THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement

DECEMBER 18, 2024 | VOLUME 66 | ISSUE 46

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

Introduction—In Part I of this series we introduced readers to what Controlled Unclassified Information (CUI) is understood to consist of under the CUI Program at 32 CFR pt. 2002, differentiating and safeguarding CUI, CUI Program Authority and Control, and CUI policy as promulgated under the U.S. Department of Defense CUI Program. See 66 GC ¶ 324. We also noted that nearly five years after first announced, DOD's Cybersecurity Maturity Model Certification (CMMC) Program will finally become operational at some point in fiscal year 2025 as the means by which DOD intends to protect CUI. As we noted in Part I, many gaps in the DOD CUI Program have yet to be filled. These gaps took center stage in comments DOD received when it issued its Final Rule. Disappointingly, DOD made no effort to fill in these gaps in responding, thus ensuring that Defense Industrial Base (DIB) contractors and subcontractors will be in for a bumpy ride.

The Government Contractor is not printed the weeks containing December 25 and January 1. The next issue will be dated January 8, 2025.

As reflected below, DOD's continued abdication and avoidance of providing effective clarity is proving challenging for DIB contractors. The examples are legion and reflected not only in the comments for the CMMC Final Rule, but also in the wave of present and pending False Claims Act enforcement actions being brought by the Department of Justice. With the definition and identification of CUI quickly taking center stage, it is imperative that DIB contractors take a deeper look at just how they are identifying and, as such, handling CUI to better prepare for the risk resident in the DOD-sponsored confusion. And, as for DOD, if CUI protection is indeed the priority it needs to be, it may be beyond time to take the necessary actions to ensure contracts (and its contract personnel) better address the handling and dissemination of CUI.

CUI Confusion On Display: The CMMC Program Final Rule—Issuing its Final Rule Oct. 15, 2024, the CMMC Program is DOD's primary means to ensure DIB contractors and subcontractors safeguard CUI. See 89 Fed. Reg. 83092 (Oct. 15, 2024). Developed by DOD to strengthen the DIB's cybersecurity posture and to better safeguard DOD information, namely CUI, from increasingly frequent and complex cybersecurity attacks, the

CMMC Program was created in alignment with DOD's existing information security requirements. See 66 GC ¶ 247. The CMMC program is structured as a three-tiered model, with each successive tier requiring a defense contractor to implement and maintain additional security controls. Codified at 32 CFR pt. 170, the CMMC Program is intended to provide DOD with a mechanism to verify contractors' implementation and maintenance of the requisite security controls. The requisite CMMC level will be specified in a DOD solicitation, and a contractor must demonstrate that it has achieved the specified CMMC level as a condition precedent to contract award.

While the release of CMMC caused a significant stir, the rampant presence of CUI confusion in the Final Rule's comments is quite telling. In fact, DOD notes that approximately 361 comments were received during the public commenting period (89 Fed. Reg. at 83103) with many specifically questioning how, precisely, DOD addresses CUI. Unfortunately, as the questions did not specifically address the CMMC program, the issues, concerns, criticisms, and complaints regarding DOD's handling of CUI went largely unanswered as beyond the rule's scope and comments.

In place of answers, the Final Rule "*DOD*-GED," choosing to allow the game of CUI hide-n-seek—or perhaps CUI Dizzy Bat—to continue, while DIB contractors struggle to identify and track the information received from DOD that qualifies as CUI. A case in point was the more than 20 comments requesting more guidance, "preferably within [requests for proposals] or contracts, to identify better what will be considered CUI for that contract, and how it should be appropriately marked." The questions were ripe with similar and related concerns, including:

- "a need for contractual instructions on whether data created in performance of a contract rises to the level of CUI."
- "when is [sic] does information created or possessed by a contractor become CUI"?
- "whether digital or physical items derived from CUI are treated as CUI"?
- "what specific information qualifies as CUI for OT and IoT assets"?
- "whether [Federal Contract Information (FCI)] and or CUI created or provided under a non-DoD agency contract, but which is also used in support of a DoD contract, would be subject to the applicable CMMC level requirement"?

