THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement

NOVEMBER 26, 2024 | VOLUME 66 | ISSUE 44

¶ 324 FEATURE COMMENT: The CUI Program: DOD, We Have A Problem (Part I)

Introduction—Almost five years after it was first announced, the U.S. Department of Defense's Cybersecurity Maturity Model Certification (CMMC) Program will finally become operational at some point in fiscal year 2025. On Oct. 15, 2024, DOD issued a Final Rule creating 32 CFR pt. 170 to address evolving cybersecurity requirements and cyber threats while defining the security controls that DOD intends defense contractors and subcontractors to implement. The program, which takes effect Dec. 16, 2024, will require defense contractors and subcontractors to obtain the requisite certification level depending on whether their respective information systems will process, store, or transmit Federal Contract Information and/or Controlled Unclassified Information (CUI). This answer, however, spawned a litany of questions during the public comment period, most notably around the area of CUI. Rather than addressing these questions directly, the Final Rule "stayed in its lane" and chose merely to identify the growing concern Defense Industrial Base (DIB) contractors have surrounding DOD-related CUI while avoiding any resolution of a, perhaps ***the*** fundamental challenge facing CMMC: how can contractors protect the controlled unclassified data that DOD can't/won't/isn't properly identifying?

THE GOVERNMENT CONTRACTOR is not printed the week after Thanksgiving. The next issue will be dated December 11, 2024.

This article is a long time coming. Building enterprise networks, instilling security controls, and even the threat of enforcing the absence of those controls all assume a fundamental understanding of the underlying data that is intended to be protected—CUI. Unfortunately, that is not the case. Rampant confusion persists around the identification and labeling of CUI that not only stokes risks in the possible leak of CUI but also in the misapplication and misidentification of protective measures (like CMMC, Defense Federal Acquistion Regulation Supplement 252.204-7012, or eventual FAR clauses) when and if regulators such as the Department of Justice enter the scene. Part and parcel to that confusion is the many-headed hydra of the Government doing its best (?) to meet its directed requirements. To cut through some of that confusion, and as a resource, the following timeline of executive orders, regulations, and final rules may provide, if not a road map, at least some context to the mess CUI control and safeguarding has become:

Date Introduced	Action	Title
Nov. 4, 2010	EO 13556	CONTROLLED UNCLASSIFIED INFORMATION
Feb. 24, 2012	DOD Manual 5200.01, Vol. 2	DOD INFORMATION SECURITY PROGRAM: MARKING OF INFORMATION
Sept. 14, 2016	32 CFR pt. 2002	CONTROLLED UNCLASSIFIED INFORMATION
Oct. 21, 2016	Final DFARS 252.204-7008	COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS
Oct. 21, 2016	Final DFARS 252.204-7012	SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING
March 6, 2020	DOD Instruction [DODI] 5200.48	CONTROLLED UNCLASSIFIED INFORMATION
March 31, 2021	Memorandum	CLARIFYING GUIDANCE FOR MARKING AND HANDLING CONTROLLED TECHNICAL INFORMATION IN ACCORDANCE WITH DEPARTMENT OF DEFENSE INSTRUCTION 5200.48, "CONTROLLED UNCLASSIFIED INFORMATION"
March 17, 2022	Final DFARS 252.204-7019	NOTICE OF NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (NIST) SPECIAL PUBLICATION (SP) 800-171 DOD ASSESSMENT REQUIREMENTS
March 17, 2022	Final DFARS 252.204-7020	NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS
Jan. 10, 2023	DODI 5230.24	DISTRIBUTION STATEMENTS ON DOD TECHNICAL INFORMATION
June 30, 2023	Memorandum	CLARIFYING GUIDANCE FOR CONTROLLED UNCLASSIFIED INFORMATION TRAINING REQUIREMENTS
May 2, 2024	Memorandum	CLASS DEVIATION – SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORT
Dec. 16, 2024	32 CFR pt. 170	CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

It is imperative that the DIB, DOD, and the Federal Government all share a common and consistent understanding of exactly what CUI is and isn't. This is no small feat. Accordingly, the following is an attempt to shed some light on the present and persistent state of confusion so that contractors—and even contracting agencies—can be better prepared to address the uncertainty that will orbit this topic for the next few years. This is a huge topic, so it's been broken down into two parts. Here below in Part I, we provide an overview of how CUI is defined under 32 CFR pt. 2002, the CUI Program's implementation through the National Archives and Records Administration's (NARA's) and DOD's CUI handling and instructions as a foundation of the CUI Program and how it's being implemented at DOD. Then, in Part II, we will provide examples of the confusion stoked by existing CUI guidance to date, the answers provided to date and suggested ways contractors can deal with the pervasive questions surrounding CUI identification.

