only other limiting principles for the definition of Covered Federal Information is that it cannot be "simple transaction information" (such as those necessary to process payments) or federally funded basic and applied research (discussed below).

Second, the proposed rule excludes from the CUI definition "[f]ederally-funded basic and applied research in science, technology, and engineering at colleges, universities, and laboratories." The proposed rule based this exclusion on National Security Decision Directive 189. Issued in 1985, this directive establishes the United States' policy that "to the maximum extent possible, the products of fundamental research remain unrestricted." It also provides that the Government may restrict the "conduct or reporting" of such research only through the classification system. Because CUI necessarily excludes classified information, the CUI program cannot restrict this information.

CUI Basic and CUI Specified. NARA differentiates between CUI Basic and CUI Specified by looking to whether the underlying statute, regulation, or policy provides specific controls for the information. 32 CFR 2002.4(h). For example, export-controlled material is CUI Specified because the laws governing it specifically restrict disclosure to foreign persons. Meanwhile, source selection information is CUI Basic because the Procurement Integrity Act only broadly prohibits its disclosure.

Contract-Specific Guidance from the Government, Finally Required

In a long overdue move, the proposed rule assigns key threshold tasks to Government officials: for each contract, the Government (specifically, the requiring activity) must identify several important pieces of information that contractors need to better understand their obligations under the CUI program. This includes whether the Government expects the contractor to handle CUI, which will determine which of the two clauses the Government includes in the contract.

If the Government expects that the contractor will handle CUI, it must also provide more information, including, what types of CUI, any special restrictions on that CUI, and where the contractor might handle it (at a Government facility only, or on the contractor's network). If the contractor will handle CUI on its network, the Government must also indicate whether it considers the network to be a federal or a non-federal (i.e., contractor) information system (a distinction discussed more below).

The Government must articulate these and many other items in a Standard Form that will be incorporated into the solicitation and then, eventually, the awarded contract. The proposed rule even contemplates that the safeguarding requirements apply only to CUI that the Government identifies on this new Standard Form. But that scoping line may not limit the contractor's responsibility as much as it seems on first glance because, as noted below, contractors still have to verify that the Government's guidance is accurate and even have to report inaccuracies or mismarked CUI within 8 hours. Still, that scoping point could be important if the

Government alters the contractor's security obligations and those changes increase the contractor's costs to perform the contract.

Safeguarding Requirements

Unlike each of the previous safeguarding rules to precede it, this proposed rule seeks to comprehensively define the security controls that contractors must follow to protect all types of CUI on all types of information systems. As summarized in the table at the end of this section, the applicable controls depend principally on four questions.

1. **Who controls the facility or the information system?**

The proposed rule recognizes that some contractors access CUI solely on government-provided resources. Under these circumstances, the proposed rule requires contractors to follow the agency's policies and procedures. It also requires the agency to identify those policies in the Standard Form.

2. **If the contractor controls the information system, is it doing so "on behalf of the agency"?**

If the contractor is going to handle CUI on an information system that it controls, the security requirements depend on whether the information system meets the definition of a "Federal Information System." Consistent with the Federal Information Security Modernization Act (FISMA), the proposed rule defines "Federal Information System" to mean an information system "used or operated by an agency, by a contractor of an agency, or by another organization on behalf of an agency." The proposed rule also clarifies that "on behalf of" refers to activities that are "not incidental to providing a service or product to the Government." Thus, in many cases, this classification turns on whether the contractor is operating the information system as part of its responsibilities expressed in the statement of work, rather than merely using it internally to manage information related to the contract.

3. **Is the information system using cloud services?**

For either type of information system controlled by a contractor, the minimum requirements under the proposed rule will depend on whether the information system uses cloud services. For all cloud services – which are essential to virtually all contractor information systems today – the contractor must ensure that the cloud service provider meets the FedRAMP Moderate baseline.

