

William F. Clark
Director, Office of Government-wide Acquisition Policy
Office of Government-wide Policy
General Services Administration
1800 F Street, NW
Washington, DC 20405

Comments regarding FAR Case 2017-016, “Federal Acquisition Regulation: Controlled Unclassified Information” (Proposed Rule), submitted at
<https://www.regulations.gov/commenton/FAR-2017-0016-0001>

Dear Mr. Clark:

On behalf of the American Council on Education (ACE), the Association of American Universities (AAU), the Association of Public and Land-grant Universities (APLU), COGR, and EDUCAUSE, we would like to thank you for the opportunity to provide input regarding FAR Case 2017-016. Our organizations are described as follows:

- ACE is the American Council on Education, the major coordinating body for American higher education. Its more than 1,700 members reflect the extraordinary breadth and contributions of public and private colleges and universities. ACE members educate two out of every three students in accredited, degree granting U.S. institutions.
- The Association of American Universities (AAU) represents 69 of America’s leading research universities. Our members are public and private research universities on the cutting edge of innovation, scholarship, and solutions that contribute to scientific progress, economic development, national security, and public health.
- APLU is a membership organization that fosters a community of university leaders collectively working to advance the mission of public research universities. The association’s U.S membership consists of more than 230 public research universities, land-grant institutions, state university systems, and affiliated organizations spanning across all 50 states, the District of Columbia, and six U.S. territories. The association and its members collectively focus on increasing student success and workforce readiness; promoting pathbreaking scientific research; and bolstering economic and community engagement.
- COGR is the national authority on federal policies and regulations affecting U.S. research institutions. We provide a unified voice for over 225 research universities, affiliated academic medical centers, and research institutes. Our work strengthens the research partnership between the federal government and research institutions and furthers the frontiers of science, technology, and knowledge. We advocate for effective and efficient research policies and regulations that maximize and safeguard research investments and minimize administrative and cost burdens.

- As the association for advancing higher education through information technology (IT), EDUCAUSE represents nearly 2,200 colleges, universities, and related organizations. Higher education IT leaders and professionals at all levels work together through EDUCAUSE to develop and strengthen the role of technology in helping colleges and universities to achieve their missions.

Higher education institutions contract with federal agencies in a variety of capacities, and thus appropriate guidance on the identification, management, and security of controlled unclassified information (CUI) is important to our members. Our associations appreciate the efforts of your office and the FAR Council to develop such guidance, and we hope that our comments will help to strengthen the final rule.

With that goal in mind, we offer our thoughts and recommendations in the following areas:

- Definitions
 - Controlled Unclassified Information (CUI)
 - Covered Federal Information (CFI)
- CUI Management
 - Unmarked or Mismarked CUI
 - Key Deadlines
- Training Requirements
- Security Requirements for Patents
- Updating CUI Marking Guidance (for further discussion)

Definitions

Controlled Unclassified Information (CUI)

We note that the definition of CUI provided throughout the proposed rule does not match exactly with the definition provided in the CUI Program rule at [32 CFR 2002\(h\)](#) and referenced in the Cybersecurity Maturity Model Certification (CMMC) Program rule at [32 CFR 170.4\(b\)](#). Given that the CUI Program rule establishes the uniform framework for the identification and handling of CUI throughout the federal government, as reflected in the CMMC Program rule, the proposed revisions to the Federal Acquisition Regulation (FAR) to incorporate the CUI Program rule requirements should reference the CUI Program rule definition. This would ensure consistent reference to the authoritative source wherever the term appears and facilitate uniform understanding and application of the CUI Program rule, which aligns with its intent.

It is clear that the differences between the definition of CUI in the proposed rule versus the CUI Program rule stem in part from a desire to incorporate the proposed exclusions from the definition's scope in the FAR version. The proposed rule could reference the CUI Program rule

definition while still including a separate provision on exclusions where necessary, however. That would support the objective of highlighting those exclusions while allowing for the consistent use of the governing definition of CUI provided in the CUI Program rule.

We support the notice of proposed rulemaking (NPRM) excluding “federally-funded basic and applied research in science, technology and engineering at colleges, universities, and laboratories in accordance with National Security Decision Directive 189” from the definition of Covered Federal Information in FAR 4.404-1 and from the requirement to include FAR 52.204-21, “Basic Safeguarding of Covered Contractor Information Systems,” in solicitations and contracts. However, the NSDD-189 definition of “fundamental research” should be considered a starting point for federal contracting with higher education research institutions. It should not be a limiting factor in determining the types of basic and applied research that the government considers “fundamental research.”