Controlled Unclassified Information: 32 CFR Pt. 2002—Let's start at the beginning. The CUI Program, codified at 32 CFR pt. 2002, serves three principal purposes: (1) the CUI Program establishes policy for designating, handling, and decontrolling information that qualifies as CUI; (2) the CUI Program standardizes the way the executive branch agencies handle CUI; and (3) ***the CUI Program prohibits agencies from implementing safeguarding or dissemination controls that are not consistent with the CUI Program.*** 32 CFR § 2002.1(a)–(c) (emphasis added). Moreover, the regulation requires that "Agency CUI policies … must be in accordance with the Order, this part, and the CUI Registry and approved by [NARA as the CUI Executive Agent (EA)]." 32 CFR § 2002.4(d). Before standardization under the CUI Program, executive agencies employed "ad hoc, agency-specific policies, procedures, and markings to handle [CUI] … caus[ing] agencies to mark and handle [CUI] inconsistently, implement unclear or unnecessarily restrictive disseminating policies, and create obstacles to sharing information." 32 CFR § 2002.1(d). The intent of the CUI Program and its codification is ultimately to standardize how information is designated CUI and prohibit continued agency ad-hoc CUI designation. This balances "the need to safeguard CUI with the public interest in sharing information appropriately and without unnecessary burdens." 32 CFR § 2002.1(e).

Differentiating CUI—It's telling that nearly 20 percent of 32 CFR pt. 2002's 27 pages address definitions; there was a lot of "new" information in the regulation that required clarification. Most prominently, CUI is defined as "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). Given how broadly the term is defined, a better means to understand the term is to know what information is not CUI. First, CUI does not include classified information. See 32 CFR § 2002.4(e). Second, "information a non-executive branch entity possesses and maintains in its own systems that did not come from or was not created or possessed by or for, an executive branch agency or an entity acting for an agency" is not CUI. 32 CFR § 2002.4(h). If the information was not created for or originated from an executive branch agency, the information does not qualify as CUI.

To determine what safeguards and dissemination controls apply to information subject to the CUI Program, one must refer to the CUI Registry, *www.archives.gov/cui/registry/category-list*, an "online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI EA other than this part. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures." 32 CFR § 2002.4(p). CUI is organized by categories then subcategories, based on the type of information, "for which laws, regulations, or Government-wide policies require or permit agencies to exercise safeguarding or dissemination controls, and which the CUI EA has approved and listed in the CUI Registry." 32 CFR § 2002.4(k); see 32 CFR § 2002.12(a).

CUI has two forms of designation: CUI Basic and CUI Specified. CUI Basic designates information where "the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls." 32 CFR § 2002.4(j). When the "authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic," that information is designated CUI Specified. 32 CFR § 2002.4(r). The distinction between the two categories does not necessarily mean CUI Specified imposes stricter requirements than CUI Basic. However, CUI Specified may require different dissemination controls when compared to CUI Basic. See 32 CFR § 2002.4(r).

Safeguarding CUI—In addition to providing definitions to critical terms, the CUI Program also identifies certain baseline methods to safeguard CUI when (1) CUI is in the control of an authorized holder, (2) shipping or mailing CUI, (3) reproducing CUI, or (4) destroying CUI. See 32 CFR § 2002.14(c)–(d). When accessing or disseminating CUI, the Program requires that CUI be properly marked to identify the appropriate dissemination controls and restrictions. See 32 CFR § 2002.16(a)(3). However, the CUI Program advises agencies to be judicious in the use of dissemination controls, and "should disseminate and permit access to CUI, provided such access or dissemination" conforms to law and regulation, furthers a lawful Government purpose, is not restricted by an authorized limited dissemination control, and is not otherwise prohibited by law. 32 CFR § 2002.16(a)(1)(i)–(iv). To prevent unnecessary limitations, "[a]gencies must impose dissemination controls judiciously and should do so only to apply necessary restrictions on access to CUI, including those required by law, regulation, or Government-wide policy." 32 CFR § 2002.16(a)(2)(i). The bottom line is that agencies should find a "Goldilocks" spot for control that will allow protection amidst the appropriate amount of presumably cost-effective measures.