89 Fed. Reg. at 83103.

But that was only the beginning. The DIB sounded in resounding harmony raising issues addressing all manners in which DOD approached CUI. In pertinent part, this includes:

- "Twenty-three comments expressed concern with or requested clarification regarding CUI marking."
- "Twelve comments specifically noted concern with CUI markings being applied to too many documents, in part because CUI was an ambiguous concept. They requested the DoD encourage personnel to mark documents as CUI only when appropriate and provide better guidance for managing flow-down clauses."
- "One comment stated there is an increased use of automatic CUI marking on DoD communications, seemingly without regard to content."
- "One comment stated that the rule fails to outline a mechanism for reporting government mishandling, and that contractors should use a reporting system to minimize their own risk and liability."
- "One comment requested the rule be edited to prevent Program Managers or requesting activities from assigning a CMMC Level 3 requirement unless they have high confidence that 80+ percent of CUI and/or FCI under the relevant contract has complete CUI markings."
- "Another comment stated that the Federal government should develop a marking schema to communicate information safeguarding requirements, while yet another stated that DoD must publish a training module for contracting officers

so that they are properly classifying documents prior to finalization of this rule."

- "One comment stated CUI across the DoD is diverse and what may be CUI for one system may not be for another. The comment then questioned how this proposed rule and [Supplier Performance Risk System (SPRS)] would accommodate these facts without assuming and mandating that all defense contractor information systems meet the same architecture, security, and cybersecurity standards."

- "Five comments stated that what DoD considers CUI is not well defined."

- "[One] comment stated that companies should be provided a reference list of what the DoD considers CUI."

- "[One comment] recommended DoD use existing mechanisms like the DD Form 254 architecture to clearly define the scope of CUI on a contract-by-contract basis."

- "Nine comments stated there was too much confusion and ambiguity regarding FCI and CUI and that the government needed to provide clear and standardized FCI and CUI definitions that are tailored to the specific requirements of the CMMC rule."

- "One comment requested clarification and examples of differences between CUI Basic and Specialized CUI."

89 Fed. Reg. at 83104. Additional questions and comments highlighted gaps by offering solutions such as the "need for CUI policy guidance for the entire Federal Government," proposing that a "CUI designation automatically applies to contractor-created information," suggestions that National Archives and Records Administration (NARA) "initiate a public comment period to reevaluate its CUI Registry," and "revise the CUI Registry to stipulate that a specific basis in statute (or a contract) is required for information to be considered CUI." See 89 Fed. Reg. at 83103–83104.

As noted above, the answers to these comments varied and largely avoided addressing the necessary changes or referencing DOD Instruction (DODI), which could provide contractors (and procuring departments) with the necessary answers. Those responses included:

- "The definition of CUI and general requirements for its safeguarding are included in 32 C.F.R. § 2002.4 and 2002.14, respectively."

- "32 C.F.R. § 2002.14(h)(2) specifically requires agencies to use [National Institute of Standards & Technology (NIST) Special Publication] 800–171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems. At the time of award, the DoD may have no visibility into whether the awardee will choose to further disseminate DoD's CUI, but [Defense Federal Acquisition Regulation Supplement] clause 252.204–7012 and DFARS clause 252.204–7021 require the prime contractor to flow down the information security requirement to any subcontractor with which the CUI will be shared."

- "Decisions regarding which DoD information must be shared to support completion of subcontractor tasks is between the prime contractor and the subcontractors. The DoD encourages prime contractors to work with subcontractors to lessen the burden of flowing down CUI."

- "Relevant information regarding what to do when there are questions regarding appropriate marking of CUI may be found at 32 C.F.R. § 2002.50—Challenges to designation of information as CUI."

- "The DoD declined to incorporate suggested edits to the CMMC Level 3 requirements regarding confidence in proper CUI and/or FCI markings."

- "Program managers have a vested interested [sic] in knowing whether a contractor can comply with these existing requirements to adequately safeguard CUI."

- "The DoD elected not to make any recommended edits to the CMMC Program related to FCI or CUI marking requirements or provide clarifying examples of the differences between Basic CUI and Specified CUI, as these are beyond the scope of this rule."