The repeated references in the NPRM to “basic and applied research in science, technology, and engineering” imply that fundamental research for which the government might contract in other fields may not be excluded from the proposed definition of CUI. Treating such research as CUI would impose cybersecurity requirements on it that run counter to its essential nature-- that it is intended for public release. As a result, researchers and institutions might feel compelled to forgo conducting fundamental research in fields outside of science, technology, or engineering for the government, severely limiting the government’s options for meeting vital needs.

Covered Federal Information (CFI)

The proposed definition of “Covered Federal Information” (CFI)¹ that is intended to replace the definition of “Federal Contract Information” (FCI)² also raises potential barriers to fundamental research. The definition of FCI that is incorporated in the current version of “Basic Safeguarding of Covered Contractor Information Systems”³ makes clear that its scope is limited to data “not intended for public release.” Thus, fundamental research, regardless of field, is excluded from FCI and the accompanying safeguarding requirements. This is important because, as our associations discussed in our comments on the initial version of the CMMC Program rule,⁴ security requirements for what is essentially administrative data are a poor fit for academic research.

¹ DOD, GSA, and NASA, “Federal Acquisition Regulation: Controlled Unclassified Information,” *Federal Register*, January 15, 2025, p. 4293 (<https://www.federalregister.gov/d/2024-30437/p-294>).

² Federal Acquisition Regulation (FAR) 52.204-21(a), “Basic Safeguarding of Covered Contractor Information Systems: Definitions,” (https://www.acquisition.gov/far/52.204-21#FAR_52_204_21_d3096e18).

³ FAR 52.204-21, “Basic Safeguarding,” (https://www.acquisition.gov/far/part-52#FAR_52_204_21).

⁴ Comments of COGR, EDUCAUSE, the Association of American Universities (AAU), the Association of Public and Land-grant Universities (APLU), and the American Council on Education (ACE) on RIN 0750-AK81 (DFARS Case 2019-D041), “Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041),” November 20, 2020, p.2 (<https://library.educause.edu/-/media/files/library/2020/11/commentsdfarscase2019d041.pdf>).

The proposed definition of CFI mirrors the proposed CUI definition by highlighting the specific exclusion of fundamental research in science, technology, and engineering, which again raises the question of whether fundamental research in other academic fields will be considered CFI if it is not considered CUI. As with the proposed definition of CUI, we urge you to revise the proposed CFI definition to ensure that fundamental research remains excluded from the “Basic Safeguarding” requirements regardless of academic field. Much of the fundamental research for which the government contracts likely falls into the fields identified in the proposed rule’s exclusion—science, technology, and engineering. However, federal agencies may need fundamental research in other academic fields given the range of missions and issues they tackle. The “Basic Safeguarding” requirements could present a significant barrier to that research since they often do not align with the open, collaborative research environments that are central to fundamental research. Ensuring access to fundamental research of whatever kind an agency may need requires that fundamental research in general continues to be excluded from CFI or CUI security requirements (except for edge cases in which the government supplies CFI or CUI for use in the research to be conducted).

As mentioned in our discussion of the CUI Program rule definition of CUI, consistency and uniformity in the definition and use of terms across related federal regulations is very important to higher education research institutions. Since researchers and institutions may conduct research for a number of different agencies, having standard terms and requirements among them wherever possible facilitates greater efficiency and ease of compliance. Thus, it is worth noting that the proposed change from FCI to CFI in the FAR would require revisions to the CMMC Program rule as well, which might shift the ground for institutional compliance with CMMC. The definition of FCI in the CMMC Program rule at 32 CFR 170.4(b)⁵ references the FCI definition in the FAR as previously cited. Thus, the proposed change in the FAR would need to be carried through the CMMC Program rule as well to ensure accuracy and consistency. In the process, it might substantially alter the established exclusion of fundamental research in general from CMMC Level 1 certification, adding to the possible problems regarding federal access to fundamental research that we have highlighted.