CUI safeguarding methods will depend on the information systems in which CUI is processed, stored, or transmitted. When non-Federal information systems store CUI, NIST SP 800-171 defines the security controls necessary to protect CUI ***Basic*** on non-Federal information systems, and "[a]gencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems." 32 CFR § 2002.14(h)(2). However, the CUI Regulation also recognizes that NIST SP 800-171 may not be the "be-all" for all CUI and also provides that SP 800-171 may not be sufficient if "the authorizing law, regulation, or Government-wide policy listed in the CUI Registry for the CUI category or subcategory of the information involved prescribes ***specific safeguarding requirements*** for protecting the information's confidentiality, or unless an agreement

establishes requirements to protect CUI Basic at higher than moderate confidentiality." Id. (emphasis added). This final explanation again recognizes the supremacy of the implementing regulations that govern the definition of individual CUI categories. In doing so, it again highlights the overarching tone of the CUI Program that not all CUI is the same and, as such, cannot always be treated uniformly or as "one size fits all."

CUI Program Authority and Control—The CUI Program is managed through the CUI Registry. As specified in the regulations, NARA is the CUI EA and is in charge of implementing the CUI Program and overseeing federal agency compliance with the Program. 32 CFR § 2002.4(m). Operated by NARA, the CUI Registry organizes the CUI categories and subcategories by Organizational Index Groupings (OIGs). There are 20 OIGs ranging from Critical Infrastructure and Defense to Tax and Transportation. These OIGs are broken down further into 126 CUI Categories, each providing details about the types of information covered and the specific laws, regulations, or Government-wide policies that require or permit agencies to exercise safeguarding or dissemination controls. The Registry also provides 11 authorized dissemination controls that an agency may apply to CUI to limit further the dissemination of CUI, such as "NOFORN" (no foreign dissemination), "Attorney-Client," "FEDONLY" (federal employees only), and others. However, the CUI Registry advises that dissemination controls should be consistent with the CUI Program and "[u]sing limited dissemination controls to unnecessarily restrict access to CUI is contrary to the goals of the CUI program." See *www.archives.gov/cui/registry/limited-dissemination*.

The CUI Registry's Frequently Asked Questions provide noteworthy information on who is responsible for marking CUI. Specifically, when CUI is shared with non-federal entities, agencies are responsible for marking or identifying any CUI. Therefore, "[q]uestions regarding the status of information (marked or unmarked) should be directed back to the government contracting activity … Contractors should not follow CUI program requirements or markings until directed to do so in a contract or agreement." Additionally, the FAQ provides that contractors must mark CUI if their contract requires it. See *www.archives.gov/cui/faqs.html*.

Within NARA, the express authority and oversight of the CUI Program is delegated to its Information Security Oversight Office (ISOO). Beyond managing the CUI program, the ISOO is responsible for executive agency policy and oversight of the Government-wide security classification system and the National Industrial Security Program commensurate with guidance from the National Security Council. In this capacity, the ISOO is, in pertinent part, empowered to recommend policy changes for CUI Programs; develop implementing guidance and approve agency-implementing regulations and policies related to CUI programs; and collect, analyze, and report information about the status of agency CUI Programs.

In its most recent report to the president on April 9, 2024, the ISOO updated the present status of CUI implementation, reflecting "continued gains in implementing CUI across the Federal Government. 40 of 81 agencies have completed their CUI policy. Additionally, nearly three-quarters of agencies have begun acquiring the funding and resources they need to fully implement their programs." See ISSO FY2023 Annual Report at 9, available at *www.archives.gov/files/isoo/reports/isoo-fy-2023-annual-report.pdf*. The Report goes on to state that "[w]hile there has been significant progress across the government, there has also been a growing interest in identifying methods and strategies to help simplify CUI where possible without sacrificing the integrity of the program." Id. So, while the ISOO describes a less than 50 percent Government-wide implementation rate and experiencing "significant progress" after 14 years of the CUI Program, it is telling that the Report also identifies a long-standing and key hurdle that must be overcome: finalizing the CUI FAR clause.