- "Mishandling of information by the government is beyond the scope of this rule."

89 Fed. Reg. at 83104–105. While some of these comments may indeed be "beyond the scope" of the issuance of the Final Rule, each is inherently germane to the CMMC Program. It concerns what DOD wants contractors to protect reasonably and how the DIB should know. One response in particular may even stoke confusion:

- "*The DoD's role as data owner is documented in the CUI Program* implementing policies and the requirements of 32 C.F.R. part 2002. DoDI 5200.48, states: *The authorized holder of a document or material is responsible for determining,* at the time of creation, *whether information in a document or material falls into a CUI category*. If so, the authorized holder *is responsible for applying CUI markings and dissemination instructions accordingly.*" 89 Fed. Reg. at 83104 (emphasis added) citing DoDI 5200.48 at 17, § 3.6.a.

Like queries into the geneses of most things, the origin of DOD CUI is not exactly clear, and the concept of the "authorized holder," like any creator-being, only muddies the water. The DODI use of the term "authorized holder" referenced in the Final Rule is borrowed from 32 CFR pt. 2002 and defined as "an individual, agency, organization, or group of users that is permitted to designate or handle CUI, in accordance with this part." 32 CFR § 2002.4(d). The challenge, however, is defining *who* that "authorized holder" is and when or how that "authorized holder" becomes so entitled. Arguably, as CUI spawns from a Government request, action, law, or regulation, the Government would be the "authorized holder" and determine what is or is not CUI. However, there are contracts where CUI does not yet exist but is contemplated to be created. In such a situation, the contractor (or subcontractor) arguably would be the "authorized holder" and make the required determination upon creation. But if that's the case, then as an "authorized holder," that contractor/subcontractor should/would/could possess all of the other authority provided to authorized holders under DODI 5200.48, no? This means that the contractor/subcontractor creating that CUI would be permitted to:

- Remove "safeguarding or dissemination controls from CUI that no longer requires such controls. Decontrol may occur automatically or through agency action." 32 CFR § 2002.4(s).

- Designate data as CUI when it "determines that a specific item of information falls into a CUI category or subcategory." 32 CFR § 2002.4(t).

- Make recipients, including DOD, "aware of the information's CUI status in accordance with this part." Id.

- "Provide access, transmit, or transfer CUI to other authorized holders through any means, whether internal or external to an agency." 32 CFR § 2002.4(v).

To be clear, 32 CFR pt. 2002 does contemplate authorized holders existing "both inside and outside the agency" 32 CFR § 2002.8. But this does not make things any easier. The difficulty lies in that neither 32 CFR § 2002 nor DODI 5200.48 designates how that authority is intended to be transferred and, when transferred, just how much authority follows.

That the Final Rule also failed to clarify, let alone incorporate by reference, existing DOD requirements governing the responsibilities and marking of CUI is a missed opportunity after 23 comments "expressed concern with or requested clarification regarding CUI marking … specifically not[ing] concern with CUI markings being applied to too many documents, in part because CUI was an ambiguous concept." 89 Fed. Reg. at 83104. This absence is glaring when both DODI 5200.48 and DOD Manual 5200.01, Volume 2, *DoD Information Security Program: Marking of Information*, place responsibility on DOD for determining whether information falls into a CUI category when created.

DOD's decision not to incorporate these references is a missed opportunity to provide contractors with a complete picture of what is expected of CUI's designation, handling, and decontrolling. Further, by failing to incorporate these references, which are tethered to the CUI program at 32 CFR pt. 2002, the CMMC Program responses fail to give due consideration to the CUI regulations or recognize that NIST SP 800-171 may not be the "be-all" for all CUI or that SP 800-171 may be insufficient or wrongly relied upon if the underlying authorizing law, regulation or Government-wide policy requires more exacting or specific safeguarding requirements to protect certain information.