Unlike DoD's rules, this proposed rule does not allow for an "equivalency" determination, although the equivalency standard has been less meaningful since DoD narrowed its view of "equivalency" in December 2023. This means contractors will need to inventory the cloud services that they rely upon and ensure each one has been authorized under the FedRAMP program. Although the FedRAMP marketplace maintains a list of authorized cloud service offerings, contractors should verify with their provider that the cloud service they are using is within the scope of the provider's FedRAMP authorization. This is particularly important for those less familiar with the FedRAMP marketplace because many cloud service providers use different infrastructure to provide essentially the same service to government and commercial customers.

4. **Does the agency or the type of information require additional security controls?**

In addition to the minimum security controls determined through the three steps above, the proposed rule also allows agencies to specify additional security controls.

Facility/System Control

Type of Information System

Cloud-Based

Non-Cloud Based

CUI located within a Federally-controlled facility

Federal Information System

> The Contractor shall follow agency CUI policies and shall ensure that any Contractor employees handling CUI with Federally-controlled facilities meet the prerequisites identified within the Standard Form for training and access

CUI located within a non-Federally-controlled facility

Federal Information System

> The Contractor shall comply with agency-identified security requirements, but at no less than the ***FedRAMP Moderate*** baseline
>
> The Contractor shall comply with agency-identified security requirements from the latest version of ***NIST SP 800–53*** and ***any CUI Specified requirements*** identified in the Standard Form

Non-Federal Information System

> The cloud service provider must meet security requirements established by the Government for the ***FedRAMP Moderate*** baseline
>
> The Contractor shall comply with ***NIST SP 800-171, Revision 2*** Agencies may also require specific additional controls from NIST SP 800-171 or other sources (for either CUI Basic or CUI Specified)

Eight-Hour Incident and Mismarking Reporting Requirements

The proposed rule requires contractors to report on two types of events within 8 hours of discovery: (1) CUI incidents and (2) mismarked, unmarked, or unidentified CUI. This is significantly faster than the 72-hour timeline for "rapidly reporting" incidents under DoD contracts (although consistent with the requirement in Department of Homeland Security contracts to report within 8 hours cybersecurity incidents that could affect CUI).

CUI Incidents. The proposed rule would require contractors to report any "suspected or confirmed CUI incident" within 8 hours of discovery. The proposed rule defines a CUI incident as "improper access, use, disclosure, modification, or destruction of CUI, in any form or medium." This approach is potentially narrower than DoD's approach. DoD defines its key reportable event – a "cyber incident" – to include anytime there's a potential adverse effect on "an information system and/or the information residing therein."

Contractors would report these CUI incidents to the "agency website or single point of contact" identified in the Standard Form. Although the proposed rule contemplates reporting outside the DIBNET portal, it still looks to the DIBNET portal to define the information to include in any report. Specifically, it requires contractors to include "as many of the applicable data elements located at *https://dibnet.dod.mil/ portal/ intranet/* as are available," and provide "any remaining applicable data elements as soon as they become available" thereafter. The proposed rule also requires the contractor to determine what CUI was accessed, construct a timeline of user activity, and provide a determination of the methods and techniques used to access the CUI.

The proposed rule would require contractors to preserve images, media, and data related to CUI incidents for 90 days from the submission of the incident report. During this period, the Government could request that information or formally decline interest. The preservation obligation would terminate upon the earlier of the contractor's receipt of a declination of interest from the Government or 90 days if the Government did not request the information.

Mismarked, Unmarked, or Unidentified CUI. The proposed rule would also require contractors (and encourages offerors) to report additional events even when no CUI is compromised. These events relate principally to the Government's obligation to accurately identify and mark CUI in the first instance. And these triggers are included in both standard clauses, so they apply even if the Government had told the contractor that it does not expect the contractor to handle CUI.