> We have been informed via the General Services Administration that the CUI FAR clause remains under review at the Office of Federal Procurement Policy (OFPP). Once that review is complete, the rule will be resubmitted to OMB's Office of Information and Regulatory Affairs (OIRA). It will then undergo the standard process for interagency review.
>
> The delay in issuing the CUI FAR clause contributes to the proliferation of nonstandardized approaches by

> agencies that disadvantage contractors and small businesses and create gaps in security and reporting. Once issued, this regulation will help standardize the way executive branch agencies enforce the requirements of the CUI framework with non-federal entities that receive CUI. This clause is a key part of how agencies will implement CUI.

Id. at 10.

The FAR Case referenced, Case Number 2017-016/ Regulation Identifier Number 9000-AN56, was born in late 2017 and deemed "necessary to ensure uniform implementation of the requirements of the CUI program in contracts across the government, thereby avoiding potentially inconsistent agency-level action." *www.reginfo.gov/public/do/eAgendaViewRule?pubId=201704&RIN=9000-AN56*. The Rule would intend to implement the NARA CUI Program, "which provides implementing regulations to address agency policies for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI." See *www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf*. As of Nov. 15, 2024, the status of Case Number 2017-016 remains open and has been at the FAR Secretariat since Oct. 21, 2024, in preparation for publishing in the Federal Register. Id.

In evaluating the present state of CUI handling throughout the Government, it looks like the FAR Case was and continues to be "spot on."

CUI Within DOD—Recognizing a need to protect CUI while the FAR Rule was still pending, DOD first filled the void for its CUI by adopting and promulgating the DFARS clauses at 252.204-7008 and 252.204-7012. Only after those clauses were firmly entrenched in contracts and haunting the waking nightmares of defense contractors/subcontractors, DOD then implemented DODI 5200.48, Controlled Unclassified Information, on March 26, 2020, right as the world retreated into the pandemic response. For those tracking, that means four years after DOD mandated contractors protect CUI, it finally decided to define exactly what it had directed the DIB to protect. Implementing its own DOD CUI Registry, DODI 5200.48 "establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout DOD in accordance with … [32 CFR pt. 2002]; and [DFARS] Sections 252.204-7008 and 252.204-7012." DODI 5200.48 at 1. DODI 5200.48 requires that non-DOD information systems that process, store, or transmit CUI provide adequate security. See DODI 5200.48 at 13, Sec. 3.3.c.

It is worth noting at the outset that DODI 5200.48 opens by stating that the policy is "part of the *phased DoD CUI Program implementation* process endorsed by the CUI Executive Agent (EA)," indicating that the 2020 DODI is intended as a means to an end, not an end in itself. DODI 5200.48 at 4, Sec. 1.2.a. (emphasis added). It is also worth recognizing that in the intervening four years since it was issued, it does not appear to have undergone any changes to reflect the dynamic nature of the environment in which it is supposed to operate and protect. Moreover, and perhaps most perplexingly, the DODI states as its policy that "the designation, handling, and decontrolling of CUI (including CUI identification, sharing, marking, safeguarding, storage, dissemination, destruction, and records management) will be conducted in accordance ***with this issuance and Sections 252.204-7008 and 252.204-7012 of the DFARS when applied by a contract to non-DoD systems***." Id. (emphasis added). With DFARS 252.204-7008 and -7012 only effectively addressing the safeguarding piece of that description, the lion's share of CUI handling and marking is expressly left to be defined by DODI 5200.48. However, as part of its apparent phased approach, the DODI contains a placeholder on whether/how DOD Components are to differentiate between Basic and Specified CUI along with the "terms and specific marking requirements" to be applied to CUI, which would be "promulgated by the [undersecretary of defense for intelligence and security] in future guidance." DODI 5200.48 at 5, Sec. 1.2.e.(2). In retrospect, perhaps DOD should not have left those two key areas open and undefined.