To Safeguard or Not to Safeguard, What Is the NIST?—Illustrative of the confusion surrounding what is CUI and how DIB contractors protect CUI that DOD can't/won't/isn't properly identifying, is the DOJ's recent intervention in an FCA qui tam action against the Georgia Institute of Technology (Georgia Tech) and Georgia Tech Research Corp. (GTRC). Filed on Aug. 22, 2024, DOJ's Complaint-in-Intervention alleges that Georgia Tech and GTRC violated the FCA at "31 U.S.C. § 3729, *et seq.* and federal common law for their failure … to meet cybersecurity requirements of [DOD] contracts." U.S. Complaint-in-Intervention at 1, *U.S. ex rel. Craig v. Georgia Tech Research Corp.*, 1:22-cv-02698-JPB (N.D. Ga. Aug. 22, 2024), ECF No. 23. The complaint, which originated from a whistleblower filed in 2022 by former senior members of Georgia Tech's cybersecurity compliance team, centers on the Astrolavos Lab at Georgia Tech, accusing it of failing to implement required cybersecurity measures, including:

- Lack of a System Security Plan (SSP): The lab allegedly did not develop or implement an SSP until February 2020, which is essential for outlining cybersecurity controls.
- Absence of Antivirus Protections: From at least May 2019 to December 2021, the lab reportedly failed to install, update, or operate antivirus or anti-malware tools on its devices, contravening both federal requirements and Georgia Tech's internal policies.
- Submission of False Cybersecurity Assessment: In December 2020, Georgia Tech and GTRC are alleged to have provided a misleading cybersecurity assessment score to the DOD, claiming a campus-wide compliance score of 98. DOJ contends this score was fabricated, as no such campus-wide IT system existed, and the score did not pertain to any actual environment handling covered defense information (CDI).

Id. at 43–44, 49, 59, ¶¶ 153, 155, 175, 209–10. The Complaint goes on to suggest a broader culture of disregarding cybersecurity protocols, with DOJ asserting that Georgia Tech prioritized accommodating prominent researchers over adhering to federal cybersecurity standards. Id. at 4, 7, ¶¶ 10, 20. The Complaint alleges that in at least two awarded DOD contracts, Georgia Tech and GTRC were obligated to implement and comply with those cybersecurity obligations to safeguard FCI and Covered Defense Information as specified under FAR 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems* and DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, respectively. See id. at 29–30, 35–36, ¶¶ 101, 106, 124, 128–29. In addition to alleging that Georgia Tech and GTRC were both aware that contract performance would include and require the safeguarding of CUI from language in the solicitation, the contracts, and inclusion of DOD Contract Security Classification Specifications (DD Form 254) and a distribution statement that restricted the sharing and disclosure of technical information, see id. at 31–34, 37–38, ¶¶ 107, 113–20, 130–33, the Complaint also asserts that defendants' employees were aware that their performance under the DOD contracts consisted of CUI and spread across multiple servers. See id. at 38–39, 41–42, ¶¶ 136–40, 143–50.

The key takeaways from the suit are rather telling for those who can read between the lines. Foremost, it reflects that DOJ's Civil Cyber-Fraud Initiative is very much active and that cybersecurity compliance is now a focus area under the FCA. As has been known for years now, DIB contractors and grant recipients are not only expected to meet their cybersecurity obligations but are also at risk of liability if they misrepresent their compliance or fail to adhere to requirements.

Secondly, no one is immune from inquiry. Academic institutions and research organizations, often considered less scrutinized compared to corporate contractors, are now clearly within DOJ's sights. Case in point is the recent Oct. 22, 2024 settlement agreement between Pennsylvania State University (PSU) and DOJ, where PSU agreed to pay $1.25 million to resolve allegations it had violated the FCA by failing to implement and comply with its cybersecurity obligations under contracts with DOD and NASA. See *www.justice.gov/opa/pr/pennsylvania-state-university-agrees-pay-125m-resolve-false-claims-act-allegations-relating*. These actions signal that no entity required or expected to protect CUI is exempt from accountability for cybersecurity deficiencies when federal funds are involved. Also, noteworthy is that these actions are being driven by whistleblower allegations, illustrating the significant role of insiders—particularly IT staff—in identifying and reporting cybersecurity non-compliance and reinforcing the FCA's qui tam provisions, which empower individuals to bring attention to violations. Finally, and perhaps most importantly, these types of suits may serve to reflect cybersecurity as a material obligation in the receipt of federal dollars. By framing Georgia Tech's alleged failures—such as not maintaining a SSP or antivirus protections—as material misrepresentations, DOJ is asserting that with DOD contracts, they view cybersecurity as not optional but a fundamental requirement for federal contracting and grants.