CUI Management

We appreciate the effort to bring clarity to when a project includes CUI, what data in the project is considered CUI, and how it should be marked and handled. The introduction of the SF XXX will hopefully ensure a shared understanding of those issues throughout the solicitation, contracting, and performance processes. With that end in mind, we particularly applaud the requirement contained in 4.403-04 that “[t]he requiring activity will identify any CUI in...” the SF-XXX “...which must be incorporated in the contract.”⁶

⁵ See 32 CFR 170.4(b), “Definitions—Federal Contract Information (FCI)”:
[https://www.ecfr.gov/current/title-32/part-170#p-170.4\(b\)\(Federal%20Contract%20Information%20\(FCI\)\)](https://www.ecfr.gov/current/title-32/part-170#p-170.4(b)(Federal%20Contract%20Information%20(FCI))).

⁶ DOD, GSA, and NASA, “Federal Acquisition Regulation: Controlled Unclassified Information,” *Federal Register*, January 15, 2025, p. 4292 (<https://www.federalregister.gov/d/2024-30437/p-258>).

Likewise, we fully support the use of NIST SP 800-171, Revision 2, (800-171 Rev. 2) in the notice of proposed rulemaking (NPRM) as the cybersecurity standard for CUI.⁷ The 800-171 Rev. 2 use aligns with the Defense Federal Acquisition Regulation Supplement (DFARS) requirements for the Cybersecurity Maturity Model Certification (CMMC) program. It will provide a more streamlined framework to ease the compliance burden for research institutions that contract with defense and non-defense agencies.

Unmarked or Mismarked CUI

We are concerned, however, with the exception to FAR 4.403.04 in FAR 52.204-XX(c)(2) and the contractor's obligations in FAR 52.204-XX(c)(3) to report a CUI incident.⁸ The requirement in FAR 52.204-XX(c)(2) that a contractor must act to safeguard information that the contractor may believe is CUI despite SF-XXX indicating no CUI is to be handled under the contract or the information being improperly marked places an unreasonable burden on the contractor by (i) presuming all contractor employees are sufficiently "skilled in the art" to determine information is CUI and (ii) unfairly shifting the liability for properly identifying unmarked CUI to the contractor.

The absence of clear markings or identification disincentivizes agencies from adopting concise marking procedures and makes it extremely difficult for the contractor to properly manage, handle, and safeguard the information, resulting in an increased potential for a CUI incident. Additionally, the obligations and cost to the contractor to train its employees will likely increase exponentially. As a result of the exception in FAR 52.204-XX(c)(2), a contractor will need to train all employees in accordance with FAR 52.204-XX(f), not just employees identified to perform under the contract.

The recognition in the proposed rule that the presence of unmarked or mismarked CUI would not constitute a CUI incident subject to reporting requirements unless it led to mishandling or inappropriate dissemination of CUI appropriately limits the scope of required reporting, thereby lessening the potential reporting burden. However, it unfortunately would not mitigate the expansive training burden that the contractor reporting requirements on unmarked/ mismarked CUI create because any access by a contractor employee who is not also covered by the contract would constitute a CUI incident in the absence of such training.

We recognize that everyone has a shared responsibility to help prevent the accidental disclosure of sensitive information. However, for the reasons above, our associations ask that a more balanced approach be considered in handling and assuming responsibility for transferring unmarked or mismarked CUI.

⁷ Ibid, p. 4298 (<https://www.federalregister.gov/d/2024-30437/p-420>).

⁸ Ibid (<https://www.federalregister.gov/d/2024-30437/p-397>).

Key Deadlines

The proposed ninety-day (90-day) limitation (in the absence of an agency request) on the period that images of systems involved in suspected or actual CUI incidents have to be held addresses a practical problem that other cyber incident regulations often overlook—the cost and operational difficulties associated with indefinitely maintaining incident information. The ninety-day requirement fairly balances the government’s potential need for such information against the burden that preserving the information imposes, and we appreciate its inclusion.

On the other hand, we are concerned that the proposed eight-hour (8-hour) deadline for reporting discovered or suspected unmarked or mismarked CUI and/or suspected or confirmed CUI incidents to the relevant contracting officer would impose an undue burden on our member institutions.⁹ In many instances, researchers and staff will still be gathering and assessing information during the initial eight hours in which a potential problem has surfaced. Such a tight deadline will no doubt generate significant over-reporting out of an abundance of caution, especially given the inclusion of suspected cases in the requirement, which will ultimately make it less likely that the government connects and collaborates with institutions on actual issues of concern.