Those blatant gaps and "can-kicking" notwithstanding, the DODI CUI Information Security Program is intended to "promote, to the maximum extent possible, information sharing, facilitate informed resource use, and simplify its management and implementation while maintaining required safeguarding and handling measures." DODI 5200.48 at 13, Sec. 3.3. To that end, it includes reference to the "DoD CUI Registry [that] mirrors the National CUI Registry, but provides ad-

ditional information on the relationships to DoD by aligning each Index and Category to DoD issuances." DODI 5200.48 at 13, Sec. 3.3d. Accordingly, DOD CUI Registry consists of 19 OIGs, rather than NARA's 20 OIGs, roughly aligning each OIG and category with the various types of DOD CUI to provide information on the CUI categories, required markings, authorities, and pertinent DOD policies.

Regarding marking CUI, DODI 5200.48 directs that relevant material "[a]t minimum … will include the acronym 'CUI' in the banner and footer of the document." DODI 5200.48 at 14, Sec. 3.4.a. Reaching beyond these "minimum" standards, DODI explains that marking should include on the "first page or cover of any document or material containing CUI, including a document with commingled classified information, … a CUI designation indicator" as reflected below:

> Controlled by: [Name of DoD Component] (Only if not on letterhead)
> Controlled by: [Name of Office]
> CUI Category: (List category or categories of CUI)
> Distribution/Dissemination Control:
> POC: [Phone or email address]

Key to this indicator is the "Controlled by" line. "In accordance with Part 2002 of Title 32, CFR, the CUI designation indicator must contain, at minimum, the name of the DoD Component determining that the information is CUI." DODI 5200.48 at 16, Sec. 3.4.f. (1). The requirement to include the "name of DOD Component determining that the information is CUI" is critical, especially for contractors and subcontractors who may receive purported CUI from on high. So often, questions related to CUI address the who, what, and why of the designation. As reflected in the DODI, that is all supposed to be covered, literally, on the first page.

Finally, as noted above, the initial phased implementation of DOD's CUI Program identifies clear gaps in its procedures in distinguishing between CUI Basic and Specified. This differentiation has been completely abdicated since 2020, with all DOD information expected to be "protected in accordance with the requirements under the Basic level of safeguards and dissemination unless specifically identified otherwise in a law, regulation, or Government-wide policy. Forthcoming guidance will address the distinction between the two levels of CUI, including a list of which categories are Basic or Specified, what makes the category one or the other, and the unique requirements, to include markings, for each." DODI 5200.48 at 16, Sec. 3.4.g.

This abdication of identifying Basic versus Specified CUI hints at the fundamental disconnect between the NARA CUI Registry and DOD implementation. The NARA CUI Registry contains a crosswalk between CUI categories and implementing regulations, highlighting the often inherent differences between Basic and Specified requirements. It provides a straightforward link between the type of information a contractor may possess and the regulation(s) defining that information as CUI, including how that type of CUI must be protected—regardless of whether it originates inside or outside DOD. For example, under the "Defense" OIG, the NARA CUI Registry contains five CUI categories:

- Controlled Technical Information
- DOD Critical Infrastructure Security Information
- Naval Nuclear Propulsion Information
- Privileged Safety Information
- Unclassified Controlled Nuclear Information – Defense

Clicking through to better understand those categories, and first using "Controlled Technical Information" as an example, one finds some additional (and perhaps surprising) information:

- The banner marking intended to denote this type of CUI: CUI//SP-CTI
- The safeguarding and/or Dissemination Authority: 48 CFR § (DFARS) 252.204-7012

In practice, this ***should*** mean that when the marking "CUI//SP-CTI" is present, contractors need to use the

safeguarding procedures identified at DFARS 252.204-7012, being "adequate security" and protecting confidentiality according to the requirements of NIST SP 800-171. But what if it's ***not*** marked "CUI//SP-CTI"? What if it is not marked "CUI//SP-CTI" because it isn't actually "CUI//SP-CTI"? What if it's marked as "DoD Critical Infrastructure Security Information," CUI/DCRIT, or, as permitted, marked "CUI"? Or if it is "Unclassified Controlled Nuclear Information – Defense," which can be marked either "CUI" or "CUI//SP-DCNI"? What then? While both are clearly CUI, do the DFARS 252.204-7012 requirements apply if the CUI EA's Registry doesn't point to it or reference the putative DODI purporting to implement NARA's guidance? Not according to the CUI Registry.