The proposed clause at FAR 52.204-YY (which is included when the contractor is not expected to handle CUI) requires contractors to report "any information that the contractor believes, or has reason to know, is CUI." This can include information that was marked, unmarked, or improperly marked. The contractor must then safeguard that information until the contracting officer coordinates with the requiring activity and determines whether it is, in fact, CUI. If the information turns out to be CUI, the contracting officer will then have to decide whether the contractor needs access and, if so, how to modify the contract. The proposed rule at least recognizes that this could constitute a change and require it to consider an equitable adjustment to the contract.

The proposed clause at FAR 52.204-XX includes a similar requirement for unmarked or mismarked CUI but also adds reporting criteria related to the accuracy of the Government's Standard Form. In particular, the proposed rule would require contractors to report any CUI not identified in the Standard Form, any CUI not marked properly as required by the Standard Form, and any inconsistency between the contract clauses and the Standard Form.

The proposed solicitation provision at FAR 52.204-WW stops short of requiring prospective offerors to make any specific notification. Instead, it provides that "[o]fferors *should* notify the Contracting Officer within 8 hours of discovery if the Offeror discovers any CUI that is not marked, not properly marked, or not identified on the [Standard Form], or is involved in a suspected or confirmed CUI incident."

Contractor Training Requirements

The proposed rule also requires contractors to ensure that their employees complete CUI training before they handle any CUI. At a minimum, this would include general CUI training and periodic refresher training every two years. But the proposed rule allows agencies to specify additional training criteria. These additional criteria can include more frequent training, training on additional topics, who can provide the training, and whether to accept training provided under a different contract. The proposed rule requires agencies to communicate these other criteria in the Standard Form. Contractors must also maintain documentation of employee training and will be required to provide it to the Contracting Officer upon request.

Flowdown and Further Dissemination

The proposed rule contemplates that virtually all of these requirements will apply to subcontractors as well. As a result, if a prime contractor expects its subcontractor to handle CUI, the proposed rule requires it to prepare a Standard Form that provides all of the types of information discussed above that the Government must provide to its prime contractors. The proposed rule also contemplates that subcontractors will notify the prime contractor or next higher-tier subcontractor of incidents within the same 8-hour window. The proposed rule is not clear as to whether this is in addition to or instead of reporting to the agency website or single point of contact.

Verification and Potential Enforcement Tools

In explaining alternatives that the FAR Council considered, it noted that it did not believe it necessary to adopt a "100 percent inspection requirement." The proposed rule also reminded contracting officers that they should not interpret a contractor's CUI incident report to mean that any entity or person failed to provide adequate safeguards. Contractors, however, should find little comfort in these statements because the Government still retains significant authority to inspect the contractor's compliance at any time, and it has many means for enforcement. Just as the Government has threatened or done with other cybersecurity requirements, it could attempt to leverage its wide-ranging enforcement tools, including contractual remedies, suspension or debarment, and False Claims Act actions.

Moreover, with this proposed rule, the Government specifically provided that contractors "may be financially liable" for the Government's response costs "in addition to any other damages at law or remedies available to the Government for noncompliance" if the contractor "is determined to be at fault for a CUI incident." The proposed rule does not specify how the Government would pursue such a claim, but we would expect that the contracting officer would have to do so on behalf of the Government under the Contract Disputes Act.

***

The FAR Council concluded its preamble to this proposed rule by requesting comments on several specific topics, including whether there is other information or guidance necessary to comply with this rule; whether there are specific situations in which contractors would be required to report on different timelines to comply with the CUI incident reporting requirements for this proposed rule, other contract requirements, or other federal regulations, as well how the contractor would handle such disparate reporting timelines; and the financial impact of this proposed rule on the products and services provided to the Government.

Wiley's cross-disciplinary Government Contracts, Privacy, Cyber & Data Governance, Telecom, Media & Technology, and National Security teams have helped companies of all sizes from various sectors proactively address risks and compliance with new cybersecurity laws and requirements. Please reach out to any of the authors with questions.