Also, many institutions do not have a twenty-four-by-seven (24x7), year-round Security Operations Center that might allow for the identification and reporting of actual or suspected cases or incidents within an eight-hour period. Imposing a reporting deadline that assumes capacities that many covered entities are likely to lack would unnecessarily create administrative and financial burdens that some institutions cannot bear. This would, in turn, likely constrain the availability of research to federal agencies.

Furthermore, the NPRM indicates that the rule is modeled on DFARS 252.204.7012,¹⁰ which in the case of the proposed rule’s reliance on 800-171 Rev. 2 facilitates consistency in compliance with CUI requirements across both the defense and non-defense contexts. That said, the proposed rule’s eight-hour deadline for incident reporting is not aligned with the DFARS 7012 provision on incident reporting, which establishes a seventy-two (72) hour deadline.¹¹ The longer timeframe in DFARS 7012 is more reasonable given the coordination, communication, and collaboration needed to assess potential cyber incidents effectively. It is notable that this longer reporting timeframe relates to cyber incidents, where the much tighter deadline in the proposed rule applies not just to CUI incidents but also to situations involving unmarked or mismarked CUI that the rule itself stipulates do not constitute incidents. To facilitate compliance across both the defense and non-defense contexts while allowing for more effective problem assessment and more constructive reporting to the government, the

⁹ Ibid, p. 4297 (<https://www.federalregister.gov/d/2024-30437/p-367>).

¹⁰ Ibid, p. 4282 (<https://www.federalregister.gov/d/2024-30437/p-78>).

¹¹ 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>): See 252.204-7012(a), “Definitions”—“Rapidly report,” and -7012(c), “Cyber incident reporting requirement,” Part (ii).

proposed rule should align its reporting deadline to the seventy-two hour deadline included in DFARS 252.204.7012.

Finally, to ensure clarity, we recommend that the proposed 52.204-WW(d), “Unmarked or mismarked CUI,”¹² should note that guidelines for providing appropriate notice regarding unmarked or mismarked CUI and/or CUI incidents are provided in 52.204-XX, “Controlled Unclassified Information,”¹³ or 52.204-YY, “Identifying and Reporting Information That Is Potentially Controlled Unclassified Information,”¹⁴ respectively, whichever is relevant to the contract in question.

Training Requirements

In addition to our concern with training caused by the exception in FAR 52.204-XX(c)(2), the proposed rule’s training requirements for agency-identified CUI require further guidance. The range of contractor staff activities that might pull a given staff person under the proposed training requirements is expansive. Without further guidance, it could be interpreted as applying training requirements to staff that are not actually exposed to the CUI in question in a meaningful way. Moreover, since agency directives on CUI training may vary from agency to agency or one agency SF XXX to another, and since a higher education research institution may have many different research contracts with many different federal agencies, the training provisions of the proposed rule could lead to a nearly constant state and variability of training across far more institutional staff than are actually relevant to the projects in question.

The proposed 52.204-XX(d)(4) states the following: “No Contractor employee shall be permitted to have or retain access to, create, collect, use, process, store, maintain, disseminate, disclose, dispose of, or otherwise handle CUI unless the employee has completed training on properly handling CUI that, at a minimum, includes the elements required in the SF XXX.”¹⁵ Depending on how terms such as “process,” “store,” “maintain,” “dispose of,” or “otherwise handle” are interpreted, the provision could conceivably apply to networking or other IT professionals as well as research staff who are not truly interacting with the CUI in question, but whose work in support of the relevant research might entail, for example, establishing and maintaining the network enclaves in which research data is manipulated, processed, and stored. The catch-all term of “otherwise handle” may readily lead to the interpretation that any staff who work with anything that CUI touches, whether the staff in question touch the CUI at all, must undergo the specific training called for in any and all SF XXXs for activities that might possibly cross their operational domains. This would create unbearably burdensome outcomes.

¹² DOD, GSA, and NASA, “Federal Acquisition Regulation: Controlled Unclassified Information,” *Federal Register*, January 15, 2025, p. 4297 (<https://www.federalregister.gov/d/2024-30437/p-367>).

¹³ Ibid, p. 4298 (<https://www.federalregister.gov/d/2024-30437/p-397>).

¹⁴ Ibid, p. 4300 (<https://www.federalregister.gov/d/2024-30437/p-484>).

¹⁵ Ibid, p. 4298 (<https://www.federalregister.gov/d/2024-30437/p-414>).