Under the "standardized" executive branch CUI Program, the safeguarding and dissemination requirements of DOD Critical Infrastructure Security Information is governed by 10 USCA § 130e, and Unclassified Controlled Nuclear Information – Defense (DOD UCNI) is governed by 10 USCA § 128(a) ***or*** 32 CFR § 223—depending on the type of DOD UCNI that contractor may possess, meaning Basic of Specified. Tellingly, when examining the DOD UCNI safeguarding regulation at 32 CFR § 223.6, it provides ample directions for controlling DOD UCNI, including labeling and handling in NATO circles, but there is no express reference to "CUI," the CUI Program, or even DFARS 252.204-7012, or DODI 5200.48. Instead, the regulations require that "DoD UCNI shall be safeguarded and controlled by measures designed to reduce the risk of access to DoD UCNI by unauthorized individuals" and, after hours, "stored to preclude disclosure. Storage of such information with other unclassified information in unlocked receptacles (e.g., desks, bookcases) is adequate if Government or Government-contractor internal building security is provided during non-duty hours." 32 CFR § 223(f). Why does this matter? Because even the DODI recognizes the uniqueness of DOD UCNI and its "need to know" requirement before access may be granted. See DODI 5200.48 at 12, Sec. 3.1.d.

These in-the-weeds issues being what they are, it is also relevant to note that DODI 5200.48's application to defense contractors is also clearly specified in its Section 5. The following guidelines govern the implementation of the CUI Program on DOD requirements:

- NIST SP 800-171, Protecting Controlled Unclassified Information in Non-federal Systems and Organizations, identifies the baseline CUI system security requirements for industry established by 32 CFR pt. 2002.
- Non-DOD information systems that process, store, or transmit CUI will safeguard CUI in accordance with the contractual requirements identified for the CUI, DODI 8582.01, and DFARS 252.204-7012.
- The program office or requiring activity must identify DOD CUI at the time of contract award and, if necessary, provide guidance on information aggregation or compilation. The program office or requiring activity must review recurring or renewed contracts for CUI to comply with this issuance.

DODI 5200.48 at 32, Sec. 5.1.a, c, and e. In this regard, the DODI reflects that defense contractors are to take their cue from DOD to ensure the necessary safeguards are applied to CUI. As noted in DODI 5200.48, DOD must (1) identify to contractors whether any information it provides to a contractor is CUI, (2) mark said documents, media, and materials accordingly, and (3) articulate the protective measures required under the contract. DODI 5200.48 at 32, Sec. 5.3.a–b.

As reflected above, the NARA CUI Registry and DOD CUI Program outlined in DODI 5200.48 are intended to be integral parts of safeguarding CUI across federal and defense landscapes. However, as we will point out in Part II of our series, the differences between the two present significant challenges that may undermine the effectiveness of CUI management. While the NARA Registry aims to provide a universal framework for consistent handling across federal agencies, DOD's Program introduces additional complexity with mission-specific requirements focusing on cybersecurity. This divergence creates confusion for contractors at all levels who must navigate varying standards between the general federal guidance and DOD's stricter, more complex protocols. While vital,

DOD's strong emphasis on cybersecurity seems to overshadow other necessary aspects of CUI protection, such as the proper and correct marking of documents in a manner seemingly contrary to the standardized system envisioned by NARA. Beyond making the overall CUI framework more difficult to implement consistently, this misalignment can increase administrative burdens, compliance costs, and operational inefficiencies, particularly for contractors working across multiple federal agencies. Part II of this series will explore the issues raised by the DIB in this regard and attempt to provide defense contractors with solutions to enhance clarity and effectiveness in DIB CUI management.

This Feature Comment was written for THE GOVERNMENT CONTRACTOR by **Alexander Major** ***and*** **Philip Lee.** ***Mr. Major, a Partner and co-leader, and Mr. Lee, an Associate, are in the Government Contracts and Global Trade Group based in the Washington, D.C. office of McCarter & English. They can be reached at*** **amajor@mccarter.com** ***and*** **plee@mccarter.com.**