Perhaps mirroring the Yellow Jackets' renowned 2024 rush defense on the football field, Georgia Tech does not appear willing to give DOJ ground. In response to the Complaint, Georgia Tech and GTRC filed a motion to dismiss asserting a number of counts to contend that the Government's FCA and Federal Common Law claims fail as a matter of law. Defendants' Brief in Support of Their Motion to Dismiss, *U.S. v. Georgia Tech Research Corp.*, 1:22-cv-02698-JPB (N.D. Ga. Oct. 10, 2024), ECF No. 34-1. With respect to the Government's FCA allegations, Georgia Tech and GTRC contend that the DOD cybersecurity requirements alleged to have been violated did not apply to the "systems [they] used to perform fundamental research in the Astrolavos Lab." Id. at 30. Georgia Tech and GTRC also contest DOJ's FCA accusation that they made "false statements relating to [their] promises to comply with DFARS [252.204-7012], its certifications of compliance with DFARS [252.204-7019], and its invoices for payment" by similarly noting that the GTRC could not have made false statements purporting to be in compliance "with DFARS [252.204-7012] and [252.204-7019] because those provisions did not apply to the fundamental research performed under the EA and SMOKE contracts." Id. at 50–51.

Finally, Georgia Tech and GTRC also challenge DOJ's federal common-law claims alleging fraud, mistake, unjust enrichment, payment by mistake, and breach of contract based on similar arguments made to challenge the Government's FCA claims. These include asserting that either the applicable cybersecurity requirement clauses did not apply or that they were not incorporated into the DOD contract and could not have applied as both contracts were for fundamental research and therefore, not subject to the clauses. See ECF No. 34-1 at 52–54 (Defendants' rebuttal to DOJ's fraud claim), 55–56 (Defendants' rebuttal to DOJ's negligent misrepresentation claim), 58–59 (Defendants' rebuttal to DOJ's breach of contract claim). Pointing out that the Government can't have its cake and eat it too, Georgia Tech and GTRC counter DOJ's claim of unjust enrichment and payment by mistake by contending that these claims fail "because (1) neither of these equitable claims can coexist with the written contracts that governed the Astrolavos Lab's research; and (2) DoD received, and GTRC and Georgia Tech were appropriately compensated for, the research performed under the contracts." ECF No. 34-1 at 56-58.

While the outcome of this ordeal remains to be determined, the Georgia Tech and GTRC motion to dismiss serves to highlight some areas of lingering confusion as to how CUI propagates into and may be handled by many in the DIB. And whether it can serve as a cautionary tale or a lessons learned, it bears a thorough reading from both DIB contractors and their DOD customers.

There are some salient points in the Georgia Tech

and GRTC motion worth emphasizing. As noted earlier, DOD noted a plethora of comments when issuing the Final Rule that highlight the struggle DIB contractors face in identifying and tracking information received from DOD that qualifies as CUI, requesting guidance and instruction on "when is [sic] does information created or possessed by a contractor become CUI." See 89 Fed. Reg. at 83103. Notably, and relevantly, this sentiment is echoed in Georgia Tech and GTRC motion: "*[n]one of the contract documents identified any CDI that would be involved in the Astrolavos Lab's research, as would be required if CDI were involved*" and "[none of] *the contract documents instruct GTRC how to mark any purported CDI*, which also would be required if CDI were involved." ECF No. 34-1 at 22 (emphasis in original). This is a poignant and, as described herein, valid concern that is now on enforcement's center stage. Until DOD is able to issue clear and directed guidance internally and externally, DIB contractors must be prepared to shoulder significant and poorly defined risk.