Fortunately, the proposed SF XXX, Part C, itself provides a ready solution to this unintended consequence. In Section III, “Training Requirements,” Part (a), “General training,” the form states that “[t]he Contractor must ensure all Contractor employees *accessing or generating CUI in association with this contract* complete initial general CUI training prior to accessing CUI” (emphasis added).¹⁶ Part (b) of the section continues by requiring the delineation of any CUI for which specific training is necessary and for which group of contractor employees.¹⁷ The text in these parts of SF XXX provides a good indication of the reasonable scope of staff and training that the proposed rule envisions. We recommend that 52.204-XX(d)(4) be revised to reflect the emphasis on training for employees “accessing or generating CUI in association with the contract” and the targeting of any unique training requirements to specific categories of CUI and relevant employees as identified in the SF XXX. Such a change should appropriately tailor the training requirements of the proposed rule to the actual training needs that the inclusion of CUI in a given contract presents.

Security Requirement for Patents

We are concerned about the proposed amendment to FAR 27.203, “Security Requirements for Patent Applications Containing Classified Subject Matter,” which under the proposed rule would become “Security requirements for patent applications and other patent information” and include “patent applications or other patent-related” CUI.¹⁸ Under the Bayh-Dole Act, universities and research institutions are responsible for licensing the discoveries and intellectual property resulting from federally-funded research to benefit the public. Including patent applications related to CUI in the review and approval process outlined by FAR 27.203 could negatively affect our members’ technology transfer efforts. Delays imposed by the review process could result in the loss of the right to file a patent application in the U.S. or other jurisdictions, as many jurisdictions follow a ‘first-to-file’ system. Under this system, the first party to file a patent application for an invention is granted the rights to the patent, potentially excluding others who may have developed the same or similar technology. As such, delays could jeopardize the ability to secure patent protection, both in the U.S. and internationally.

We encourage you to engage directly with our community to better understand these concerns and ensure that the United States maintains its leadership in commercializing innovations arising from federally funded research.

For Discussion: Updating CUI Marking Guidance

While it is beyond the scope of the NPRM, we wanted to raise an issue for discussion among the stakeholders in CUI management, including the National Archives and Records Administration (NARA). Since data transfers would fall under CUI management per the proposed rule, it may be time to revise the CUI Marking Handbook to require the inclusion of CUI markings in the names of digital files, feeds, code, containers, algorithms, integrations, and

¹⁶ Ibid, p. 4302 (<https://www.federalregister.gov/d/2024-30437/page-4302>).

¹⁷ Ibid, p. 4303 (<https://www.federalregister.gov/d/2024-30437/page-4303>).

¹⁸ Ibid, p. 4295 (<https://www.federalregister.gov/d/2024-30437/p-amd-58>).

so forth. This may be the best way to ensure recognition of CUI by recipients' systems and the appropriate handling of CUI in transferred files, especially as encryption mandates increase. One may argue, however, that including CUI markings in filenames might increase security risks by making it easier for bad actors to identify the CUI that they want to extract. Balancing effectiveness, efficiency, and security is a constant challenge as the government strives to improve CUI management and security. Determining whether to mandate such a requirement via the CUI Marking Handbook should involve a range of relevant parties. We encourage the FAR Council to initiate such a process at its earliest opportunity.

Again, we thank the agencies and representatives involved in the development of the proposed rule for their significant, thoughtful efforts. We look forward to continued progress toward the final rule and the opportunity to provide further input should it arise.

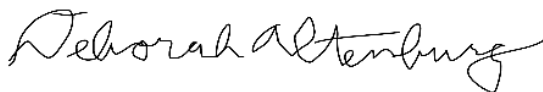
Sincerely,



Sarah Spreitzer
Vice President and Chief of Staff
Government Relations
American Council on Education



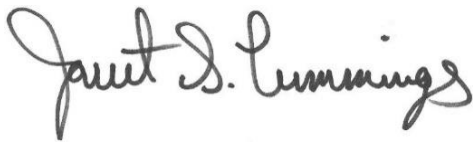
Tobin L. Smith
Senior Vice President
Government Relations and Public Policy
Association of American Universities



Deborah Altenburg
Vice President
Research Policy and Advocacy
Association of Public and Land-Grant Universities

A stylized, handwritten signature in black ink, appearing to be 'KW'.

Kevin Wozniak
Director
Research Security and Intellectual Property
COGR

A handwritten signature in black ink that reads 'Jarret S. Cummings'.

Jarret S. Cummings
Senior Advisor
Policy and Government Relations
EDUCAUSE