A second particularly noteworthy point is that Georgia Tech's motion suggests that DOJ's reliance on NIST SP 800-171 may be insufficient to reflect any violation. It notes that the purpose of NIST SP 800-171 is to provide "federal agencies with *recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations* … [and] apply to components of nonfederal systems that process, store, or transmit CUI *or* that provide protection for such components." NIST SP 800-171 rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, (May 14, 2024). Unlike the CUI Program, which has not undergone changes or updates from when NARA issued its Final Rule in 2016, see 81 Fed. Reg. 63324 (Sep. 14, 2016), NIST SP 800-171 has undergone multiple revisions (four versions in total) with incremental updates being applied to each version.

The particular NIST SP 800-171 in effect for a DOD contract is especially important, as certain CUI safeguarding requirements may exist in one version of the NIST 800-171. Foreshadowing perhaps the Final Rule's failure to give due consideration to the CUI regulations or recognize that NIST SP 800-171 may not be the "be-all" for all CUI, the following rebuttals from Georgia Tech's and GTRC's Brief in Support of their Motion to Dismiss are noteworthy in addressing CUI safeguarding:

- The particular security controls specified in NIST SP 800-171 are pertinent to determine safeguarding requirements when DIB contractors perform under multiple, long-running DOD contracts. See ECF No. 34-1 at 35 ("[t]he Complaint's confused assertions that GTRC violated NIST SP 800-171 by not creating an SSP or installing antivirus software fail because *those requirements were not in NIST SP 800-171 when the EA contract was solicited, awarded, and executed*.") (emphasis in original).

- Alleging a violation for failure to implement a security control in NIST SP 800-171 seems fictitious given that the security requirements identified therein are recommended. As Georgia Tech and GTRC note, the violations DOJ alleged Georgia Tech and GTRC to have violated either did not apply, were too vague, or the violations "rely on 'imprecise statements or differences in interpretation' that the FCA does not punish." ECF No. 34-1 at 37. In particular, the Brief in Support of Defendants' Motion to Dismiss states that DOJ "ignores that NIST SP 800-171 allows entities to 'limit the scope of the security requirements' to those 'specific system components' handling CUI." Id. at 37.

- The nature of the contract requirements may not fit within the rubric of the CUI Program. Perhaps most critically, Georgia Tech and GTRC contend that the nature of the work they performed under the contracts consisted of fundamental research, which by definition, cannot involve any covered defense information or CUI. See id. at 16 citing DFARS 252.2004-7000(a)(3) ("The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium … unless … the information results from or arises during the performance of a project that involves … fundamental re-

search (which by definition cannot involve any covered defense information)").

The Georgia Tech and GRTC Brief in Support of their Motion to Dismiss highlights the confusion DIB contractors have been clamoring for clarity on from DOD. Further, if the information DOJ alleges to constitute CUI was information first developed by Georgia Tech and GRTC pursuant to its DOD contracts, Georgia Tech and GRTC would operate as the authorized holders to determine whether the information in question constituted CUI. See 32 CFR § 2002.8 (recognizing that authorized holders exist "both inside and outside the agency"). As the authorized holder, Georgia Tech and GRTC would be vested with all the privileges and responsibilities that accompany being an authorized holder under the CUI Program, including any necessary safeguard and dissemination controls. However, DOJ does not hold the same opinion, and its Complaint highlights the complexity and myriad of issues that DOD has failed to answer or provide guidance on.

Contractors should also realize that the recent PSU settlement and Georgia Tech/GTRC Complaint are not one-off's in the Government's pursuit of enforcing cybersecurity obligations. Launched Oct. 6, 2021, DOJ's Civil Cyber-Fraud Initiative was created to utilize the FCA to pursue cybersecurity related fraud by Government contractors and grant recipients. See *www.justice.gov/opa/pr/pennsylvania-state-university-agrees-pay-125m-resolve-false-claims-act-allegations-relating*. The PSU settlement and Georgia Tech/GTRC whistleblower complaints originated from the same Georgia whistleblower attorney. Furthermore, according to that attorney, she has 10 more whistleblower suits under seal. See Health Care Compliance Association, Report on Research Compliance 21, no. 12 (Dec. 2024) available at *compliancecosmos.org/usga-tech-tussle-over-fca-allegations-cybersecurity*. Accordingly, contractors of all sorts should take note that these cases are merely the latest salvos with many more likely still being investigated by the Government.

Taking the Confusion out of CUI—Although you can't spell "confusion" without CUI, there is no reason that CUI has to be a lingering area of concern for federal contractors. As noted above, issues abound regarding how the Federal Government and DOD handle CUI, but that doesn't negate the importance of protecting this information, irrespective of the inarticulate and imprecise regulations and policies. If anything, one might suggest it's up to the voluntary graciousness of contractors to see how/if they can help their federal customers get their CUI directions straight. Although the authors understand that contractors are neck deep in CMMC prep, SPRS analyses, and the like, the DIB needs to understand that the safeguarding schema starts with identifying the germ of CUI. This means ensuring that enterprises have a clear and precise understanding of how CUI is identified, handled, and disseminated.

Beyond the recognized contractual compliance dictating safeguarding controls distilled at FAR 52.204-21, DFARS 252.204-7012, and even CMMC, a key component of proper CUI management is developing comprehensive CUI policies. These policies should outline access controls, secure storage and transmission methods, and procedures for identifying and marking CUI. In the atmosphere of uncertainty surrounding CUI, a company that has defined and supported its understanding of the CUI it does or may possess is critical. In this regard, contractors should focus on identifying CUI within contracts, communications, or other materials, including:

1. Understanding the Source of CUI: As CUI is information that the Government designates as requiring safeguarding or dissemination controls, it can come directly from Government agencies or may be created by contractors while fulfilling a contract—understand the genesis of that CUI.

2. Reviewing the Contract: Federal contracts may specify which information is considered CUI through references to regulations like DFARS 252.204-7012 or direct mentions of the NARA CUI Registry. Check for clauses that mandate adherence to safeguarding practices for certain categories of information, such as export-controlled data, proprietary business information, or Personally Identifiable Information.

3. Understanding CUI Markings: CUI should arrive properly marked to ensure it is recognizable and managed according to the appropriate safeguarding standards. If CUI is anticipated to be created, specific guidance should be provided by the Federal Agency in the contract that describes how that CUI-created material will be marked along with any warranted dissemination controls. This guidance should also apply to physical media.

4. Understanding CUI *Non*-Markings: If the enterprise receives information that may qualify as CUI but is not marked, it should review the contract and other *supporting* documentation to confirm if it should be treated as CUI, consult with the CO for guidance, and assess whether it should treat the information as CUI until clarification is received to avoid accidental disclosure.

5. Understanding CUI Categories: The policy should address and reference handling according to NARA and DOD CUI Registries to better link the data received with detailed guidance on the varying categories of CUI.

6. Communicating Proactively with the Government: When in doubt or in the presence of something you believe is contrary to NARA or DOD policy and regulations, seek clarification from the CO or designated point of contact about whether specific data qualifies as CUI. Don't be afraid to ask questions!

With appropriate policies in place, training on these requirements is imperative. A knowledgeable workforce that understands its role in protecting CUI is a critical defense against mishandling or breaches and a welcomed data point for regulators. Training should cover what CUI is, why it matters, and how to handle it securely. Role-specific guidance would also help IT, compliance, business capture, and project management employees understand their unique risks. Regular refresher sessions ensure the workforce remains informed about evolving threats and regulations.

Since maintaining compliance is ongoing, regular audits will help identify gaps in policies or practices, while procedure updates can ensure alignment with ever-evolving regulations. Achieving and maintaining the appropriate level of CMMC certification further demonstrates a contractor's commitment to protecting CUI.

As the DIB enters the new phase of contracting under CMMC, managing CUI effectively is increasingly important. Contractors want to protect data; they just need the necessary underpinnings of the data they must protect. This means more than meeting requirements—it's about building trust within your enterprise, with your partners, and with your customers that demonstrate a commitment to ensuring the integrity of sensitive information. By understanding the rules, creating robust policies, training employees, maintaining secure systems, and communicating with Government customers and primes, contractors can protect CUI while avoiding much of the confusion and uncertainty facing the DIB over this period of cyber transition.

♦

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.

